Microsoft

Microsoft Official Academic Course

Administering Windows Server 2012 R2

EXAM 70-411

Microsoft® Official Academic Course

Administering Windows Server® 2012 R2 Exam 70-411

Patrick Regan

WILEY

Credits

VP & PUBLISHER	Don Fowley
EXECUTIVE EDITOR	John Kane
DIRECTOR OF SALES	Mitchell Beaton
EXECUTIVE MARKETING MANAGER	Chris Ruel
MICROSOFT PRODUCT MANAGER	Keith Loeber of Microsoft Learning
EDITORIAL PROGRAM ASSISTANT	Allison Winkle
TECHNICAL EDITORS	Jeff T. Parker
	Brien Posey
	Kenneth Hess
	Brian Svidergol
ASSISTANT MARKETING MANAGER	Debbie Martin
ASSOCIATE PRODUCTION MANAGER	Joyce Poh
CONTENT EDITOR	Wendy Ashenberg
CREATIVE DIRECTOR	Harry Nolan
COVER DESIGNER	Tom Nery
SENIOR PRODUCT DESIGNER	Thomas Kulesa

This book was set in Garamond by Aptara, Inc. and printed and bound by Bind-Rite Robbinsville. The covers were printed by Bind-Rite Robbinsville.

Copyright © 2014 by John Wiley & Sons, Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc. 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, (201) 748-6011, fax (201) 748-6008. To order books or for customer service, please call 1-800-CALL WILEY (225-5945).

Microsoft, Active Directory, AppLocker, Bing, BitLocker, DreamSpark, Hyper-V, Internet Explorer, SQL Server, Visual Studio, Win32, Windows Azure, Windows, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

The 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, John Wiley & Sons, Inc., Microsoft Corporation, nor their resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

ISBN 978-1-118-88283-2

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

www.wiley.com/college/microsoft *or*
call the MOAC Toll-Free Number: 1+(888) 764-7001 (U.S. & Canada only)

Foreword from the Publisher

Wiley's publishing vision for the Microsoft Official Academic Course series is to provide students and instructors with the skills and knowledge they need to use Microsoft technology effectively in all aspects of their personal and professional lives. Quality instruction is required to help both educators and students get the most from Microsoft's software tools and to become more productive. Thus, our mission is to make our instructional programs trusted educational companions for life.

To accomplish this mission, Wiley and Microsoft have partnered to develop the highest-quality educational programs for information workers, IT professionals, and developers. Materials created by this partnership carry the brand name "Microsoft Official Academic Course," assuring instructors and students alike that the content of these textbooks is fully endorsed by Microsoft and that they provide the highest-quality information and instruction on Microsoft products. The Microsoft Official Academic Course textbooks are "Official" in still one more way—they are the officially sanctioned courseware for Microsoft IT Academy members.

The Microsoft Official Academic Course series focuses on *workforce development*. These programs are aimed at those students seeking to enter the workforce, change jobs, or embark on new careers as information workers, IT professionals, and developers. Microsoft Official Academic Course programs address their needs by emphasizing authentic workplace scenarios with an abundance of projects, exercises, cases, and assessments.

The Microsoft Official Academic Courses are mapped to Microsoft's extensive research and job-task analysis, the same research and analysis used to create the Microsoft Certified Solutions Associate (MCSA) exam. The textbooks focus on real skills for real jobs. As students work through the projects and exercises in the textbooks and labs, they enhance their level of knowledge and their ability to apply the latest Microsoft technology to everyday tasks. These students also gain resume-building credentials that can assist them in finding a job, keeping their current job, or furthering their education.

The concept of life-long learning is today an utmost necessity. Job roles, and even whole job categories, are changing so quickly that none of us can stay competitive and productive without continuously updating our skills and capabilities. The Microsoft Official Academic Course offerings, and their focus on Microsoft certification exam preparation, provide a means for people to acquire and effectively update their skills and knowledge. Wiley supports students in this endeavor through the development and distribution of these courses as Microsoft's official academic publisher.

Today educational publishing requires attention to providing quality print and robust electronic content. By integrating Microsoft Official Academic Course products, MOAC Labs Online, and Microsoft certifications, we are better able to deliver efficient learning solutions for students and teachers alike.

Joseph Heider

General Manager and Senior Vice President

Preface

Welcome to the Microsoft Official Academic Course (MOAC) program for becoming a Microsoft Certified Solutions Associate for Windows Server 2012 R2. MOAC represents the collaboration between Microsoft Learning and John Wiley & Sons, Inc. Microsoft and Wiley teamed up to produce a series of textbooks that deliver compelling and innovative teaching solutions to instructors and superior learning experiences for students. Infused and informed by in-depth knowledge from the creators of Windows Server 2012 R2, and crafted by a publisher known worldwide for the pedagogical quality of its products, these textbooks maximize skills transfer in minimum time. Students are challenged to reach their potential by using their new technical skills as highly productive members of the workforce.

Because this knowledgebase comes directly from Microsoft, architect of Windows Server 2012 R2 and creator of the Microsoft Certified Solutions Associate exams, you are sure to receive the topical coverage that is most relevant to students' personal and professional success. Microsoft's direct participation not only assures you that MOAC textbook content is accurate and current, it also means that students will receive the best instruction possible to enable their success on certification exams and in the workplace.

■ The Microsoft Official Academic Course Program

The Microsoft Official Academic Course series is a complete program for instructors and institutions to prepare and deliver great courses on Microsoft software technologies. With MOAC, we recognize that because of the rapid pace of change in the technology and curriculum developed by Microsoft, there is an ongoing set of needs beyond classroom instruction tools for an instructor to be ready to teach the course. The MOAC program endeavors to provide solutions for all these needs in a systematic manner in order to ensure a successful and rewarding course experience for both instructor and student, including technical and curriculum training for instructor readiness with new software releases; the software itself for student use at home for building hands-on skills, assessment, and validation of skill development; and a great set of tools for delivering instruction in the classroom and lab. All are important to the smooth delivery of an interesting course on Microsoft software, and all are provided with the MOAC program.

Conventions and Features Used in This Book

This book uses particular fonts, symbols, and heading conventions to highlight important information or to call your attention to special steps.

Convention	Meaning
THE BOTTOM LINE	This feature provides a brief summary of the material to be covered in the section that follows.
WARNING	*Warning* points out instances when error or misuse could cause damage to the computer or network.
A ***shared printer*** can be used by many individuals on a network.	Key terms appear in bold italic.
`cd\windows\system32\ServerMigrationTools`	Commands that are to be typed are shown in a special font.
Click Install Now.	Any button on the screen you are supposed to click on or select will appear in blue.

Instructor Support Program

The Microsoft Official Academic Course programs are accompanied by a rich array of resources that incorporate the extensive textbook visuals to form a pedagogically cohesive package.

- **Instructor's Guide.** The Instructor's Guide contains chapter summaries and lecture notes.
- **Test Bank.** The Test Bank contains hundreds of questions organized by lesson in multiple-choice, best answer, build a list, and essay formats. A complete answer key is provided.
- **PowerPoint Presentations.** A complete set of PowerPoint presentations is available to enhance classroom presentations. Tailored to the text's topical coverage, these presentations are designed to convey key Windows Server 2012 R2 concepts addressed in the text.
- **MOAC Labs Online.** MOAC Labs Online is a cloud-based environment that enables students to conduct exercises using real Microsoft products. These are not simulations but instead are live virtual machines where faculty and students can perform any activities they would on a local virtual machine. MOAC Labs Online relieves the need for local setup, configuration, and most troubleshooting tasks. This represents an opportunity to lower costs, eliminate the hassle of lab setup, and support and improve student access and portability. Contact your Wiley rep about including MOAC Labs Online with your course offering.

About the Author

Patrick Regan has been a PC technician, network administrator/engineer, design architect, and security analyst for the past 23 years since graduating with a bachelor's degree in physics from the University of Akron. He has taught many computer and network classes at Sacramento local colleges (Heald Colleges and MTI Colleges) and participated in and led many projects (Heald Colleges, Intel Corporation, Miles Consulting Corporation, and Pacific Coast Companies). For his teaching accomplishments, he received the Teacher of the Year award from Heald Colleges and he has received several recognition awards from Intel. Previously, he worked as a product support engineer for the Intel Corporation Customer Service, a senior network engineer for Virtual Alert supporting the BioTerrorism Readiness suite and as a senior design architect/engineer and training coordinator for Miles Consulting Corporation (MCC), a premiere Microsoft Gold partner and consulting firm.

He is currently a senior network engineer and consultant supporting a large enterprise network at Pacific Coast Companies, which is also a Microsoft Gold Partner and consulting firm. As a senior system administrator, he supports approximately 120 servers and 1,500 users spread over 5 subsidiaries and 70 sites. He has designed, implemented, and managed systems running Exchange Server 2010, SharePoint 2010, and SQL Server 2008 R2. To manage the servers and client computers, Pat and his team use group policies, SCOM, SCCM, and Symantec server.

He has earned several certifications, including Microsoft's MCSE, MCSA, and MCT; CompTIA's A+, Network+, Server+, Linux+, and Security+; Cisco's CCNA; and Novell's CNE and CWNP Certified Wireless Network Administrator (CWNA).

Over the past several years, he has written several textbooks for Prentice Hall, including *Troubleshooting the PC, Networking with Windows 2000 and 2003, Linux, Local Area Networks, Wide Area Networks*, and the Acing Series (*Acing the A+*, *Acing the Network+*, *Acing the Security+*, and *Acing the Linux+*). For Que Publishing has written several Exam Cram books for Windows Server 2008 certification tracks. For Wiley Publishing, he has written books on SharePoint 2010, Windows 7, and Windows Server 2012.

Brief Contents

1 Deploying and Managing Server Images 1
2 Implementing Patch Management 17
3 Monitoring Servers 34
4 Configuring Distributed File System (DFS) 59
5 Configuring File Server Resource Manager (FSRM) 76
6 Configuring File Services and Disk Encryption 87
7 Configuring Advanced Audit Policies 100
8 Configuring DNS Zones 123
9 Configuring DNS Records 136
10 Configuring VPN and Routing 148
11 Configuring Direct Access 167
12 Configuring a Network Policy Server 179
13 Configuring NPS Policies 192
14 Configuring Network Access Protection (NAP) 203
15 Configuring Service Authentication 218
16 Configuring Domain Controllers 226
17 Maintaining Active Directory 238
18 Configuring Account Policies 253
19 Configuring Group Policy Processing 261
20 Configuring Group Policy Settings 273
21 Managing Group Policy Objects 288
22 Configuring Group Policy Preferences 295

Contents

Lesson 1: Deploying and Managing Server Images 1

Using Windows Deployment Services 1
- Installing the Windows Deployment Services Role 2
- Configuring the WDS Server 3
  - Performing the Initial Configuration of WDS 4
  - Configuring the WDS Properties 6
  - Starting WDS 7
- Configuring and Managing Boot, Install, and Discover Images 7
  - Adding Boot Images 7
  - Adding Image Files 8
  - Creating an Image File with WDS 9
  - Creating a Discover Image 11
  - Using Wdsutil 12
- Updating Images with Patches, Hotfixes, and Drivers 14
- Installing Features for Offline Images 15
- Configuring Driver Groups and Packages 15

Business Case Scenarios 16

Lesson 2: Implementing Patch Management 17

Deploying Windows Server Update Services (WSUS) 17
- Installing WSUS 19
- Configuring WSUS 21
  - Configuring WSUS Synchronization 22
  - Configuring WSUS Computer Groups 25
  - Configuring Group Policies for Updates 27
  - Configuring Client-Side Targeting 28
- Approving Updates 30

Managing Patch Management In Mixed Environments 32

Business Case Scenarios 33

Lesson 3: Monitoring Servers 34

Introducing the Microsoft Management Console (MMC) 34
- Using Server Manager 35
- Using Computer Management 35

Using Event Viewer 36
- Understanding Logs and Events 37
- Filtering Events 38
- Configuring Event Subscriptions 39

Managing Performance 42
- Using Task Manager 42
- Using Resource Monitor 45
- Using Performance Monitor 48
- Configuring Data Collector Sets (DCS) 50
- Configuring Performance Alerts 51
- Scheduling Performance Monitoring 52

Monitoring the Network 52
- Using the netstat Command 53
- Using Protocol Analyzers 54

Monitoring Virtual Machines (VMs) 58

Business Case Scenarios 58

Lesson 4: Configuring Distributed File System (DFS) 59

Using Distributed File System 59
- Installing and Configuring DFS Namespace 59
  - Installing DFS Namespace 60
  - Configuring DFS Namespaces 61
  - Managing Referrals 63
  - Managing DFS Security 64
- Installing and Configuring DFS Replication 65
  - Installing DFS Replication 65
  - Configuring DFS Replication Targets 66
- Scheduling Replication 68

Configuring Remote Differential Compression 69
Configuring Staging 71
Cloning a DFS Database 72
Recovering DFS Databases 73
Optimizing DFS Replication 73
Configuring Fault Tolerance Using DFS 74
Business Case Scenarios 75

Lesson 5: Configuring File Server Resource Manager (FSRM) 76

Using File Server Resource Manager 76
Installing File Server Resource Manager 76
Using Quotas 77
Creating Quotas 78
Managing Files with File Screening 81
Creating File Groups 81
Creating a File Screen 81
Using Storage Reports 83
Enabling SMTP 84
Configuring File Management Tasks 84
Business Case Scenarios 86

Lesson 6: Configuring File Services and Disk Encryption 87

Securing Files 87
Encrypting Files with EFS 88
Configuring EFS 88
Configuring the EFS Recovery Agent 89
Managing EFS Certificates 90
Encrypting Files with BitLocker 92
Configuring BitLocker Encryption 93
Configuring BitLocker Policies 95
Managing BitLocker Certificates 97
Configuring the Network Unlock Feature 97
Business Case Scenarios 99

Lesson 7: Configuring Advanced Audit Policies 100

Enabling and Configuring Auditing 100
Implementing Auditing Using Group Policies 100
Implementing an Audit Policy 101
Implementing Object Access Auditing Using Group Policies 101
Implementing Advanced Audit Policy Settings 103
Implementing Advanced Audit Policy Settings Using Group Policies 103
Removing Advanced Audit Policy Configuration 117
Implementing Auditing Using AuditPol.exe 117
Creating Expression-Based Audit Policies 119
Creating Removable Device Audit Policies 121
Business Case Scenarios 122

Lesson 8: Configuring DNS Zones 123

Understanding DNS 123
Configuring and Managing DNS Zones 124
Installing DNS 124
Configuring Primary and Secondary Zones 126
Configuring Active Directory-Integrated Zones 127
Configuring Zone Delegation 129
Configuring Stub Zones 130
Configuring Forwarding and Conditional Forwarding 131
Configuring Zone Transfers 133
Understanding Full and Incremental Transfers 133
Configuring Notify Settings 134
Business Case Scenarios 135

Lesson 9: Configuring DNS Records 136

Configuring DNS Record Types 136
Creating and Configuring DNS Resource Records 136
Start of Authority (SOA) Records 137
Name Server (NS) Records 138
Host (A and AAAA) Records 139
Canonical Name (CNAME) Records 139
Pointer (PTR) Records 140
Mail Exchanger (MX) Records 140
Service Location (SRV) Records 141
Configuring Record Options 142
Configuring Round Robin 143
Configuring Secure Dynamic Updates 144
Configuring Zone Scavenging 145
Business Case Scenarios 147

www.wiley.com/college/microsoft *or*
call the MOAC Toll-Free Number: 1+(888) 764-7001 (U.S. & Canada only)

Lesson 10: Configuring VPN and Routing 148

The Remote Access Role 148
Installing and Configuring the Remote Access Role 148
Installing Routing and Remote Access 148
Configuring Routing and Remote Access 150
Configuring RRAS for Dial-Up Remote Access 150
Configuring VPN Settings 152
Configuring the VPN Connection on the Server 153
Creating a VPN Connection on a Client 155
VPN Reconnect 156
Configuring Split Tunneling 156
Configuring Remote Dial-In Settings for Users 157
Implementing NAT 158
Configuring Routing 159
Managing Static Routes 160
Configuring RIP 161
Configuring Demand-Dial Routing 163
Configuring the DHCP Relay Agent 163
Configuring Web Application Proxy in Passthrough Mode 163
Business Case Scenarios 166

Lesson 11: Configuring Direct Access 167

Understanding DirectAccess 167
Understanding DirectAccess Requirements 167
Understanding DirectAccess Server Requirements 167
Understanding DirectAccess Client Requirements 168
Running the Remote Access Setup Wizard 169
Implementing Client Configuration 169
Implementing DirectAccess Server 171
Implementing Infrastructure Servers 172
Preparing for DirectAccess Deployment 173
Configuring DNS for DirectAccess 173
Configuring Certificates for DirectAccess 174
Business Case Scenarios 178

Lesson 12: Configuring a Network Policy Server 179

Configuring a Network Policy Server Infrastructure 179
Installing and Configuring a RADIUS Server 180
Configuring RADIUS Clients 181
Configuring NPS Templates 185
Configuring RADIUS Accounting 187
Understanding NPS Authentication Methods 189
Using Password-Based Authentication 189
Using Certificates for Authentication 189
Business Case Scenarios 191

Lesson 13: Configuring NPS Policies 192

Managing NPS Policies 192
Configuring Connection Request Policies 193
Configuring Network Policies 197
Multilink and Bandwidth Allocation 198
IP Filters 199
Encryption 200
IP Addressing 200
Exporting and Importing the NPS Configuration Including NPS Policies 201
Business Case Scenarios 202

Lesson 14: Configuring Network Access Protection (NAP) 203

Using Network Access Protection (NAP) 203
Installing Network Access Protection 205
Configuring NAP Enforcement 205
Configuring NAP Enforcement for DHCP 206
Configuring NAP Enforcement for VPN 211
Configuring System Health Validators 212
Configuring Health Policies 213
Configuring Isolation and Remediation 215
Configuring NAP Client Settings 216
Business Case Scenarios 217

Lesson 15: Configuring Service Authentication 218

Configuring Service Authentication 218
Managing Service Principal Names 218
Configuring Kerberos Delegation 220
Managing Service Accounts 221
Creating and Configuring Service Accounts 222

Creating and Configuring Managed Service Accounts 223
Creating and Configuring Group Managed Service Accounts 224
Configuring Virtual Accounts 225
Business Case Scenarios 225

Lesson 16: Configuring Domain Controllers 226

Understanding Domain Controllers 226
Managing Operations Masters 227
Transferring the Operations Masters Role 229
Seizing the Operations Masters Role 230
Installing and Configuring an RODC 231
Cloning a Domain Controller 234
Business Case Scenario 237

Lesson 17: Maintaining Active Directory 238

Backing Up and Restoring Active Directory 238
Using Windows Backup 239
Performing a Backup of Active Directory and Sysvol 239
Performing an Active Directory Restore 240
Configuring Active Directory Snapshots 243
Performing Object- and Container-Level Recovery 245
Configuring and Restoring Objects by Using the Active Directory Recycle Bin 247
Managing Active Directory Offline 250
Optimizing an Active Directory Database 250
Cleaning Up Metadata 251
Business Case Scenarios 252

Lesson 18: Configuring Account Policies 253

Working with Account Policies 253
Configuring Domain User Password Policy 254
Configuring Password Policy Settings 254
Configuring Account Lockout Settings 256
Configuring and Applying Password Settings Objects 257
Configuring Local User Password Policy 258
Delegating Password Settings Management 258
Configuring Kerberos Policy Settings 260
Business Case Scenarios 260

Lesson 19: Configuring Group Policy Processing 261

Understanding Group Policy Processing 261
Configuring Processing Order and Precedence 261
Understanding Group Policy Inheritance 262
Using Filtering with Group Policies 264
Configuring Blocking of Inheritance 264
Configuring Enforced Policies 265
Configuring Security Filtering and WMI Filtering 265
Using Security Filtering 265
Using WMI Filtering 267
Configuring Loopback Processing 268
Configuring Client-Side Extension Behavior 269
Looking at GPOs and Disconnected Computers 270
Configuring and Managing Slow-Link Processing and Group Policy Caching 270
Forcing Group Policy Update 271
Business Case Scenarios 272

Lesson 20: Configuring Group Policy Settings 273

Configuring Group Policy Settings 273
Performing Software Installation Using Group Policy 275
Assigning or Publishing a Package 275
Using Folder Redirection 277
Using Scripts with Group Policy 279
Using Administrative Templates 281
Managing Administrative Templates 281
Creating a Central Store 283
Using Security Templates 284
Using Custom Administrative Template Files 286
Configuring Property Filters for Administrative Templates 287
Business Case Scenario 287

Lesson 21: Managing Group Policy Objects 288

Managing Group Policy Objects 288
Backing Up and Restoring GPOs 288
Using a Migration Table 290
Resetting the Default GPOs 292
Delegating Group Policy Management 292
Business Case Scenarios 294

Lesson 22: Configuring Group Policy Preferences 295

Using Group Policy Preferences 295
Configuring Preference Settings 295
Configuring Windows Settings 296
Configuring Network Drive Mappings 297
Performing File and Folder Deployment 297
Performing Shortcut Deployment 299
Configuring Control Panel Settings 300
Configuring Printer Settings 300
Configuring Custom Registry Settings 302
Configuring Power Options 302
Configuring Internet Explorer Settings 303
Configuring Item-Level Targeting 304
Business Case Scenarios 306

Deploying and Managing Server Images

LESSON 1

TAKE NOTE*

Before beginning this course, you should have some experience installing Windows, including installing Windows Server 2012. In an enterprise environment, many administrators will need to install Windows numerous times. In addition, administrators in many enterprise environments will have a need to deploy servers to remote site. Therefore, as a server administrator, you must be familiar with the various methods to install and deploy Windows.

Using Windows Deployment Services

THE BOTTOM LINE

In the 70-410 course, you learned how to install Windows from a Windows installation disk. It is not difficult to figure out that installing 100 computers using an installation disk is a daunting task. In these situations, rather than do a manual install on each computer, you can use Windows Deployment Services to automatically deploy Windows to multiple computers. While Windows Deployment Services takes a little bit of work up front, it can save you a lot of work later.

Windows Deployment Services (WDS) is a software platform and technology that allows you to perform automated network-based installations based on network-based boot and installation media. In other words, you can perform an installation over a network with no operating system or local boot device on it. The WDS server will store the installation files and help you manage the boot and operating system image files used in the network installations. Although WDS is included with later versions of Windows Server, including Windows Server 2012 R2, it can be used to deploy Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.

An ***image file*** is basically a snapshot of a computer's hard drive taken at a particular moment in time. The image file is sometimes referred to as an install image and is used to install an operating system. It contains the following:

- All of the operating system files on the computer
- Any updates and drives that have been applied
- Any applications that have been installed
- Any configuration changes that have been made

For client computers to communicate with a WDS server without an operating system, the client computer must have support ***preboot execution environment (PXE)***, pronounced "pixie." PXE is a technology that boots computers using the network interface without a

data storage device, such as a hard drive or an installed operating system. For a computer to perform a PXE boot, you must configure the BIOS setup program to perform a network boot. Depending on your system, you must enable the PXE boot and/or change the boot order so that the PXE boot occurs before the system tries other boot devices to boot from.

When PXE is used with WDS, the client computer downloads a boot image that loads ***Windows Preinstallation Environment (Windows PE)***. Windows PE is a minimal Windows operating system with limited services. Windows PE is then used to install the operating system using an operating system image file. Windows PE 4.0 is based on the Windows 8 operating system.

Installing the Windows Deployment Services Role

WDS is a server role that is included with Windows Server 2012 R2. Therefore, before you can use WDS, you must install the WDS role and configure the services. Then you need to create and add the images that you want to deploy.

WDS is a standard server role that can be installed using the Server Manager console and includes the following two role services:

- ***Deployment Server:*** Provides full functionality of WDS. It includes an image repository (including boot images, install images, and other files necessary for remote installation over a network), PXE server for remote computers to boot, and a Trivial File Transfer Protocol (TFTP) server to transfer files over the network. TFTP is similar to FTP, but uses User Datagram Protocol (UDP) instead of Transmission Control Protocol (TCP) for less overhead (simpler packets that can be processed faster than TCP packets because UDP does not require the use of acknowledgments). In addition, the Deployment Server includes tools to create and customize images.
- ***Transport Server:*** While required by the Deployment Server, the Transport Server role is a subset of WDS functionality, but can also be used for custom solutions. The Transport Server can also use ***multicasting***, which allows one set of packets to be sent to multiple computers simultaneously.

DEPLOY WDS

GET READY. To deploy WDS on Windows Server 2012 R2, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar. The *Server Manager* opens.
2. At the top of *Server Manager*, click Manage and then click Add Roles and Features. The Add Roles and Feature Wizard opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation, and then click Next.
5. Click Select a server from the server pool, click the name of the server to install WDS to, and then click Next.
6. Scroll down and select Windows Deployment Services (see Figure 1-1).

Figure 1-1

Selecting Windows Deployment Services

7. When the *Add Roles and Features Wizard* dialog box opens, click Add Features.
8. Click Next.
9. Back on the *Select server roles* page, click Next.
10. On the *Select features* page, click Next.
11. On the *WDS* page, click Next.
12. On the *Select role services* page, make sure that the Deployment Server option and the Transport Server option are selected, and then click Next.
13. On the *Confirm installation selections* page, click Install.
14. When the installation finishes, click Close.

Configuring the WDS Server

Before you can use WDS, you must configure the WDS server, including performing the initial server configuration, adding a default startup and install images, and configuring a boot menu.

WDS is inactive until you perform the initial configuration of the service and add images to the server. To use WDS, your system must meet the following requirements:

- The server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain.
- There is an active DHCP server on the network.
- There is an active DNS server on your network.
- The WDS server has an NTFS file system partition to store images.

PERFORMING THE INITIAL CONFIGURATION OF WDS

Before you can use WDS, you must configure WDS by determining if the server will be part of Active Directory, determining where the boot and install images will be stored, and configuring the DHCP server so that clients can boot to the WDS server. To perform the initial configuration using the Windows Deployment Services Configuration Wizard, open the Windows Deployment Services console, right-click the WDS server, and then select Configure Server.

PERFORM THE INITIAL CONFIGURATION OF WDS

GET READY. To perform the initial configuration of WDS on Windows Server 2012 R2, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar. The *Server Manager* opens.
2. At the top of *Server Manager*, click Tools > Windows Deployment Services (see Figure 1-2). The *Windows Deployment Services* console opens.

Figure 1-2

Opening the Windows Deployment Services console

3. Expand Servers, right-click the WDS server, and then select Configure Server.
4. When the *Before You Begin* page appears, click Next.
5. On the *Install Options* page, select the Integrated with Active Directory option, and then click Next.

6. On the *Remote Installation Folder Location* page, specify the location of the remote installation folder and then click Next.
7. If you use the C drive, you will be warned that you have selected the Windows system volume and that you should use a separate volume. To continue, click Yes. Of course, in a production environment, for performance and system reliability, you should create a separate volume to store the WDS images.
8. If your WDS server is also a DHCP server, another page appears (see Figure 1-3), enabling you to configure the server so that there is not a port conflict.

Figure 1-3

Specifying the DHCP Server options

By default, when a DHCP client is looking for a DHCP server, it will perform a broadcast using UDP port 67. If the WDS server is also the DHCP server, you must tell WDS not to listen on port 67 so that DHCP can function properly. To do this, select the Do not listen on DHCP and DHCPv6 ports check box.

If the local DHCP server is a Microsoft DHCP server, you should select the Configure DHCP options for Proxy DHCP check box so that the DHCP server is automatically configured to forward the PXE requests to the WDS server. If the local DHCP server is not a Microsoft DHCP server, you will have to manually configure the DHCP server to forward the request to the WDS server.

9. Click Next.
10. On the *PXE Server Initial Settings* page, select the appropriate options:
    - **Do not respond to any client computers:** By selecting this option, WDS cannot perform installations. You would typically use this option to keep WDS disabled until you are ready to use it.

- **Respond only to known client computers:** A known client computer is a computer that has a computer account pre-staged or created in Active Directory before you perform the installation. By selecting this option, WDS responds to computers that you have prestaged; it does not respond to unstaged or rogue systems. This option is selected by default.
- **Respond to all client computers (known and unknown):** By selecting this option, WDS responds to any client system that makes an installation request. Because it responds to any computer that attempts a PXE boot, it is the least secure option.

11. Click Next.
12. When the task is completed, click Finish.

CONFIGURING THE WDS PROPERTIES

After you perform the initial configuration, you must reconfigure the WDS server by accessing the WDS Properties (right-click the server in the Windows Deployment Services console and then select Properties). The WDS properties include the following tabs:

- **General:** Displays server name, mode, and location of the remote installation folder where images are stored.
- **PXE Response:** Enables you to specify which types of computers (known or unknown) can download and install images from the server. In addition, you can determine the PXE boot delay in seconds (zero by default).
- **AD DS:** Allows you to determine the automatic naming format for WDS clients in AD DS that are not prestaged, and it allows you to specify where the computer account will be created in Active Directory.
- **Boot:** Allows you to specify the default network boot image for each architecture type (x86, x64, and ia64) and the PXE Boot Policy settings for known and unknown clients. It also allows you to specify if a user must press F12 to continue the PXE boot.
- **Client:** Allows you to enable and configure unattended installations of the WDS clients. In addition, if you do not want to add a computer to the domain, you can select the *Do not join the client to a domain after an installation* option.
- **DHCP:** Allows you to enable or disable if a server listens on the DHCP ports (port 67) and to automatically configure DHCP option 60 on a DHCP server.
- **Multicast:** Allows you to use one set of packets to install operating systems on multiple computers simultaneously. As a result, you minimize network traffic. The Multicast tab also allows you to configure Transfer Settings.
- **Advanced:** Allows you to authorize your WDS server in DHCP. It also allows you to specify a domain controller and global catalog or to allow WDS to discover them on its own.
- **Network:** Allows you to specify the UDP port ranges WDS uses. Typically, you would leave the default setting (*Obtain dynamic ports from Winsock*) selected. You should note that the Network profile option is grayed out in Windows Server 2012 R2, which would allow you to specify the bandwidth of your network. Instead, the bandwidth is determined automatically.
- **TFTP:** Allows you to configure the maximum block size used for FTP transfers. The TFTP option was introduced in Windows Server 2012.

STARTING WDS

After you perform the initial configuration, you reconfigure the WDS server by accessing the WDS Properties. To access the WDS Properties, right-click the server in the Windows Deployment Services console, choose All Tasks, and then choose Start. Then you will need to add the images that you want to deploy, which is discussed in the next section.

Configuring and Managing Boot, Install, and Discover Images

To deploy Windows, you must create two types of images: a boot image and an install image. Just as the name implies, the boot image boots the computer. In addition, the ***boot image*** starts the operating system installation. The ***install image*** contains the operating system that WDS installs.

There are two types of image formats:

- ***Sector-based image formats***, whereby each sector is stored within the file and each sector is the smallest unit of information. One common example of a disk image is the .ISO file used for a CD image and a DVD image.
- ***File-based image formats***, whereby each file is the smallest unit. The advantage of using a file-based image is that it is hardware-independent and a file can be referenced multiple times within the file system tree. A common example is a WIM image used with WDS.

The boot images and the install images use the ***Windows Imaging Format (WIM)***, a file format that allows a file structure (folders and files) to be stored inside a single WIM database. By using a database, the system does not have to open and close several individual files during the data transfer.

ADDING BOOT IMAGES

The Windows Server installation DVDs include a boot image file named *boot.wim*, located in the *\sources* folder (see Figure 1-4), which loads Windows PE 4.0 on the client computer. Since it is used to boot the computer and start the installation of an operating system, it can be used for virtually any operating system deployment without modification.

Figure 1-4

Viewing the sources folder

ADD A BOOT IMAGE

GET READY. To add a boot image file to WDS, perform the following steps:

1. Open Server Manager.
2. Click Tools > Windows Deployment Services. The *Windows Deployment Services* console opens.
3. Expand Servers and then expand the server so that you can see the *Install Images* folder and the *Boot Images* folder (see Figure 1-5).

Figure 1-5

Viewing the Install Images folder and the Boot Images folder

4. To add a boot image, right-click the *Boot Images* folder and choose Add Boot Image. The *Add Image Wizard* opens.
5. Browse to the location of the image file (such as the *Sources* folder located on the installation DVD), click the boot.wim file, and then click Open.
6. On the *Image File* page, click Next.
7. On the *Image Metadata* page, type a name and description of the image and then click Next. Most of the time, you can use the default values.
8. On the *Summary* page, click Next.
9. When the image is added to the server, click Finish.

ADDING IMAGE FILES

As previously mentioned, the image file contains the operating system that WDS will install on the client computer. Included in the Sources folder on the Windows Server 2012 R2 installation disk is an *install.wim* file for Windows Server 2012 R2 that allows you to perform a standard Windows Server 2012 R2 installation similar to performing a manual installation from disk.

When you create image files, you place the image file in an image group. An ***image group*** is a folder within the image repository of WDS that shares security options and file resources. The image group consists of the following two components:

- The resource *.wim* file (*Res.rwm*). This contains the file resources for all of the images in an image group. Although the file name seems to indicate otherwise, the .rwm file is actually a .wim file.
- The *<imagename>.wim* files. Each *.wim* image file contains the metadata that describes the image, but the actual file resources for the image reside in *Res.rwm*.

  Any permission assigned to an image group is inherited by all of the images in the group. By default, authenticated users are granted read access to image groups and images while administrators have full control. You can control who can receive specific images by modifying the permissions of the images or by placing the images in image groups and modifying the permissions of the groups.

ADD AN INSTALL IMAGE FILE

GET READY. To add an install image file to WDS, perform the following steps:

1. Open Server Manager.
2. Click Tools > Windows Deployment Services. The *Windows Deployment Services* console opens.
3. Expand *Servers* and then expand the server so that you can see the *Install Images* folder and the *Boot Images* folder (see Figure 1-5).
4. Right-click the *Install Images* folder and select Add Install Image. The *Add Image Wizard* page opens.
5. On the *Image Group* page, the Create an image group named option is selected. If desired, type a different name of the image group and then click Next.
6. Browse to the location of the image file (such as the *Sources* folder located on the installation DVD), select the install.wim file, and then click Open.
7. On the *Image File* page, click Next.
8. On the *Available Images* page, select the images you want to include, and then click Next.
9. On the *Summary* page, click Next.
10. When the images are added to the server, click Finish.

CREATING AN IMAGE FILE WITH WDS

The install images that are included on a Windows installation disk are images of a basic Windows installation, with no patches, updates, or additional drivers. If you would like to create your own image files, you must first set up a master computer with all of the patches, drivers, applications, and configurations applied. Then use WDS to create your own image file by modifying an existing boot image, booting the master computer with the modified boot image, and running the ***Windows Deployment Services Capture Utility***. The Windows Deployment Services Capture Utility will create an image file and write it to the computer's drive, which will eventually be copied to the WDS server. You can then use it to be deployed to other computers.

CREATE AN IMAGE FILE

GET READY. To create an image file, perform the following steps:

1. Open Server Manager.
2. Click Tools > Windows Deployment Services. The *Windows Deployment Services* console opens.
3. Expand Servers and then expand the server so that you can see the *Install Images* folder and the *Boot Images* folder.
4. If you have not done so already, add the Windows Server 2012 R2 boot.wim image to the Boot Images store by following the steps provided in the Add a Boot Image exercise.
5. Right-click the boot image and choose Create Capture Image. The *Create Capture Image Wizard* opens.
6. Specify a name and description for the new image. Then specify the Location and file name for the new image file (see Figure 1-6). Click Next.

Figure 1-6

Specifying the location and file name

7. When the task is complete, you can select Add image to the Windows Deployment Server now (if desired). Then click Finish.

Before capturing a computer with WDS, you must prepare a master or reference computer with the Sysprep.exe utility and reboot the computer using the capture image. Microsoft's ***System Preparation Utility (Sysprep.exe)*** prepares a Windows computer for cloning by removing specific computer information such as the computer name and Security Identifier (SID). On Windows Server 2012 R2, the Sysprep.exe is located in the C:\Windows\System32\Sysprep folder. When you reboot the computer with the capture image, a Wizard guides you through the process of capturing an image of the computer and uploading it to the WDS server.

When running `sysprep` on the master computer, use the following syntax:

```
sysprep /generalize /oobe
```

The `/generalize` parameter removes the unique values, such as the computer name and the SID, so that they are not captured in the image file and replicated to the target workstations. The `/oobe` parameter configures Windows to present the Windows Welcome Wizard the next time the computer starts. The Windows Welcome Wizard allows you to name the computer and generate a SID and any other required unique information.

CREATING A DISCOVER IMAGE

If you have a computer that does not support a PXE boot, you can boot the computer from disk using a discover image. A ***discover image*** is an image file that you can burn to a CD-ROM or other boot medium. When you boot the client computer using the discover image disk, the computer loads Windows PE, connects to a specified WDS server, and proceeds with the operating system installation process.

CREATE A DISCOVER IMAGE

GET READY. To create a discover image file, perform the following steps:

1. Open Server Manager.
2. Click Tools > Windows Deployment Services. The *Windows Deployment Services* console appears.
3. Expand Servers and then expand the server so that you can see the *Install Images* folder and the *Boot Images* folder.
4. To create a discover boot image, right-click a boot image in the *Windows Deployment Services* console and choose Create Discover Image. Click Next.
5. On the *Metadata and Location* page, leave the default Image name and Image description as-is. Then specify where you want to store the discover image file. In addition, you can *Enter the name of the Windows Deployment Services server*...(see Figure 1-7). Click Next.

Figure 1-7

Specifying the image name, the image description, and where to store the discover image file

6. On the *Summary* page, click Next.
7. When the images are added to the server, click Finish.

To convert the discover image to a bootable .ISO image, you first must download and install the ***Windows Assessment and Deployment Kit (ADK)*** for Windows 8. ADK is a set of tools provided by Microsoft to customize, assess, and deploy a Windows operating system to new computers. It is located at Microsoft's Download Center. Then use the oscdimg.exe command to create the .ISO image.

INSTALL THE WINDOWS ASSESSMENT AND DEPLOYMENT KIT (ADK)

GET READY. To install the ADK, perform the following steps:

1. Start the Windows Assessment and Deployment Kit by double-clicking adksetup.exe.
2. On the *Specify Location* page, leave the default settings, and then click Next.
3. When you are prompted to join the *Customer Experience Improvement Program (CEIP)*, click Next.
4. On the *License Agreement* page, click Accept.
5. With the *Deployment Tools and Windows Preinstallation Environment (Windows PE)* already selected, click Install.
6. When the installation is complete, click Close.

CREATE A BOOTABLE ISO IMAGE

GET READY. After you have installed the ADK for Windows 8.1, perform the following steps to create a bootable ISO Image:

1. Create a folder named C:\WinPE_x64\ISO.
2. Copy the contents of the C:\Program Files (x86)\Windows Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\Media folder to C:\WinPE_x64\ISO.
3. Create the C:\WinPE_x64\ISO\Sources folder.
4. Copy the discover image to the C:\WinPE_x64\ISO\Sources folder.
5. Rename the discover.wim file in the C:\WinPE_x64\ISO\Sources folder to boot.wim.
6. Copy the etfsboot.com file from the C:\Program Files (x86)\Windows Kits\8.1\Assessment and Deployment Kit\Deployment and Imaging Tools\amd64\Oscdimg folder to the C:\WinPE_x64 folder.
7. Create the bootable ISO by running the following command:

```
oscdimg -b"c:\WinPE_X64\etfsboot.com" -n C:\WinPE_X64\ISO C:\
WinPE_X64\WinPE_X64.iso
```

USING WDSUTIL

Different from most of the components that are included with Windows, you cannot install and configure Windows Deployment Services by using Windows PowerShell. Instead, the wdsutil command is used for managing the Windows Deployment Services server. To use the wdsutil command line, you will need to open a Command Prompt as an administrator.

The wdsutil commands include:

- **/add** – Adds prestaged computers, images, or image groups.
- **/approve-AutoAddDevices** – Approves computers that are pending administrator approval.
- **/convert-RiprepImage** – Converts an existing Remote Installation Preparation (RIPrep) image to a Windows Image (.wim) file.

- **/copy** – Copies an image or a driver group.
- **/delete-AutoAddDevices** – Deletes computers that are in the Auto-Add database (which stores information about the computers on the server).
- **/disable** – Disables all services for Windows Deployment Services.
- **/disconnect-Client** – Disconnects a client from a multicast transmission or namespace.
- **/enable** – Enables all services for Windows Deployment Services.
- **/export-Image** – Exports an image from the image store to a .wim file.
- **/get** – Retrieves properties and attributes about the specified object.
- **/initialize-Server** – Configures a Windows Deployment Services server for initial use.
- **/new** – Creates new capture and discover images, multicast transmissions, and namespaces.
- **/progress** – Displays the progress status while a command is being executed.
- **/reject-AutoAddDevices** – Rejects computers that are pending administrator approval.
- **/remove** – Removes objects.
- **/replace-Image** – Replaces a boot or installation image with a new version of that image.
- **/set** – Sets properties and attributes on the specified object.
- **/start** – Starts all services on the Windows Deployment Services server, including multicast transmissions, namespaces, and the Transport Server.
- **/stop** – Stops all services on the Windows Deployment Services server.
- **/uninitialize-Server** – Reverts changes made during server initialization.
- **/update-ServerFiles** – Updates server files on the RemoteInstall share.
- **/verbose** – Displays verbose output for the specified command.

For example, to show the WDS configuration, you can use one of the following commands:

```
wdsutil /get-server /show configure
wdsutil /get-server /show:all /detailed
```

To show the WDS configuration, you can use one of the following commands:

```
wdsutil /get-server /show configure
wdsutil /get-server /show:all /detailed
```

To stop or start the WDS server, use the following commands:

```
wdsutil /stop-server
wdsutil /start-server
```

To show the WDS configuration, you can use one of the following commands:

```
wdsutil /get-server /show configure
wdsutil /get-server /show:all /detailed
```

To show the WDS configuration, you can use one of the following commands:

```
wdsutil /get-server /show configure
wdsutil /get-server /show:all /detailed
```

To add a computer by using a MAC address, you would use the following command:

```
wdsutil /Add-Device /Device:PC1 /ID:00-C1-46-8A-1F-EB
```

To add a boot image, use the following command:

```
wdsutil /Add-Image /ImageFile:"C:\Data\Boot.wim" /ImageType:Boot
```

To add an install image, use the following command:

```
Wdsutil /Add-Image /ImageFile:"C:\Data\Install.wim" /ImageType:Install
```

Updating Images with Patches, Hotfixes, and Drivers

When you create an image file, you install Windows on a master computer, update and configure the computer, and then install any applications – all of which can take many hours to get everything just right. When Microsoft releases updates that you want to include in the new image, instead of going through the entire process of creating and setting up a new master computer, you can update the image file using Deployment Image Servicing and Management (Dism.exe).

Deployment Image Servicing and Management (Dism.exe) is a command-line tool that can be used to service a Windows image or to prepare a Windows PE image. With Dism, you can mount an image offline and then add, remove, update, or list the features, packages, drivers, or international settings stored on that image. Dism.exe is not included with Windows.

To make changes to an image, you must mount the Windows image in the Windows file structure using the `Mount-Wim` option. To mount the *D:\RemoteInstall\install.wim* file to the *C:\Offline* folder, use the following command:

```
Dism /Mount-Wim /WimFile: D:\RemoteInstall\install.wim /index:1 /
MountDir:C:\Offline
```

After you make changes to the image, you need to commit the changes by using the `/Commit-Wim` option:

```
Dism /Commit-Wim /MountDir:C:\Offline
```

To unmount the image, use the `/Unmount-Wim` option. If you want to commit the changes while you unmount the image, add the `/Commit` option. To discard the changes, use the `/Discard` option. For example, to unmount the image mounted to the *C:\Offline folder* while saving the changes, execute the following command:

```
Dism /Unmount-Wim /MountDir:C:\offline /commit
```

To get information about an image or WIM file, use the `/Get-WimInfo` option. For example, in the previous WIM file, execute the following command:

```
Dism /Get-WimInfo /WimFile:C:\offline\install.wim /index:1
```

Packages are used by Microsoft to distribute software patches, hotfixes, service packs, language packages, and Windows features. If a Windows package is provided as a cabinet (*.cab*) file or as a Windows Update Stand-alone Installer (*.msu*) file, you can add the package using the `/Add-Package` command. For example, to add the *C:\Update\Update.cab* file, execute the following command:

```
Dism /image:C:\offline /Add-Package /Packagepath:C:\Update\Update.cab
```

To remove a package, use the `/Remove-Package` option. For example, to remove the *update.cab* file, execute the following command:

```
Dism /image:C:\offline /Remove-Package /PackagePath:C:\Update\Update.cab
```

You can use the `/Add-Driver` option to add third-party driver packages that include a valid INF file. For example, to add *mydriver* to the Windows image, execute the following command:

```
Dism /image:C:\offline /Add-Driver /driver:C:\Drivers\mydriver.INF
```

If you point to a path and use `/Recurse`, all subfolders will be checked for valid drivers. For example, to add drivers from the *C:\Drivers* folder, execute the following command:

```
Dism /image:C:\offline /Add-Driver /driver:C:\drivers /recurse
```

To remove a third-party device driver, use the `/Remove-Driver` option to specify the name of a device driver (such as *oem0.inf*, *oem1.inf*, and so on). For example, to remove the second third-party driver (*oem1.inf*) that has been added to the system, execute the following command:

```
Dism /image:C:\offline /Remove-Driver /driver:oem1.inf
```

Installing Features for Offline Images

Features are a set of Windows programs that can be enabled or disabled by an administrator and are included with Windows. Examples of features include FreeCell, Hearts, Solitaire, FTP Server, World Wide Web Service, and Microsoft .NET Framework 3.5. To add or remove features in Windows Server 2012 R2, you would use Server Manager. To add or remove features in Windows 8, you would use *Control Panel* > *Programs and Features*. Similarly, you can use Dism.exe to add to or remove features from of offline image.

Similar to adding or removing packages, you can use Dism.exe to mount an image offline and then use Dism.exe to add, remove, update, or list the Windows feature. For example, to list the features, execute the following command:

```
Dism /image:C:\offline /Get-Features
```

To enable a feature, use the `/Enable-Feature` option. For example, to install the Hearts game, execute the following command:

```
Dism /image:C:\offline /Enable-Feature /FeatureName:Hearts
```

To remove the Hearts game, use the `/Disable-Features` option. For example, to remove the Hearts game, execute the following command:

```
Dism /Image:C:\offline /Disable-Feature /FeatureName:Hearts
```

`Of course, after you add or remove features, remember to commit the changes with the Dism /Commit-Wim` command that was discussed previously.

Configuring Driver Groups and Packages

You can use Windows Deployment Services to add driver packages to the server, so that they can be deployed to client computers when you deploy an install image. In addition, you can deploy driver packages to the boot images without manually adding the packages to the images.

Starting with Windows Server 2008 R2, WDS includes ***dynamic driver provisioning***, which allows you to add driver packages to WDS and then deploy them when you deploy an image. Using dynamic driver provisioning requires the following:

- The boot image from either Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 (from \Sources\Boot.wim on the DVD).
- The install images for Windows Vista SP1, Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012, or Windows 2012 R2.

To deploy drivers based on the plug-and-play hardware of the client, you must extract the drivers; they cannot be an .msi file or an .exe file.

A ***driver group*** is a collection of driver packages. You can then apply filters to a driver group to specify which group of client computers receives the packages. If there are no filters on a driver group, all clients that have the matching hardware will receive the package.

ADD DRIVERS TO AN IMAGE

GET READY. To add drivers to an image, perform the following steps:

1. Open Server Manager.
2. Click Tools > Windows Deployment Services. The *Windows Deployment Services* console opens.
3. Expand the server node.
4. Right-click the Drivers node and then choose Add Driver Package.
5. On the *Driver Package Location* page, select either the Select driver packages from an .inf file option or the Select all driver packages from a folder option. Specify the location of the .inf file or folder, and then click Next.
6. On the *Available Driver Packages* page, select the drivers that you want to include (see Figure 1-8), and then click Next.

Figure 1-8

Selecting driver packages

7. On the *Summary* page, click Next.
8. When the tasks are completed, click Next.
9. Select a current driver group or create a new driver group, and then click Next.
10. On the *Tasks Complete* page, click Finish.

Business Case Scenarios

Scenario 1-1: Deploying Servers Using WDS

Your organization decides to build a second data center to be used as a backup site. You need to deploy roughly 150 servers. What steps will you need to take to deploy 150 servers at the new data center?

Scenario 1-2: Adding a Service Pack to WDS Install Image

Several months ago, you deployed a WDS server to deploy computers running Windows 2012 R2. Service Pack 2 was just released and you need to add Service Pack 2 to your image so that future installations will automatically have the service pack. What steps will you need to take to make this happen?

Implementing Patch Management

LESSON 2

Deploying Windows Server Update Services (WSUS)

THE BOTTOM LINE

An organization that needs to update hundreds of computers can present a daunting challenge for administrators. First, hundreds of computers downloading updates can affect network performance. Second, because an update can cause unforeseen problems, it is better to have the patch or update tested before it is applied. Windows Server Update Services (WSUS) provides a solution to these problems.

Windows Server Update Services (WSUS) is a program that is included with today's Windows Servers that allows administrators to manage the distribution of updates and other patches to computers within an organization. In the simplest configuration, which is ideal for a single site with a few hundred computers, you have a single WSUS that downloads updates directly from Microsoft. Then the client computers get updates from the WSUS server. Figure 2-1 shows a simple WSUS configuration.

If you administer more than a few hundred computers or you administer multiple sites, you can create a hierarchy of WSUS servers (see Figure 2-2). The number of WSUS servers will be determined by the number of sites, the speed and load of the links between sites, and the number of clients that you must support.

Figure 2-1

A simple WSUS configuration

Figure 2-2

The WSUS hierarchy

WSUS can retrieve updates directly from Microsoft Update or from another WSUS server on your network. If you have two WSUS servers connected with a high-speed link, one server can get the updates from the Microsoft Update while the other gets from the first server. If you have multiple sites that are linked together through a VPN, you can place a WSUS server at each site and have each WSUS server get the updates from Microsoft Update.

You can configure WSUS in one of two modes:

- **Autonomous mode:** Offers distributed management
- **Replica mode:** Offers central management

Both modes have the upstream WSUS servers share updates with the downstream servers during synchronization. However, with ***autonomous mode***, approval of updates is done on each WSUS server. With ***replica mode***, you approve the updates on the upstream server and those approvals are replicated to the downstream servers.

Installing WSUS

WSUS has been part of the Windows Server operating systems for quite some time. To install WSUS on Windows Server 2012 R2, you must install WSUS as a role.

As with most network services, you should perform a little bit of planning before deploying WSUS. To implement WSUS on Windows Server 2012 or Windows Server 2012 R2, the minimum hardware and software requirements are as follows:

- **Processor:** 1.4 gigahertz (GHz) x64 (2 GHz or faster is recommended).
- **Memory:** WSUS requires an additional 1.5 GB of RAM, above and beyond what is required by Windows Server 2012 or Windows Server 2012 R2, not including the WSUS database requirements.
- **Available disk space:** 10 GB (40 GB or greater is recommended)
- **Network adapter:** 100 megabits per second (Mbps) or greater
- Microsoft .NET Framework 4.0 on the server where the WSUS server role is installed.
- SQL Server 2012, SQL Server 2008, or the Windows Internal Database (WID). The WID database has minimum RAM memory requirements of 2 GB, in addition to the standard Windows Server system requirements.
- To view WSUS reports, you will need Microsoft Report Viewer Redistributable 2008 or later.
- The NT Authority\Network Service account must have Full Control permissions for the following folders so that the WSUS Administration snap-in displays correctly:
  - %windir%\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files
  - %windir%\Temp
- The account used to install WSUS must be a member of the Local Administrators group.

A single WSUS server can support thousands of clients. A single WSUS server with 4 GB of RAM and dual quad-core processor can support up to 100,000 clients. However, most organizations of that size will have multiple WSUS servers to reduce the load on wide area network (WAN) links.

Lastly, the WSUS server or servers will need to communicate with Microsoft Update. Therefore, if you are having problems communicating with Microsoft Update, you might need to check the firewalls of an organization.

INSTALL WSUS

GET READY. To install WSUS, perform the following steps:

1. On the C drive, create an Updates folder.
2. Open Server Manager.
3. At the top of *Server Manager*, click Manage > Add Roles and Features. The *Add Roles and Feature Wizard* appears.
4. On the *Before you begin* page, click Next.
5. Select Role-based or feature-based installation and then click Next.
6. Click Select a server from the server pool, click the name of the server to install WSUS to, and then click Next.
7. Scroll down and select Windows Server Update Services.
8. When the *Add Roles and Features Wizard* opens, click Add Features.
9. Back on the *Select server roles* screen, click Next.
10. On the *Select features* page, click Next.
11. On the *Windows Server Update Services* page, click Next.
12. By default, the WID database and WSUS Services are selected.
13. Click Next.

MORE INFORMATION

WID is short for Windows Internal Database. If you want to use a dedicated SQL server, deselect WID Database and select Database.

14. On the *Current Location* selection, type C:\Updates (see Figure 2-3), and then click Next.

Figure 2-3

Specifying the content location

MORE INFORMATION

In a production environment, you should store the updates on a non-system drive.

15. On the *Web Server Role (IIS)* page, click Next.
16. On the *Select Role services* page, click Next.

17. On the *Confirm installation selections* page, click Install.
18. When the installation is done, click Close.

If you are upgrading any version of Windows Server that supports WSUS 3.2 to Windows Server 2012 or Windows Server 2012 R2, you must first uninstall 3.2. If you are upgrading from Windows Server with WSUS 3.2 to Windows Server 2012, the installation process will be blocked and you will be prompted to uninstall WSUS prior to upgrading Windows Server 2012. However, if you are upgrading from any version of Windows Server with WSUS 3.2 to Windows Server 2012 R2, the installation is not blocked and the post installation tasks for WSUS in Windows Server 2012 R2 will fail. When this happens, reinstall Windows Server 2012 R2, which includes reformatting the drive.

Configuring WSUS

After WSUS is installed, you need to configure it before you can use it. First, the WSUS server needs to be configured to download updates from the Microsoft Update site, download the updates, and configure groups based on how you want to deploy the updates to the computers within your organization.

After you install WSUS, you need to perform the following actions:

- You need to configure how the WSUS server will download updates, what updates will be downloaded, and if the downloads will occur automatically or manually. You also must determine what updates need to be downloaded.
- You then need to organize the client computers into computers groups in a way that you deploy the updates into phases, starting with a test group and eventually deploying the updates to all of the computers.
- You need to configure the clients to use the WSUS using Group Policy.
- You need to approve the updates for deployment.
- You need to review the update status of the computers and generate reports as necessary.

The primary tool to manage WSUS is the Update Services console.

INITIAL CONFIGURATION OF WSUS USING THE UPDATE SERVICES CONSOLE

GET READY. To initially configure WSUS using the Update Services console, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. When the *Complete WSUS Installation* dialog box opens, click Run.
4. When the post-installation successfully is completed, click Close.
5. When the *Before You Begin* page opens, click Next.
6. On the *Join the Microsoft Update Improvement Program* page, click Next.
7. The *Choose Upstream Server* page appears. If you want to synchronize with another WSUS server, select the Synchronize from another Windows Server Update Services server option. Then specify the name of the server and the port (the default port is 8530). To synchronize the updates from Microsoft Update, leave the Synchronize from Microsoft Update option selected, and then click Next.
8. The *Specify Proxy Server* page appears. If your organization is using a proxy server to access the Internet, select the Use a proxy server when synchronizing option. Then

specify the Proxy server name, Port number, and the various credentials necessary to accessing the proxy server. Click Next.

9. On the *Connect to Upstream Server* page, click Start Connecting. This might take some time to complete.
10. When the connection is complete, click Next.
11. On the *Choose Languages* page, select the languages that you need to support, and then click Next.
12. On the *Choose Products* page, select the products that you want to download the updates for, and then click Next.
13. On the *Choose Classifications* page, select the classifications that you want to download and then click Next.
14. On the *Set Sync Schedule* page, select either Synchronize manually or Synchronize automatically. If you choose to synchronize automatically, you must specify when the first synchronization occurs and how often to synchronize. Click Next.
15. On the *Finish* page, select Begin initial synchronization and then click Next.
16. On the *What's Next* page, click Finish.

After you run the initial configuration, you can configure the most important options by selecting the Options node in the Update Services console. These options include the following:

- **Update Source and Proxy Server:** Allows you to choose if the WSUS server gets updates from Microsoft Update or another WSUS Server. It also allows you to specify proxy settings if necessary.
- **Products and Classifications:** Allows you to specify which products you want to download updates for and what type of updates you want to download.
- **Update Files and Languages:** Allows you to specify where updates are stored and which languages to download for.
- **Automatic Approvals:** Specifies how to automatically approve installation of updates for selected groups and how to approve revisions to existing updates.
- **Synchronization Schedule:** Allows you to specify to synchronize updates manually or to set a schedule.
- **Computers:** Specifies how to assign computers to groups, which will be used in rolling out the updates.
- **Server Cleanup Wizard:** Used to remove old computers, updates, and update files from the server.
- **Reporting Rollup:** Allows you to specify how information is replicated to downstream servers.
- **E-Mail Notifications:** Allows you to configure e-mail notifications of new updates and of status reports.
- **Microsoft Update Improvement Program:** Specifies if you want to send information to Microsoft so that Microsoft can improve the quality of Microsoft products.
- **Personalization:** Allows you to specify how and what information is displayed in WSUS.
- **WSUS Server Configuration Wizard:** Allows you to run the same Wizard used during the initial configuration.

CONFIGURING WSUS SYNCHRONIZATION

To perform synchronization from Windows Update site or another WSUS server, you will need to perform the following:

- Configure the update source and proxy server.
- Specify what products and type of updates you want to download.

- Specify where to store the files.
- Specify what languages you want to support.
- Specify a synchronization schedule.

CONFIGURE THE UPDATE SOURCE AND PROXY SERVER

GET READY. To configure the update source and proxy server, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. In the left pane, expand the nodes under the server and then click Options.
4. In the *Options* pane, click Update Source and Proxy Server. The *Update Source and Proxy Server* dialog box appears (see Figure 2-4).

Figure 2-4

Configuring the Update Source settings

5. On the *Update Source* tab, the *Synchronize from Microsoft Update* option is selected by default. If you need to synchronize with another WSUS server, select the Synchronize from another Windows Server Update Services server option. Then specify the Server name and Port number (the default port is *8530*).
6. If the upstream WSUS server requires SSL, select the Use SSL when synchronizing update information option.
7. If you want to replicate update approvals, settings, computers, and groups from the upstream server, select This server is a replica of the upstream server.
8. If your server requires a proxy server to download from Microsoft Update, click the Proxy Server tab.
9. Select the Use a Proxy server when synchronizing option, and then type the Server name of the proxy server and the Port number.

10. If the proxy server requires a user name and password, select the Use user credentials to connect to the proxy server option, and then type the user name, domain, and password. If necessary, select Allow basic authentication (password is sent in cleartext).
11. Click OK to apply your settings and to close the *Update Source and Proxy Server* dialog box.

SPECIFY WHAT WSUS WILL SYNCHRONIZE

GET READY. To specify what WSUS will synchronize, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. In the left pane, expand the nodes under the server, and then click Options.
4. In the *Options* pane, click Products and Classifications. The *Products and Classifications* dialog box appears.
5. On the *Products* tab, select any of the products that you want to synchronize and deselect any products that you do not want to synchronize.
6. Click the Classifications tab.
7. Select the updates that you want to synchronize and deselect the type of updates that do not want to synchronize.
8. Click OK to apply your settings and to close the *Products and Classifications* dialog box.
9. Click Update Files and Languages. The *Update Files and Languages* dialog box opens.
10. By default, the updates are stored on the local server and the files are only downloaded when approved. If you want the files to download regardless of whether they are approved or not, deselect the Download update files to this server only when updates are approved.
11. If you want to download express installation files, select Download express installation files.
12. If you have an upstream WSUS server and you want to download directly from the Microsoft update server instead, select Download files from Microsoft Update; do not download from upstream server. (This option is grayed out unless you have an upstream server.)
13. If you do not want to store the files locally and download the files from Microsoft Updates as needed, select Do not store update files locally; computers install from Microsoft Update.
14. To select or deselect languages, click the Update Languages tab.
15. Select the languages that you want to download and deselect the languages that you don't want to download.
16. Click OK to apply your settings and to close the *Products and Classifications* dialog box.

You can manually synchronize the updates or you can schedule the updates. To manually synchronize, open the Update Services console and expand the nodes under the server in the left pane, click Synchronization > Synchronize Now (see Figure 2-5). To view if a synchronization succeeded or failed, view the center pane.

Figure 2-5

Performing a synchronization

SPECIFY A SYNCHRONIZATION SCHEDULE

GET READY. To specify when WSUS will synchronize, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. In the left pane, expand the nodes under the server and click Options.
4. Click Synchronization Schedule. The *Synchronization Schedule* dialog box opens.
5. To automatically synchronize updates, select the Synchronize automatically option. Then select the time when you want the first synchronization to occur and how many times per day.
6. Click OK to apply your settings and to close the *Synchronization Schedule* dialog box.

CONFIGURING WSUS COMPUTER GROUPS

To specify what updates go to which computers at what time, organize your computers into ***computer groups***. By default, each computer is always assigned to the All Computers group. As new computers are added, they will be assigned to the Unassigned Computers group until you assign them to another group. Other than the computers that are members of the All Computers group, a computer can only be assigned to one other group.

When planning the computer groups, you should create several groups so that you can use a layered approach when pushing the updates. A layered approach allows you to push updates to a test group. You can then roll out the updates to other groups as needed.

CREATE A COMPUTER GROUP

GET READY. To create computer group, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. In the left pane, expand Computers so that you can see *All Computers* (see Figure 2-6).

Figure 2-6

Viewing Computers node

4. Right-click All Computers and choose Add Computer Group. The *Add Computer Group* dialog box opens.
5. In the *Name* text box, type the name of the computer name group.
6. Click Add to apply your settings and to close the Add Computer Group dialog box.

To assign computers to groups, use:

- ***Server-side targeting***, whereby you manually assign the computer to a group.
- ***Client-side targeting***, whereby the computers are automatically assigned to a computer group by using Group Policy or whereby someone manually modifies the registry.

With server-side targeting, you manually move the selected computer task on the Computers page to move to another computer group. With client-side targeting, you use Group Policy or you edit the registry settings on client computers to enable those computers to automatically add themselves into the computer groups. You must specify which method you will use by selecting one of the two options on the Computers Options page.

SPECIFY THE METHOD OF ASSIGN COMPUTERS TO GROUPS

GET READY. To specify the method on how computers are assigned to a group, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.

3. In the left pane, expand the nodes under the server, and then click Options.
4. In the main pane, click Computers. The *Computers* dialog box opens.
5. To perform server-side targeting, select Use the Update Services console.
6. To perform client-side targeting, select Use Group Policy or registry settings on computers.
7. Click OK to apply your settings and to close the *Computers* dialog box.

MOVE A COMPUTER TO A DIFFERENT GROUP BY USING SERVER-SIDE TARGETING

GET READY. To move a computer to a different group by using Server-Side Targeting, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. In the left pane, expand the nodes under the server. Expand the Computers node, and then click All Computers.
4. In the *All Computers* pane in the middle of the screen, right-click the computer you want to move, and then choose Change Membership.
5. When the *Set Computer Group Membership* dialog box opens, select the computer group you want to move the computer to, and then click OK.
6. Click OK to apply your settings and to close the *Computers* dialog box.

CONFIGURING GROUP POLICIES FOR UPDATES

By default, Windows computers will get their updates from Windows Update. You can use Group Policy to have the domain computers use the specified WSUS server.

CONFIGURE A COMPUTER TO USE WSUS FOR UPDATES USING GROUP POLICY

GET READY. To configure a computer to use WSUS for updates using Group Policy, perform the following steps on a domain controller or any computer that has Group Policy Management console:

1. Open Server Manager.
2. Click Tools > Group Policy Management.
3. Using the Group Management console, open Group Policy Management Editor for a group policy.
4. In *Group Policy Management Editor*, expand Computer Configuration, expand Policies, expand Administrative Templates, expand Windows Components, and then click Windows Update.
5. In the details pane, double-click Specify Intranet Microsoft update service location. The *Specify intranet Microsoft update service location* page appears (see Figure 2-7).

Figure 2-7

Specifying the intranet Microsoft update service location using Group Policy

6. Select Enabled.
7. In the *Set the intranet update service for detecting updates* text box and in the *Set the intranet statistics server* text box, type the HTTP or the HTTPS URL of the WSUS server. The default URLs are http://<name of WSUS server>:8530 and https://<name of WSUS server>:8531.
8. Click OK to apply your settings and to close the *Specify intranet Microsoft update service location* page.

CONFIGURING CLIENT-SIDE TARGETING

If you have several computers, client-side targeting is an excellent option that automates the process of assigning computers to computer groups. For domain computers, you should use Group Policy.

ENABLE CLIENT-SIDE TARGETING USING GROUP POLICY

GET READY. To enable client-side targeting using Group Policy, perform the following steps on a domain controller or any computer that has Group Policy Management console:

1. Open Server Manager.
2. Click Tools > Group Policy Management.
3. Using the *Group Management* console, open Group Policy Management Editor for a group policy.

4. In *Group Policy Management Editor*, expand Computer Configuration, expand Policies, expand Administrative Templates, expand Windows Components, and then click Windows Update.
5. In the details pane, double-click Enable client-side installations. The *Enable client-side targeting* page appears (see Figure 2-8).

Figure 2-8

Enabling client-side targeting using Group Policy

6. Select Enabled and in the *Target group name for this computer* box, type the name of the computer group name.
7. Click OK to apply your settings and to close the *Reschedule Automatic Updates scheduled installations* page.

For computers that are not part of the domain, you will have to modify the registry if you want to enable client-side targeting. The registry entries for the WSUS environment options are located in the following subkey:

`HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate`

To enable client-side targeting, change the `TargetGroupEnabled (Reg_DWord)` value to a 1 and use the `TargetGroup (Reg_SZ)` value to specify the group that you want the computer to be a member of (see Figure 2-9). You also need the following subkey:

`HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU`

The `AU` key needs to have a `UseWUServer` value (`Reg_DWord`) set to `1`.

Figure 2-9

Modifying Windows Update Registry settings

Approving Updates

One of the advantages of using WSUS is that you control which updates clients receive and when clients receive those updates. This gives you an opportunity to test the updates and then roll them out to the computer groups.

Although you can have updates automatically approve every update that is downloaded from Windows Update, you shouldn't do that until you've had an opportunity to test the updates. Updates are thoroughly tested by Microsoft, but every organization is different; a single update might cause unforeseen problems affecting hundreds of computers.

You can specify a deadline when you approve an update or set of updates on the WSUS server. Setting a deadline causes clients to install the update at a specific time. If the client contacts the server after the update deadline has passed, it tries to install the update as soon as possible. If you wish computers to install an update immediately, you can specify a deadline in the past. If an update has a deadline and requires a restart and the computer has not been restarted, the system reboots at the time of the deadline.

APPROVE UPDATES

GET READY. To approve updates in WSUS, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Tools > Windows Server Update Services.
3. Expand the server and then expand Updates. Select one of the following options:
   - All Updates: Displays all updates.
   - Critical Updates: Displays only critical updates, which are high-priority updates and are not security related.
   - Security Updates: Displays only updates that fix known security problems.
   - WSUS Updates: Displays updates related to the update process.
4. On the top of the screen, on the *Approval* drop-down, make sure Unapproved is selected.
5. On the top of the screen, on the *Status* drop-down menu, make sure Any is selected.
6. Click Refresh to display the updates.
7. To sort the updates so that the newest updates appear first, right-click any of the column headings and then select the Release Date option (see Figure 2-10). Then click the Release Date column header to sort by that date.

Figure 2-10

Choosing the Release Date option

8. Select the updates that you want to approve. You can select multiple updates by pressing and holding the Ctrl key. When you're finished selecting your updates, release the Ctrl key.
9. Right-click the selected update and choose Approve. Alternatively, select Decline if you want to prevent an update from being distributed.
10. If the Approve Updates dialog box appears, select the computer group you want to apply the updates to and then choose Approved For Install.
11. To force an update to be installed where a user cannot delay the installation, right-click the computer group, choose Deadline, and then select a deadline (see Figure 2-11).

Figure 2-11

Selecting a deadline

12. Click OK.
13. If a license agreement appears, prompting you for an update, click I Accept.
14. Click Close.

Managing Patch Management in Mixed Environments

Most organizations will be running several vtersions of Windows and several versions of other Microsoft products (such as Microsoft Office). WSUS allows you to manage the updates for the various versions of Windows and other Microsoft products.

A single WSUS server can manage updates for thousands of computers, even if the computers have a mix of Windows operating systems. For example, you can use WSUS to install updates for Windows XP, Windows Vista, Windows 8 (including Windows 8.1), Windows Server 2003, Windows Server 2003R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. When you first install WSUS, WSUS will not include the newer operating systems (such as Windows 8, Windows Server 2012, and Windows Server 2012 R2). However, when WSUS first synchronizes with Microsoft or another WSUS server, it will add support for newer operating systems and for other Microsoft products.
If you have a mix of Windows updates, you don't have to put the computers into computer groups based on operating system. Instead, you can deploy the updates as you deploy any other updates. If the update does not apply to the system because the update was specified for one version of Windows yet the system has another version, the patch will not be deployed to the system and the WSUS console will show that the patch was not needed.

The WSUS console is installed on the servers that are running WSUS. If you have a computer running Windows 8.1, you can install the Remote Server Administration Tools for Windows 8.1, which includes Server Manager, Windows PowerShell modules, and other management tools (including the WSUS console) for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

Business Case Scenarios

Scenario 2-1: Updating Computers

You were just hired by the Contoso Company, which has more than 1,000 client computers at two office buildings located at two sites. You have determined that computers have not been patched in 18 months. What solution would you recommend, and how would you implement this solution?

Scenario 2-2: Creating Computer Groups in WSUS

You have the following departments within your organization:

Sales	150 computers
Marketing	75 computers
Management	50 computers
Manufacturing	200 computers
Information Technology	50 computers

How many groups should you create in WSUS? Why?

3 LESSON

Monitoring Servers

Introducing the Microsoft Management Console (MMC)

THE BOTTOM LINE

The ***Microsoft Management Console (MMC)*** is one of the primary administrative tools used to manage Windows and many of the network services provided by Windows. It provides a standard method to create, save, and open the various administrative tools provided by Windows. When you open Administrative Tools, most of these programs are MMC.

To start an empty MMC, go to the command prompt (or the Run box), type *mmc* or *mmc.exe*. To open the command prompt or the Run box in Windows Server 2012 R2, right-click the Start button and choose *Run* or choose *Command Prompt (Admin)*.

Every MMC has a console tree that displays the hierarchical organization of snap-ins (or pluggable modules) and extensions (a snap-in that requires a parent snap-in). By adding and deleting snap-ins and extensions, users can customize the console or access tools that are not located in Administrative Tools. You can add snap-ins to a MMC by clicking File > Add/Remove Snap-ins. Figure 3-1 shows the Add or Remove Snap-ins dialog box.

Figure 3-1

Adding snap-ins

Administrative Tools is a folder in the Control Panel that contains tools for system administrators and advanced users. To access Administrative Tools, open the Control Panel. If you are in Category view, click System and Security > Administrative Tools. If you are in Icon view, double-click Administrative Tools. The Administrative Tools are also available in the tools menu of Server Manager.

After you install server roles, additional administrative tools will be loaded. You might assume these tools are used only to manage the local computer. However, many of them can be used to manage remote computers as well. For example, you can use the Computer Management tool or the Server Management console to connect to and manage other computers, assuming you have administrative rights to the computer.

Using Server Manager

Server Manager is a management console that helps you manage local and remote Windows-based servers. By managing servers as groups, you can perform the same administrative tasks quickly across multiple servers that have the same role or members of the same group.

You can use Server Manager to perform the following tasks on both local and remove servers:

- Add roles and features.
- Launch Windows PowerShell sessions.
- View events.
- Perform server configuration tasks.
- Add remote servers to a pool of servers that Server Manager can be used to manage.
- Install or uninstall roles, role services, and features on the local server or on remote servers that are running Windows Server 2012 R2 or previous versions of Windows servers.
- View and make changes to server roles and features that are installed on local or remote servers.
- Perform management tasks (such as starting or stopping services or configuring network settings, users and groups, and Remote Desktop connections).
- Scanning roles for compliance with best practices.
- Running role-management tools.
- Determine server status, identify critical events, and analyze and troubleshoot configuration issues or failures.
- Restart servers.

Using Computer Management

The ***Computer Management*** console is one of the primary tools used to manage Windows computers and servers. It includes the most commonly used MMC snap-ins.

The Computer Management console (see Figure 3-2) includes multiple snap-ins, including Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, Device Management, Routing and Remote Access, Services, and WMI Control.

Figure 3-2

Viewing the Computer Management console

Using Event Viewer

THE BOTTOM LINE

One of the most useful troubleshooting tools is the Event Viewer, which is essentially a log viewer. Whenever you have problems, you should look in the Event Viewer to see any errors or warnings that might reveal what the problem is.

The ***Event Viewer*** is an MMC snap-in that enables you to browse and manage event logs. It is included in the Computer Management and is included in Administrative Tools as a stand-alone console. You can also execute the `eventvwr.msc` command.

Event Viewer enables you to perform the following tasks:

- View events from multiple event logs (see Figure 3-3).
- Save useful event filters as custom views that can be reused.
- Schedule a task to run in response to an event.
- Create and manage event subscriptions.

Figure 3-3

Event Viewer

Understanding Logs and Events

To get the best use of Windows logs, you need to understand how the logs are organized and how the events are categorized.

When you examine the Event Viewer more closely, you will see the following items:

- **Custom Views:** Allows you to create custom views of events. By default, it includes Administrative Events, which collects Critical, Error, and Warnings from all logs on the server. However, you can create your own customer view by right-clicking Custom Views and selecting Create Custom View.
- **Windows Logs:** Includes logs that were available in previous versions of Windows. They include:
  - **Application:** Contains events logged by applications or programs.
  - **Security:** Contains events such as valid and invalid logon attempts and access to designated objects such as files and folders, printers, and Active Directory objects. By default, the Security log is empty until you enable auditing.

- **Setup:** Contains events related to application setup.
- **System:** Contains events logged by Windows system components, including errors displayed by Windows during boot and errors with services.
- **Forwarded Events:** Stores events collected from remote computers. To collect events from remote computers, you must create an event subscription. It should be noted that Forwarded Events does not work with pre-Windows 7 and Windows Server 2008 operating systems.

- **Applications and Services Logs:** Displays a set of events related to an application or service. Some examples include DHCP, DNS, and Active Directory.

When you open an event (see Figure 3-4), you will see the Log Name, Source, Event ID, Level, User (if applicable), Logged details (date and time), Computer, and other information.

Figure 3-4

Viewing an event

Filtering Events

When looking at the logs shown by Event Viewer, you can be overwhelmed by the number of events. Therefore, you need to know how to filter events so that you can focus on what you want to focus on.

When you open any of these logs, particularly the Application, Security, or System logs, they might display thousands of entries. Unfortunately, this means that it might take some time to find what you are looking for.

To begin with, you can sort the Event Viewer by clicking the column header. For example, by clicking the *Date and Time* column header, you can sort the events by date and time. This comes in handy when you know that a problem started at a certain time and you want to view the events that were generated at that time.

To reduce the number of items that are displayed, you can use a filter to reduce the number of entries shown. To filter a log, click *Action* > *Filter Current Log*. When the Filter Current Log appears (see Figure 3-5), you can select when the event was logged, the *Event level*, *Task category*, *Keywords*, *User*, and *Computer(s)*.

Figure 3-5

Filtering an event log

Configuring Event Subscriptions

Originally, the Event Viewer allowed you to view events on a single computer. However, troubleshooting an issue might require you to examine a set of events stored in multiple logs on multiple computers. Therefore, Microsoft enhanced Event Viewer to capture events from multiple computers so that you can view the events using one console.

Today's Event Viewer can be used to collect copies of events from multiple remote computers and store them locally. To specify which events to collect, you create an ***event subscription***. Among other details, the subscription specifies exactly which events will be collected and in which log they will be stored locally. Once a subscription is active and events are being collected, you can view and manipulate these forwarded events as you would any other locally stored events. Events are forwarded using Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS).

To configure event subscriptions, perform the following steps:

1. Configure the forwarding computer.
2. Configure the Collecting Computer.
3. Create an Event Subscription.

CONFIGURE THE FORWARDING COMPUTER

GET READY. To configure a forwarding computer to forward events, perform the following steps:

1. Right-click Start and choose Command Prompt (Admin).
2. At the command prompt, execute the following command:

```
Winrm quickconfig
```

3. To add the collecting computer name to the Administrators group, execute the following command:

```
Net localgroup "Administrators"
<collecting_computer_name>$@<domain_name> /add
```

4. If a message appears, indicating that changes must be made, type ***Y*** and then press ***Enter***.
5. Close the *Command Prompt* window.

Executing the `winrm quickconfig` command on the forwarding computer accomplishes the following:

- It sets the Windows Remote Management (WS-Management) service to Automatic (Delayed Start) and starts the service.
- It configures the Windows Remote Management HTTP listener.
- It creates a Windows Firewall exception.

CONFIGURE THE COLLECTING COMPUTER

GET READY. To configure a collecting computer to forward events, perform the following steps:

1. Right-click Start and choose Command Prompt (Admin).
2. At the command prompt, execute the following command:

```
Wecutil qc
```

3. Close the *Command Prompt* window.

By executing the `wecutil qc` command, you configure the receiving computer to receive events. The last step is to then specify the events you want to send to the receiving computer.

CREATE AN EVENT SUBSCRIPTION

GET READY. To create an event subscription on the collecting computer, perform the following steps:

1. Open Server Manager.
2. Click Tools > Event Viewer.
3. Right-click Subscriptions and choose Create Subscription. The Subscription Properties dialog box opens.
4. In the *Subscription name* text box, type the name for the subscription (see Figure 3-6).

Figure 3-6

Configuring subscription properties

5. If necessary, in the *Description* text box, type a description.
6. In the *Subscription type and source computers* section, choose one of the following two options:
   - Collector initiated: The collecting computer polls the source computers to retrieve events. Then click the Select Computers button to select which computers to poll.
   - Source computer initiated: The forwarding computer contacts the collection computer. Then click the Select Computer Groups button to specify the forwarding computers.
7. Click Select Events. The *Query Filter* dialog box opens.
8. Specify the time range (by using the *Logged* drop-down box), event level (by selecting the appropriate check box), event logs (by using the *Event Logs* drop-down box), event sources (by using the *Event sources* drop-down box), keywords (by typing in the *Keywords* text box), or other parameters that specify which events you want forwarding.
9. Click OK to apply your settings and close the *Query Filter* dialog box.
10. Optionally, you can click the Advanced button to open the Advanced Subscription Settings dialog box and then configure the bandwidth used (Normal, Minimize Bandwidth, and Minimize Latency) and the protocol (HTTP or HTTPS). Click OK to close the Advanced Subscription Settings dialog box.
11. Close the *Event Viewer*.

Managing Performance

THE BOTTOM LINE

Performance is the overall effectiveness of how data moves through the system. Of course, it is important to select the proper hardware (processor, memory, disk system, and network) to satisfy the expected performance goals. Without the proper hardware, bottlenecks limit the effectiveness of software.

When a component limits overall performance, that component is known as a bottleneck. When you relieve one bottleneck, another bottleneck might be triggered. For example, one of the most common bottlenecks is the amount of memory the system has. By increasing the memory, you can often increase the overall performance of a system (up to a point). However, when you add more RAM, then RAM needs to be fed more data from the disk. Therefore, the disk becomes the bottleneck. So, although the system might become faster, if your performance is still lacking, you will have to look for new bottlenecks.

You usually cannot identify performance problems just by taking a quick look at performance. Instead, you need a baseline. You can get one by analyzing the performance when the system is running normally and within design specifications. Then when a problem occurs, compare the current performance to your baseline to see what is different. Because performance can also change gradually over time, it is highly recommended that you baseline your computer regularly so that you can chart your performance measures and identify trends. This will give you an idea about when the server needs to be upgraded or replaced or the workload of the server reduced.

There are several tools available with Windows for you to analyze performance. They include:

- Task Manager
- Performance Monitor
- Resource Monitor

Using Task Manager

Task Manager gives you a quick glance at performance and provides information about programs and processes running on your computer. A ***process*** is an instance of a program that is being executed.

Task Manager is one of the handiest programs you can use to take a quick glance at performance to see which programs are using the most system resources on your computer. You can see the status of running programs and programs that have stopped responding, and you can stop a program running in memory.

To start Task Manager, right-click the empty space on the taskbar and click *Task Manager* (or you can open the Security menu by pressing the *Ctrl+Alt+Del* keys and choosing *Start Task Manager*). When Task Manager starts, it displays only the running applications.

Click the *More Details* down-arrow to show all the available tabs. When you first start the Task Manager on a computer running Windows Server 2012 R2, five tabs are opened for Task Manager:

- Processes
- Performance
- Users
- Details
- Services

The Processes tab shows all processes running in memory and how much processing and memory each process uses. The processes will display applications (as designated by apps), background processes, and Windows Processes. On the Processes tab, you can perform the following tasks:

- To see the processes that use the most CPU utilization and memory, click the *CPU* column header.
- To stop a process, right-click the process and select *End task*.
- To jump to the *Details* tab for a particular process, right-click the process and choose *Go to details*.
- If you want to see the executable that is running the processes, right-click the process and choose *Open file location*.

The *Performance* tab displays the amount of *CPU* usage (see Figure 3-7), physical *Memory* usage, and *Ethernet* throughput. For CPU usage, a high percentage indicates the programs or processes are requiring a lot of CPU resources, which can slow your computer. If the percentage seems frozen at or near 100%, then a program might not be responding.

Figure 3-7

Viewing CPU usage

Click *Memory* (see Figure 3-8) to display how much of the paging file is being used (*In use* and *Available*), the amount of *Committed* and *Cached* memory, *Paged pool* and *Non-paged pool*. It also shows you the total amount of RAM, the *Speed* of the RAM, and the number of *Slots used* for memory on the motherboard.

Figure 3-8

Viewing Memory usage

The *Users* tab displays the users who are currently logged in, the amount of CPU and memory usage that the each user is using, and the processes the user is running. It also gives you the ability to disconnect them.

The *Details* tab displays a more detailed look at the processes running on the computer, including the *Process Identification (PID)*. The PID is composed of unique numbers that identify a process while it is running. Similarly, you can stop the process and you can increase or decrease the process priority (see Figure 3-9).

Figure 3-9

Setting a priority level

If you are an advanced user, you might want to view other advanced memory values on the Processes tab. To do so, click View > Select Columns and then select or deselect values to be displayed or not displayed.

The Services tab displays all services on the computer that are running and not running. Similar to the Services console, you can start, stop, or restart services.

Using Resource Monitor

Resource Monitor is a system tool that allows you to view information about the use of hardware (CPU, memory, disk, and network) and software resources (file handlers and modules) in real time. You can filter the results according to specific processes or services that you want to monitor. In addition, you can use Resource Monitor to start, stop, suspend, and resume processes and services, and to troubleshoot when an application does not respond as expected.

Resource Monitor (see Figure 3-10) is a powerful tool for understanding how your system resources are used by processes and services. In addition to monitoring resource usage in real time, Resource Monitor can help you analyze unresponsive processes, identify which applications are using files, and control processes and services. To start Resource Monitor, start Server Manager and click *Tools* > *Resource Monitor*. Or, you can use Windows PowerShell and execute the `resmon.exe` command.

Figure 3-10

Viewing Resource Monitor

Resource Monitor includes five tabs:

- Overview
- CPU
- Memory
- Disk
- Network

The *Overview* tab displays basic system resource usage information; the other tabs display information about each specific resource. Each tab in Resource Monitor includes multiple tables that display detailed information about the resource featured on that respective tab.

The next four exercises cover common tasks for which to use the resource monitor. For example, if you want to find and determine the program (process) that is hogging the processor resources, you can use *Identify the highest current CPU usage*. If a file is locked and you cannot delete it because it is in use, you can use the *Identify the process that is using a file exercise* to see which process has the file open.

IDENTIFY THE HIGHEST CURRENT CPU USAGE

GET READY. To identify a process that is using the highest current CPU usage, perform the following steps:

1. Open Server Manager.
2. Click Tools > Resource Monitor.
3. Click the CPU tab.
4. In the *Processes* section, click CPU to sort processes by current CPU resource consumption.

VIEW THE CPU USAGE OF A PROCESS

GET READY. To view the CPU usage for each process, perform the following steps:

1. Open Server Manager.
2. Click Tools > Resource Monitor.
3. Click the CPU tab.
4. In the *Processes* section, in the *Image* column, select the check box next to the name of the service for which you want to see usage details. You can select multiple services. Selected services are moved to the top of the column.
5. Click the title bar of Services to expand the table. Review the data in Services to see the list of processes hosted by the selected services and to view their CPU usage.

IDENTIFY THE PROCESS THAT IS USING A FILE

GET READY. To identify the process that is using a file, perform the following steps:

1. Open Server Manager.
2. Click Tools > Resource Monitor.
3. Click the CPU tab and then click the title bar of Associated Handlers to expand the table.
4. Click in the Search Handlers box, type the name of the file you want to search for, and then click Search.

IDENTIFY THE NETWORK ADDRESS TO WHICH A PROCESS IS CONNECTED

GET READY. To identify the network address that a process is connected to, perform the following steps:

1. Open Server Manager.
2. Click Tools > Resource Monitor.
3. Click the Network tab and then click the title bar of TCP Connections to expand the table.
4. Locate the process whose network connection you want to identify. If there are a large number of entries in the table, you can click Image to sort by executable filename.
5. Review the *Remote Address* column and the *Remote Port* column to see which network address and port the process is connected to.

Using Performance Monitor

Performance Monitor is an MMC snap-in that provides tools for analyzing system performance. It is included in the Computer Management and it can be opened as a stand-alone console from Administrative Tools. It can also be started by executing the `perfmon` command. From a single console, you can monitor application and hardware performance in real time, specify which data you want to collect in logs, define thresholds for alerts and automatic actions, generate reports, and view past performance data in a variety of ways.

Performance Monitor (see Figure 3-11) provides a visual display of built-in Windows performance counters, either in real time or as a way to review historical data.

Figure 3-11

Viewing Performance Monitor

You can add performance counters to Performance Monitor by right-clicking the main pane and choosing Add Counters. Another way to add performance counters is to create and use custom Data Collector Sets. (Data Collector Sets will be explained later in this lesson.) Figure 3-12 shows the Add Counters dialog box. You can create custom views that can be exported as Data Collector Sets for use with performance and logging features.

Figure 3-12

Adding counters to Performance Monitor

To control how and what is displayed, right-click Performance Monitor and choose Properties. The Performance Monitor Properties dialog box displays the following five tabs:

- **General:** Allows you to adjust the samples, such as how often samples are taken and how much data is displayed on the graph before the graph is redrawn. You can also choose to display the legend, the value bar, and the toolbar.
- **Source:** Allows you to display real-time data or to open a log file that you have saved.
- **Data:** Allows you to choose counters to appear as well as the color and scale of those counters.
- **Graph:** Allows you to configure the available views and if the view starts over or you can scroll to look at previous displayed data. It allows you to display or not display the vertical grid, horizontal grid, vertical scale numbers, time axis labels, as well as determine the maximum scale.
- **Appearance:** Allows you to display the color and fonts used by various components so that you can distinguish one Performance Monitor window from another.

Performance Monitor has multiple graph types that enable you to visually review performance log data. They include:

- **Line:** The default graph type; connects points of data with lines.
- **Histogram Bar:** A bar graph showing data.
- **Report:** Values are displayed as text.

Performance programs and performance information is not available to everyone. Therefore, if a user needs to use Performance Monitor to view performance information, the user can be added to one of the following groups:

- Administrators can access all of the performance tools and data.
- Performance Monitor Users can view both real-time and historical data within the

Performance Monitor console and can use the CQQ. However, they cannot create or modify Data Collector Sets or use the Resource View.

- Performance Log Users group can view both real-time data and historical data within the Performance Monitor console. However, these users can create or modify Data Collector Sets if the user has *Log on as a batch user* rights on the server.

Configuring Data Collector Sets (DCS)

Rather than add individual performance counters each time you want to view the performance of a system, you can create ***Data Collector Sets (DCS)*** that allow you to organize a set of performance counts, event traces, and system configuration data into a single object that can be reused as needed.

Windows Performance Monitor uses performance counters, event trace data, and configuration information, which can be combined into Data Collector Sets as follows:

- Performance counters are measurements of system state or activity. They can be included in the operating system or can be part of individual applications. Windows Performance Monitor requests the current value of performance counters at specified time intervals.
- Event trace data is collected from trace providers, which are components of the operating system or of individual applications that report actions or events. Output from multiple trace providers can be combined into a trace session.
- Configuration information is collected from key values in the Windows registry.

Windows Performance Monitor can record the value of a registry key at a specified time or interval as part of a file.

CREATE A DATA COLLECTOR SET

GET READY. To create a DCS, perform the following steps:

1. Open Server Manager.
2. Click Tools > Performance Monitor.
3. In the left pane, expand Data Collector Sets.
4. Right-click the User Defined folder and choose New > Data Collector Set.
5. On the *Create new Data Collector Set* page, type a name in the Name text box. Ensure that the Create from a template (Recommended) option is selected and then click Next.
6. When you are prompted to choose a template, click System Performance, and then click Next.
7. When you are prompted to choose where you would like the data to be saved, click Next. If you run Performance Monitor to collect data over an extended period, you should change the location to a nonsystem data drive.
8. When you are prompted to create the data collector set, with the Save and close option selected, click Finish.
9. To start the Data Collector Set, right-click the DCS and choose Start.
10. Close *Performance Monitor*.

Configuring Performance Alerts

In Performance Monitor, a ***performance alert*** is a notification or task that is executed when a performance value is reached. Performance Monitor can also be used to start certain tasks when certain counters reach a particular value. For example, if the processor reaches 90%, you can have Performance Monitor run a command to stop a service or perform some other action in an effort to reduce burden on the processor.

When you configure performance alerts, you can perform almost any action that you can think. You can send a network message or log events into the application event log. You can configure alerts to start applications and performance logs.

CREATE A PERFORMANCE ALERT

GET READY. To create a performance alert, perform the following steps:

1. Open Server Manager.
2. Click Tools > Performance Monitor.
3. In the left pane, expand Data Collector Sets.
4. Right-click the User Defined folder, and then choose New > Data Collector Set.
5. On the *Create new Data Collector Set* page, when you are prompted to create a new data collector set, type a name in the Name text box.
6. Select Create manually (Advanced), and then click Next.
7. Select Performance Counter Alert, and then click Next.
8. When you are prompted to identify the performance counter you would like to monitor, click Add to open a dialog box, in which to select the desired counter. When you have added the counter, click OK.
9. The limit will define when a performance alert is triggered. For the *Alert when* option, select either Above or Below and then in the Limit box, type the value. Click Next.
10. When you are prompted to create the data collector set, select Open properties for this data collector set. Click Finish.
11. When the Properties dialog box opens, click the Task tab.
12. In the Run this scheduled task when the data collector set stops text box, type the path of a script or command that you want to execute when the condition is met. If necessary, specify any task arguments in the Task Arguments text box.
13. To specify when the Data Collector Set will run, click the Schedule tab.
14. Click Add. In the *Folder Action* dialog box, specify the Beginning date that the task will run, the Expiration date for the task, and the Launch time.
15. Click OK to apply your settings and then click OK again to close the *Properties* dialog box.
16. Close *Performance Monitor*.

Scheduling Performance Monitoring

Performance monitoring can be scheduled so that you can collect performance information when you are not actually at the computer.

To schedule performance monitoring, while you are running the Create New Data Collector Set Wizard, you can select the *Open properties for this data collect set* option at the end of the Wizard. After the DCS has been created, you can just right-click the Data Collector Set name in the Performance Monitor console, choose Properties, and then click the Schedule tab. In either case, you will click the Add button to specify when you want to schedule performance monitoring.

CREATE A DATA COLLECTOR SET (DCS)

GET READY. To create a DCS, perform the following steps:

1. Open Server Manager.
2. Click Tools > Performance Monitor.
3. In the left pane, expand Data Collector Sets.
4. Right-click the User Defined folder and choose New > Data Collector Set.
5. On the *Create new Data Collector Set* page, type a name in the *Name* text box. Ensure that the Create from a template (Recommended) option is selected and then click Next.
6. When you are prompted to choose a template, click System Performance and then click Next.
7. When you are prompted to choose where you would like the data to be saved, click Next.
8. When you are prompted to create the data collector set, select the Open properties for this data collector set option and then click Finish.
9. Click the Schedule tab.
10. Click the Add button.
11. In the *Folder Action* dialog box, specify the beginning date and the optional expiration date. Then specify the start time and select which days of the week the action will occur.
12. Click OK to close the *Folder Action* dialog box.
13. Click OK to close the *New Data Collector Set Properties* dialog box.

Monitoring the Network

THE BOTTOM LINE

Because a Windows server is made to provide services and to use services, it is essential that the server communicates over the network. Therefore, when the server is having network problems, you need to know what tools are available to troubleshoot those problems.

When looking at any problem, don't forget the basic commands that are available to any computer running Windows. Of course, when looking at any problem, you must be systematic so that you can quickly isolate the problem. The following steps are typical of troubleshooting networking issues:

1. Make sure you are connected. Check to make sure the network cable is properly connected or make sure that the wireless connection is on.

2. Make sure the network interface is enabled.
3. Check local IP configuration using `ipconfig`.
4. Use the `ping` command to determine what you can reach and what you cannot reach:
   Ping the loopback address (127.0.0.1).
   Ping a local IP address.
   Ping a remote gateway.
   Ping a remote computer.
5. Identify each hop (router) between two systems using the `tracert` command.
6. Verify DNS configuration using the `nslookup` command.

Using `ipconfig` with the `/all` switch will show you the IP configuration of the computer. If the subnet mask is incorrect, the computer will not be able to calculate the correct network ID, which might cause packets to be sent to the wrong destination. If the default gateway is incorrect or missing, the computer will not be able to communicate with remote subnets. If the DNS server is incorrect or missing, the computer might not be able to resolve names and communication might fail because it cannot determine the correct IP address.

If the computer is using DHCP to get the address and a DHCP server does not respond, the computer will use Automatic Private IP addressing, which generates an IP address in the form of 169.254.xxx.xxx and the subnet mask of 255.255.0.0. When you have an Automatic Private IP address, you can only communicate with computers on the same network/subnet that have an Automatic Private IP address. So as a result, you will not be able to communicate with other hosts.

The process of pinging a local computer should last only a couple hundred milliseconds (ms) at most. For WAN connections, a time of 200 milliseconds is considered very good and a time between 200 and 500 ms is marginal. Anything over 500 ms is unacceptable.

If a "Request Timed Out" message appears, the message indicates that there is a known route to the destination computer but one or more hosts or routers along the path, including the source and destination, are not configured correctly. If a "Destination Host Unreachable" message appears, the message indicates that the system cannot find a route to the destination system and therefore does not know where to send the packet on the next hop.

If you can successfully ping the IP address but not the name, name resolution is the problem. Therefore, you need to check if you are pointing to a valid DNS server and ensure that the DNS server can properly resolve the name you are trying to reach. In addition, if you are using a HOSTS file, you should make sure there is no corresponding entry that could cause the system from not resolving the name using DNS.

Besides the basic troubleshooting tools just discussed, don't forget to check the Event Viewer for potential events that could cause network problems. If you suspect that an individual computer is sending or receiving too much data, you can use the Event Viewer or Performance Monitor. Lastly, you should check any firewalls to ensure that no packets are being blocked by the Windows Firewall or any other firewall on the network.

Using the netstat Command

The ***`netstat`*** command is used to view the TCP/IP connections, both inbound and outbound, on your computer. You can also use to view the packet statistics, such as how many packets have been sent and received and the number of errors.

When `netstat` is used without any options, `netstat` shows all the outbound TCP/IP connections (see Figure 3-13). If you use `-n` addresses, the addresses are converted to names.

Figure 3-13

Using the netstat command

```
Administrator: Command Prompt

C:\Users\Administrator.WIN2012SRV.000>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.3.120:3389     PAT7A:57310            ESTABLISHED
  TCP    [::1]:389              WIN2012SRV:49159       ESTABLISHED
  TCP    [::1]:389              WIN2012SRV:49160       ESTABLISHED
  TCP    [::1]:389              WIN2012SRV:49164       ESTABLISHED
  TCP    [::1]:49159            WIN2012SRV:ldap        ESTABLISHED
  TCP    [::1]:49160            WIN2012SRV:ldap        ESTABLISHED
  TCP    [::1]:49164            WIN2012SRV:ldap        ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:389  WIN2012SRV:54884       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:389  WIN2012SRV:54887       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:445  WIN2012SRV:49173       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:3268  WIN2012SRV:50252       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:49155  WIN2012SRV:49172       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:49155  WIN2012SRV:51956       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:49155  WIN2012SRV:54770       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:49155  WIN2012SRV:56234       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:49172  WIN2012SRV:49155       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:49173  WIN2012SRV:microsoft-ds  ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:50252  WIN2012SRV:msft-gc     ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:50300  WIN2012SRV:8530        TIME_WAIT
  TCP    [fe80::e9dc:84f5:3789:857b%12]:50304  WIN2012SRV:49155       TIME_WAIT
  TCP    [fe80::e9dc:84f5:3789:857b%12]:51956  WIN2012SRV:49155       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:54770  WIN2012SRV:49155       ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:54884  WIN2012SRV:ldap        ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:54887  WIN2012SRV:ldap        ESTABLISHED
  TCP    [fe80::e9dc:84f5:3789:857b%12]:56234  WIN2012SRV:49155       ESTABLISHED

C:\Users\Administrator.WIN2012SRV.000>_
```

You can also use the following options with `netstat`:

- `netstat -a` displays all connections
- `netstat -r` displays the route table plus active connections
- `netstat -e` displays Ethernet statistics
- `netstat -s` displays per-protocol statistics

You might also place a number after the `netstat` to have `netstat` update the list every few seconds. For example, when you perform the following command:

```
netstat -e 15
```

the command executes, waits the number of seconds specified by the number (in this example, `15`), and then repeats until you press Ctrl+C.

Using Protocol Analyzers

For more complicated problems, you might need to dig deeper. One of the most powerful tools is a protocol analyzer/network analyzer, which allows you to view the actual packets on the network. Popular software protocol analyzers include WireShark, ***Microsoft Network Monitor*** and Microsoft Message Analyzer.

A protocol analyzer grabs every packet on a network interface, puts a timestamp on the packet, and stores the packets in a storage area. You would use a filter to specify the packets that will be displayed. Then open each packet to look at the various TCP/IP layers to see what is happening. The packets can be saved to a file so that they can be analyzed later.

When you first capture packets on an interface, you will soon see that there are hundreds of packets. Usually, most of these packets can be ignored because they will have nothing to do with the problem you are trying to analyze. In these cases, you will need to use a filter to show only the packets that you are concerned with.

To install Microsoft Network Monitor 3.4, you must first download Microsoft Message Analyzer from the Microsoft website. Then double-click the msi file and step through the Wizard.

CAPTURE PACKETS

GET READY. To capture packets, perform the following steps:

1. Double-click Microsoft Network Monitor 3.4. Microsoft Network Monitor opens (see Figure 3-14).

Figure 3-14

Using Microsoft Network Monitor

2. Click File > New > Capture. A new capture tab opens.
3. To select the interface, click Capture Settings. The *Capture Settings* dialog box opens. Select the interface that you want to capture packets from and make sure the other interfaces are deselected. Click Close.
4. To begin capturing packets, click Start.
5. When you are done capturing packets, click Stop.
6. If you want to save the captures, click the Save As button. Specify the location and the name the capture file and then click Save.
7. Close *Network Monitor*.

Network Monitor also has a command-line utility called NMCap.exe, which can be used in scripts and when you want to minimize the effect on system resources.

To learn about NMCap.exe, use one of the following commands:

- `nmcap /?` displays the options available with `nmcap`.
- `nmcap /example` displays several examples on how to use `nmcap`.

If you want to capture all traffic on all network adapters, execute the following command:

```
nmcap /network * /capture /file d:\test.cap
```

You can stop the capturing of packets using NMCap.exe by pressing Ctrl+C or Ctrl+Break on the keyboard. If you are scripting, use the */TimeAfter xx minutes* option to specify the number of minutes that NMCap.exe will run.

If you use a .cap filename extension, the default limit size of the capture file is 20 Megs. To change the default size, add a colon and the size after the file. For example, if you want the maximum size to be 50 MB, use the */File t.cap:50M* option. Alternatively, you can use .chn extensions to create a chain of files—for example, to create a chain of chain.chn files (chain(1).chn, chain(2).chn, chain(3).chn, chain(4).chn, and so on).

Most packets will be using the TCP/IP mode, which is a simplified OSI model that will have up to four parts:

- The Ethernet (data link layer) header includes the destination and source MAC addresses.
- The IP header (network layer) shows the packet as an IPv4 or IPv6 packet and the source and destination IP addresses.
- The TCP header or UDP header (transport layer) includes the source and destination ports.
- The Protocol payload, which is the actual data for the specified protocol.

Figure 3-15 shows the four parts of a packet in the *Frame Details* pane.

Figure 3-15

Viewing the frame details

Using filters, you can capture or display only those frames that meet the criteria you specify. You can filter on any protocol, protocol element, or property. For example, you can only capture frames that originate from a particular IP address.

Typically, when you are trying to figure out a problem and you choose to use a protocol analyzer, you should already know what you are looking for. For example, if you are trying to figure out why a client is not getting an IP address from a DHCP server, you want to look for the four-part handshake that occurs when a computer gets an IP address. Therefore, you will need to use a filter that shows only the DHCP packets.

There are several pre-made filters that can help you isolate common problems. To access them, click *Filter* > *Display Filter* > *Load Filter* > *Standard Filters*.

NMCap.exe also supports filtering. If you want to display remote desktop packets (TCP port 3389), execute the following command:

```
nmcap /network * /capture "tcp.port = = 3389"
/file d:\test.cap
```

If you want to show all packets except for the packets using TCP port 3389, execute the following command:

```
nmcap /network * /capture "!(tcp.port = = 3389)"
/file d:\test.cap
```

You can also use the same protocol names that are available in the graphical interface version of Network Monitor. For example, to capture all LDAP packets, execute the following command:

```
nmcap /network *
d:\test.cap
```

To capture all packets that go to 10.0.01, execute the following command:

```
nmcap /network * /capture Ipv4.address = =
10.0.01 /file d:\test.cap
```

When you view the packets, you will see the IP addresses of the hosts. However, to make the packets easier to read, you can use Aliases, which allow you to turn IP addresses into names.

CREATE ALIASES

GET READY. To create an alias in Network Monitor, perform the following steps:

1. Open Network Monitor by clicking Start > Microsoft Network Monitor.
2. In the *Recent Captures* pane, click New capture tab. A new *Capture* tab opens.
3. In the Frame Summary pane, click Aliases and then select Manage Aliases. The *Aliases* dialog box opens.
4. In the *Manage aliases* window, click New. The *Create New Alias* dialog box opens.
5. In the *Address* text box and the *Name* text box, type the address and name.
6. Click OK to accept your settings and close the *Create New Alias* dialog box.
7. Click Close to close the *Aliases* dialog box.
8. Close *Network Monitor*.

Monitoring Virtual Machines (VMs)

THE BOTTOM LINE

Just as you need to monitor physical computers, you also need to monitor virtual machines (VMs). Everything you have learned in this lesson applies to VMs. To monitor a virtual machine running Windows, you can still use Server Manager, Computer Management, Event Viewer, Performance Monitor, and all of the other tools. Since a single host can have many virtual servers, you need to make sure that one virtual computer does not use all of the resources that would take away from the other machines.

Hyper-V Resource Metering is a tool that allows you to view the resource usage of a host and individual VMs. In Windows Server 2012 R2, it is activated and viewed with Windows PowerShell. Hyper-V Resource metering includes the following cmdlets:

- `Enable-VMResourceMetering` starts collecting data per virtual machine.
- `Disable-VMResourceMetering` disables resource metering per virtual machine.
- `Reset-VMResourceMetering` resets virtual machine resource-metering counters.
- `Measure-VM` displays resource-metering statistics for a specific virtual machine.

To retrieve metering data for a particular VM, execute the following command:

```
Get-VM -ComputerName <HostName> -Name
"<VMName>" | Measure-VM
```

Business Case Scenarios

Scenario 3-1: Troubleshooting a Performance Problem

You have several file servers. Several times during the day, the file server performance degrades significantly. What steps should you perform to determine the cause of the problem?

Scenario 3-2: Monitoring the Event Viewer of Multiple Computers

You have 40 essential servers that must be running as best as they can at all times. What is the most efficient way to review key events on all 40 servers each day?

Configuring Distributed File System (DFS)

LESSON 4

Using Distributed File System

THE BOTTOM LINE

Distributed File System improves on the use of the shared folders by enabling you to organize your shared folders and enabling you to distribute shares on multiple servers.

Distributed File System (DFS) is a set of technologies that enable a Windows server to organize multiple distributed SMB file shares into a distributed file system. Although the shares can be on different servers, the location is transparent to the users. Finally, DFS can provide redundancy to improve data availability while minimizing the amount of traffic passing over the WAN links. The two technologies in DFS include:

- DFS Namespaces
- DFS Replication

Installing and Configuring DFS Namespace

If you have a site with many file servers and many shared folders, some users will have difficulty finding the files that they need as they have to remember the server name and shared folder name that make up the UNC. ***DFS Namespace*** enables you to group shared folders into a single logical structure. In other words, a DFS Namespace is a shared folder of shared folders (which can be on multiple servers).

DFS is a virtual namespace technology that enables you to create a single directory tree that lists other shared folders. Creating a DFS Namespace allows users to locate their files more easily. See Figure 4-1.

Figure 4-1

Linking to shared folders with DFS Namespace

The actual shared folders are referred to as the targets of the virtual folders in the namespace. DFS can be combined with DFS Replication, which increases availability and automatically connects users to shared folders in the same Active Directory site, when available, instead of connecting to another folder connected over a slower WAN link.

INSTALLING DFS NAMESPACE

Installing DFS Namespace is a simple process of adding the appropriate role using Server Manager. However, you should also install the File Server service so that you can create file shares. The DFS Management Tools installs the DFS Management snap-in, the DFS Namespace module for Windows PowerShell, and command-line tools.

INSTALL DFS NAMESPACE

GET READY. To install DFS Namespace, perform the following steps:

1. Click the Server Manager button on the task bar to open *Server Manager*.
2. At the top of Server Manager, select Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install DFS to, and then click Next.
6. Scroll down and expand File and Storage Services and then expand File and iSCSI Services. Select File Server and DFS Namespace (see Figure 4-2).

Figure 4-2

Selecting File Server and DFS Namespaces

7. When asked to add features to DFS Namespace, click Add Features.
8. When you are back on the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Confirm installation selections*, click Install.
11. When the installation is complete, click the Close button.

CONFIGURING DFS NAMESPACES

There are two types of DFS namespaces:

- Domain-based namespace
- Stand-alone namespace

With ***domain-based namespaces***, the configuration is stored in Active Directory, which means that you don't have to rely on a single server to provide the namespace information to your clients. By using a domain-based namespace, if you change the name of the server that runs the DFS Namespace service and the name of the server changes, you will not have to change the namespace. The namespace changes only if you rename the domain. With a ***stand-alone DFS***, the configuration is stored on the server and the server name becomes part of the main path to the namespace.

When you create a namespace, the Windows Server 2008 mode is selected by default, which supports up to 50,000 folders with targets per namespace and access-based enumeration. Access-based enumeration means that users can see only the folders and files that they have

permission to access. If a user does not have permission to the folder or file, the folder or file does not even show in a directory listing. To use Windows Server 2008 mode, Active Directory must use the Windows Server 2008 domain functional level. If you deselect the Windows Server 2008 mode, you will use the Windows 2000 Server mode, which supports only up to 5,000 folders.

CREATE A DFS NAMESPACE

GET READY. To create a DFS Namespace, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management to open the *DFS Management console*.
3. In the left-pane, right-click Namespaces and select New Namespace. The *New Namespace Wizard* starts.
4. On the *Namespace Server* page, type in the name of the server that hosts the DFS Namespace in the *Server* text box. Click Next.
5. On the *Namespace Name and Settings* page, type the name of the namespace in the *Name* text box. The name appears after the server (stand-alone namespace) or domain name (domain-based namespace). Click Next.
6. To change the location of the shared folder on the server and the shared permissions, click Edit Settings. The *Edit Settings* dialog box opens.
7. Specify the location of the Shared Folder and specify the Shared folder permissions. Click OK to close the *Edit Settings* dialog box.
8. On the *Namespace Name and Settings* page, click Next.
9. On the *Namespace Type* page (see Figure 4-3), select either Domain-based namespace or Stand-alone namespace.

Figure 4-3

Selecting the namespace on the Namespace Type page

10. Leave the Enable Windows Server 2008 mode enabled. Notice the entire path of the domain-based namespace. Click Next.
11. On the *Review Settings and Create Namespace* page, click Create.
12. When the installation is complete, click the Close button.

After you create the namespace, you need to add folders to it that point to the share folders on your network. If you have a DFS replicated folder, you add each replicated folder to the target. By using the DFS replicated folder with the DFS namespace, you provide fault tolerance and better.

ADD FOLDERS TO THE NAMESPACE

GET READY. To add folders to the namespace, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management to open the *DFS Management console*.
3. In the left pane, expand the Namespaces folder and select the desired namespace.
4. Under *Actions*, click New Folder. The *New Folder* dialog box opens.
5. Type the name of the shared folder in the *Name* text box. The name should be a descriptive name, but does not have to be the same name as the shared folder that you will be referencing.
6. To specify the shared folder, click Add.
7. In the *Add Folder Target* dialog box, type in the UNC to the desired shared folder. Click OK.
8. If you have DFS replicated folder for your target, add the replicated paths of the folder.
9. Click OK to close the *New Folder* dialog box.

MANAGING REFERRALS

A ***referral*** is an ordered list of servers or targets that a client computer receives from a domain controller or namespace server when the user accesses a namespace root or a DFS folder with targets. After a computer receives a referral, it reaches the first server on the list. If the server is not available, it tries to access the second server. If that server is not available, it goes to the next server.

If you right-click the namespace and select Properties, you can help choose which server the client uses when you have multiple folders for a shared folder. No matter what ordering method is selected, if a client is on the same site as the target, it always chooses the target. Then, by default, it chooses the closest server (lowest cost). You can also select *Random order*, which performs a load balancing for the targets at the other sites. Lastly, you can select the *Exclude targets outside of the client's side* option, which prevents the clients from accessing targets at other sites.

If a server becomes unavailable, you can have a client fall back to targets that were previously unavailable if the server becomes available again and at lower cost than the target the client uses. This is done by selecting the *Clients fail back to preferred targets* option.

In the Advanced tab, you can optimize polling. To maintain a consistent domain-based namespace across namespace servers, the namespace servers periodically poll Active Directory Domain Services (AD DS) to obtain the most current namespace data.

By default, the *Optimize for consistency* option is selected. It causes the namespace servers to poll the PDC emulator each time the namespace changes. If you have more than 16 namespace servers, you should choose the *Optimize for scalability* to reduce the load on the PDC Emulator. Unfortunately, this option increases the time it requires for changes to the namespace to replicate to all namespace servers, which may cause users to see inconsistent view of the namespace while namespace changes are replicated to all servers.

To control how targets are ordered, you can set priority on individual targets. For example, if you want one server to always be first or always be last, you can use the following procedure:

SET TARGET PRIORITY ON A ROOT TARGET FOR A DOMAIN-BASED NAMESPACE

GET READY. To set the target priority on a root target for a domain-based namespace, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management to open the *DFS Management console*.
3. In the left pane, expand the Namespaces folder and select the desired namespace.
4. In the center pane, click Namespace Servers tab.
5. Right-click the root target with the priority that you want to change, and then click Properties.
6. Click the Advanced tab.
7. Click Override referral ordering, and then click the priority that you want.
   - First among all targets: Specifies that users should always be referred to this target if the target is available.
   - Last among all targets: Specifies that users should never be referred to this target unless all other targets are unavailable.
   - First among targets of equal cost: Specifies that users should be referred to this target before other targets of equal cost (which usually means other targets in the same site).
   - Last among targets of equal cost: Specifies that users should never be referred to this target if there are other targets of equal cost available (which usually means other targets in the same site).
8. Click OK to close the *Properties* dialog box.
9. Close the DFS Management console.

MANAGING DFS SECURITY

Because DFS Namespace is a specialized shared folder of shared folders, you still secure these folders with share permissions and NTFS permissions. It is recommended that you first configure the share and NTFS permissions on folders that host namespace roots and folder targets before configuring DFS. If you have multiple namespace root servers or folder target servers will be utilized, you need to manually synchronize permissions between the servers to avoid access problems.

Access-based enumeration hides files and folders that users do not have permission to access. To control access-based enumeration of files and folders in folder targets, you must enable access-based enumeration on each shared folder by using the following procedure.

ENABLE ACCESS-BASED ENUMERATION FOR A NAMESPACE

GET READY. To enable access-based enumeration for a namespace, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management to open the *DFS Management console*.
3. In the left pane, right-click the namespace and click Properties.
4. Click the Advanced tab.
5. Select the Enable access-based enumeration for this namespace.
6. Click OK to close the *Properties* dialog box.
7. Close the *DFS Management console*.

Installing and Configuring DFS Replication

The other part of DFS is DFS Replication. ***DFS Replication (DFSR)*** enables you to replicate folders between multiple servers. To allow efficient use of the network, it propagates only the changes, uses compression, and uses scheduling to replicate the data between the servers.

To enable replication between multiple targets, you first create a replication group. The ***replication group*** is a collection of servers, known as servers, each of which holds a target of a DFS folder. You need a minimum of two targets to perform DFS Replication.

When you create a DFS replication group, you designate one server as the primary member of the replication group. Files then copy from the primary member to the other target servers. If any of the files in the target folders are different, DFS Replication overwrites the other files.

The primary disadvantage of using DFS Replication is that you need to have sufficient storage space available on each server that hosts the server and you need extra space so that DFS Replication can process the replication.

When using DFS Replication, you should keep in mind the following limitations:

- A replication group can have up to 256 members with 256 replicated folders.
- Each server can be a member of up to 256 replication groups, with as many as 256 connections (128 incoming and 128 outgoing).

The best method to recover from a disaster is to use backups. DFS Replication can also be used in conjunction with backups to provide a WAN backup solution. For example, if you have multiple sites, it becomes more difficult to perform backups, particular over the slower WAN links. One solution for this is to set up DFS Replication between the site servers to a central server or servers at the corporate office. Replication occurs when the WAN links are utilized the least such as in the evenings and during the weekends. You then back up the central computers located at the corporate office.

INSTALLING DFS REPLICATION

DFS Replication is another server role, similar to DFS Namespace. Therefore, you would use Server Manager to install DFS Namespace.

INSTALL DFS REPLICATION

GET READY. To install DFS Replication, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, select Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install DFS to, and then click Next.
6. Scroll down and expand File and Storage Services and expand file and iSCSI Services. Select DFS Replication. If *File Server* is not already installed, select it.
7. If you are asked to add features to DFS Namespace, click Add Features.
8. When you are back on the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When the installation is complete, click the Close button.

CONFIGURING DFS REPLICATION TARGETS

When you replicate folders using DFS, you are replicating local folders on a server to another local folder on another server. The folder is most likely shared so that users can access the folder, but this is not necessary.

By default, replication groups use a ***full mesh topology***, which means that all members replicate to all other members. If you have a simple DFS implementation consisting of two servers, there is some replication traffic between the two servers. However, by adding multiple servers to a replication group, replication traffic increases even more. Therefore, instead of using a full mesh topology, you can use a ***hub/spoke topology***, were as one server is used to replicate to the other members, which limit the replication traffic to specific pairs of members.

When you configure DFS Replication, you can configure the following settings:

- Bidirectional or unidirectional
- Percentage of available bandwidth
- Schedule when replication will occur

By default, DFS replication between two members is bidirectional. Bidirectional connections occur in both directions and include two one-way connections. If you desire only a one-way connection, you can disable one of the connections or use share permissions to prevent the replication process from updating files on certain member servers.

Because DFS Replication often occurs over a WAN link, you have to be aware of how much traffic DFS uses and how you can configure it when replication occurs to best utilize the WAN links. Therefore, you can schedule replication to occur only during the night when the WAN links are not used as much or you can specify the bandwidth used by DFS Replication.

CREATE A DFS REPLICATION GROUP

GET READY. To create a DFS replication group, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management. The *DFS Management console* opens.

3. Right-click Replication and select New Replication Group.
4. On the *Replication Group Type* page, select Multipurpose replication group, and then click Next.
5. On the *Name and Domain* page, type a descriptive name for the replication group in the Name of replication group text box. Click the Next button.
6. On the *Replication Group Members* page, click the Add button.
7. When the *Select Computers* dialog box opens, type the name of the first server of the group and click OK.
8. Repeat step 7 until all of the target servers are added to the group.
9. On the *Replication Group Members* page, click Next.
10. On the *Topology Selection* page, select Full Mesh, and then click Next.
11. On the *Replication Group Schedule and Bandwidth* page, click one of the following:
    a. Replicate continuously using the specified bandwidth. Specify the bandwidth that you want to use. The default bandwidth is Full.
    b. Replicate during the specified days and times. Then click Edit Schedule to specify which days and time you can replicate and the bandwidth used during those days and time.

    Click Next.
12. On the *Primary Member* page, specify which server acts as the Primary member. Click Next.
13. On the *Folders to Replicate* page, click Add.
14. When the *Add Folder to Replicate* dialog box opens (see Figure 4-4), specify the local path name of the folder that you want to replicate. Do not type the UNC name.

Figure 4-4

Specifying the local folders to replicate

15. Click OK to close the *Add Folder to Replicate* dialog box.
16. Back on the *Folders to Replicate* page, click Next.
17. On the *Local Path on Other Members* page (see Figure 4-5), select each member server listed and click Edit.

Figure 4-5

Adding the remote folder to replicate

18. When the *Edit* dialog box opens, select Enabled and type the local path on the member server. Click OK to close the *Edit* dialog box.
19. Back on the *Local Path of Public on Other Members* page, click Next.
20. On the *Review Settings and Create Replication Group* page, click Create.
21. When the replication group has been created, click Close.
22. If you get a Replication Delay message, click OK.

Scheduling Replication

When the replication group is created, you can define the scheduled group. You can also modify the schedule after the replication group is created by right-clicking the replication group in the DFS Management console and selecting Edit Replication Group Schedule. When the *Edit Schedule* dialog box opens, you can select and deselect a range of time and then select the bandwidth usage (see Figure 4-6).

Figure 4-6

Specifying the scheduled bandwidth for replication

Configuring Remote Differential Compression

DFS Replication is an efficient, multiple-master replication engine that synchronizes DFS folders and replicates Active Directory Domain Services (AD DS) SYSVOL folder on domain controllers. It replaced the File Replication Service (FRS), which was deprecated in Windows Server 2012 and thus is not available in Windows Server 2012 R2.

DFS Replication uses a compression algorithm known as ***remote differential compression (RDC)***, which detects changes to the data in a file and replicates only those file blocks that changed instead of the entire file. As a result, not as much data needs to be transferred. If you disable RDC, you can conserve processor and disk input/output (I/O). Of course, you will consume much more bandwidth.

DISABLE REMOTE DIFFERENTIAL COMPRESSION

GET READY. By default, RDC is enabled. To disable RDC, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management to open the *DFS Management console*.
3. In the left pane, expand Replication, and select the replication group that you want to modify. Figure 4-7 shows the *DFS Replication* Group tabs.

Figure 4-7

Showing a created DFS Replication Group

4. Select the Connections tab (see Figure 4-8).

Figure 4-8

Showing the connections used in DFS Replication.

5. Right-click a connection and select Properties to display the *Properties* dialog box.
6. Deselect the Use remote differential compression (RDC) option.
7. Click OK to close the *Properties* dialog box.

Configuring Staging

To figure what needs to be replicated, DFS uses staging folders. The ***staging folder*** acts as a cache for new and changed files that need to be replicated. It also is used to compress files that need to be sent. When received on the other end, it is used to decompress the file and install the file into the replicated folder.

Each replicated folder has its own staging folder, which, by default, is located under the local path of the replicated folder in the DfsrPrivate\Staging folder. The default size of each staging folder is 4,096 MB, which is determined by a quota. When the staging folder reaches 90%, it purges the oldest staged file until it reaches 60%.

It should also be noted that the staging folder quota does not determine the largest file that can be replicated. If a large file is still in the process of being replicated, any cleaning that occurs is retried later after the file has been replicated. You should increase the quota size only if you have multiple large files that change frequently. To keep processor and disk utilization to a minimum, the quota should be configured to the size of the combined nine largest files in the replicated folder.

On occasion, when the same file gets changed at approximately the same time on two different targets, a conflict occurs. DFS Replication uses a last-writer wins model, which determines which file it should keep and replicate. The losing file is renamed and stored in the Conflict and Deleted folder on the member that resolves the conflict.

Each replicated folder has its own ***Conflict and Deleted folder***, which is located under the local path of the replicated folder in the DfsrPrivate\ConflictandDeleted folder. By default, the quota size of the Conflict and Deleted folder is 660 MB. While the access control lists (ACLs) on the conflicted files are preserved, only members of the local Administrators group can access the files. You can view a log of conflict files and their original file names by viewing the ConflictandDeletedManifest.xml file in the DfsrPrivate folder.

MANAGE THE STAGING FOLDER AND CONFLICT AND DELETED FOLDER

GET READY. To edit the quota size or location of the staging folder and Conflict and Deleted folder, perform the following steps:

1. Open Server Manager.
2. Click Tools > DFS Management. The *DFS Management console* opens.
3. In the left pane, expand Replication.
4. In the left pane, click the replication group that contains the replicated folder with the quotas that you want to edit.
5. On the *Memberships* tab, right-click the replicated folder on the member with the quota that you want to edit, and then click Properties. The *Properties* dialog box opens.
6. Select the Staging tab.
7. Change the Staging path and the quotas as needed and adjust the staging folder quota and path as necessary.
8. Select the Advanced tab.
9. Adjust the Conflict and Deleted folder quota as necessary.
10. Click OK to close the *Properties* dialog box.

Windows Server 2012 R2 includes several tools to help monitor and troubleshoot DFS Replication. To generate a diagnostic report, you can right-click a replication group in the DFS Management console and click *Diagnostic Report*. You can also use the DfrsAdmin.exe in a script and schedule the script to run with task scheduler. Finally, you can use DfsrDiag.exe to perform diagnostic tests of DFS Replication.

Cloning a DFS Database

If you have a large file repository that you want to replicate to another server, it could take quite a bit of time to synchronize the files. Windows Server 2012 R2 provides you with the ability to export the DFS database, preseed the files on the destination server, and then import the database.

Before Windows Server 2012 R2, each server recorded the information in a local database, exchanged the information with the remote nodes, staged files, created hashes, and then transmitted the files over the network. If you preseed the files by copying the files to a destination server and then implement DFS replication, DFSR has to go through each file, record the information in a local database, then exchange the information with the remote nodes. If any differences are found, the two servers will reconcile the differences.

For larger repositories, the DFS replication can take days or even weeks, even if you preseed the data files. If you preseed a server and the database, you can reduce the setup time by approximately 99 percent.

PRESEED A SERVER AND DATABASE

GET READY. To preseed a server and database, perform the following steps:

1. On the source computer, create a replication group and replicated folder, but do not add the destination server. Let the initial build complete.
2. Export the cloned database from the source server.
3. Preseed the files to the target server by copying the files using an external drive, from a backup, or over the network.
4. Copy the exported clone DB files to the target computer.
5. Import the cloned database on the downstream server.
6. Add the target server to the replication group and add the replicated folders.

The DFS replication database exists on every volume that contains a DFS replicated folder and a single database that contains references for all replicated folders on the volume. To export the DFS database and volume configuration XML file settings for a volume, use the `Export-DfrsClone` Windows PowerShell cmdlet. However, you will not be able to clone SYSVOL or read-only replicas in Windows Server 2012 R2.

To export the DFS Replication database clone for the C: volume into the *C:\Dfsrclone* destination folder and display the associated replicated folders, use the following Windows PowerShell command:

```
Export-DfsrClone -Volume C: -Path C:\Dfsrclone | Format-List
```

To monitor the export process, use `Get-DfsrCloneState.`

To import a cloned DFS replication database and volume configuration settings, use the `Import-DfrsClone` PowerShell cmdlet.

For example, to clone and import the DFS Replication database and volume configuration XML to the C: volume from the *C:\ Dfsrclone* folder, use the following command:

```
Import-DfsrClone -Volume c: -Path C:\dfsrclone
```

Recovering DFS Databases

Windows Server 2012 R2 features automatic recovery after a loss of power or an unexpected stoppage of the DFS Replication service; this automatic recovery feature validates the database against the file system and then resumes replication normally.

If a system experiences a power loss, the volume hosting the replicated folder gets disconnected, or the DFSR service stops abnormally for any reason, the database and file system could get out of sync. With Windows Server 2008 and Windows Server 2008 R2, DFSR is designed to automatically recover from these types of situation.

Using Windows Server 2012 R2, or by installing a hot fix for Windows Server 2008 R2, you can change the automatic auto-recovery to manual recovery so that you have to approve the unexpected shutdown recovery. By using a manual recovery, you have the opportunity to fix any underlying problems and to back up existing replicated folders on the volume before the recovery operation begins. If SYSVOL is the only replicated folder, replication automatically begins. If a database becomes corrupted, the database will be deleted and a nonauthoritative initial sync process begins.

In Windows Server 2012 R2, to manually resume the unexpected shutdown recovery and replication of the replicated folder(s) in a volume, use the following command using an elevated command prompt:

```
wmic /namespace:\\root\microsoftdfs path dfsrVolumeConfig where
volumeGuid="<volume-GUID>" call ResumeReplication
```

To configure Windows Server 2012 R2 to automatically perform an unexpected shutdown recovery, use the following command using an elevated command prompt:

```
wmic /namespace:\\root\microsoftdfs path dfsrmachineconfig set
StopReplicationOnAutoRecovery=FALSE
```

In Windows Server 2012 R2, when DFS Replication detects an unexpected shutdown, it automatically triggers a recovery process, during which corrupt databases are rebuilt using the local file and update sequence number (USN) change journal information. When a file is marked as having a normal replicated state, DFS Replication then contacts the partner server and merges the changes. If you don't want DFSR Replication to resume when a DFS database unexpectedly stops, open the registry and change *HKey_Local_Machine\System\CurrentControlSet\Services\DFSR\Parameters\StopReplicationOnAutoRecovery (DWORD)* to 1.

Optimizing DFS Replication

Windows Server 2012 R2 provides several changes that enhance DFS, including file staging tuning, support for larger repositories, and the ability to disable cross-file RDC.

Since its introduction with Windows 2000, DFS has been expanded significantly. For example, Windows Server 2003 R2 supported only 8 million files and up to 1 TB of data. However, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 support the following:

- Size of all replicated files on a server: 10 TB
- Number of replicated files on a volume: 11 million
- Maximum file size: 64 GB

The scalability of Windows Server 2012 R2 has been expanded even further:

- Size of all replicated files on a server: 100 terabytes
- Number of replicated files on a volume: 70 million
- Maximum file size: 250 gigabytes

Of course, if you need to replicate large amounts of data over a slower WAN link, you should consider preseeding the data files and import/export the DFS database.

Cross-file RDC uses a similar file to construct another file so that less data is replicated. However, cross-file RDC might increase processing, particularly on high-bandwidth network connections with large data sets. In this situation, with Windows Server 2012 R2, you can disable cross-file RDC between servers. For servers connected with fast LAN connections, turning off cross-file RDC might reduce server resource overhead and increase replication performance. However, for slower WAN links, you should keep cross-file RDC enabled between servers.

In Windows Server 2012 and earlier, DFS replication uses a 256 KB file size to determine if a file is to be staged. If the RDC minimize size, which by default is 64 KB, is larger than 256 KB, a file will be staged before it is replicated. When files are staged, the replication time is increased because of RDC operations. With Windows Server 2012 R2, you can configure a staging minimum size between 256 KB to 512 TB. Increasing the minimum staging size for files can increase the replication performance.

If you are not using RDC or staging, files are no longer compressed or copied to the staging folder, which can increase performance. However, without compression, you will use higher bandwidth.

Configuring Fault Tolerance Using DFS

To make shared files fault tolerant, you need to use both DFS Namespace and DFS Replication.

Each technology used in DFS has some impressive capabilities. DFS Namespace offers ease of use when trying to locate a shared folder and DFS Replication replicates files from one server to another. However, when they are combined, they can offer fault tolerance on the network.

1. Create the same folder on multiple servers. While the folders don't have to have the same name, it makes management easier and cuts down on confusion.
2. Share the folders.
3. Configure DFS Replication between the folders on the various servers.
4. Create a DFS Namespace that includes targets of all target folders for a replication group.

DFS Replication ensures the files are replicated between the servers, providing multiple copies of the files. The DFS namespace makes the access of the replicated folders transparent to the users when accessing the replicated folder. As far as the users are concerned, they access the DFS namespace/shared folder, and then they go to one of the replicated folders. If one of the replicated folders is not available, it is rerouted to another replicated folder.

Business Case Scenarios

Scenario 4-1: Backing up Remote File Servers

You have 10 file site servers located with 2048 Mb/s WAN links. You tried to run backups over the WAN links and the backups took too long to execute. What can you do to alleviate this problem?

Scenario 4-2: Protecting Essential File Servers

You have a Project server that has key files that must be accessed from people in multiple sites throughout the country. These files must be accessible 24/7 while keeping performance as high as possible. What solution would you provide?

5 LESSON

Configuring File Server Resource Manager (FSRM)

Using File Server Resource Manager

THE BOTTOM LINE

File Server Resource Manager (FSRM) is a suite of tools that enables you to control and manage the quantity and type of data stored on a file server. It enables you to define how much data a person can store, define what type of files that a user can store on a file server, and generate reports about the file server being used.

Using File Server Resource Manager enables you to perform the following tasks:

- Create quotas for a volume or folder tree, including generating e-mails when the quota limits are approached or exceeded.
- Create file screens to control the type of files that users can save.
- Send notifications when users try to save a blocked file.
- Schedule periodic storage reports or manually generate a storage report that helps you to identify trends in disk usage.
- Classify files based on defined properties and apply policies based on the classification. You can restrict access to files, encrypt files, and have files expire. File classification is discussed in more detail in the 70-412 course.

Installing File Server Resource Manager

Installing FSRM is a simple process because it is a Windows server role.

Similar to the previous Windows server roles, the FSRM is installed with Server Manager as a server role.

INSTALL FILE SERVER RESOURCE MANAGER

GET READY. To install FSRM, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, select Manage and click Add Roles and Features to open the *Add Roles and Feature Wizard*.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install FSRM to, and then click Next.
6. Scroll down and expand File and Storage Services and expand file and iSCSI Services. Select File Server Resource Manager (see Figure 5-1).

Figure 5-1

Selecting File Server Resource Manager

7. When you are asked to add additional features, click Add Features.
8. On the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Confirm installation selections*, click Install.
11. When the installation is complete, click the Close button.

Using Quotas

In the 70-410 course, you studied NTFS file quotas that defined how much data a user can store on a volume. ***Quotas*** defined with FSRM limit how much space a folder or volume can use.

By using FSRM to create a quota, you limit the amount of disk space allocated to a volume or folder. The quota limit applies to the entire folder's subtree.

When you define the quotas, you can define either a hard quota or a soft quota:

- A ***hard quota*** prevents users from saving files after the space limit is reached and generates notifications when the volume of data reaches the configured threshold.
- A ***soft quota*** does not enforce the quota limit but generates a notification when the configured threshold is met.

NTFS quotas can create FSRM, can use e-mail, log an event, run a command or script, or generate a storage report for notification.

CREATING QUOTAS

You can create a quota on a volume or a folder using a ***quota template*** or by using custom properties. It is recommended that you use quota templates because quota templates can be applied to other volumes and folders in the future. In addition, if you modify the template, you have the option to change any quotas that used the quota template in the past.

CREATE A QUOTA TEMPLATE

GET READY. To create a quota template, perform the following steps:

1. Open Server Manager.
2. Click Tools > File Server Resource Manager. The *File Server Resource Manager console* opens (see Figure 5-2).

Figure 5-2

Viewing the File Server Resource Manager console

3. Under *Quota Management*, right-click Quota Templates and select Create Quota Template. The *Create Quota Template* dialog box opens.
4. If you want to copy the properties of an existing template, you can select a template from the Copy properties from quota template drop-down list. Then click Copy.
5. In the *Template name* text box, type a name.
6. In the *Description (optional)* text box, type a description of the quota.
7. In the *Space limit* section, in the *Limit* text box, type a number and specify the unit (KB, MB, GB, or TB).
8. Select Hard quota or Soft quota.
9. To add a notification, click the Add button. The *Add Threshold* dialog box opens (see Figure 5-3).

Figure 5-3

Displaying the Add Threshold dialog box

10. To set a quota limit percentage that generates a notification, type a number in the *Generate notifications when usage reaches (%)* text box. The default is 85%.
11. To configure e-mail notifications, on the *E-mail Message* tab, set the following options:
    - Select the Send e-mail to the following administrators check box, and then enter the names of the administrative accounts that receive the notifications using the account@domain format. Use semicolons to separate multiple accounts.
    - To send e-mail to the person who saved the file that reached the quota threshold, select the Send e-mail to the user who exceeded the threshold check box.
    - To configure the message, edit the default subject line and message body that are provided. Brackets indicate variable information. For example, [Source Io Owner] variable inserts the name of the user who saved the file that reached the quota threshold.
    - To configure additional headers (including From, Cc, Bcc, and Reply-to), click Additional E-mail Headers.
12. To log an event, select the Event Log tab. Then select the Send warning to event log check box and edit the default log entry.
13. To run a command or script, select the Command tab. Then select the Run this command or script check box. Type the command. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.
14. To generate one or more storage reports, select the Report tab. Select the Generate reports check box, and then select which reports to generate. Optionally, you can enter one or more administrative e-mail recipients for the report or e-mail the report to the user who reached the threshold.

15. Click OK to save your notification threshold and close the *Add Threshold* dialog box.
16. Click OK to close the *Create Quota Template* dialog box. The quota template will be listed.

CREATE A QUOTA FROM A QUOTA TEMPLATE

GET READY. To create a quota from a Quota template, perform the following steps:

1. Open Server Manager.
2. Click Tools > File Server Resource Manager. The *File Server Resource Manager console* opens.
3. Under the *Quota Management* node, click the Quota Templates node.
4. Right-click the template on which you will base your quota and click Create Quota from Template. The *Create Quota* dialog box opens (see Figure 5-4).

Figure 5-4

Creating a quota using a template

5. Type the volume or folder that the quota applies to in the *Quota path* text box.
6. Select the Create quota on path option.
7. Click Create.

If you want to create a quota without using a template, right-click *Quotas* and select *Create Quota* to open the *Create Quota* dialog box. You can then pull values from a quota template or manually configure the settings.

File Server Resource Manager can also generate quotas automatically by selecting the *Auto apply template* and create quotas on existing and new subfolders. When it is applied to a parent volume or folder, it is applied to each subfolder and each subfolder that is created in the future.

Managing Files with File Screening

Often on a corporate network, users try to save files such as movies, music, and games on the corporate server. Unfortunately, although much of this can cause legal problems associated with copyright, it also takes up disk space that can be used for something else, it costs money to provide the storage space, and it makes the backup sets larger. Therefore, Microsoft developed ***file screening*** that allows you to control the type of files that users can save and send notifications when users try to save a blocked file.

In the File Screening Management node of the File Server Resource Manager MMC snap-in, you can perform the following tasks:

- Create and manage file groups, which are used to determine which files are blocked and which are allowed.
- Create file screens to control the types of files that users can save and generate notifications when users attempt to save unauthorized files.
- Create file screen exceptions that override file-screening rules.
- Define file-screening templates to simplify file-screening management.

CREATING FILE GROUPS

A ***file group*** is used to define a namespace for a file screen, file screen exception, or Files by File Group storage report. It consists of a set of file name patterns, which are grouped by the following:

- Files to include
- Files to exclude

FSRM already includes pre-built file groups.

CREATE FILE GROUPS

GET READY. To create a file group, perform the following steps:

1. Open Server Manager.
2. Click Tools > File Server Resource Manager. The *File Server Resource Manager console* opens.
3. In *File Screening Management*, click the File Groups node.
4. Right-click File Groups and select Create File Group. The *Create File Group Properties* dialog box opens.
5. In the *File group name* text box, type a name of the file group.
6. To add files to include, type a filename or filename pattern using the * wildcard character in the *Files to include* text box, and then click Add.
7. To add files to exclude, type a filename or filename pattern using the * wildcard character in the Files to exclude text box and click Add.
8. Click OK to close the *Create File Group Properties* dialog box.

CREATING A FILE SCREEN

When you create a file screen, there are two screening types:

- ***Active screening***: Prevents users from saving the defined unauthorized files.
- ***Passive screening***: Allows users to save a file, but allows the monitoring and notification when a user saves an unauthorized file.

CREATE A FILE SCREEN

GET READY. To create a file screen, perform the following steps:

1. Open Server Manager.
2. Click Tools > File Server Resource Manager. The *File Server Resource Manager console* opens.
3. Under *File Screening Management*, click the File Screens node.
4. Right-click File Screens, and then click Create File Screen. The *Create File Screen* dialog box opens.
5. Type the path to a folder to be used by the file screen in the *File screen path* text box. The file screen applies to the selected folder and all of its subfolders.
6. Select Define custom file screen properties, and then click Custom Properties. The *File Screen Properties* dialog box opens.
7. If you want to copy the properties of an existing template to use as a base for your file screen, select a template from the *Copy properties from template* drop-down list. Then click Copy.
8. Under *Screening* type, click the Active screening or Passive screening option.
9. Under *File groups*, select each file group that you want to include in your file screen.
10. To configure e-mail notifications, click the E-mail Message tab, and then set the following options:
    - Select the Send e-mail to the following administrators check box, and then enter the names of the administrative accounts that will receive the notifications using the account@domain format. Use semicolons to separate multiple accounts.
    - To send e-mail to the person who saved the file that reached the quota threshold, select the Send e-mail to the user who exceeded the threshold check box.
    - To configure the message, edit the default subject line and message body that are provided. Brackets indicate variable information. For example, the [Source Io Owner] variable inserts the name of the user who saved the file that reached the quota threshold.
    - To configure additional headers (including From, Cc, Bcc, and Reply-to), click Additional E-mail Headers.
11. To log an event, select the Event Log tab. Then select the Send warning to event log check box, and edit the default log entry.
12. To run a command or script, select the Command tab. Then select the Run this command or script check box. Type the command. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.
13. To generate one or more storage reports, select the Reports tab. Then select the Generate reports check box, and then select which reports to generate. Optionally, you can enter one or more administrative e-mail recipients for the report or e-mail the report to the user who reached the threshold.
14. Click OK to close the *File Screen Properties* dialog box.
15. In the *Create File Screen* dialog box, click Create to save the file screen. The *Save Custom Properties as a Template* dialog box opens.
16. To save a template that is based on these customized properties (recommended) and apply the settings, select Save the custom properties as a template and enter a name for the template.
17. If you do not want to save a template when you save the file screen, select Save the custom file screen without creating a template.
18. Click OK to close the *Save Custom Properties as a Template* dialog box. The new file screen appears under *File Screens*.

Using Storage Reports

To help you manage storage, you can use FSRM to generate ***storage reports*** that show the state of file server volumes and anyone who exceeds the quota or uses files that aren't allowed.

The reports that FSRM can create are as follows:

- **Duplicate Files:** Shows a list of files that are the same size and have the same last modified date.
- **File Screening Audit:** Creates a list of the audit events generated by file-screening violations for specific users during a specific time period.
- **Files by File Group:** Creates a list of files sorted by selected file groups defined with FSRM.
- **Files by Owner:** Creates a list of files sorted by selected users that own them.
- **Large Files:** Creates a list of files that are larger than a specified size.
- **Least Recently Accessed Files:** Creates a list of files that have not been accessed for a specified number of days.
- **Most Recently Accessed Files:** Creates a list of files that have been accessed within a specified number of days.
- **Quota Usage:** Creates a list of quotas that exceed a specified percentage of the storage limit.

When reports are generated, they are automatically saved in the C:\StorageReports\Scheduled folder. You can also have reports e-mailed to administrators.

SCHEDULE A STORAGE REPORT

GET READY. To schedule a storage report, perform the following steps:

1. Open Server Manager.
2. Click Tools > File Server Resource Manager. The *File Server Resource Manager console* opens.
3. Right-click Storage Reports Management, and select Schedule a new report task. The *Storage Reports Task Properties* dialog box opens (see Figure 5-5).

Figure 5-5

Creating a storage report

4. In the *Report Name* text box, type the name of the report.
5. In the *Report data* section, select the report that you want to generate and deselect the reports that you don't want to generate.
6. Click the Scope tab to display it.
7. Select the file groups that you want to include in the report.
8. Click Add and browse to the volume or folder that you want to report on, and click OK.
9. Click the Delivery tab to display it.
10. If you want the reports e-mailed to a user, select the Send reports to the following administrators and specify the e-mail address. If you need to send to multiple users, separate the e-mail addresses with semicolons (;).
11. Click the Schedule tab to display it.
12. Specify the time and select the days that you want the report to be generated.
13. Click OK to close the *Storage Reports Task Properties* dialog box.

After the reports have been scheduled, you can run a report at any time by right-clicking the storage report and selecting *Run Report Task Now*. If you need to change a scheduled report, right-click the report and select *Edit Report Task Properties*.

Enabling SMTP

Various components of the FSRM can send notifications via e-mail. However, to send e-mail, you need to configure FSRM to use Simple Mail Transfer Protocol (SMTP) so that FSRM knows where to forward the e-mail to be delivered.

An SMTP server must be specified as part of the initial FSRM configuration so that quota or file screening e-mail notifications can be sent. However, you must be a member of the Administrators group to enable SMTP.

ENABLE SMTP FOR FSRM

GET READY. To enable SMTP for FSRM, perform the following steps:

1. Open Server Manager.
2. Click Tools > File Server Resource Manager. The *File Server Resource Manager console* opens.
3. Right-click File Server Resource Manager in the left pane and select Configure Options. The *File Server Resource Manager Options* dialog box opens.
4. On the E-mail Notifications tab, type the computer name or the IP address of the SMTP server in the *SMTP server name or IP address* text box.
5. If you have not already specified an e-mail account to which the e-mail notifications will be sent, type the e-mail address under *Default administrator recipients*.
6. Click OK to save the new e-mail notification settings.

Configuring File Management Tasks

There are times when you need to perform routing file maintenance on certain folders, such as when you're removing old files when a volume becomes full. Windows Server 2012 R2 FSRM can be used to automatically perform these file management tasks.

By using the File Management Tasks node in FSRM, you can create file management tasks to handle expiring files. These tasks can automatically move all files that match specified criteria to a specified expiration directory. An administrator can then back those files up and delete them. In addition, you can apply Active Directory Rights Management Services (AD RMS) encryption or perform a custom action.

CREATE A FILE MANAGEMENT TASK

GET READY. To create a file management task, perform the following steps:

1. Using FSRM, click the File Management Tasks node.
2. Right-click the File Management Tasks node and choose Create File Management Task.
3. When the *Create File Management Task* dialog box opens, on the *General* tab, in the *Task name* text box and the *Description* text box, type the name and description for the task.
4. On the *Scope* tab (see Figure 5-6), use one of the following options to specify the folders you want to classify:
   - Select the folders based on *Folder Usage* properties, such as *Application Files, Backup and Archival Files,* or *User Files*.
   - Click Add to manually choose the folder to include.
   - Click Set Folder Management Properties to assign Folder Usage the purpose of the folder and the kind of files that are assigned to the folders.

Figure 5-6

The *Scope* tab

5. On the *Action* tab, specify the following information:
   - *Type:* Select File expiration, RMS Encryption, or Custom. Custom action allows you to run an executable program.
   - *Expiration Directory:* Select the directory or file share to which the files will expire.

6. Optionally, on the *Notification* tab, click the Add button to specify to send an e-mail to the administrators, send an email to users with affected files, send a warning to the event log, or to run a command or script.
7. Optionally, use the *Report* tab to generate one or more logs or storage reports.
8. Optionally, use the *Condition* tab to run this task only on files that match a defined set of conditions. Use the *Property conditions* section to add, edit, or remove conditions based on the file's classification. Use the remaining fields on the tab to specify time-related conditions and file name pattern conditions.
9. On the *Schedule* tab, specify when the task should run and then click OK.

Business Case Scenarios

Scenario 5-1: Blocking Audio and Video Files

You were just hired as an administrator for Contoso Corporate. You looked for a file server and discovered that several users have been using the file server as a personal repository for audio and video files that have been downloaded using the corporate network. How should you stop users form saving these files?

Scenario 5-2: Managing Disk Space

You have a file server that is used to store files used by the various projects throughout your organization. After a while, you realize that you are quickly running out of disk space. When you look at the usage, you determine that the reason the system is filling up is that older projects are never removed or archived. What solution would you propose to deal with this?

Configuring File Services and Disk Encryption

LESSON 6

Securing Files

THE BOTTOM LINE

Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. ***Decryption*** is the process of converting data from encrypted format back to its original format.

Encryption algorithms can be divided into three classes:

- Symmetric
- Asymmetric
- Hash function

Symmetric encryption uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption. To use symmetric key algorithms, you need to initially send or provide the secret key to both the sender and the receiver.

Asymmetric key, also known as public-key cryptography, uses two mathematically related keys. One key is used to encrypt the data and the second key is used to decrypt the data. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. Instead, you can make the public key known to anyone and use the other key to encrypt or decrypt the data. The public key can be sent to someone or it can be published within a digital certificate via a Certificate Authority (CA). Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Pretty Good Privacy (PGP) use asymmetric keys.

For example, say you want a partner to send you data. Therefore, you send the partner the public key. The partner then encrypts the data with the key and sends you the encrypted message. You then use the private key to decrypt the message. If the public key falls into someone else's hands, that person still cannot decrypt the message.

The last type of encryption is the hash function. Different from the symmetric and asymmetric algorithms, a hash function is meant as one-way encryption. That means that after the data has been encrypted, it cannot be decrypted. One example of its use is to use the hash function to encrypt a password that is stored on disk. Anytime a password is entered and it needs to be verified that it is the correct password, the same hash calculation is performed on the entered password and compared to the hash value of the password stored on disk. If the two match, the user must have typed in the password. This avoids storing the passwords in a readable format that a hacker might try to access.

No matter what encryption algorithm you choose, they all use keys to encrypt data. The key must be long enough so that an attacker cannot try all possible combinations to figure out what the key is. Therefore, a key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms. 128-bit keys are commonly used and considered strong.

Today, newer versions of Windows offer two file encrypting technologies: Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders, whereas BitLocker protects entire volumes.

Encrypting Files with EFS

In addition to protecting data files on a stolen system or drive, encryption can protect files.

Encrypting File System (EFS) can encrypt files on an NTFS volume that cannot be used unless the user has access to the keys required to decrypt the information. By default, when you encrypt a file with EFS, the file or folder turns green to show that the file is encrypted.

After a file has been encrypted, you do not have to manually decrypt an encrypted file before you can use it. Instead, you work with the file or folder just like any other file that is not encrypted. When you open a file that is encrypted with EFS, the file is automatically decrypted as needed. When you save the file, it is automatically decrypted. However, if another user tries to access the same file, he cannot open it because he does not have the proper key to open the file.

EFS uses an encryption key to encrypt your data, which is stored in a digital certificate. The first time a user encrypts a file or folder, an encryption certificate and key are created and bound to the user account. The user who creates the file is the only person who can read it. As the user works, EFS encrypts the files using a key generated from the user's public key. Data encrypted with this key can be decrypted only by the user's personal encryption certificate, which is generated using a private key.

CONFIGURING EFS

To encrypt or decrypt a folder or file, enable or disable the encryption attribute just as you set any other attribute, such as read-only, compressed, or hidden. If you encrypt a folder, all files and subfolders created in the encrypted folder are automatically encrypted. Microsoft recommends that you encrypt at the folder level.

ENCRYPT A FOLDER OR FILE USING EFS

GET READY. To encrypt a folder or file, perform the following steps:

1. Right-click the folder or file you want to encrypt, and then click Properties. The *Properties* dialog box opens.
2. Click the General tab, and then click Advanced. The *Advanced Attributes* dialog box appears.
3. Select the Encrypt contents to secure data checkbox.
4. Click OK to close the *Advanced Attributes* dialog box.
5. Click OK to close the *Properties* dialog box.
6. If you encrypt a file in an unencrypted folder, it gives you a warning. If you want to encrypt only the file, select Encrypt the file only and click OK. If you want to encrypt the folder and all content in the folder, select the Encrypt the file and its parent folder (recommended) option. Click OK.

7. If you encrypt a folder, it asks you to confirm the changes. If you want to encrypt only the folder, select Apply changes to this folder only. If you want to apply to all folders, select Apply changes to this folder, subfolders and files. Click OK to close the Confirm Attribute Changes dialog box.

DECRYPT A FOLDER OR FILE

GET READY. To decrypt a folder or file, perform the following steps:

1. Right-click the folder or file you want to decrypt, and then click Properties. The *Properties* dialog box opens.
2. Click the General tab, and then click Advanced. The *Advanced Attributes* dialog box opens.
3. Clear the Encrypt contents to secure data checkbox.
4. Click OK to close the *Advanced Attributes* dialog box.
5. Click OK to close the *Properties* dialog box.
6. When it asks you to confirm the changes. If you want to decrypt only the folders, select Apply changes to this folder only. If you want to apply to all folders, select Apply changes to this folder, subfolders and files. Click OK.

When working with EFS, keep the following in mind:

- You can encrypt or compress NTFS files only when using EFS; you can't do both. If the user marks a file or folder for encryption, that file or folder is uncompressed.
- If you encrypt a file, it is automatically decrypted if you copy or move the file to a volume that is not an NTFS volume.
- Moving unencrypted files into an encrypted folder automatically causes those files to be encrypted in the new folder.
- Moving an encrypted file from an EFS-encrypted folder does not automatically decrypt files. Instead, you must explicitly decrypt the file.
- Files marked with the System attribute or that are in the root directory cannot be encrypted.
- Remember that an encrypted folder or file does not protect against the deletion of the file, listing the files or directories. To prevent deletion or listing of files, use NTFS permissions.
- Although you can use EFS on remote systems, data that is transmitted over the network is not encrypted. If encryption is needed over the network, use SSL/TLS (Secure Sockets Layer/Transport Layer Security) or IPsec.

CONFIGURING THE EFS RECOVERY AGENT

If for some reason, a person leaves the company or a person loses the original key and the encrypted files cannot be read, you can set up a ***data recovery agent (DRA)*** that can recover EFS-encrypted files for a domain. To define DRAs, you can use Active Directory group policies to configure one or more user accounts as DRAs for your entire organization. However, to accomplish this, you need to have an enterprise CA.

ADD RECOVERY AGENTS FOR EFS

GET READY. To add new users as recovery agents, assign the EFS recovery certificates issued by the enterprise CA to the user account, and then perform the following steps:

1. Log in as the DRA account.
2. Open the Group Policy Management console.
3. Expand Forest, Domains, and then the name of your domain.
4. Right-click the Default Domain Policy and click Edit.
5. Expand Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\.
6. Right-click Encrypting File System, and select Create Data Recovery Agent.
7. Click Encrypting File System and notice the certificates that are displayed (see Figure 6-1).
8. Close the Group Policy Editor.
9. Close Group Policy Management console.

Figure 6-1

Viewing the Encrypting File System certificates

Managing EFS Certificates

The first time you encrypt a folder or file, an encryption certificate is automatically created. If your certificate and key are lost or damaged and you don't have a backup, you won't be able to use the files that you have encrypted. Therefore, you should back up your encryption certificate.

BACK UP AN EFS CERTIFICATE

GET READY. To back up your EFS certificate, perform the following steps:

1. Open a command prompt.
2. Execute the `certmgr.msc` command. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. The certmgr console opens (see Figure 6-2).

Figure 6-2

Opening the certmgr console

3. In the left pane, double-click Personal, and then click Certificates.
4. In the main pane, right-click the certificate that lists *Encrypting File System under Intended Purposes*. Select All Tasks, and then click Export. If there is more than one EFS certificate, you should back up all of them one by one.
5. When the *Certificate Export Wizard* starts, click Next.
6. On the *Export Private Key* page, click Yes, export the private key, and then click Next.
7. On the *Export File Format* page, click Personal Information Exchange—PKCS #12 (.PFX), and then click Next.
8. On the *Security* page, select the Password checkbox, and type in the password in the *Password* and *Confirm password* text boxes. Click Next.
9. On the *File to Export* page, type a name for the file and the location (include the whole path) or click Browse, navigate to a location, type a filename, and then click Next.
10. Click Next, and then click Finish.
11. When the export is successful, click OK.

You should then place the certificate in a safe place.

RESTORE AN EFS CERTIFICATE

GET READY. To restore your EFS certificate, perform the following steps:

1. Open a command prompt.
2. Execute the `certmgr.msc` command. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the left pane, double-click Personal, and then click Certificates.
4. Right-click Certificates, select All Tasks, and then select Import.
5. When the *Certificate Import Wizard* starts, click Next.
6. On the *File to Import* page, specify the path and name of the certificate, and click then Next.

7. If it asks for a password, provide the password and click Next.
8. On the *Certificate Store* page, click Next.
9. On the *Completing the Certificate Import Wizard* page, click Finish.
10. When the import is successful, click OK.

Encrypting Files with BitLocker

Unlike EFS, BitLocker allows you to encrypt the entire volume. Therefore, if a drive or laptop is stolen, the data is still encrypted even if the thief installs it in another system for which he is an administrator.

BitLocker Drive Encryption (BDE) is the feature that can use a computer's ***Trusted Platform Module (TPM)***, which is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft. BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at startup, and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. BitLocker Drive Encryption also stores measurements of core operating system files in the TPM.

The system requirements of BitLocker are:

- Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk, you must have one of the following:
  - A computer with TPM. If your computer was manufactured with TPM version 1.2 or higher, BitLocker stores its key in the TPM.
  - A removable USB memory device, such as a USB flash drive. If your computer doesn't have TPM version 1.2 or higher, BitLocker stores its key on the flash drive.
- Have at least two partitions: a system partition (contains the files needed to start your computer and must be at least 350 MB for computers running Windows 8) and an operating system partition (contains Windows). The operating system partition is encrypted, and the system partition remains unencrypted so that your computer can start. If your computer doesn't have two partitions, BitLocker creates them for you. Both partitions must be formatted with the NTFS file system.
- Your computer must have a BIOS that is compatible with TPM and supports USB devices during computer startup. If this is not the case, you need to update the BIOS before using BitLocker.

BitLocker supports NTFS, FAT16, FAT32 and ExFAT on USB, Firewire, SATA, SAS, ATA, IDE, and SCSI drives. It does not support CD File System, iSCSI, Fiber Channel, eSATA, and Bluetooth. BitLocker also does not support dynamic volumes; it supports only basic volumes.

BitLocker has five operational modes for OS drives, which define the steps involved in the system boot process. These modes, in a descending order from the most to least secure, are as follows:

- **TPM + startup PIN + startup key:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a personal identification number (PIN) and insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup key:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.

- **TPM + startup PIN:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a PIN before the system can unlock the BitLocker volume and complete the system boot sequence.
- **Startup key only:** The BitLocker configuration process stores a startup key on a USB flash drive, which the administrator must insert each time the system boots. This mode does not require the server to have a TPM chip, but it must have a system BIOS that supports access to the USB flash drive before the operating system loads.
- **TPM only:** The system stores the BitLocker volume encryption key on the TPM chip, and accesses it automatically when the chip has determined that the boot environment is unmodified. This unlocks the protected volume and the computer continues to boot. No administrative interaction is required during the system boot sequence.

When you use BitLocker on fixed and removable data drives that are not the OS volume, you can use one of the following:

- Password
- Smart card
- Automatic Unlock

When you enable BitLocker using the BitLocker Drive Encryption control panel, you can select the *TPM + startup key, TPM + startup PIN,* or *TPM only* option. To use the *TPM + startup PIN + startup key* option, you must first configure the *Require additional authentication at startup* Group Policy setting, found in the Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives container.

CONFIGURING BITLOCKER ENCRYPTION

Before you can use BitLocker on a server running Windows Server 2012 R2, you must first install BitLocker using Server Manager. You can then determine whether you have TPM and turn on BitLocker.

INSTALL BITLOCKER

GET READY. To install BitLocker, perform the following steps:

1. Click the Server Manager button on the task bar to open Server Manager.
2. At the top of Server Manager, select Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install BitLocker to, and then click Next.
6. On the *Select server roles* page, click Next.
7. On the *Select features page*, select BitLocker Drive Encryption (see Figure 6-3).

Figure 6-3

Using the Select Features page

8. When the *Add Roles and Features Wizard* dialog box appears, click Add Features.
9. On the *Select Features* page, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When BitLocker is installed, click Close.
12. Reboot Windows.

DETERMINE WHETHER YOU HAVE TPM

GET READY. To find out whether your computer has Trusted Platform Module (TPM) security hardware, perform the following steps:

1. Open the Control Panel.
2. Click System and Security and click BitLocker Drive Encryption. The *BitLocker Drive Encryption* window opens.
3. In the left pane, click TPM Administration. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

The TPM Management on Local Computer snap-in tells you whether your computer has the TPM security hardware. If your computer doesn't have it, you'll need a removable USB memory device to turn on BitLocker and store the BitLocker startup key that you need whenever you start your computer.

TURN ON BITLOCKER

GET READY. To turn on BitLocker, perform the following steps:

1. Click the Start button, and then click the Control Panel.
2. Click System and Security and click BitLocker Drive Encryption. The *BitLocker Drive Encryption* window opens.

3. Click Turn on BitLocker for the volume that you want to encrypt. A *BitLocker Drive Encryption (X:)* window opens.

MORE INFORMATION

If your computer has a TPM chip, Windows provides a Trusted Platform Module (TPM) Management console that you can use to change the chip's password and modify its properties.

4. On the *Choose how you want to unlock this drive* page, select the Use a password to unlock the drive. Type a password in the *Enter your password* and *Reenter your password* text boxes, and then click Next.
5. On the *How do you want to back up your recovery key?* page, click Save to a file option.
6. When the *Save BitLocker recovery key as* dialog box appears, click Save.
7. After the file is saved, make sure the key is stored in a safe place. Then click Next.
8. On the *Choose how much of your drive to encrypt* page, select either Encrypt used disk space only or the Encrypt entire drive option, and then click Next.
9. On the *Are you ready to encrypt this drive?* page, click Start encrypting.
10. When the drive is encrypted, click Close.

When the encryption process is complete, you can open the BitLocker Drive Encryption Control Panel to ensure that the volume is encrypted, or turn off BitLocker, such as when performing a BIOS upgrade or other system maintenance.

The BitLocker Control Panel applet enables you to recover the encryption key and recovery password at will. You have the following options available after you use BitLocker to encrypt a drive:

- Back up recovery key
- Change password
- Add smart card
- Turn off Bit Locker

You should consider carefully how to store this information, because it allows access to the encrypted data. It is also possible to escrow this information into Active Directory.

Standard users can change the password or PIN if they know the current PIN or password. By default, a user has five attempts to type in the current PIN or password. When this happens, the administrator has to reset the volume PIN or password, or the system needs to be rebooted. To make sure that password or pin is not too easy to guess, you can define how complex the password is using a group policy. To define the complexity, enable and configure the Configure use of passwords for fixed data drives settings found in Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\.

CONFIGURING BITLOCKER POLICIES

If for some reason, the user loses the startup key and/or startup PIN needed to boot a system with BitLocker, the user can supply the recovery key created during the BitLocker configuration process and regain access to the system. If the user loses the recovery key, you can use a data recovery agent designated within Active Directory to recover the data on the drive.

Similar to EFS, a data recovery agent is a user account that is an administrator who is authorized to recover BitLocker drives for an entire organization with a digital certificate on a smart card. In most cases, administrators of Active Directory Domain Services (AD DS) networks use DRAs to ensure access to their BitLocker-protected systems while avoiding maintaining a large number of individual keys and PINs.

It is a little bit more complicated to create a DRA for BitLocker than it is for EFS. To create a DRA for BitLocker, you must do the following:

- Add the user account you want to designate to the Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption container in a GPO or to the system's Local Security Policy.
- Configure the Provide the unique identifiers for your organization policy setting in the Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption container with unique identification fields for your BitLocker drives (see Figure 6-4).
- Enable DRA recovery for each type of BitLocker resource you want to recover (see Figure 6-5):
  - Choose how BitLocker-protected operating system drives can be recovered.
  - Choose how BitLocker-protected fixed drives can be recovered.
  - Choose how BitLocker-protected removable drives can be recovered.

Figure 6-4

Configuring the *Provide the unique identifiers for your organization* policy setting

Figure 6-5

Configuring how BitLocker-protected fixed drives can be recovered

Managing BitLocker Certificates

Similar to EFS, you should back up the necessary digital certificates and keys. You can use the Certificate Management console to back up any digital certificates, such as DRA certificates. It has also been mentioned earlier that you can use the Control Panel to back up the recovery key.

You can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives and the TPM to AD DS. Recovery information includes the recovery password for each BitLocker-protected drive, the TPM owner password, and the information required to identify which computers and drives the recovery information applies to. To store information in Active Directory, you can enable the *Store BitLocker Recovery Information* in AD DS.

MORE INFORMATION

By default, Windows Server 2012 R2 does not have the BitLocker DRA template. Therefore, if you need information on creating the BitLocker DRA template, visit Microsoft's TechNet Blogs.

Configuring the Network Unlock Feature

Network Unlock provides an automatic unlock of operating system volumes at system reboot when connected to a trusted wired corporate network.

The hardware and software requirements for Network Unlock include:

- Windows 8 or 8.1 installation on UEFI firmware with UEFI DHCP drivers
- BitLocker Network Unlock feature using Server Manager
- Windows Server 2012 R2 Windows Deployment Services (WDS) role
- DHCP server, separate from the WDS server and the Domain Controller
- A Network Unlock certificate
- Network Unlock Group Policy settings configured (see Figure 6-6)

Figure 6-6

Configuring Network Unlock Group Policy settings

Network Unlock works similarly to the TPM plus startup key, but instead of reading a startup key from a USB device, Network Unlock uses an unlock key. The key is composed of a key that is stored on the machine's local TPM and a key that Network Unlock receives from Windows Deployment Services. If the WDS server is unavailable such as when you are not connected directly to the organization's network, BitLocker cannot communicate with a WDS server and instead displays the startup key unlock screen.

The client requires a DHCP driver implemented in the Unified Extensible Firmware interface. As the server boots, it gets the key from the WDS server using DHCP. BitLocker Network Unlock is installed on the server with WDS server role installed. To protect the keys being transferred over the network, the WDS server needs a special X.509 certificate that must be installed on all that clients that use Network Unlock.

Business Case Scenarios

Scenario 6-1: Protecting the Laptop Computer

You have just purchased 75 new laptops that will be given to the sales team and 50 new laptops that will be given to the engineering team. Last year, a person from the marketing department left her computer at the hotel, which had details about upcoming products. This information was leaked to the Internet. What can you do to make sure that if this happens again, the information is still safe?

Scenario 6-2: Accessing EFS-Encrypted Files

You have a user who encrypts many of his data files with EFS. So his manager tries to open the files but cannot read the files because the user does not have the correct key. What can you do to unlock these files?

7 LESSON

Configuring Advanced Audit Policies

Enabling and Configuring Auditing

THE BOTTOM LINE

Security can be divided into three areas. Authentication is used to prove the identity of a user. Authorization gives access to the user who was authenticated. To complete the security picture, you need to enable ***auditing*** so that you can have a record of the users who have logged in, what the users accessed or tried to access, and what action the users performed such as rebooting, shutting down a computer, or accessing a file.

It is important that you protect your information and service resources from people who should not have access to them, and at the same time, it's important you make those resources available to authorized users. Along with authentication and authorization, you need to enable auditing so that you can have a record of the following:

- Who has successfully logged in
- Who has attempted to log in but failed
- Who has made changes to accounts in Active Directory
- Who has accessed or changed certain files
- Who has used a certain printer
- Who restarted a system
- Who has made system changes

Using auditing logs enables you to determine whether any security breaches have occurred and to what extent.

Implementing Auditing Using Group Policies

To enable auditing, you specify what types of system events to audit using Group Policy or the local security policy (Computer Settings\Policies\Security Settings\Local Policies\Audit Policy).

Although it is easy to enable auditing for everything, it is usually not a good idea. Any time that you enable auditing, you need to select only what you need because of the following reasons:

- High levels of auditing can affect the performance of the computer that you audit.
- When you search through the security logs, you will find far too many events, which can make it more difficult for you to find the potential problems you need to find.
- The logs quickly fill up, replacing older events with newer events.

Most audit settings require you to enable only specific audit settings. However, object auditing is a little bit more complex. After you enable object access auditing, you have to enable auditing on the specific object that you want to enable. These objects include registry objects, files, folders, and printers.

When you enable object auditing, you generate many other events that also get recorded including Audit Filtering Platform Connection and Audit Filtering Platform Packet Drop, which shows packets that get connected or dropped at the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) level. To cut these packets, you can use the advanced audit policy Configuration for Object Access or the `AuditPol.exe` command not to record these events. Advanced audit policy configuration and `AuditPol` are discussed in the following section.

IMPLEMENTING AN AUDIT POLICY

AUDIT ACCOUNT LOGON

GET READY. To audit account logon successes and failures, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management to open the *Group Policy Management console*.
3. Expand the Domain Controllers to show the *Default Domain Controllers Policy*. Then right-click the Default Domain Control Default Policy and click Edit. *Group Policy Management Editor* appears.
4. Expand Computer Configuration, Windows Settings, Security Settings, Local Policies, and select Audit Policy.
5. Double-click Audit account logon events. The *Audit account logon events Properties* dialog box opens.
6. Select Define these policy settings and select both Success and Failure.
7. Click OK to close the *Audit account logon events Properties* dialog box.

IMPLEMENTING OBJECT ACCESS AUDITING USING GROUP POLICIES

Auditing NTFS files, NTFS folders, and printers is a two-step process. You must first enable object access using Group Policy. Then you must specify which objects you want to audit.

AUDIT FILES AND FOLDERS

GET READY. To audit files and folders, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management to open the *Group Policy Management console*.
3. Right-click a group policy and click Edit. The *Group Policy Management Editor* opens.
4. Expand Computer Configuration, Windows Settings, Security Settings, Local Policies, and select Audit Policy.
5. Double-click Audit object access. The *Audit object access Properties* dialog box appears.
6. Select Define these policy settings and select both Success and Failure.
7. Click OK to close the *Audit account logon events Properties* dialog box.
8. Close the *Group Policy Management Editor* and *Group Policy Management*.
9. Open Windows Explorer.

10. Right-click the file or folder that you want to audit, click Properties, and then click the Security tab.
11. Click the Advanced button. The *Advanced Security Settings for Updates* dialog box opens.
12. In the *Advanced Security Settings for Updates* dialog box, click the Auditing tab.
13. To add an auditing entry, click Add. The *Auditing Entry for Updates* dialog box opens (see Figure 7-1).

Figure 7-1

Opening the *Auditing Entry for Updates* dialog box

14. To specify a user or group, click Select a principal. When the *Select User, Computer, Service Account, or Group* dialog box opens, type a name for a *username* or *group*, and then click OK.
15. For *Type*, select Success, Fail, or All.
16. Specify the permissions that you want to audit by selecting or deselecting the appropriate permission.
17. Click OK to close the *Auditing Entry for Updates* dialog box.
18. Click OK to close the *Advanced Security Settings for Updates* dialog box.
19. Click OK to close the *Properties* dialog box.

AUDIT PRINTER EVENTS

GET READY. To audit printer events, make sure the audit object access is enabled. Then, perform the following steps:

1. Open the Control Panel and click View devices and printers.
2. Right-click a printer and select Printer properties.
3. Select the Security tab.
4. On the *Security* tab, click Advanced. The *Advanced Security Settings for Microsoft XPS Document Writer* dialog box opens.
5. Select the Auditing tab.
6. Click the Add button. The *Auditing Entry for Microsoft XPS Document Writer* dialog box opens.
7. To specify a user or group, click Select a principal. When the *Select User, Computer, Service Account, or Group* dialog box opens, type a name for a *username* or *group,* and then click OK.
8. For Type, select Success, Fail, or All.
9. Specify the permissions that you want to audit by selecting or deselecting the appropriate permission.
10. Click OK to close the *Auditing Entry for Microsoft XPS Document Writer* dialog box.
11. Click OK to close the *Advanced Security Settings for Microsoft XPS Document Writer* dialog box.
12. Click OK to close the *Properties* dialog box.

By default, when a group policy is applied to an Active Directory domain or OU, the group policy is inherited by all OUs at the lower levels. However, inherited policy can be overridden by a Group Policy Object (GPO) that is linked at a lower level.

Implementing Advanced Audit Policy Settings

Starting with Windows Server 2008 R2, Windows introduced ***advanced audit policy settings***, which enable you to have more control over what events get recorded by using multiple subsettings instead of the traditional nine basic audit settings. Windows Server 2008 R2 introduced 53 subsettings. Windows Server 2012 has 56 subsettings and Windows Server 2012 R2 has 58 subsettings. As result of using advanced audit policy settings, you cut down the number of log entries, so that you can focus on what is important to you.

IMPLEMENTING ADVANCED AUDIT POLICY SETTINGS USING GROUP POLICIES

To access a new policy, open Group Policy Editor for a group policy and go to Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration. Tables 7-1 through 7-9 show the nine primary groups with the subsettings and common events generated by the subsettings.

Table 7-1

Account Logon

Setting	Description	Common Events:
Audit Credential Validation	Generates audit events on credentials submitted for a user account logon request. Events show on the domain controller for domain accounts and on the local computer for local accounts. Note: Event volume: High on domain controllers	4774: An account was mapped for logon. 4775: An account could not be mapped for logon. 4776: The domain controller attempted to validate the credentials for an account. 4777: The domain controller failed to validate the credentials for an account.
Audit Kerberos Authentication Service	Generates audit events for Kerberos authentication ticket-granting ticket (TGT) requests. Note: Event volume: High on Kerberos Key Distribution Center (KDC) servers	4768: A Kerberos authentication ticket (TGT) was requested. 4771: Kerberos pre-authentication failed. 4772: A Kerberos authentication ticket request failed.
Audit Kerberos Service Ticket Operations	Generates security audit events for Kerberos service ticket requests. Note: Event volume: High on a domain controller that is a Key Distribution Center	4769: A Kerberos service ticket was requested. 4770: A Kerberos service ticket was renewed.
Audit Other Account Logon Events	Generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets when working with Remote Desktop session, locking and unlocking a workstation, working with a screen saver, and accessing a wireless network granted to a user or computer account.	4649: A replay attack was detected. 4778: A session was reconnected to a Window station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network.

Table 7-2

Account Management

Setting	Description	Common Events:
Audit Application Group Management	Generates audit events when application group management tasks are performed, such as when an application group is created, changed, or deleted, or a member is added to or removed from an application group.	4783: A basic application group was created. 4784: A basic application group was changed. 4790: An LDAP query group was created.
Audit Computer Account Management	Generates audit events when a domain computer account is created, changed, or deleted.	4741: A computer account was created. 4742: A computer account was changed. 4743: A computer account was deleted.
Audit Distribution Group Management	Generates audit events when a distribution group is created, changed, deleted, or when a member is added to or removed from a distribution group.	4744: A local distribution group was created. 4746: A member was added to a local distribution group. 4747: A member was removed from a local distribution group. 4748: A local distribution group was deleted. 4749: A global distribution group was created. 4750: A global distribution group was changed. 4751: A member was added to a global distribution group. 4752: A member was removed from a global distribution group. 4753: A global distribution group was deleted. 4759: A universal distribution group was created. 4760: A security-disabled universal group was changed. 4761: A member was added to a universal distribution group. 4762: A member was removed from a universal distribution group.
Audit Other Account Management Events	Generates user account management audit events when the password hash of an account is accessed, when the Password Policy Checking application programming interface (API) is called or when changes are made to the domain password policy or domain account lockout policy.	4782: The password hash for an account was accessed. 4793: The Password Policy Checking API was called.

(continued)

Table 7-2

(continued)

Setting	Description	Common Events:
Audit Security Group Management	Generates audit events when a security group is created, changed, or deleted, a member is added to or removed from a security group, or a group's type is changed.	4727: A global security group was created. 4728: A member was added to a global security group. 4729: A member was removed from a global security group. 4730: A global security group was deleted. 4731: A local security group was created. 4732: A member was added to a local security group. 4733: A member was removed from a local security group. 4734: A local security group was deleted. 4735: A local security group was changed. 4737: A global security group was changed. 4754: A universal security group was created. 4755: A universal security group was changed. 4756: A member was added to a security-enabled universal group. 4757: A member was removed from a universal security group. 4758: A security-enabled universal group was deleted. 4764: A group's type was changed.
Audit User Account Management	Generates audit events when the following user account management tasks are performed: A user account is created, changed, deleted, renamed, disabled, enabled, locked out, or unlocked. A user account password is set or changed. Security identifier (SID) history is added to a user account. The Directory Services Restore Mode password is set. Permissions on accounts that are members of Administrators groups are changed. Credential Manager credentials are backed up or restored.	4720: A user account was created. 4722: A user account was enabled. 4723: An attempt was made to change an account's password. 4725: A user account was disabled. 4726: A user account was deleted. 4738: A user account was changed. 4740: A user account was locked out. 4767: A user account was unlocked. 4780: The ACL was set on accounts that are members of Administrators groups. 4781: The name of an account was changed.

Table 7-3

Detailed Tracking

Setting	Description	Common Events:
Audit DPAPI Activity	Generates audit events when encryption or decryption calls are made into the data protection application interface (DPAPI), which is used to protect secret information such as stored passwords and key information.	4692: Backup of data protection master key was attempted. 4693: Recovery of data protection master key was attempted. 4694: Protection of auditable protected data was attempted. 4695: Unprotection of auditable protected data was attempted.
Audit Process Creation	Generates audit events when a process is created (starts) and the name of the program or user that created it.	4688: A new process has been created. 4696: A primary token was assigned to a process.
Audit Process Termination	Generates audit events when an attempt is made to end a process.	4689: A process has exited.
Audit RPC Events	Generates audit events when inbound remote procedure call (RPC) connections are made.	5712: A remote procedure call (RPC) was attempted.

Table 7-4

DS Access

Setting	Description	Common Events:
Audit Detailed Directory Service Replication	Generates security audit events with detailed tracking information about the data that is replicated between domain controllers. Note: Event volume: These events can create a very high volume of event data.	4928: An Active Directory replica source naming context was established. 4929: An Active Directory replica source naming context was removed. 4934: Attributes of an Active Directory object were replicated. 4935: Replication failure begins. 4937: A lingering object was removed from a replica.
Audit Directory Service Access	Generates events when an Active Directory Domain Services (AD DS) object is accessed for those objects that have configured system access control lists (SACLs) in the method specified. Note: Audit events are generated only on objects with configured SACLs and only when they are accessed in a manner that matches the SACL settings.	4662: An operation was performed on an object.

(continued)

Table 7-4

(continued)

Setting	Description	Common Events:
Audit Directory Service Changes	Generates audit events when changes are made to objects in Active Directory Domain Services (AD DS) including when objects are created, deleted, modified, moved, or undeleted. Note: Directory Service Changes auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed.	5136: A directory service object was modified. 5137: A directory service object was created. 5138: A directory service object was undeleted. 5139: A directory service object was moved. 5141: A directory service object was deleted.
Audit Directory Service Replication	Generates audit events when replication between two domain controllers begins and ends.	4932: Synchronization of a replica of an Active Directory naming context has begun. 4933: Synchronization of a replica of an Active Directory naming context has ended.

Table 7-5

Logon/Logoff

Setting	Description	Common Events:
Audit Account Lockout	Generated by a failed attempt to log on to an account that is locked out.	4625: An account failed to log on.
Audit User/Device Claims	Allows you to audit user and device claims information in the user's logon tokens. This setting was introduced with Windows Server 2012.	
Audit IPsec Extended Mode	Generates audit events for the results of the Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations.	4978: During Extended Mode negotiation, IPsec received an invalid negotiation packet. 4979: IPsec Main Mode and Extended Mode security associations were established. 4980: IPsec Main Mode and Extended Mode security associations were established. 4984: An IPsec Extended Mode negotiation failed.

(continued)

Table 7-5

(continued)

Setting	Description	Common Events:
Audit IPsec Main Mode	Generates events for the results of the IKE protocol and AuthIP during Main Mode negotiations.	4650: An IPsec Main Mode security association was established. 4651: An IPsec Main Mode security association was established. 4652: An IPsec Main Mode negotiation failed. 5049: An IPsec Security Association was deleted. 5453: An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.
Audit IPsec Quick Mode	Generates audit events for the results of the IKE protocol and AuthIP during Quick Mode negotiations.	4977: During Quick Mode negotiation, IPsec received an invalid negotiation packet. 5451: An IPsec Quick Mode security association was established.
Audit Logoff	Generates audit events when logon sessions are terminated.	4634: An account was logged off. 4647: User initiated logoff.
Audit Logon	Generates audit events when a user attempts to log on to a computer including logon success and failure, logon attempts by using explicit credentials, and security identifiers (SIDs) are filtered.	4624: An account successfully logged on. 4625: An account failed to log on. 4648: A logon was attempted using explicit credentials.
Audit Network Policy Server	Generates audit events for RADIUS (IAS) and Network Access Protection (NAP) activity on user access requests (Grant, Deny, Discard, Quarantine, Lock, and Unlock).	6272: Network Policy Server granted access to a user. 6273: Network Policy Server denied access to a user. 6276: Network Policy Server quarantined a user. 6278: Network Policy Server granted full access to a user because the host met the defined health policy.

(continued)

Table 7-5

(continued)

Setting	Description	Common Events:
Audit Other Logon/Logoff Events	Generates audit events for other logon or logoff events, such as the following: • A Remote Desktop session disconnects or connects. • A workstation is locked or unlocked. • A screen saver is invoked or dismissed. • A replay attack is detected. This event indicates that a Kerberos request was received twice with identical information. • A user or computer is granted access to a wireless network. • A user or computer is granted access to a wired 802.1x network.	4649: A replay attack was detected. 4778: A session was reconnected to a Window Station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network.
Audit Special Logon	Generates audit events when a special logon is used or a member of a special group logs on.	4964: Special groups have been assigned to a new logon.

Table 7-6

Object Access

Setting	Description	Common Events:
Audit Application Generated	Generates audit events when applications attempt to use the Windows Auditing APIs.	4665: An attempt was made to create an application client context. 4666: An application attempted an operation: 4667: An application client context was deleted. 4668: An application was initialized.
Audit Certification Services	Generates events when Active Directory Certificate Services (ADCS) operations are performed, such as the following: • ADCS starts. • ADCS shuts down. • ADCS is backed up or is restored. • Certificate revocation list (CRL)-related tasks are performed. • Certificates are requested, issued, or revoked. • ADCS templates are modified.	4868: The Certificate Manager denied a pending certificate request. 4870: Certificate Services revoked a certificate. 4886: Certificate Services received a certificate request. 4887: Certificate Services approved a certificate request and issued a certificate. 4888: Certificate Services denied a certificate request. 4889: Certificate Services set the status of a certificate request to pending.

(continued)

Table 7-6

(continued)

Setting	Description	Common Events:
		4895: Certificate Services published the CA certificate to ADDS. 4896: One or more rows have been deleted from the certificate database. 4898: Certificate Services loaded a template.
Audit Detailed File Share	Records attempts to access files and folders on a shared folder. It logs an event every time a file or folder is accessed. Note: Event volume: High on a file server or domain controller because of SYSVOL network access required by Group Policy.	5145: A network share object was checked to see whether the client can be granted desired access.
Audit File Share	Records events when a file share is accessed. Note: Event volume: High on a file server or domain controller because of SYSVOL network access required by Group Policy.	5140: A network share object was accessed. 5142: A network share object was added. 5143: A network share object was modified. 5144: A network share object was deleted.
Audit File System	Records user attempts to access file system objects as specified by the configured SACLs, and only if the type of access requested (such as Write, Read, or Modify) and the account making the request match the settings in the SACL.	4664: An attempt was made to create a hard link. 4985: The state of a transaction has changed. 5051: A file was virtualized.
Audit Filtering Platform Connection	Generates audit events when connections are allowed or blocked by the Windows Filtering Platform, such as the following: • The Windows Firewall service blocks an application from accepting incoming connections on the network. • The Windows Filtering Platform allows or blocks a connection. • The Windows Filtering Platform permits or blocks a bind to a local port. • The Windows Filtering Platform permits or blocks the listening of an application or service on a port for incoming connections. Note: Event volume: High	5031: The Windows Firewall Service blocked an application from accepting incoming connections on the network. 5150: The Windows Filtering Platform blocked a packet. 5151: A more restrictive Windows Filtering Platform filter has blocked a packet. 5154: The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections. 5155: The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections. 5156: The Windows Filtering Platform has allowed a connection. 5157: The Windows Filtering Platform has blocked a connection. 5158: The Windows Filtering Platform has permitted a bind to a local port. 5159: The Windows Filtering Platform has blocked a bind to a local port.

(continued)

Table 7-6

(continued)

Setting	Description	Common Events:
Audit Filtering Platform Packet Drop	Records packets that are dropped by the Windows Filtering Platform.	5152: The Windows Filtering Platform blocked a packet. 5153: A more restrictive Windows Filtering Platform filter has blocked a packet.
Audit Handle Manipulation	Generates audit events when a handle to an object is opened or closed. Note: Event volume: High, depending on how SACLs are configured.	4656: A handle to an object was requested. 4658: The handle to an object was closed. 4690: An attempt was made to duplicate a handle to an object.
Audit Kernel Object	Records attempts to access the system kernel, which includes mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events.	4659: A handle to an object was requested with intent to delete. 4660: An object was deleted. 4661: A handle to an object was requested. 4663: An attempt was made to access an object.
Audit Other Object Access Events	Generates audit events for the management of Task Scheduler jobs or COM+ objects.	4698: A scheduled task was created. 4699: A scheduled task was deleted. 4700: A scheduled task was enabled. 4701: A scheduled task was disabled. 4702: A scheduled task was updated. 5148: The Windows Filtering Platform has detected a Denial of Service (DoS) attack and entered a defensive mode; packets associated with this attack will be discarded. 5149: The DoS attack has subsided and normal processing is being resumed. 5888: An object in the COM+ Catalog was modified. 5889: An object was deleted from the COM+ Catalog. 5890: An object was added to the COM+ Catalog.
Audit Registry	Records user attempts to access registry objects based on the SACLs.	4657: A registry value was modified. 5039: A registry key was virtualized.
Audit Removable Storage	Records user attempts to access file system objects on a removable storage device. This setting was introduced with Windows Server 2012.	4663: Successful attempts to access a removal storage device. 4656: Failed attempts to access removal storage device.

(continued)

Table 7-6

(continued)

Setting	Description	Common Events:
Audit SAM	Generated by attempts to access Security Accounts Manager (SAM) objects.	4659: A handle to an object was requested with intent to delete. 4660: An object was deleted. 4661: A handle to an object was requested. 4663: An attempt was made to access an object.
Audit Central Access Policy Staging	Records access requests where the permission granted or denied by a proposed policy differs from the current central access policy on an object. This setting was introduced with Windows Server 2012.	

Table 7-7

Policy Change

Setting	Description	Common Events:
Audit Audit Policy Change	Generates audit events when changes are made to audit policy.	4715: The audit policy (SACL) on an object was changed. 4719: The system audit policy was changed. 4817: Auditing settings on an object were changed. 4907: Auditing settings on an object were changed.
Audit Authentication Policy Change	Generates audit events when changes are made to authentication policy.	4713: Kerberos policy was changed. 4739: Domain Policy was changed. 4865: A trusted forest information entry was added. 4866: A trusted forest information entry was removed. 4867: A trusted forest information entry was modified.
Audit Authorization Policy Change	Generates audit events when the following changes are made to the authorization policy.	4704: A user right was assigned. 4705: A user right was removed.
Audit Filtering Platform Policy Change	Generates audit events for IPsec services status, changes to IPsec settings, status and changes to the Windows Filtering Platform engine and providers, and changes to the IPsec Policy Agent service activities.	4709: IPsec Services was started. 4710: IPsec Services was disabled.

(continued)

Table 7-7

(continued)

Setting	Description	Common Events:
Audit MPSSVC Rule-Level Policy Change	Generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe), which is used by Windows Firewall.	4946: A change has been made to Windows Firewall exception list. A rule was added. 4947: A change has been made to Windows Firewall exception list. A rule was modified. 4948: A change has been made to Windows Firewall exception list. A rule was deleted. 4950: A Windows Firewall setting has changed. 4954: Windows Firewall Group Policy settings have changed. The new settings have been applied. 4956: Windows Firewall has changed the active profile. 4957: Windows Firewall did not apply the specified rule.
Audit Other Policy Change Events	Generates events for security policy changes that are not otherwise audited in the Policy Change category, such as Trusted Platform Module (TPM) configuration changes, Kernel-mode cryptographic self tests, Cryptographic provider operations, and Cryptographic context operations or modifications.	4670: Permissions on an object were changed. 4909: The local policy settings for the TPM Base Services (TBS) were changed. TPM is short for Trusted Platform Module. 4910: The group policy settings for the TBS were changed. 5447: A Windows Filtering Platform filter has been changed. 6144: Security policy in the group policy objects has been applied successfully. 6145: One or more errors occurred while processing the security policy in the group policy objects.

Table 7-8

Privilege Use

Setting	Description	Common Events:
Audit Non-Sensitive Privilege Use	Generated when sensitive privileges (user rights) such as the following are used: • Act as part of the operating system • Back up files and directories • Create a token object • Debug programs	4672: Special privileges assigned to new logon. 4673: A privileged service was called. 4674: An operation was attempted on a privileged object.

(continued)

Table 7-8

(continued)

Setting	Description	Common Events:
	• Enable computer and user accounts to be trusted for delegation • Generate security audits • Impersonate a client after authentication • Load and unload device drivers • Manage auditing and security log • Modify firmware environment values • Replace a process-level token • Restore files and directories • Take ownership of files or other objects	
Audit Sensitive Privilege Use	Generated by the use of non-sensitive privileges (user rights), such as access this computer from the network, add workstation to domain, allow logon locally, change the system time, create a page file, and shut down the system.	4672: Special privileges assigned to new logon. 4673: A privileged service was called. 4674: An operation was attempted on a privileged object.

Table 7-9

System

Setting	Description	Events:
Audit IPsec Driver	Audits the activities of the IPsec driver, including the startup and shutdown of IPsec services, packets dropped due to integrity check failure, and packets dropped due to replay check failure.	4960: IPsec dropped an inbound packet that failed an integrity check. 4961: IPsec dropped an inbound packet that failed a replay check. 4962: IPsec dropped an inbound packet that failed a replay check. 4963: IPsec dropped an inbound clear text packet that should have been secured. 5478: IPsec Services has started successfully. 5479: IPsec Services has been shut down successfully.

(continued)

Table 7-9

(continued)

Setting	Description	Events:
Audit Other System Events	Records the events of startup and shutdown of the Windows Firewall service and driver, security policy processing by the Windows Firewall service, cryptography key file operations, and migration operations.	5024: The Windows Firewall Service has started successfully. 5025: The Windows Firewall Service has been stopped. 5030: The Windows Firewall Service failed to start. 5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. 5033: The Windows Firewall Driver has started successfully. 5034: The Windows Firewall Driver has been stopped. 5035: The Windows Firewall Driver failed to start.
Audit Security State Change	Audits changes in the security state of a system, including system startup and shutdown, change of system time, and system recovery from CrashOnAuditFail.	4608: Windows is starting up. 4609: Windows is shutting down. 4616: The system time was changed. 4621: Administrator recovered system from CrashOnAuditFail.
Audit Security System Extension	Audits events related to security system extensions, including when a security extension code is loaded (such as an authentication, notification, or security package) or a service is installed.	4610: An authentication package has been loaded by the Local Security Authority. 4697: A service was installed in the system.
Audit System Integrity	Audit events that violate the integrity of the security subsystem include the following: • Auditing events are lost due to a failure of the auditing system. • A process uses an invalid local procedure call (LPC) port in an attempt to impersonate a client, and a remote procedure call (RPC) integrity violation is detected. • A code integrity violation with an invalid hash value of an executable file is detected. • Cryptographic tasks are performed.	4612: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. 4615: Invalid use of LPC port. 5056: A cryptographic self-test was performed. 5060: Verification operation failed.

REMOVING ADVANCED AUDIT POLICY CONFIGURATION

It is not recommended you use both basic audit policy settings and advanced audit policy settings because they may cause conflicts or erratic behavior. By default, when you apply Advanced Audit Configuration Policy, the basic audit policies are ignored.

If you need to go back to the basic audit settings after enabling Advanced Audit Policy Configuration, you need to perform the following:

1. Set all *Advanced Audit Policy* subcategories to `Not configured`.
2. Delete the `%systemroot%\security\audit\audit.csv` on the domain controllers for group policies and on the local computer for local policies.
3. Reconfigure and apply the *basic audit policy settings*.

Implementing Auditing Using AuditPol.exe

To manage auditing at the command prompt or by creating scripts, you use the ***AuditPol.exe*** command, which displays information about and performs functions to manipulate audit policies.

The syntax for `AuditPol.exe` includes the following commands:

- `/get`: Displays the current audit policy.
- `/set`: Sets the audit policy.
- `/list`: Displays selectable policy elements.
- `/backup`: Saves the audit policy to a file.
- `/restore`: Restores the audit policy from a file that was previously created by using `auditpol /backup`.
- `/clear`: Clears the audit policy.
- `/remove`: Removes all per-user audit policy settings and disables all system audit policy settings.
- `/resourceSACL`: Configures global resource SACLs.
- `/?`: Displays help at the command prompt.

`Auditpol.exe` also includes the following subcommands:

- `/user:<username>`: Specifies the security principal for a per-user audit. Specify the username by security identifier (SID) or by name. Requires either the `/category` or `/subcategory` subcommand when used with the `/set` command.
- `/category:<name>`: Specifies one or more auditing categories separated by a pipe (|) and specified by a name or Globally Unique Identifier (GUID).
- `/subcategory:<name>`: Specifies one or more auditing subcategories separated by a pipe (|) and specified by a name or GUID.
- `/success:enable`: Enables success auditing when using the `/set` command.

- `/success:disable`: Disables success auditing when using the `/set` command.
- `/failure:enable`: Enables failure auditing when using the `/set` command.
- `/failure:disable`: Disables failure auditing when using the `/set` command.
- `/file`: Specifies the file to which an audit policy is to be backed up or from which an audit policy is to be restored.

For example, to configure auditing for user account management for success and failed attempts, execute the following command:

```
auditpol.exe /set /subcategory:"user account management" /
success:enable /failure:enable
```

To disable the Filtering Platform Connection successful events, use the following command:

```
auditpol.exe /set /subcategory:"Filtering
Platform Connection" /success:disable
```

To delete the per-user audit policy for all users, reset, or disable the system audit policy for all subcategories, and you want to set the audit policies settings to disable, execute the following command:

```
auditpol.exe /clear
```

If you want to delete the per-user audit policy for all users, reset, or disable the system audit policy for all subcategories, and you want to set all the audit policies settings to disable without a confirmation prompt, execute the following command:

```
auditpol.exe /clear /y
```

To remove the per-user audit policy for the jsmith account, perform the following command:

```
auditpol.exe /remove /user:jsmith
```

To remove the per-user audit policy for all users, perform the following command:

```
auditpol.exe /remove /allusers
```

To see all possible categories and subcategories, execute the following command:

```
auditpol.exe /list /subcategory:*
```

If you want to get an authoritative report on what audit settings are being applied, use the following command:

```
auditpol.exe /get /category:*
```

To back up the audit policy for all users into a .CSV text file called auditpolicy.csv, execute the following command:

```
auditpol.exe /backup /file:C\auditpolicy.csv
```

To restore system audit policy settings from the auditpolicy.csv file, execute the following command:

```
auditpol.exe /restore /file:c:\auditpolicy.csv
```

Creating Expression-Based Audit Policies

Windows Server 2012 R2 features advanced audit policies to implement more detailed and more precise auditing on the file system, including configure global based audit policies and expression-based audit. Expression-based audit policies allow you to specify what to audit based on defined properties or attribute for documents (such as a department or country).

Global Object Access Auditing lets you define computer-wide system access control lists for either the file system or registry. Therefore, instead of manually altering and maintaining SACLs on large sets of shared files or registry entry. In addition, the auditing is implicitly specified, which does not actually modify the files at all.

For example, with Dynamic Access Control, you can define certain attributes that define what a department a file belongs to, such as the Finance department, which is assigned to a large set of files. You would then specify auditing based on the attribute. Dynamic Access Control is discussed in the 70-412 course.

DEFINE GLOBAL OBJECT ACCESS AUDITING

GET READY. To define Global Object Access Auditing, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management to open the *Group Policy Management console*.
3. Right-click a group policy and click Edit. *Group Policy Management Editor* opens.
4. Expand Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit policy\Audit Policies and click Global Object Access Auditing to display the *Global Object Access Auditing* settings (see Figure 7-2).

Figure 7-2

Displaying the Global Object Access Auditing settings

5. Under *Resource Manager*, double-click File System to display the *File system Properties* dialog box.
6. Select Define this policy settings and click Configure. The *Advanced Security Settings for Global File SACL* dialog box opens.
7. In the *Advanced Security Settings for Global File SACL* dialog box, click Add. The *Auditing Entry for Global File SACL* dialog box opens.
8. Click Select a principal. The *Select User, Computer, Service Account, or Group* dialog box opens. Type a name of a user or group in the *Enter the object name to select* box and click OK.

9. For the Type, select Success, Fail, or All.
10. Select the permissions that you want and deselect the permissions that you don't want.
11. Click Add a condition. A condition is added.
12. Select the following options: Resource, Department, Any of, Value, and Finance.
13. Click OK to close the *Auditing Entry for Global File SACL* dialog box.
14. Click OK to close the Advanced Security Settings for Global File SACL dialog box.
15. Click OK to close the *File system Properties* dialog box.
16. Close the *Group Policy Management Editor* and *Group Policy Management*.

Creating Removable Device Audit Policies

In previous versions of Windows, it was difficult to determine whether a user connects a removal storage device such as a USB thumb drive to the computer. Because the USB devices can be used to copy confidential information and might introduce malware to the organization, the organization might want to keep track of who uses removable storage devices.

Organizations can limit or deny users the ability to use removable storage devices by using the ***Removable Storage Access policy***. However, in earlier versions of the Windows and Windows Server operating systems, administrators could not track the use of removable storage devices.

CONFIGURE THE MONITORING OF REMOVABLE STORAGE DEVICES

GET READY. To configure the monitoring of removal storage devices such as USB drives, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management to open the *Group Policy Management console*.
3. In the console tree, right-click a group policy object, and then click Edit.
4. Double-click Computer Configuration, double-click Security Settings, double-click Advanced Audit Policy Configuration, and double-click Object Access.
5. Double-click Audit Removable Storage. The *Audit Removal Storage Properties* dialog box opens.
6. Select the Configure the following audit events check box, select the Success check box, and then click OK.
7. Click OK to close the *Group Policy Management Editor*.

Business Case Scenarios

Scenario 7-1: Establishing an Audit Policy

You just established an audit policy that enables account logon, logon, object access, and account management. However, when you look at the logs, you see a large number of Audit Filtering Platform Connection and Audit Filtering Platform Packet Drop events that consume most of the security logs. What can you do to alleviate this problem?

Scenario 7-2: Monitoring the Use of Mobile Storage Devices

Your manager assigns you the task of seeing how many users use mobile storage devices such as USB thumb drives. What would you use to accomplish this?

Configuring DNS Zones

LESSON 8

Understanding DNS

THE BOTTOM LINE

Domain Name System (DNS) is a naming service that is used by TCP/IP network and is an essential service used by the Internet. Every time a user accesses a web page, the user must type a URL. Before the client communicates with the web server, the client computer needs to use DNS to retrieve the IP address of the web server, similarly to someone using a phone book to find a phone number. When an enterprise client needs to communicate with a corporate server, the enterprise client also uses DNS to find the IP address of the corporate service. The DNS servers are often referred to as ***name servers***.

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the most popular networking protocol suite used in the world and is the same protocol used with the Internet. Of course, the Internet is a worldwide network that links billions of computers. For a client computer or host to communicate on a TCP/IP network, a client must have an IP address.

Traditional IP addresses based on IPv4 were based on a four-byte address written in a four-octet format. Each octet ranges from 0 to 255. An example of an IP address is 24.64.251.189 or 192.168.1.53. Most users would have difficulty remembering hundreds of telephone numbers and hundreds of IP addresses. Naming resolution enables an administrator to assign logical names to a server or network resource by IP address and translates a logical name to an IP address.

With early TCP/IP networks, name resolution was done with hosts files, which were stored locally on each computer. The hosts files were simple text files with a host name and IP addresses on each line. In Windows, the hosts file is located in the C:\Windows\System32\Drivers\etc folder. The disadvantage of using hosts files is that every time you need to add a new entry, you need to add or modify the hosts file on every computer in your organization, which is not a practical way to provide up-to-date name resolution.

DNS was developed as a system and a protocol to provide up-to-date name resolution. The benefits of DNS include the following:

- Ease of use and simplicity: Allows users to access computers and network resources with easy-to-remember names.
- Scalability: Allows the workload of name resolution to be distributed across multiple servers and databases.
- Consistency: Allows the IP addresses to be changed while keeping the host names consistent, making network resources easier to locate.

A DNS resolver is a service that uses the DNS protocol to query for information about DNS servers using UDP and TCP port 53.

Configuring and Managing DNS Zones

THE BOTTOM LINE

To provide DNS services, you first need to deploy DNS. Then after you have DNS servers, you have to create each zone and then add resource records to each zone. Because DNS is an essential service for a network, you should give some thought to it and plan before you deploy DNS.

The steps in deploying DNS include the following:

1. Install DNS on one or more servers.
2. Configure the DNS server, if necessary.
3. Create forward and reverse lookup zones.
4. Add resource records to the forward and reverse lookup zones.
5. Configure the clients to use the DNS servers.

Installing DNS

Before you can start using DNS, you have to install DNS. As you do with other Windows server roles, use Server Manager to deploy DNS.

As with any server role, before you deploy DNS, you need to plan your infrastructure. Some of the considerations involve how busy the servers are, what kind of fault-tolerance is needed, what kind of performance is required, and what kind of security is needed.

INSTALL DNS

GET READY. To install DNS, perform the following steps:

1. Open *Server Manager* by clicking the Server Manager button on the task bar.
2. At the top of Server Manager, select Manage and click Add Roles and Features.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation, and then click Next.
5. Click Select a server from the server pool, click the name of the server to install DNS to, and then click Next.
6. Click DNS Server (see Figure 8-1).

Figure 8-1

Selecting DNS Server to install

7. When the *Add Roles and Features Wizard* dialog box appears, select Add Features, and then click Next.
8. When the *Select features* page opens, click Next.
9. On the *DNS Server* page, click Next.
10. On the *Confirm installation selections* page, click the Install button.
11. When the installation is done, click the Close button.

When DNS is installed, you use the DNS console (see Figure 8-2). To open the DNS console, perform one of the following:

- Open *Server Manager*, open the *Tools* menu, and then select *DNS*.
- Open *Administrative Tools* and double-click *DNS*.

Figure 8-2

Viewing the DNS Manager console

Configuring Primary and Secondary Zones

On DNS original implementation, the DNS server would host either a primary or secondary zone or both. The ***primary zone*** provides an authoritative, read-write copy of the zone, while the ***secondary zone*** provides an authoritative, read-only copy of the primary zone.

When you need to make changes to the DNS zone, make the changes on the primary zone and the changes are replicated to the secondary zone. The secondary DNS zone enables the administrator to offload DNS query traffic and provide redundancy for name resolution queries. You then have to configure replication between the primary servers and the secondary servers.

Originally, the DNS was stored on a local file. By default, the primary zone file is named *zone_name.dns*, which is located in the *%systemroot%*\System32\DNS folder. By default, the *%systemroot%* is in the C:\Windows folder.

A server can host all primary zones, all secondary zones, or a mix of primary and secondary zones. Sometimes, servers that host primary zones are referred to as ***primary name servers*** and servers that host secondary zones are referred to as ***secondary name servers***.

When creating zones, there are two types of lookup zones to create:

- Forward lookup zone
- Reverse lookup zone

A ***forward lookup zone*** contains most of the resource records for a domain. Of course, as the name indicates, a forward lookup zone is used primarily to resolve host names to IP addresses. A ***reverse lookup zone*** is used to resolve IP addresses to host names. In the next two exercises, you create a standard primary zone for the contoso.com and a secondary zone for the contoso.com.

CREATE A STANDARD FORWARD LOOKUP PRIMARY ZONE

GET READY. To create a standard forward lookup primary zone, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the DNS Manager console.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click Forward Lookup Zones, and then click New Zone.
6. When the *Welcome to the New Zone Wizard* page opens, click Next.
7. On the *Zone Type* page, select the Primary zone radio button, and then click Next.
8. The *Zone Name* page opens. In the Zone name text box, enter the name of the domain, such as contoso.com, and then click Next.
9. On the *Zone File* page, ensure that the Create a new file with this file name radio button is selected, and then click Next.
10. On the *Dynamic Update* page, ensure that the Do not allow dynamic updates radio button is selected, and then click Next.
11. When the *Completing the New Zone Wizard* page appears, click Finish.

CREATE A STANDARD FORWARD LOOKUP SECONDARY ZONE

GET READY. To create a standard forward lookup secondary zone, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click Forward Lookup Zones, and then click New Zone.
6. When the *Welcome to the New Zone Wizard* page opens, click Next.
7. On the *Zone Type* page, select the Secondary zone radio button and click Next.
8. The *Zone Name* page appears. In the *Zone name* text box, enter the name of the domain such as *subdomain.contoso.com*, and then click Next.
9. On the *Master DNS Servers* page (see Figure 8-3), type the IP address of the server that hosts the primary record, and then press the Enter key. Click Next.

Figure 8-3

Entering the IP address on the Master DNS Servers page

10. When the *Completing the New Zone Wizard* page opens, click Finish.

Because a forward lookup zone is used to look up IP addresses based on domain name and host names, you specify the name of the domain when you create the forward lookup zone. Because a reverse lookup zone is used to look up a host name based on an IP address, you have to specify the subnet that the zone covers. In the next two exercises, you create a standard reverse lookup primary zone and a standard reverse lookup secondary zone.

Configuring Active Directory-Integrated Zones

Today, DNS can instead be stored in and replicated with Active Directory, as an ***Active Directory-integrated zone***. By using Active Directory-integrated zones, DNS follows a multi-master model, whereas each server enables all DNS servers to have authoritative read-write copies of the DNS zone. When a change is made on one DNS server, it is replicated to the other DNS servers.

Microsoft recommends using Active Directory to store DNS and for good reason. The benefits include:

- Fault tolerance: Because each server is an authoritative read-write copy of DNS, you have the DNS information stored on multiple servers. In addition, you can update the DNS records from any DNS server.
- Security: Zone transfers are securely replicated as part of Active Directory. In addition, similar to Active Directory objects, you can manage who can access which records by using discretionary access control lists (DACL). Finally, you can configure secure dynamic updates, which allow records to be updated only by the client that first registered the record.
- Efficient replication: Zone transfers are replicated more efficiently when using Active Directory, especially if the information has to be replicated over slow WAN links.

There are three different replication scopes available for Active Directory-integrated zones. They include:

- To all domain controllers in the domain (the only replication scope available in Windows 2000)
- To all domain controllers that are DNS servers in the local domain (default), which is known as the DomainDNSZones application partition
- To all domain controllers that are also DNS servers in the entire forest, which is known as the ForestDNSZones application

In the following exercise, you create an Active Directory-integrated zone.

CREATE AN ACTIVE DIRECTORY-INTEGRATED STANDARD FORWARD LOOKUP PRIMARY ZONE

GET READY. To create a standard forward lookup primary zone, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click Forward Lookup Zones and click New Zone.
6. When the *Welcome to the New Zone Wizard* page opens, click Next.
7. On the *Zone Type* page, select the Primary zone radio button.
8. Make sure the Store the zone in Active Directory option is selected and click Next.
9. On the *Active Directory Zone Replication Scope* page, make sure that To all DNS servers running on domain controllers in this domain option is selected and click Next.
10. The *Zone Name* page appears. In the *Zone name* text box, enter the name of the domain, such as contoso.com, and then click Next.
11. On the *Zone File* page, ensure that the Create a new file with this file name radio button is selected, and then click Next.
12. On the *Dynamic Update* page, ensure that the Do not allow dynamic updates radio button is selected, and then click Next.
13. When the *Completing the New Zone Wizard* page appears, click Finish.

Configuring Zone Delegation

A DNS ***subdomain*** is a child domain that is part of a parent domain and has the same domain suffix as the parent domain. Subdomains allow you to assign unique names to be used by a particular department, subsidiary, function, or service within the organization. However, you can create a different zone for the subdomain, which can be stored on another server. As a result, you can increase performance for the DNS zones as the traffic is delegated to multiple servers.

Subdomains allow you to break up larger domains into smaller, more manageable domains. For example, if you have *contoso.com*, you can create a *sales* subdomain and a *support* subdomain. When done, you will have the parent domain *contoso.com* and two subdomains: *sales.contoso.com* and *support.contoso.com*.

In the following exercise, you create a subdomain.

CREATE A SUBDOMAIN

GET READY. To create a subdomain, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click Forward Lookup Zones and click New Domain. The *New DNS Domain* dialog box appears.
6. Type the name of the subdomain in the text box, and then click the OK button to close the *New DNS Domain* dialog box.

When you delegate a DNS zone, you add subdomains within a domain, except the subdomain is stored in another zone. If the subdomain is placed on another server, you can distribute the DNS traffic among multiple servers, allowing for better performance.

DELEGATE A DNS DOMAIN

GET READY. To delegate a DNS domain, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click a forward lookup zone and click New Delegation.
6. When the *Welcome to the New Delegation Wizard* starts, click Next.
7. Type the name of the delegated subdomain in the delegated domain text box, and then click Next.
8. On the *Name Servers* page (see Figure 8-4), click the Add button and enter the IP addresses. Click the OK button to close the *New Name Server* record. Click Next.

Figure 8-4

Specifying name servers for the delegated zone

9. When the wizard is complete, click the Finish button.

Configuring Stub Zones

A ***stub zone*** is a copy of a zone that contains only necessary resource records (Start of Authority (SOA), Name Server (NS), and Address/Host (A) record) in the master zone and acts as a pointer to the authoritative name server. The stub zone allows the server to forward queries to the name server that is authoritative for the master zone without going up to the root name servers and working its way down to the server. While a stub zone can improve performance, it does not provide redundancy or load sharing.

In the following exercise, you create a stub zone.

CREATE A STUB ZONE

GET READY. To create a stub zone, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click Forward Lookup Zones and click New Zone.
6. When the *Welcome to the New Zone Wizard* page opens, click Next.
7. When the *Zone Type* page opens, select the Stub zone radio button and click Next.
8. When the *Zone Name* page opens, enter the domain name such as contoso.com in the *Zone name* text box, and then click Next.
9. On the *Zone File* page, click Next.
10. On the *Master DNS Servers* page (see Figure 8-5), type the IP address of the server that hosts the primary record and press the Enter key. Click Next.

Figure 8-5

Specifying the master DNS server for a stub zone

11. When the *Completing the New Zone Wizard* appears, click Finish.

Configuring Forwarding and Conditional Forwarding

By default, when a client contacts a DNS server and the DNS server does not know the answer, it performs an iterative query to find the answer, which means it first contacts the root domain and additional DNS servers until it finds the authoritative DNS server for the zone. However, DNS servers can be configured to be forwarded to another DNS server or a conditional forwarder based on the domain name queried.

Many organizations have multiple levels of DNS servers. For example, an organization can have multiple DNS servers for its internal users and multiple DNS servers for Internet access, which provide addresses for external websites and other network services. Another example is an organization that has one level of DNS servers for internal users and an Internet Service Provider (ISP) that DNS services. In either of these two cases, you can configure the internal DNS servers to forward the DNS queries to the external DNS servers or the ISP servers. As a result, clients and the internal DNS servers perform recursive queries, and the external or ISP DNS performs iterative queries.

By using a ***forwarder***, you control name resolution queries and traffic, which can improve the efficiency of name resolution for the computers in your network. You can manage the DNS traffic between the organization's network and the Internet by allowing only internal DNS servers to communicate over the Internet, allowing for a more secure environment because DNS information can be used to hack into a network. In addition, by having all DNS traffic going through single DNS servers, a single server can build a larger cache of DNS data. As a result, Internet traffic is decreased and clients receive faster response times.

CONFIGURE FORWARDERS

GET READY. To configure a DNS server to forward DNS queries to another DNS server, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Right-click the DNS server and select Properties. The *Server Properties* dialog box opens.

5. Select the Forwarders tab.
6. Click the Edit button. The *Edit Forwarders* dialog box opens (see Figure 8-6).

Figure 8-6

Modifying the Forwarders list

7. In the *IP address column*, type the IP address of the DNS server that you want to forward DNS queries to and press the Enter key.
8. Click the OK button to close the *Forwarders* dialog box.
9. Click the OK button to close the server Properties dialog box.
10. When the installation is done, click the Close button.

Conditional forwarding expands on the idea of forwarding, where you forward those queries to other DNS servers based on the DNS domain names in the query. Therefore, if you have a partner organization where you connect with a VPN tunnel, you can forward those request to the partner's DNS when you try to access a network resource on the partner network. Of course, coordination is needed between the two organizations because firewalls have to be configured to allow DNS traffic to traverse the VPN tunnel.

The *conditional forwarder* setting consists of the following:

- The domain names for which the DNS server forwards queries
- One or more DNS server IP addresses for each domain name specified

CONFIGURE CONDITIONAL FORWARDERS

GET READY. To configure a DNS server to forward DNS queries to another DNS server, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Conditional Forwarders* folder.
5. Right-click Conditional Forwarders Zones and click New Conditional Forwarder. The New Conditional Forwarder dialog box appears.

6. Type the name of the DNS domain included in DNS queries that you want to forward in the *DNS Domain* text box (see Figure 8-7).

Figure 8-7

Identifying the name and IP address of a conditional forwarder

7. In the *IP Address* column, type the IP address of the DNS server that you want to forward to, and then press the Enter key.
8. Click the OK to close the *New Conditional Forwarder* dialog box. The zone appears under Conditional Forwarders.

Configuring Zone Transfers

Zone transfers are the complete or partial transfer of DNS data from a zone on a DNS server to another DNS server. After the initial zone transfer, the primary DNS server notifies the secondary DNS server that changes have occurred. The secondary servers then request for the records to be transferred and the changes are then replicated to all the secondary DNS servers using zone transfers.

The following events trigger a zone transfer:

- The initial transfer occurs when a secondary zone is created.
- The zone refresh interval expires.
- The DNS Server service is started at the secondary server.
- The master server notifies the secondary server that changes have been made to a zone.

There are three types of transfers. They include:

- Full transfer
- Incremental transfer
- DNS Notify

UNDERSTANDING FULL AND INCREMENTAL TRANSFERS

A ***full zone transfer (AXFR)***, which copies the entire zone, is used when you first add a new DNS secondary server for an existing zone. With large zones, AXFRs can be time-consuming and resource-intensive.

An ***incremental zone transfer (IXFR)*** retrieves only resource records that have changed within a zone. To determine whether a zone transfer is needed, the serial number on the secondary server is compared with the serial number of the primary server. If the primary server database is higher, than a transfer of resource records is needed. Because the IXFR does only a partial zone transfer, it uses less bandwidth.

CONFIGURING NOTIFY SETTINGS

Instead of the secondary zone servers polling the primary server for serial numbers, the ***DNS Notify*** method allows the primary DNS server to use a "push" mechanism to notify secondary servers that it has been updated and that the resource records need to be transferred. The DNS is not a mechanism for transferring data. Instead, it is used with AXFR and IXFR to notify a secondary server that new records are available for transfer.

By default, zone transfers are disabled. When you enable them, you can choose one of the following:

- To any server: Allows a data transfer to any server that asks for a zone transfer (least secure).
- Only to servers listed on the Name Servers tab: Restricts zone transfers to secondary DNS servers as defined with NS resource records.
- Only to the following servers: Restricts zone transfers to those servers specified in the accompanied list.

In the following exercise, you enable and configure a zone transfer.

CONFIGURE ZONE TRANSFER SETTINGS

GET READY. To deploy DNS, perform the following steps:

1. Open Server Manager.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can see the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click the forward or reverse lookup zone that you want to configure and click Properties. The *Properties* dialog box opens.
6. Click the Zone Transfers tab.
7. Select the Allow zone transfers option.
8. Select the type of zone transfer:
   - To any server
   - Only to servers listed on the Name Servers
   - Only to the following servers

   If you select Only to the following servers, click the Edit button to specify the addresses that you want to perform zone transfers.
9. To configure the Notify options, click the Notify button to display the *Notify* dialog box. Then select the Servers listed on the Name Servers tab option or select The following servers option and specify which servers you want to notify. Click the OK button to close the *Notify* dialog box.
10. Click OK to close the *Properties* dialog box.

To configure notifications, open the Properties dialog box for the zone and click the *Notify in the Zone Transfers* tab.

If you right-click a primary or secondary zone, you can select to *Reload*, which reloads the secondary zone from local storage. If you right-click a secondary zone, you can also select one of following options:

- **Transfer from Master:** Determines whether the local secondary zone serial number has expired and then pulls a zone transfer from the master server.
- **Reload from Master:** Performs a zone transfer regardless of the serial number in the secondary zone's SOA resource records.

Business Case Scenarios

Scenario 8-1: Implementing DNS

You have three large sites in your organization: the corporate office, the engineering site, and the manufacturing site. You want to make sure that you install DNS so that all of the zones have fault tolerance while still allowing changes on any DNS server and for the best performance possible. What do you recommend, and why do you recommend this particular solution?

Scenario 8-2: Controlling DNS Updates

You have an organization that often has visitors connect to the organization's network. You are worried that someone might modify a DNS record so to hijack a computer name. What can you use to prevent this, and how do you implement it?

9 LESSON

Configuring DNS Records

Configuring DNS Record Types

THE BOTTOM LINE

A ***DNS zone database*** is made up of a collection of resource records, which are used to answer DNS queries. Each ***resource record*** (RR) specifies information about a particular object. Each record has a type, an expiration time limit, and some type-specific data.

On an organization's network, many of the resource records are automatically created. For example, the clients or the DHCP servers create the host and Pointer (PTR) records. When you install a DNS server, NS records are usually created. When you install domain controllers, Service Location (SRV) records are created.

Creating and Configuring DNS Resource Records

When you create a user account, certain properties define the user account, such as first name, last name, and login name. When you define a printer in Active Directory, you define a name of the printer and a location. A printer does not have a first name or a last name. Just as you have different types of objects in Active Directory, you also have different types of resource records in DNS, with different fields.

When you create a new zone, two types of records are automatically created:

- ***Start of Authority (SOA) record:*** Specifies authoritative information about a DNS zone, including the primary name server, the e-mail of the domain administrator, the domain serial number, and the expiration and reload timers of the zone.
- ***Name Server (NS) record:*** Specifies an authoritative name server for the host.

You have to add additional resource records as needed. Figure 9-1 shows a zone with common resource records. The most common resource records are as follows:

- ***Host (A and AAAA) record:*** Maps a domain/host name to an IP address.
- ***Canonical Name (CNAME) record:*** Sometimes referred to as an Alias, maps an alias DNS domain name to another primary or canonical name.
- ***Pointer (PTR) record:*** Maps an IP address to a domain/host name.
- ***Mail Exchanger (MX) record:*** Maps a DNS domain name to the name of a computer that exchanges or forwards e-mail for the domain.
- ***Service Location (SRV) record:*** Maps a DNS domain name to a specified list of host computers that offer a specific type of service, such as Active Directory domain controllers.

Figure 9-1

Viewing the zone with common resource records

The PTR records in the reverse lookup zone and all of the other record types are in the forward lookup zone.

START OF AUTHORITY (SOA) RECORDS

The SOA record specifies authoritative information about the zone. Therefore, there is only one SOA record for a zone. It includes the following fields:

- **Authoritative server:** Contains the name of the primary DNS server authoritative for the zone.
- **Responsible person:** Shows the e-mail address of the administrator who is responsible for the zone. Instead of using the at (@) symbol, it uses a period (.).
- **Serial number:** Shows the version or how many times the zone has been updated. As explained previously, it is used to determine whether the zone's secondary server needs to initiate a zone transfer with the master server. If the serial number of the master server is higher, the secondary server initiates a zone transfer.
- **Refresh shows:** Determines how often the secondary server for the zone checks to see whether the zone data is changed.
- **Retry:** After sending a zone transfer request, the Retry value determines how long (in seconds) the zone's secondary server waits before sending another request.
- **Expire:** After a zone transfer, Expire determines how long (in seconds) the zone's secondary server continues to respond to zone queries before discarding its own zone as invalid.
- **Minimum TTL:** Specifies a default Time to Live (TTL) value, which defines the default time. A resource record remains in a DNS cache after a DNS query has retrieved a record. If a resource record has its own TTL value, the TTL value of the resource record is used instead of the TTL defined in the SOA record.

Figure 9-2 shows the SOA resource record.

Figure 9-2

Viewing the SOA resource record

NAME SERVER (NS) RECORDS

The Name Server (NS) resource record identifies a DNS server that is authoritative for a zone, including the primary and secondary copies of the DNS zone. Because a zone can be hosted on multiple servers, there is a single record for each DNS server hosting the zone. The Windows Server DNS Server service automatically creates the first NS record for a zone when the zone is created. Figure 9-3 shows the NS resource record.

Figure 9-3

Viewing the NS resource record

HOST (A AND AAAA) RECORDS

The most common resource records found in DNS are the Host (A and AAAA) records. The A stands for address. The A record maps a domain/host name to an IPv4 address; the AAAA record maps a domain/host name to an IPv6 address.

For example, the following A resource record is located in the zone *server1.sales.contoso.com* and maps the Fully Qualified Domain Name (FQDN) of a server to an IP address of 192.168.3.41:

```
Server1.sales.contoso.com. IN A 192.168.3.41
```

Figure 9-4 shows the Host resource record.

Figure 9-4

Viewing the Host resource record

CANONICAL NAME (CNAME) RECORDS

The Canonical Name (CNAME) resource record is an alias for a host name. It is used to hide the implementation details of your network from the clients that connect to it, particularly if you need to make changes in the future.

For example, instead of creating a Host record for www, you can create a CNAME that specifies the web server that hosts the www websites for the domain. If you need to change servers, you just point the CNAME to another server's Host record. Of course, you need to have Host records that specify the IP address. Figure 9-5 shows the CNAME resource record.

Figure 9-5

Viewing the CNAME resource record

POINTER (PTR) RECORDS

The Pointer records (PTR) are used for the opposite reason of the Host records. They resolve host names from an IP address. Different from the Host record, the IP address is written in reverse. For example, the IP address 192.168.3.41 that points to `server1.sales.contoso` is:

```
41.3.168.192.in-addr.arpa. IN PTR
server1.sales.contoso.com.
```

Figure 9-6 shows the PTR resource record.

Figure 9-6

Viewing the PTR resource record

MAIL EXCHANGER (MX) RECORDS

The Mail Exchanger (MX) resource record specifies an organization's mail server, service, or device that receives mail via Simple Mail Transfer Protocol (SMTP). For fault tolerance, you can designate a second mail server. Therefore, if the primary mail server is not available, the e-mail can be sent to the secondary server. Although each mail external mail server requires an MX record, the primary server is designed with a lower priority number.

For example, if you have three mail servers that can receive e-mail over the Internet, you would have three MX records for the `contoso.com` domain:

```
@ IN MX 5 mailserver1.contoso.com.
@ IN MX 10 mailserver2.contoso.com.
@ IN MX 20 mailserver3.contoso.com.
```

The primary mail server is the first one because it has a lower priority number. Figure 9-7 shows the MX resource record.

Figure 9-7

Viewing the MX resource record

SERVICE LOCATION (SRV) RECORDS

SRV resource records are used to find specific network services. For example, when you install Active Directory via a domain controller, SRV records are automatically added to the DNS zone. If users cannot connect to DNS services or the SRV records are not in the zone, users cannot log in to the Active Directory domain.

The format for an SRV record is as follows:

```
Service_Protocol.Name [TTL] Class SRV Priority Weight Port Target
```

For example, to log in with Lightweight Directory Access Protocol (LDAP), you could have the following SRV records for two domain controllers:

```
ldap._tcp.contoso.com. IN SRV 0 0 389 dc1.contoso.com.
ldap._tcp.contoso.com. IN SRV 10 0 389 dc2.contoso.com.
```

Because these examples do not specify a TTL, the DNS client uses the minimum TTL specified in the SOA resource record. Figure 9-8 shows the SRV resource record, and Figure 9-9 shows the SRV records for a domain controller, specifically to find the LDAP and Kerberos servers.

Figure 9-8

Viewing the SRV record

Figure 9-9

Viewing the SRV resource record for a domain

TAKE NOTE* With SRV records, for the domain to be added to a DNS zone, the zone must allow dynamic updates.

Configuring Record Options

Managing resources is easy with Windows servers because the DNS console provides a GUI interface.

Before you can create resource records, you need to first create the appropriate forward lookup zones and reverse lookup zones.

CREATE A HOST RECORD

GET READY. To create a Host record, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server to display the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click the zone that you want to create a Host resource record for and select New Host (A or AAAA). The *New Host* dialog box appears.
6. In the *Name* text box, type the name of the host.
7. In the *IP address* text field, type the IP address (IPv4 or IPv6).
8. If you want to also create a PTR record, select the Create associated pointer (PTR) record option.

9. Click Add Host.
10. If you need to create additional Host records, add the appropriate host names and IP addresses. If you do not want to create more, click the Done button.

If the reverse lookup zone does not exist to store the PTR record, a warning that the associated pointer (PTR) record cannot be created.

To change a resource record, you just double-click the resource record to display the Properties dialog box, and then you make the appropriate changes. Of course, when you create resource records or change resource records, it takes time to replicate the resource records to the other DNS servers for the domain.

By opening the View menu and selecting the Advanced option in the DNS console, administrators can see additional options when managing and configuring the resource records, including the TTL for the resource record.

To view the TTL settings for individual resource records, you need to use the DNS Manager console in Advanced mode.

MODIFY THE TTL VALUE FOR A RESOURCE RECORD

GET READY. To modify the Time to Live (TTL) value for a resource record, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server to display the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. To view additional options, click View > Advanced.
6. To modify a record, double-click a resource record. The *Properties* dialog box opens.
7. Type the TTL using the DDDDD:HH.MM.SS format where DDDDD is days, HH is hours, MM is minutes, and SS is seconds.
8. To close the *Properties* dialog box, click OK.

As mentioned before, many records can have multiple records assigned with the same name. For example, you can have multiple A or AAAA records that have the same name or you have multiple MX records for the same domain. With A and AAAA records, you don't define a weight to each record. Instead, each record is equal. With MX records, you must define a weight or priority (lowest number takes priority), so that it knows which SMTP server an e-mail should be sent to first. If that one is not available, it tries the second SMTP server listed with the next lowest priority.

Configuring Round Robin

Round robin is a DNS balancing mechanism that distributes network load among multiple servers by rotating resource records retrieved from a DNS server.

By default, DNS uses round robin to rotate the resource records returned in a DNS query where multiple resource records of the same type exist for a query's DNS host name.

For example, you can create the following Host records for webserver.contoso.com:

192.168.3.151	webserver.contoso.com
192.168.3.152	webserver.contoso.com
192.168.3.153	webserver.contoso.com

When the first client queries for webserver.contoso.com, the client gets back 192.168.3.151. When the second client queries for webserver.contoso.com, the client gets back 192.168.3.152. The third client gets back 192.168.3.153. When the fourth client accesses the webserver, the client gets 192.168.3.151. If one of these clients tries to access the webserver a second time before the TTL time expires, the client goes back to the same address because that address is in the client's DNS cache.

Round robin can be enabled or disabled by opening the server properties within the DNS Manager console. If round robin is disabled, the order of the response for these queries is based on a static ordering of resource records because they are stored in the zone.

DISABLE ROUND ROBIN

GET READY. To disable round robin, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Right-click the DNS server and choose Properties. The *Properties* dialog box opens.
5. Click the Advanced tab.
6. Deselect the Enable round robin option.
7. Click the OK button to close the *Properties* dialog box.

Configuring Secure Dynamic Updates

DNS supports ***dynamic updates***, where resource records for the clients are automatically created and updated at the host's primary DNS server. For Active Directory-integrated zones, these records are automatically replicated to the other DNS servers. However, because standard dynamic updates are insecure, Microsoft added secure dynamic updates.

For years, Windows DNS has supported dynamic updates, whereas a DNS client host registers and dynamically updates the resource records with a DNS server. If a host's IP address changes, the resource record (particularly the A record) for the host is automatically updated, while the host utilizes the DHCP server to dynamically update its Pointer (PTR) resource record. Therefore, when a user or service needs to contact a client PC, it can look up the IP address of the host. With larger organizations, this becomes an essential feature, especially for clients that frequently move or change locations and use DHCP to automatically obtain an IP address. For dynamic DNS updates to succeed, the zone must be configured to accept dynamic updates.

Unfortunately, standard dynamic updates are not secure because any one can update a standard resource record. However, if you enable ***secure dynamic updates***, only updates from the same computer can update a registration for a resource record.

Configuring Zone Scavenging

By default, Windows updates its own resource record at startup time and every 24 hours after startup. This is to ensure the records are up-to-date and to help guard against accidental deletion. However, as some records become stale and are not removed or updated, the DNS database becomes outdated and provides some inaccurate information to clients. To help with stale data, you can configure zone scavenging to clean up the stale records. ***Aging*** in DNS is the process of using timestamps to track the age of dynamically registered resource records. ***Scavenging*** is the mechanism to remove stale resource records.

Typically, stale DNS records occur when a computer is permanently removed from the network. Mobile users who abnormally disconnect from the network can also cause stale DNS records. To help manage stale records, Windows adds a time stamp to dynamically added resource records in primary zones where aging and scavenging are enabled. Manually added records are time stamped with a value of 0, and they are automatically excluded from the aging and scavenging process.

To enable aging and scavenging, you must do the following:

- Resource records must be either dynamically added to zones or manually modified to be used in aging and scavenging operations.
- Scavenging and aging must be enabled both at the DNS server and on the zone.

TAKE NOTE*

Scavenging and aging must be enabled at the DNS server and on the zone.

Scavenging is disabled by default.

DNS scavenging depends on the following two settings:

- **No-refresh interval:** The time between the most recent refresh of a record time stamp and the moment when the time stamp can be refreshed again. When scavenging is enabled, this is set to *7 days* by default.
- **Refresh interval:** The time between the earliest moment when a record time stamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period. When scavenging is enabled, this is set to *7 days* by default.

WARNING Be careful when enabling scavenging because it can accidently remove records that you want to keep. As a result, users cannot resolve certain DNS queries, making some network services unavailable.

A DNS record becomes eligible for scavenging after both the no-refresh and refresh intervals have elapsed. If the default values are used, this is a total of 14 days.

ENABLE AGING/SCAVENGING AT THE SERVER

GET READY. To enable aging/scavenging at the server, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Right-click the DNS server and click Set Aging/Scavenging for all Zones. The *Server Aging/Scavenging Properties* dialog box opens (see Figure 9-10).

Figure 9-10

Opening the Server Aging/Scavenging Properties dialog box

5. Click the Scavenge stale resource records option.
6. Modify the no-refresh interval and refresh interval as needed.
7. Click the OK button to close the *Server Aging/Scavenging Properties* dialog box.
8. If you want the aging/scavenging settings to apply to all existing Active Directory-integrated zones, select the Apply these settings to the existing Active Directory-integrated zones option. Click OK to close the Server Aging/Scavenging Confirmation dialog box.

TAKE NOTE*

It is best that you enable scavenging on only one DNS server. This gives you better control of the aging/scavenging settings and more control when scavenging occurs and how often.

ENABLE AGING/SCAVENGING AT THE ZONE

GET READY. To enable aging/scavenging at the zone, perform the following steps:

1. Open Server Manager by clicking the Server Manager button on the task bar.
2. Click Tools > DNS to open the *DNS Manager console*.
3. If necessary, expand the DNS console to a full-screen view.
4. Expand the server so that you can display the *Forward Lookup Zones* and *Reverse Lookup Zones* folders.
5. Right-click the zone and click Properties.
6. On the *General* tab, click the Aging button. The *Zone Aging/Scavenging Properties* dialog box opens.
7. Click the Scavenge stale resource records option.
8. Modify the no-refresh interval and refresh interval as needed.
9. Click the OK button to close the *Server Aging/Scavenging Properties* dialog box.
10. When you are prompted to apply aging/scavenging settings to the Standard Primary zone, click Yes.
11. Click the OK button to close the *Properties* dialog box.

Business Case Scenarios

Scenario 9-1: Distributing Traffic Web Servers

You just installed three web servers, which are used to serve your company's web page on the Internet. You want to ensure that web requests are evenly distributed to the three web servers. What do you need to do, and what are the steps you need to perform to accomplish this?

Scenario 9-2: Configuring DNS Time To Live (TTL)

Where is the default Time To Live (TTL) information defined at, and how do you override the default TTL for individual records?

10 LESSON

Configuring VPN and Routing

The Remote Access Role

THE BOTTOM LINE

Today, it is common for an organization to use a ***remote access server (RAS)***. A RAS enables users to connect remotely to a network using various protocols and connection types. By connecting to the RAS over the Internet, users can connect to their organization's network so that they can access data files, read e-mail, and access other applications just as if they were sitting at work.

To provide RAS, Microsoft includes ***Routing and Remote Access (RRAS)***, which provides the following functionality:

- A virtual private network (VPN) gateway where clients can connect to an organization's private network using the Internet.
- Connect two private networks using a VPN connection using the Internet.
- A dial-up remote access server, which enables users to connect to a private network using a modem.
- Network address translation (NAT), which enables multiple users to share a single public network address.
- Provide routing functionality, which can connect subnets and control where packets are forwarded based on the destination address.
- Provide basic firewall functionality and allow or disallow packets based on addresses of source and/or destination and protocols.

An early method to connect to an organization's network is over an analog phone line or ISDN line using a modem. Because the modem creates a dedicated connection to the server, the connection does not typically need to be encrypted. However, by today's networking standards and bandwidth requirements, the phone and ISDN system do not have the bandwidth needed. Therefore, this method typically is not used today.

Installing and Configuring the Remote Access Role

Before you can use RRAS, you need to first add the Remote Access Role. Then, you need to initially configure RRAS so that you can specify which options are available with it.

INSTALLING ROUTING AND REMOTE ACCESS

To install the Remote Access Role, you use the Server Manager to install the proper role. Because the remote access computer is used to connect an organization's internal private network with the Internet, the server should have two network cards.

INSTALL THE REMOTE ACCESS ROLE

GET READY. To install the Remote Access Role, perform the following steps:

1. Click the Server Manager button on the task bar to open the *Server Manager*.
2. At the top of *Server Manager*, click Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install Remote Access Role to, and then click Next.
6. Scroll down and select Remote Access (see Figure 10-1). If you need Routing Information Protocol (RIP), expand Remote Access and select Routing.

Figure 10-1

Selecting the Remote Access role

7. When the *Add Roles and Features Wizard* dialog box opens, select Add Features, and then click Next.
8. On the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Remote Access* page, click Next.
11. On the *Select role services* page, keep DirectAccess and VPN (RAS) selected and select Routing. Click Next.
12. On the *Confirm installation selections* page, click Install.
13. When the installation is complete, click Close.

CONFIGURING ROUTING AND REMOTE ACCESS

After you install RRAS, you need to enable the server and configure RRAS. When you start the RRAS Setup Wizard, you can use the wizard to automatically configure RRAS for specific applications or configure the service manually.

The wizard offers five basic options for configuring RRAS:

- **Remote access (dial-up or VPN):** Sets up the server to accept incoming remote access connections (dial-up or VPN).
- **Network address translation (NAT):** Sets up the server to provide NAT services to clients on the private network that need to access the Internet.
- **Virtual private network (VPN) access and NAT:** Sets up the server to support incoming VPN connections and to provide NAT services.
- **Secure connection between two private networks:** Sets up a demand-dial or persistent connection between two private networks.
- **Custom configuration:** Enables you to choose individual services, including NAT, LAN routing, and VPN access.

TAKE NOTE*

You cannot have Windows Firewall service running while enabling and configuring RRAS.

CONFIGURING RRAS FOR DIAL-UP REMOTE ACCESS

Dial-up remote access enables remote computers that have a modem to connect to the organization's network as if the remote computers were connected locally. Because it uses the public phone system or ISDN phone lines, it is at much slower transfer speeds when compared to DSL, cable technology, and other forms of networking found at home. For this reason, dial-up remote access is becoming less common. To support multiple dial-users that connect simultaneously, you must have a modem bank that supports multiple modem connections over the phone lines.

CONFIGURE DIAL-UP REMOTE ACCESS

GET READY. To configure dial-up remote, perform the following steps:

1. Open Server Manager.
2. Click Tools > Routing and Remote Access. The *Routing and Remote Access console* opens.
3. Right-click the server and select Configure and Enable Routing and Remote Access. The *Routing and Remote Access Server Setup Wizard* opens.
4. On the *Welcome* page, click Next.
5. On the *Configuration* page, select Remote access (dial-up or VPN) and then click Next.
6. On the *Remote Access* page, select Dial-Up and click Next.
7. If your server has more than one network interface, the *Network Selection* page will appear. Click the interface to which you wish to assign remote clients, and then click Next.

TAKE NOTE*

If you intend to protect your RRAS server by using a firewall instead, do not enable the *Enable security on the selected interface by setting up static packet filters* option. In addition, if you enable this option, by default, you will not be able to ping the IP address of the public network adapter because Internet Control Message Protocol (ICMP) packets are blocked by the packet filters.

8. On the *IP Address Assignment* page, you can select either Automatically (to use a DHCP server to assign addresses) or From a specified range of addresses (addresses are supplied by the routing and remote access server). Select From a specified range of addresses and then click Next.
9. On the *Address Range Assignment* page, click New.
10. When the *New IPv4 Address Range* dialog box opens, fill in start IP address and End IP address (see Figure 10-2). Click OK.

Figure 10-2

Using the New IPv4 Address Range dialog box

11. Back on the *Address Range Assignment* page, click Next.
12. On the *Managing Multiple Remote Access Servers* page, select No, use Routing and Remote Access to authenticate connection requests. Click Next.
13. On the *Summary* page, click Finish. The *Routing and Remote Access service* starts and initializes automatically.
14. When you are asked to support the relaying of DHCP messages from remote access clients message, click OK.
15. When the configuration is complete, the console looks similar to Figure 10-3.

Figure 10-3

Viewing the configured *Routing and Remote Access* console

Configuring VPN Settings

Virtual private networks (VPNs) link two computers or network devices through a wide-area network (WAN) such as the Internet. Because the Internet is a public network and is considered insecure, the data sent between the two computers or devices is encapsulated and encrypted.

VPN connections provide the following:

- **Encapsulation:** Private data is encapsulated or placed in a packet with a header containing routing information that allows the data to traverse the transit network such as the Internet.
- **Authentication:** Proves the identity of the user or computer that tries to connection.
- **Data encryption:** Ensures confidentiality is maintained by the sender encrypting the data before it is sent so that unauthorized people cannot read the private data. When it is received, the intended recipient decrypts it. Of course, the encryption and decryption depend on the sender and receiver. Both must have a common or related encryption key; larger keys offers better security.
- **Data integrity:** Verifies that the data sent over the VPN connection has not been modified in transit. This is usually done with a cryptographic checksum that is based on an encryption key that is known only to the sender and receiver. When the data is received, the same checksum calculation is done and the value is compared to the one that was calculated before the data was sent. If the values match, the data has not been tampered with.

The VPN can be used in the following scenarios:

- A client connects to the RAS server to access internal resources from off-site.
- Two remote sites together by creating a VPN tunnel between a RAS server located at each site.
- Two different organizations create a VPN tunnel so that users from one organization can access the resources in the other organization.

The three types of tunneling protocols used with a VPN/RAS server running on Windows Server 2012 R2 include:

- ***Point-to-Point Tunneling Protocol (PPTP):*** A VPN protocol based on the legacy Point-to-Point protocol used with modems. PPTP uses a Transmission Control Protocol (TCP) connection for tunnel management, and a modified version of Generic Route Encapsulation (GRE) to encapsulate PPP frames for tunneled data. Payloads of the encapsulated PPP frames can be encrypted, compressed, or both. The PPP frame is encrypted with Microsoft Point-to-Point Encryption (MPPE) by using encryption keys that are generated from the MS-CHAPv2 or EAP-TLS authentication process. PPTP is easy to set up but has weak encryption technology. PPTP-based VPN connections, however, do not provide data integrity (proof that the data was not modified in transit) or data origin authentication (proof that the data was sent by the authorized user). PPTP uses TCP port 1723 and IP protocol ID 47.
- ***Layer 2 Tunneling Protocol (L2TP):*** Used with IPsec to provide security. L2TP is the industry standard when setting up secure tunnels. L2TP supports either computer certificates or a preshared key as the authentication method for IPsec. By using IPsec, L2TP/IPsec VPN connections provide data confidentiality, data integrity, and data authentication. The L2TP message is encrypted with either Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) by using encryption keys that the IKE negotiation process generates. L2TP uses UDP Port 500, UDP Port 1701, UDP Port 4500, and IP Protocol ID 50.

- ***IKEv2:*** IKE is short for Internet Key Exchange, which is a tunneling protocol that uses IPsec Tunnel Mode protocol over UDP port 500. IKEv2 encapsulates datagrams by using IPsec ESP or AH for transmission over the network. The message is encrypted with one of the following protocols by using encryption keys that are generated from the IKEv2 negotiation process: AES 256, AES 192, AES 128, and 3DES encryption algorithms. It supports mobility (MOBIKE), whereas the VPN connection is more resilient when moving from one wireless hotspot to another or switching from wireless to a wired connection. It also supports VPN Reconnect. IKEv2 is supported only on Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012 R2.
- ***Secure Socket Tunneling Protocol (SSTP):*** Introduced with Windows Server 2008, which uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and web proxies that might block PPTP and L2TP/IPsec. By using SSL, SSTP VPN connections provide data confidentiality, data integrity, and data authentication.

Authentication for VPN connections takes one of the following forms:

TAKE NOTE*

If you need to use a VPN connection behind a firewall that only allows https, you have to use SSTP.

- User-level authentication by using Point-to-Point Protocol (PPP) authentication. User-level authentication is usually username and password. With a VPN connection, if the VPN server authenticates, the VPN client attempts the connection using a PPP user-level authentication method and verifies that the VPN client has the appropriate authorization. If the method uses mutual authentication, the VPN client also authenticates the VPN server. By using mutual authentication, clients are ensured that the client does not communicate with a rogue server masquerading as a VPN server.
- Computer-level authentication that uses IKE to exchange either computer certificates or a pre-shared key. Microsoft recommends using computer-certificate authentication because it is a much stronger authentication method. Computer-level authentication is performed only for L2TP/IPsec connections.

When using VPNs, Windows 8.1 and Windows Server 2012 R2 support the following forms of authentication:

- ***Password Authentication Protocol (PAP):*** Uses plain text (unencrypted passwords). PAP is the least secure authentication and is not recommended.
- ***Challenge Handshake Authentication Protocol (CHAP):*** A challenge-response authentication that uses the industry standard md5 hashing scheme to encrypt the response. CHAP was an industry standard for years and is still quite popular.
- ***Microsoft CHAP version 2 (MS-CHAP v2):*** Provides two-way authentication (mutual authentication). MS-CHAP v2 provides stronger security than CHAP. Finally, MS-CHAP v2 is the only authentication protocol that Windows Server 2012 R2 provides that allows you to change an expired password during the connection process.
- ***Extensible Authentication Protocol (EAP-MS-CHAPv2):*** A universal authentication framework that allows third-party vendors to develop custom authentication schemes, including retinal scans, voice recognition, fingerprint identifications, smart cards, Kerberos, and digital certificates. It also provides a mutual authentication method that supports password-based user or computer authentication.

TAKE NOTE*

If you wish to use smart cards for remote connections, you need to use Extensible Authentication Protocol (EAP)

If you have multiple remote access servers, you can choose to use a RADIUS server. A RADIUS server provides authentication, authorization, and accounting for the remote access clients. RADIUS servers are discussed in detail in Lesson 12.

CONFIGURING THE VPN CONNECTION ON THE SERVER

To configure the Windows server to accept VPN connection, you first need to run the Routing and Remote Access Server Setup wizard, so that it knows which network adapters will be used to accept VPN connections and how the IP addresses will be assigned. You can also configure a RADIUS server during this time to handle authentication request.

CONFIGURE AND ENABLE VPN REMOTE ACCESS

GET READY. To configure and enable VPN Remote Access, perform the following steps:

1. Open Server Manager.
2. Click Tools > Routing and Remote Access. The *Routing and Remote Access console* opens.
3. Right-click the server and select Configure and Enable Routing and Remote Access. The *Routing and Remote Access Server Setup Wizard* opens.
4. On the *Welcome* page, click Next.
5. On the *Configuration* page, select Remote access (dial-up or VPN) and click Next.
6. On the *Remote Access* page, select VPN and click Next.
7. On the *VPN Connection* page, select the external network card that is connected to the Internet.
8. On the *IP Address Assignment* page, click from a specified range of addresses and click Next.
9. On the *Address Range Assignment* page, click New.
10. When the *New IPv4 Address Range* dialog box opens, fill in the Start IP address and End IP address. Click OK.
11. Back on the *Address Range Assignment* page, click Next. On the *Managing Multiple Remote Access Servers* page, if you have a RADIUS server, click Yes, set up this server to work with a RADIUS server and then click Next.
12. On the *RADIUS Server Selection* page, enter the Primary RADIUS server and Alternate RADIUS server. Then, in the *Shared secret* text box, type in the shared secret password. Click Next.
13. If you do not have RADIUS server, click No, use Routing and Remote Access to authenticate connection requests. Click Next.
14. On the *Completing the Routing and Remote Access Server Setup Wizard* page, click Finish.
15. When it asks to support the relaying of DHCP messages from remote access clients message, click OK.

After the VPN server is configured using the Configure and Enable Routing and Remote Access Wizard, you can further configure the VPN server by right-clicking the server in RRAS and selecting *Properties*. The General tab allows you to enable routing and remote access without using the wizard.

From the *Security* tab, you can configure authentication methods, specify the Preshared key for IPsec and L2TP/IKv2 connections, and specify the SSL certificate that is used by SSTP.

The IPv4 tab allows you to configure the IPv4 address assignments, whereas the IPv6 allows you to specify the IPv6 prefix assignment. The IKEv2 allows you configure IKEv2 parameters, such as idle-timeout and network outage time.

By default, RRAS allows up to 128 ports for each of the VPN protocol types. If you want to change the number of ports, right-click *Ports* and select *Properties*. You can then click the Configure button to open the Configure Device – WAN miniport dialog box so that you can specify the maximum number of ports (see Figure 10-4).

Figure 10-4

Specifying the number of ports

CREATING A VPN CONNECTION ON A CLIENT

If you want to configure a client so that it can connect to a VPN server, you will use the Network and Sharing Center to start the wizard to set up a new connection or network. When you run the wizard, you will define the name or IP address that will be used when connecting to the remote network.

CREATE A VPN TUNNEL

GET READY. To create a VPN connection on Windows Server 2012 R2, perform the following steps:

1. From the Control Panel, select Network and Internet to access the *Network and Sharing Center*.
2. From the *Network and Sharing Center*, choose Set up a new connection or network.
3. On the Set Up a Connection or Network page, choose Connect to a workplace. Click Next.
4. On the *Connect to a Workplace* page, answer the question, "How do you want to connect?" Choose Use my Internet connection or Dial directly.
5. When it asks you to type the Internet address to connect to, type the DNS name or IP address of the VPN server on the Internet in the *Internet address* text box. In the *Destination name* text box, type a meaningful name for the VPN connection. Click Create.

When the connection is created, it shows under Network Connections. To use the VPN client, you still need to configure the VPN connection. To configure the client, you need to right-click the *VPN connection* you just created and click *Properties*.

On the *General* tab, you can change the host name or IP address of the VPN server. The *Options* tab allows you to specify if the VPN connection remembers your credentials or not and how much idle time it waits before the VPN connection hangs up (disconnects).

On the *Security* tab, you can specify the type of VPN, whether data encryption is required, and the type of authentication. If you use L2TP, click the *Advanced settings* button to specify the pre-shared key used for authentication or if you are to use a digital certificate.

To connect using the VPN once the VPN connection is created and configured, open the Network and Sharing Center and click *Change adapter settings*. Then, right-click your VPN connection and click the *Connect/Disconnect*.

VPN RECONNECT

To provide constant connectivity, you use Internet Key Exchange version 2 (IKEv2), which automatically establishes a VPN connection when Internet connectivity is available. Only Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 R2 support VPN Reconnect.

On the server, you must do the following:

1. Create a user account with remote access permission.
2. Install a certificate with Server Authentication and IP security IKE intermediate extended key usage on the VPN server.
3. Install Routing and Remote Access and configure it as a VPN server.
4. Configure the Network Policy Server (NPS) to grant access for Extensible Authentication Protocol-Microsoft Challenge-Handshake Authentication Protocol version 2 (EAP-MSCHAPv2) authentication. NPS is discussed in Lessons 12 and 13.

On the client, you would do the following:

1. Specify the VPN server address or host name when configuring the VPN connection properties.
2. When you specify the VPN tunnel type, in the *Type of VPN* list, select *IKEv2* and select an encryption and authentication. VPN Reconnect supports two types of Authentication: *Extensible Authentication Protocol (EAP)* and *X.509 Machine Certificates*.
3. By default, the *Mobility* check box is enabled for *VPN Reconnect in Advanced properties*. If the check box is clear, the client cannot switch its local tunnel endpoint.
4. On the *Networking* tab, you can select *IPv4*, *IPv6*, or both protocols.
5. After the VPN connection is established, you can view the connection status on the *Details* tab of the *connection status* page.

CONFIGURING SPLIT TUNNELING

By default, when you connect to a VPN using the previous configuration, all web browsing and network traffic goes through the default gateway on the Remote Network unless you are communicating with local home computers. Having this option enabled helps protect the corporate network because all traffic also goes through firewalls and proxy servers, which prevent a network from being infected or compromised.

If you wish to route your Internet browsing through your home Internet connection rather than going through the corporate network, you can disable the *Use Default Gateway on Remote Network* option. Disabling this option is called using a ***split tunnel***.

ENABLE A SPLIT TUNNEL

GET READY. To enable a split tunnel, perform the following steps:

1. Right-click a VPN connection and click Properties.
2. Click the Networking tab.
3. Double-click the Internet Protocol Version 4 (TCP/IPv4).
4. On the *Internet Protocol Version 4 (TCP/IPv4) Properties* dialog box, click the Advanced button.
5. On the *Advanced TCP/IP Settings* dialog box, deselect the Use default gateway on remote network.
6. Click OK to close the *Advanced TCP/IP Settings* dialog box.

7. Click OK to close the *Internet Protocol Version 4 (TCP/IPv4) Properties* dialog box.
8. Click OK to close the *VPN Connection Properties* dialog box.

If you have to configure multiple clients to connect to a remote server, it can be a lot of work and it can be easy to make an error. To help simplify the administration of the VPN client into an easy-to-install executable, you can use the RAS Connection Manager Administration Kit (CMAK), which can also be installed as a feature in Windows Server 2012 and Windows Server 2012 R2. After an executable file is created that includes all of the VPN settings, the executable file is deployed on the client computers.

Configuring Remote Dial-In Settings for Users

When you connect through a dial-in connection or a VPN connection, the remote access connection must be authorized by the server running Network Policy Server (NPS) RRAS role service or another third-party RADIUS server.

Besides making sure that the username and password are valid, the remote access server verifies the dial-in properties of the user account and verifies if any NPS Network Policies have been applied, which specify which users can connect through the RRAS server and which users cannot connect.

For domain users, the dial-in properties are configured in the user account Properties dialog box, specifically the Dial-in tab, which is accessed in the Active Directory Users and Computers console, as shown in Figure 10-5. If you are dialing into a standalone server, you would open the user account in Local Users and Groups console in Computer Management.

Figure 10-5

Configuring Dial-in Properties

In Windows Server 2012 R2, by default, the Control access through NPS Network Policy is selected. By selecting the Control access through the NPS Network Policy, access permissions are determined by first matching the NPS Network Policy applied to the connection. NPS is discussed in more detail in Lessons 12 and 13.

If the Deny Access option is selected, the user will be blocked and will not be able to connect to the RRAS server. If the Allow Access option is selected, the use is automatically granted. It should be noted that NPS Network Policy can also perform some restrictions such as time restrictions.

If the Verify Caller ID check box is selected, the server verifies the caller's phone number. If the phone number does not match the configured phone number, the connection attempt is denied, assuming the caller, the phone system between the caller and the server, and the remote access server all support caller ID. If you configure a caller ID phone number for a user and one of the components do not support caller ID, the connection attempt is denied.

By default, the Callback Options setting is No Callback. If the Set By Caller option is selected, the server calls the caller back at a number specified by the caller. This option is used to avoid phone charges for the client.

If the Always Callback To: option is selected, an administrator must specify a number that the server always uses during the callback process. This option helps to make sure that only users from a certain number can call in. If the username and password have been compromised for a user, the user can still call in only from a specified number.

Finally, you can configure a static IP address or addresses and static routes that should apply to this user whenever he or she connects to a Remote Access server. These options make sure that the same IP address is assigned to a client and to make sure the user has the desired routes to resources.

Implementing NAT

Although CIDR helped use the IPv4 addresses more efficiently, additional steps had to prevent the exhaustion of IPv4 addresses. ***Network address translation (NAT)*** is used with masquerading to hide an entire address space behind a single IP address. In other words, it allows multiple computers on a network to connect to the Internet through a single IP address.

NAT enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. The NAT computer or device is usually a router (including routers made for home and small-office Internet connections) or a proxy server. As a result, you can do the following:

- Provide a type of firewall by hiding internal IP addresses.
- Enable multiple internal computers to share a single external public IP address.

The private addresses are reserved addresses not allocated to any specific organization. Because these private addresses cannot be assigned to global addresses used on the Internet and are not routable on the Internet, you must use a NAT gateway or proxy server to convert between private and public addresses. The private network addresses are expressed in RFC 1918:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

NAT obscures an internal network's structure by making all traffic appear originated from the NAT device or proxy server. To accomplish this, the NAT device or proxy server uses stateful translation tables to map the "hidden" addresses into a single address and then

rewrites the outgoing Internet Protocol (IP) packets on exit so that they appear to originate from the router. As data packets are returned from the Internet, the responding data packets are mapped back to the originating IP address using the entries stored in the translation tables.

When NAT is used to connect a private network to a public network, the following process occurs:

1. The client on the internal private network creates an IP packet, which is forwarded to the computer or device running NAT.
2. The computer or device running NAT changes the outgoing packet header to indicate the packet originated from the NAT computer or device's external address. It then sends the remapped packet over the public network such as the Internet to its intended destination. During this process, it will store the source address and the remapped NAT information in a table so that it can keep track of all source computers.
3. When the destination computer responds with packets, the destination computer sends packets back to the computer or device running NAT.
4. When the computer or device receives the packets back from the destination computer, the computer or device running NAT changes the packet header to the private address of the destination client. It then sends the packet to the client computer.

Enabling NAT is a simple process, which can be selected using the Routing and Remote Access Server Setup Wizard. To support NAT, you must have a server that has two network interfaces, one for the private network and one for the public network.

Configuring Routing

Routing is the process of selecting paths in a network where data will be sent. Routing is required to send traffic from one subnet to another within an organization, and it is required to send traffic from one organization to another. A computer running Windows can act as a router and include its own routing table, so that you can specify which direction data is sent toward its final destination.

Routers operate at the OSI Reference Model Layer 3, Network layer. Therefore, they are sometimes referred to as Layer 3 devices. Routers join subnets together to form larger networks and join networks together over extended distances or WANs. They can also connect dissimilar LANs, such as Ethernet LAN to a Fiber Distributed Data Interface (FDDI) backbone.

As larger networks are formed, there may be multiple pathways to get from one place to another. As WAN traffic travels multiple routes, the router chooses the fastest or cheapest route between the source and destination, while sometimes taking consideration of the current load.

Routing can also be performed by a layer 3 switch. ***Layer 2 switches*** (which operate at the layer 2 OSI model) are used to connect a host to a network by performing packet switching that allows traffic to be sent only to where it needs to be sent based on mapping MAC addresses of local devices. ***Layer 3 switches*** can perform layer 2 switching, but also perform routing based on IP addresses within an organization. Different from a router, layer 3 switches cannot be used for directly connecting WAN connections.

A server running Windows can have multiple network cards, each network card can be connected to a different subnet. To allow packets to be sent from one subnet to another subnet through the server, you need to configure routing on the server.

A ***routing table*** is a data table that is stored in a router or networked computer that lists the routes of particular network distances and the associated metrics or distances associated with those routes. The routing tables are manually created with ***static routes***, or are dynamically

created with routing protocols such as ***Routing Information Protocol (RIP)***, based on the current routing topology.

Microsoft Windows supports the Routing Information Protocol through RRAS. RIP has been a popular distance-vector routing protocol for small organizations. RIP uses broadcasts where the entire routing table is sent to the other routers within the network. To determine the distance or cost between networks, RIP uses the metric of hop count, which is the count of routers. The maximum number of hops allowed for RIP is 15. The hop count of 16 is considered infinite distance and therefore, it is considered nonreachable.

RIP was improved with RIP version 2 (RIPv2) by using multicasts to send the entire routing table to all adjacent routers at the address of 224.0.0.9 instead of using broadcast. It also incorporates classless routing, which includes the network mask to allow classless routing advertisement. Finally, RIPv2 uses authentication to ensure that routes being distributed throughout the network are coming from authorized sources.

Routing can be enabled using RRAS. You will use RRAS to configure RIP or define static routes. You can also define static routes using the `Route` command.

Windows Server 2012 R2 supports ***Border Gateway Protocol (BGP)***, which enables dynamic distribution and learning of routes by site-to-site (S2S) interfaces of RRAS. By adding BGP, the server can act as a gateway to the Internet, tenant premises, and tenant virtual networks. To enable BGP on an interface, use the `Add-BgpRouter cmdlet.`

CONFIGURE ROUTING

GET READY. To configure routing on Windows Server 2012 and Windows Server 2012 R2, perform the following steps:

1. Open Server Manager.
2. Click Tools > Routing and Remote Access.
3. Right-click the server and select Configure and Enable Routing and Remote Access.
4. When the *Routing and Remote Access Server Setup Wizard* opens, click Next.
5. On the *Configuration* page, select Custom configuration and click Next.
6. On the *Custom Configuration* page, select LAN routing and click Next.
7. On the *Completing the Routing and Remote Access Server Setup Wizard* page, click Finish.
8. When the Routing and Remote Access service is ready to use, click the Start service button.

MANAGING STATIC ROUTES

Static-routed IP networks are best suited for small, single-paths that don't change much. To view the IP routing table usingi RRAS, expand the server node, expand the IPv4 or IPv6 nodes, right-click the static routes node, and then click *Show IP Routing Table* (see Figure 10-6).

Figure 10-6

Displaying static routes using RRAS

When you define routes, you specify the network address of the destination, the network mask, and the local router or next hop to get to its destination. When the packet reaches the local router, the router will then use its routing table to determine what the next hop that the packet needs to be sent to. The process will continue until the packet reaches the destination network, where the packets are then sent to the destination host.

CREATE A NEW STATIC ROUTE USING RRAS

GET READY. To create a new static route using RRAS, perform the following steps:

1. Open Server Manager.
2. Click the Tools > Routing and Remote Access.
3. Expand server note and expand the IPv4 node.
4. Right-click Static Routes node and select New Static Route.
5. When the *IPv4 Static Route* dialog box opens, specify the interface that you want to assign the static route.
6. For the destination, type in the network address, such as 172.24.0.0 or 192.168.5.0. You can also specify a single address.
7. Specify the network mask for the network such as 255.255.00 or 255.255.255.0. If you define a single address for the destination, specify 255.255.255.255.
8. For the *Gateway*, specify the router that is the next hop toward the final destination.
9. Specify a metric for the specified route.
10. Click OK.

CONFIGURING RIP

Microsoft Windows supports the Routing Information Protocol through RRAS. RIP has been a popular distance-vector routing protocol for small organizations. RIP uses broadcasts where the entire routing table is sent to the other routers within the network. To determine the distance or cost between networks, RIP uses the metric of hop count, which is the count

of routers. The maximum number of hops allowed for RIP is 15. The hop count of 16 is considered infinite distance and therefore, it is considered nonreachable.

RIP was improved with RIP version 2 (RIPv2) by using multicasts to send the entire routing table to all adjacent routers at the address of 224.0.0.9, instead of using broadcasts. It also incorporates classless routing, which includes the network mask to allow classless routing advertisement. Lastly, RIPv2 uses authentication to ensure that routes being distributed throughout the network are coming from authorized sources.

CONFIGURE ROUTING

GET READY. To configure RIP on Windows Server 2012 or Windows Server 2012 R2, perform the following steps:

1. Open Server Manager.
2. Click Tools > Routing and Remote Access.
3. Expand the server node, and expand IPv4.
4. Right-click the General tab and select New Routing Protocol. The *New Routing Protocol* dialog box opens.
5. Select RIP Version 2 for Internet Protocol.
6. Click OK to close the *New Routing Protocol* dialog box. A RIP node will appear under IPv4.
7. Right-click RIP and select New Interface. The *New Interface for RIP Version 2 for Internet Protocol* dialog box opens.
8. Select the interface on which you want to use RIP.
9. Click OK to close the *New Interface for RIP Version 2 for Internet Protocol* dialog box. The *RIP Properties* dialog box opens.
10. Click OK to close the *RIP Properties* dialog box.

If you need to configure RIP, right-click the *RIP node* and select *Properties*. For example, if you want to specify which routes to accept, select the *Security* tab; if you want to specify the neighbors that the RRAS router interfaces with, select the *Neighbors* tab (see Figure 10-7).

Figure 10-7

Configuring the RIP Security and Neighbors tabs

CONFIGURING DEMAND-DIAL ROUTING

Routing and Remote Access also supports ***demand-dial routing***, which is a connection to a remote site that is activated when data is sent to the remote site. When there is not more data to be sent, the link is disconnected. The use of demand-dial routing can be used with dial-up telephone lines or VPN connections, which can reduce connection costs.

To use demand-dial routing, you must enable demand-dial routing by right-clicking the server, selecting *Properties* and selecting the *General* tab. Then select *LAN and demand-dial routing*. Then, right-click *Network Interfaces*, select *New Demand-dial Interface* to go through a wizard to define the dial-up connection or VPN connection.

CONFIGURING THE DHCP RELAY AGENT

Before your DHCP server can provide IP address leases, you have to define a scope that includes a range of IP addresses that can be distributed. A scope defines a single physical subnet on your network to which DHCP services are offered.

By default, routers do not allow broadcasts to be sent to routers. Therefore, for the DHCP server to hand out addresses to a subnet, it has to be physically connected to the subnet, or you have to install a DHCP Relay Agent or DHCP Helper on the subnet that relays the DHCP requests to the DHCP server. The DHCP relay agent could be a Windows server or workstation or built into a router or switch.

The relay agent is already installed for IPv4. If you need it for IPv6, right-click the *General node* under IPv6, and select *New Routing Protocol*. When the New Routing Protocol dialog box opens, DHCP v6 relay Agent is already highlighted. Click *OK*.

CONFIGURE THE DHCP RELAY AGENT

GET READY. To configure the DHCP Relay Agent, perform the following steps:

1. Open Server Manager.
2. Click Tools > Routing and Remote Access.
3. Expand the server node and the IPv4 node.
4. Right-click DHCP Relay Agent and select Properties. The *DHCP Relay Agent Properties* dialog box opens.
5. In the *Server* address box, type in the address of the DHCP server and click Add.
6. Click OK to close the *DHCP Relay Agent Properties* dialog box.

Configuring Web Application Proxy in Passthrough Mode

The ***Web Application proxy*** is a Remote Access role service introduced in Windows Server 2012 R2 that provides reverse proxy functionality for web applications inside an organization network so users can access applications externally no matter what device they are using. In addition, the Web Application proxy preauthenticates access to web applications using Active Directory Federation Services (AD FS) and also functions as an AD FS proxy (in fact, it replaces the AD FS proxy that was included with Windows Server 2012).

A ***reverse proxy*** is a proxy server that retrieves resources from servers on behalf of a client by publishing internal applications to external users or publishing applications (although mostly external) to internal users. The resources are then relayed through the proxy server to the client. As far as the client is concerned, the resources originate from the server itself. The Web Application proxy can be used to hide the existence of the resource server and can selectively access the necessary applications on the servers inside the organization.

Without a reverse proxy server, you will have to allow network communications from external networks (such as the Internet) to your internal network. The Web Application proxy resides in the DMZ, which is a secure zone and ensures that the communication meets security requirements before it's allowed into the internal networks. Therefore, by using a reverse proxy, you protect applications from external threats and help protect internal resources by providing a Defense in Depth approach (in which several layers of security controls are used throughout your network).

In Windows Server 2012 R2, a reverse proxy is provided by a Remote Access Role service: the Web Application proxy. The Web Application proxy is integrated into the Remote Access Management console, which allows you to manage your Web Application proxy servers and other Remote Access technologies using one console.

When using the Web Application proxy, you should place the Web Application proxy server behind a front-end firewall to separate the server from the Internet or you should place it between two firewalls (one to separate it from the Internet and one to separate it from the corporate network).

TAKE NOTE*

The Web Application proxy configuration is stored on the AD FS servers in your organization; therefore, Web Application proxy servers require connectivity to the AD FS servers.

The process for configuring the Web Application proxy server is as follows:

1. Install the Web Application proxy server.
2. Connect the Web Application proxy server to the AD FS server using the Web Application Proxy Configuration Wizard.
3. Publish the sample application.
4. Validate connectivity to the sample application using the default AD FS authentication scheme.

Preauthentication is the process by which users and devices are authenticated before they access an application. Web Application proxy servers support two forms of preauthentication:

- **AD FS preauthentication:** Users must authenticate to AD FS servers before Web Application proxy redirects users to the published web applications.
- **Pass-through preauthentication:** Users are not required to enter credentials before they connect to published web applications.

INSTALL THE WEB APPLICATION PROXY ROLE SERVICE

GET READY. To install the Web Application Proxy Role Service, perform the following steps:

1. On the server in the DMZ, open Server Manager.
2. Click Manage > Add roles and features.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install Remote Access Role to, and then click Next.
6. On the *Select server roles* page, select Remote Access and then click Next.
7. Click Next twice.
8. In the *Select role services* dialog box, select Web Application Proxy, click Add Features, and then click Next.
9. In the *Confirm installation selections* dialog box, click Install.
10. When the installation is complete, click the Close button.

CONFIGURE THE WEB APPLICATION PROXY

GET READY. To configure the Web Application proxy, perform the following steps:

1. Using *Server Manager*, click the yellow triangle with the black exclamation point. Then click Open the Web Application Proxy Wizard.
2. On the *Welcome* page, click Next.
3. On the *Federation Server* page, in the *Federation service name* text box, type the federation service name (such as adfs.contoso.com).
4. In the *User name* text box and the *Password* text box, type the name of an administrator and the password for the federation server. Then click Next.
5. On the *AD FS Proxy Certificate* page, select the digital certificate used with the AD FS and then click Next.
6. On the *Confirmation* page, click Configure.
7. On the *Results* page, click Close.

A message might display, indicating that you must configure the spn for the service account (for example, if AD FS is running on server01.contoso.com and the Group Managed Service Account is contoso\adfs). If so, execute the following command on a domain controller.

```
setspn -S http/server01.contoso.com adfs
```

PUBLISH AN APPLICATION

GET READY. To publish an application, perform the following steps:

1. Using *Server Manager*, open the Remote Access Management console.
2. On the Web Application proxy server, using the *Remote Access Management* console, click Web Application Proxy. In the *Tasks* pane, click Publish.
3. When the *Publish New Application Wizard* page displays, on the *Welcome* page, click Next.
4. On the *Preauthentication* page, click Pass-through and then click Next.
5. On the *Publishing Settings* page, type the following information and then click Next:
   - *Name:* This name is used only in the list of published applications in the Remote Access Management console.
   - *External URL:* This is the external URL for this application.
   - *External certificate list:* Select a certificate whose subject covers the external URL.
   - *Backend server URL:* This is the URL of the backend server. The value is automatically entered when you type the external URL and you should change it only if the backend server URL is different.
6. On the *Confirmation* page, review the settings and then click Publish.
7. On the *Results* page, validate connectivity to the web application and then click Close.

Business Case Scenarios

Scenario 10-1: Installing a VPN Server

Your manager comes up to you and says that you need to install a VPN server so that users can work while they are doing sales calls with customers. Your manager wants you to make it as secure as possible with the VPN technologies that appear in this lesson. How would you configure the server?

Scenario 10-2: Configuring Routing

You have a corporate office with 12 remote sites. Each remote site has a site server that also acts as a router. When you look at each of the servers, you realize that the previous administrator used the route command to specify static routes. However, as you have had to do maintenance and move some of the network connections, you find it difficult to modify all of the servers to reflect the changes. In addition, you will be adding four more sites over the next six months. What do you recommend to your manager so that you don't have to buy any more network equipment?

Configuring Direct Access

LESSON 11

Understanding DirectAccess

THE BOTTOM LINE

DirectAccess is a new feature introduced with Windows 7 and Windows Server 2008 R2 that provides seamless intranet connectivity to DirectAccess client computers when they are connected to the Internet. Different from the traditional virtual private network (VPN) connections, DirectAccess connections are automatically established and they provide always-on seamless connectivity.

DirectAccess overcomes the limitations of VPNs by automatically establishing a bi-directional connection from client computers to the organization's network using IPsec and Internet Protocol version 6 (IPv6). For organizations that have not deployed IPv6, you can use transition mechanisms such as 6to4 and Teredo IPv6 transition technologies for connectivity across the IPv4 Internet and the Intra-Site Automatic Tunnel Addressing (ISATAP) IPv6 transition technology, so that DirectAccess clients can access IPv6-capable resources across your IPv4-only intranet. As a result, remote client computers are automatically connected to the organization's network so that they can be easily managed and kept up-to-date with critical updates and configuration changes.

Understanding DirectAccess Requirements

Compared to other forms of remote access, DirectAccess is more complex, which has more required components. Of course, with the complexity, you get much more functionality that you did with other remote access technologies.

Besides installing DirectAccess on the VPN server, you need to make sure that you prepare the network, the server, and the clients. A little planning also goes a long way when implementing DirectAccess.

UNDERSTANDING DIRECTACCESS SERVER REQUIREMENTS

To use DirectAccess, the DirectAccess server requires the following:

- The server must be part of an Active Directory domain.
- The server must be running Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- If the DirectAccess server is connected to the intranet and published over Microsoft Forefront Threat Management Gateway (TMG) or Microsoft Forefront Unified Access Gateway 2010 (UAG), a single network adapter is required. If the DirectAccess server is connected as an edge server, it will need two network adapters (one for the Internet and one for the intranet).

- Implementation of DirectAccess in Windows Server 2012 R2 does not require two consecutive static, public IPv4 addresses as was required with Windows Server 2008 R2. However, to achieve two-factor authentication with a smart card or Operational Data Provider (OTP) deployment, DirectAccess server still needs two public IP addresses.
- You can deploy Windows Server 2012 R2 DirectAccess behind a NAT support, which avoids the need for additional public addresses. However, only IP over HTTPS (IP-HTTPS) is deployed, allowing a secure IP tunnel to be established using a secure HTTP connection.
- With Windows Server 2012, you can use Network Load Balancing (up to eight nodes) to achieve high availability and scalability for both DirectAccess and RRAS.

In addition, you need the following in your network infrastructure:

- An Active Directory domain that runs a minimum of Windows Server 2008 R2 domain functional level.
- Group policy for central administration and deployment of DirectAccess client settings.
- One domain controller running Windows Server 2008 SP2, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- Public Key Infrastructure (PKI) to issue computer certificates for authentication and health certificates when NAP is deployed and computer certificates for authentication. The SSL certificates installed on the DirectAccess server must have a Certificate Revocation List (CRL) distribution point that is reached from the Internet. Finally, the certificate Subject filed must contain the Fully Qualified Domain Name (FQDN)that can be resolved to a public IPv4 address assigned to the DirectAccess server by using the DNS on the Internet.
- When using Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), DNS must run on at least Windows Server 2008 R2, Windows Server 2008 with the Q958194 hotfix, Windows Server 2008 SP2 or later, or a third-party DNS server that supports DNS message exchanges over the ISATAP.
- IPsec policies. DirectAccess utilizes IPsec policies that are configured and administered with Windows Firewall with Advanced Security.
- Internet Control Message Protocol Version 6 (ICMPv6) Echo Request traffic. You must create separate inbound and outbound rules that allow ICMPv6 Echo Request messages. DirectAccess clients that use Teredo for IPv6 connectivity to the intranet use the ICMPv6 message when establishing communication.
- IPv6 and transition technologies such as ISATAP, Teredo, and 6to4 must be available for use on the DirectAccess server. For each DNS server running Windows Server 2008 or higher, you need to remove the ISATAP name from the global query block list.
- Network Access Protection (NAP) is an optional component of the DirectAccess solution that allows you to provide compliance checking and enforce security policy for DirectAccess clients over the Internet. Unlike Windows Server 2008 R2, Windows Server 2012 R2 DirectAccess provides the capability to configure NAP health checks directly from the setup user interface.

UNDERSTANDING DIRECTACCESS CLIENT REQUIREMENTS

To use DirectAccess, the clients must be Windows 7 Enterprise Edition, Windows 7 Ultimate Edition, Windows 8, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2. You will not be able to deploy DirectAccess for Windows Vista or earlier or Windows Server 2008 or earlier. Finally, the client must be joined to an Active Directory domain.

Running the Remote Access Setup Wizard

To configure DirectAccess itself, you use the newly created Remote Access Management console. By using the Remote Access Management console, you can configure DirectAccess using the Remote Access Setup Wizard.

The Remote Access Setup Wizard breaks the installation to the following steps, as shown in Figure 11-1:

Step 1: Remote Clients: Allows you to specify which clients within your organization can use DirectAccess. You specify the computer groups that you want to include and specify if you want to include Windows 7 clients.

Figure 11-1

Using the the Access Setup Wizard

Step 2: Remote Access Server: Allows you to configure the network connections based on one or two network cards and which adapters are internal and which adapters are external. You can also specify the use of smartcards and specify the certificate authority (CA) to use for DirectAccess to provide secure communications.

Step 3: Infrastructure Servers: Allows you to configure how the clients access the core infrastructure services, such as Active Directory domain controllers and DNS servers. You also specify an internal web server that can provide location services for infrastructure components to your DirectAccess clients.

Step 4: Application Servers: Allows you to configure your end-to-end authentication and security for the DirectAccess components. It also allows you to provide secure connections with individual servers that you want to establish secure connections with.

IMPLEMENTING CLIENT CONFIGURATION

With Window 7 and Windows Server 2008 R2, DirectAccess used the ***DirectAccess Connectivity Assistant (DCA)***, which is a free Solution Accelerator that is installed on the

DirectAccess clients and adds an icon to the notification area of the desktop. The DCA provides tools to help users reconnect if a problem occurs. It also helps with diagnostics used by the help desk. It is also used to detect whether one-time passwords (OTP) are required, and it helps your system determine whether it is connected to the intranet or the Internet.

In Windows 8, the DCA was replaced by the ***Network Connectivity Assistant (NCA)***. Although the DCA has to be downloaded from Microsoft, the NCA is included in the Windows 8 operating system, and installation and deployment are not required.

CONFIGURE REMOTE CLIENTS

GET READY. To configure the Direct Access Server, perform the following steps:

1. Start Server Manager.
2. Click Tools > Remote Access Management. The *Remote Access Management console* opens.
3. In the left pane, under *Configuration*, click the DirectAccess and VPN node.
4. Under *Step 1, Remote Clients*, click Edit. The *DirectAccess Client Setup Wizard* opens.
5. On the *Deployment Scenario* page, select Deploy full DirectAccess for client access and remote management. Click Next.
6. If you need to add additional groups that specify which client computers can access the corporate network using DirectAccess, on the *Select Groups* page, select Add. Type the name of the group of computers that you want to include as DirectAccess clients and click OK.
7. Back on the *Select Groups* page, if Forefront UAG is configured to use force tunneling for DirectAccess clients, select Use force tunneling. Click Next.
8. On the *Network Connectivity Assistant* page (see Figure 11-2), double-click a blank resource space.

Figure 11-2

Configuring the Network Connectivity Assistant

9. When the Configure Corporate Resources for NCA dialog box opens, specify HTTP or ping and specify an URL or FQDN in the text box. Click Add.
10. In the *Helpdesk email address* text box, specify an address to the organization's help desk.
11. By default, the DirectAccess connection name is *Workplace Connection*. If you wish to change it, do so.
12. If you want DirectAccess clients to use local DNS servers for name resolution, select the Allow DirectAccess clients to use local name resolution.
13. Click Finish.

IMPLEMENTING DIRECTACCESS SERVER

Using the Remote Access Server Setup Wizard, you can configure the DirectAccess server. It also allows you to specify what method of authentication to use.

CONFIGURE THE DIRECTACCESS REMOTE ACCESS SERVER

GET READY. To configure the DirectAccess server, perform the following steps:

1. Continuing with the *Remote Access Setup Configuration* page, under *Step 2, Remote Access Server*, click Edit. The *Remote Access Server Setup Wizard* starts.
2. On the *Network Topology* page, select the appropriate topology and specify the public name or IPv4 address used by clients to connect to the Remote Access server. Click Next.
3. On the *Network Adapters* page (see Figure 11-3), make sure that the appropriate network adapters are selected for the external and internal networks.

Figure 11-3

Configuring the network adapters

4. Specify the digital certificate that you want to use for-HTTPS connections or select the Use a self-signed certificate created automatically by DirectAccess. Click Next.
5. On the *Prefix Configuration* page, specify the internal network IPv6 and IPv6 prefix assigned to DirectAccess client computers. Click Next.
6. On the *Authentication* page, specify whether you want to use Active Directory credentials (username/password) or Two-factor authentication. If you choose *Two-factor authentication*, you can select Use OTP.
7. If desired, you can use computer certificates. If you select the Use computer certificates, you have to choose the *root* or *intermediate certification authority (CA)*. If you decide to use *intermediate certification authority*, you need to select the *Use an intermediate certificate*.
8. If you wish to allow Windows 7 clients, enable the *Enable Windows 7 client computers* to connect via DirectAccess.
9. If you want to use Network Access Protection (NAP), select the Enforce corporate compliance for DirectAccess clients with NAP.
10. Click Next.
11. On the VPN Configuration page, the *IP Address Assignment* is set to *Assign addresses automatically*. Click Finish.

IMPLEMENTING INFRASTRUCTURE SERVERS

After the DirectAccess server is configured, you need to configure the infrastructure servers to support DirectAccess. For example, you will need to configure the DNS servers, and you need to specify your management servers such as WSUS servers.

DirectAccess clients use the ***network location server (NLS)*** to determine their locations. The network location server is an internal web server. If the client computer can connect with HTTPS to the URL specified, the client computer assumes it is on the intranet and disables DirectAccess components. If the client cannot reach the NLS, it assumes it is on the Internet. The URL for the NLS is distributed using a GPO.

To configure a network location server, install IIS on a Windows server. Then for a website, bind a name such as nsl.contoso.com and associate a NLS DNS name to the IP address. Finally, you should make sure that this server is highly available. So use technology such as Network Load Balancing and make sure you have redundant hardware.

To ensure that DirectAccess clients can correctly detect when they are on the Internet, you can configure IIS server to deny connections from Internet-based clients with the IP and Domain Restrictions Web server (IIS) role service. Alternatively, you can ensure that the CRL distribution point location in the certificate being used for network location cannot be accessed from the Internet.

CONFIGURE THE DIRECTACCESS INFRASTRUCTURE SERVERS

GET READY. To configure the DirectAccess Infrastructure servers, perform the following steps:

1. Continuing with the *Remote Access Setup Configuration* page, under *Step 3, Infrastructure Server*, click Edit. The *Infrastructure Server Setup Wizard* starts.
2. On the *Network Location Server* page, type the URL of the network location in the appropriate box. Click Next.
3. On the *DNS* page (see Figure 11-4), verify the DNS suffixes and internal DNS servers. Then, click Next.

Figure 11-4

Specifying the DNS servers

4. On the *DNS Suffix Search List* page, verify the domain suffixes and click Next.
5. On the *Management* page, double-click the first line of the *Management Servers* box.
6. When the *Add a Management Server* dialog box opens, add the names of your management servers, such as your Windows Update Server. Click OK.
7. Click Finish.

Preparing for DirectAccess Deployment

Before installing and configuring DirectAccess, there is some work that needs to be completed. You need to make sure that you have IPv6 and any transitional IPv6 technologies in place. You need a certificate server, and you need to have external and internal DNS entries.

CONFIGURING DNS FOR DIRECTACCESS

As a VPN technology that has internal resources and external clients, DirectAccess requires internal and external DNS. DirectAccess requires two external DNS A records, both of which point to the first of your two consecutive IP addresses that you specified for the DirectAccess server. These are:

- DirectAccess server, such as directaccess.contoso.com
- Certificate Revocation List (CRL), such as crl.contoso.com

Internally, DNS needs the DNS records for the NLS server and one for the CRL.

The dynamic update feature of DNS makes it possible for a DNS client computer to register and dynamically update the resource records with a DNS server whenever a client changes its networks address or host name. However, it also allows any authorized client to register any unused host name, including those special or reserved names, such as Web Proxy Automatic Discovery Protocol (WPAD) and the Intra-site Automatic Tunnel Addressing Protocol (ISATAP).

ISATAP provides a transition between networks that are based on IPv4 to IPv6, which is used to encapsulate IPv6 packets with an IPv4 header, making it possible for the IPv6 packets to be transmitted through an ISATAP router. Because ISATAP does not support automatic router discovery, ISATAP hosts a potential list (PRL) to discover available ISATAP routers.

The host name would be isatap, such as found in isatap.contoso.com. Therefore, if you need to use ISATAP, you need to remove ISATAP from the DNS global query block list by executing the following command at a command prompt:

```
dnscmd /config /globalqueryblocklist isatap
```

CONFIGURING CERTIFICATES FOR DIRECTACCESS

To implement DirectAccess, you are going to need a Certificate Services public key infrastructure (PKI), which requires installing an Active Directory Certificate Services (AD CS) role and Certificate Authority (CA) role. The CA has to be configured as an Enterprise Root CA.

Each DirectAccess client needs to have a computer certificate to establish the IPsec connection to the DirectAccess server and IP-HTTPS connection. The computer certificates are usually assigned using the Microsoft Certificate Server via group policy-based computer certificate auto-enrollment.

The DirectAccess server requires the following certificates:

- The IP-HTTPS listener on the DirectAccess server requires a website certificate. The IP-HTTPS listener requires a website certificate, and the DirectAccess client must be able to contact the server hosting the CRL for the certificate. If the CRL check fails, the IP-HTTPS connection fails. It is recommended you use a third-party commercial certificate for the IP-HTTPS listener.
- The DirectAccess server requires a computer server to establish the IPsec connections with the DirectAccess clients.

CONFIGURE CERTIFICATE REQUIREMENTS

GET READY. To configure the certificate requirements on the domain controller with the CA (Enterprise CA), perform the following steps:

1. If necessary, open Server Manager.
2. Click Tools > Certificate Authority. The *Certification Authority console* opens.
3. Right-click the server and select Properties.
4. When the *Properties* dialog box opens, select the Extensions tab.
5. On the *Extensions* tab, click Add.
6. On the *Add Location* dialog box, type http://crl.contoso.com/crld/ in the *Location* text box.
7. Select the CAName variable and click Insert.
8. Select CRLNameSuffix variable and click Insert.
9. Select DeltaCRLAllowed variable and click Insert.
10. At the end of the text in the *Location* text box, add .crl. When you are finished, the Add Location dialog box should look like Figure 11-5.

Figure 11-5

An example location for CRL

11. Click OK to close the *Add Location* dialog box.
12. Select Include in CRLs. Clients use this to find Delta CRL locations. option and the Include in the CDP extensions of issued certificates option.
13. On the *Add Location* dialog box, type \\win2012srv\crldist$\ in the *Location* text box.
14. Select the CAName variable and click Insert.
15. Select CRLNameSuffix variable and click Insert.
16. Select DeltaCRLAllowed variable and click Insert.
17. After you insert DeltaCRLAllowed, at the end of the text in the *Location* text box, add .crl.
18. Click OK to close the *Add Location* dialog box.
19. Click OK to close the *Properties* dialog box.
20. When it asks you to restart Active Directory Certificate Services, click Yes.
21. On the *Certificate Authority console*, right-click Certificate Templates and click Manage. The *Certificate Templates console* opens.
22. Right-click the Web Server template, and select Duplicate Template.
23. When the *Properties of New Template* dialog box opens, select the General tab.
24. On the *General* tab, type Contoso Web Server Certificate in the *Template display name* text box.
25. Select the Request Handling tab.
26. In the *Request Handling* tab, select the Allow private key to be exported.
27. Select the Security tab.
28. On the *Security* tab, make sure Authenticated Users is selected. Then click Enroll under the *Allow* column.
29. Click OK to close the *Properties of New Template* dialog box.
30. Close the *Certificate Template console*.
31. In the *Certification Authority console*, right-click Certificate Templates, select New, and select the Certificate Template to Issue.
32. Select the Contoso Web Server Certificate and click OK.
33. Close the *Certification Authority console*.
34. In *Server Manager*, click Tools > click Group Management.
35. In the *Group Management console*, right-click Default Domain Policy and select Edit.

36. On the *Group Policy Management Editor*, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies, as shown in Figure 11-6.

Figure 11-6

Viewing the Public Key policies

37. Right-click Automatic Certificate Request, select New, and select Automatic Certificate Request.
38. When the *Welcome to the Automatic Certificate Request Setup Wizard* starts, click Next.
39. On the *Certificate Template* page, select the Computer certificate template and click Next.
40. When the wizard is complete, click Finish.

INSTALL A DIGITAL CERTIFICATE ON THE NETWORK LOCATOR SERVER

GET READY. To install a digital certificate on the Network Locator Server, perform the following steps:

1. To acquire the Computer certificate, open a command prompt and execute the following command:

   `gpudate /force`

2. At the command prompt, execute the following command, and then press Enter:

   `mmc`

3. When the console opens, open the File menu and select Add/Remove Snap-in.
4. On the *Add or Remove Snap-ins* dialog box, double-click Certificates.

5. When the *Certificates Snap-in* dialog box opens, select Computer account, and click Finish.
6. When the *Select Computer* dialog box opens, click Finish.
7. Click OK to close the *Add or Remove Snap-ins* dialog box.
8. In the console, navigate to \Personal\Certificates. You should see the Computer certificate, as shown in Figure 11-7.

Figure 11-7

Viewing the computer certificate

9. Right-click Certificates, select All Tasks, and then select Request New Certificate.
10. When the *Certificate Enrollment Wizard* opens, click Next.
11. On the *Select Certificate Enrollment Policy* page, click Next.
12. On the *Request Certificates* page, select Contoso Web Server Certificate.
13. Click More information is required to enroll for this certificate. Click here to configure settings.
14. When the *Certificate Properties* dialog box opens, select Common name for the *Subject name Type*.
15. In the *Value* text box, type nls.contoso.com. Click the top Add button. The CN=nls.contoso.com value should appear on the right side of the dialog box.
16. Click OK to close the *Certificate Properties* dialog box.
17. Back on the *Request Certificates* page, click Enroll.
18. When the certificate installation succeeds, click Finish. The certificate appears in the *Personal\Certificates* folder.
19. Close the console window. If you are prompted to save settings, click No.
20. Open Server Manager.
21. Click Tools > Internet Information Services (IIS) Manager.
22. In the console tree of Internet Information Services (IIS), navigate to and click Default Web site.

23. On the *Default Web Site Home* page, click Bindings under *Edit Site in the Actions pane*. The *Site Bindings* dialog box opens.
24. Click Add.
25. For the *Type*, select https.
26. For the *Host name*, type nls.contoso.com.
27. For the *SSL certificate*, select nls.contoso.com. The *Add Site Binding* dialog box should look similar to Figure 11-8.

Figure 11-8

Configuring an IIS site binding

28. Click OK to close the *Add Site Bindings* button.
29. Click Close to close the *Site Bindings* dialog box.
30. Close the *Internet Information Services (IIS) Manager console*.

Business Case Scenarios

Scenario 11-1: Understanding DirectAccess

You are an administrator with the Contoso Corporation. The Contoso Corporation has about 1,100 users. Among those 1,100 users, there are 200 users who use VPN to connect to the organization network when they are not in the office. However, you realize that you are having trouble keeping the clients updated and performing other maintenance tasks as needed because these clients are often not connected to the network. What should you do?

Scenario 11-2: Installing DirectAccess

You are installing DirectAccess on an internal server. However, you need to configure the network location server (NLS). Your manager wants to know what the NLS is and what is required. What do you tell your manager?

Configuring a Network Policy Server

LESSON 12

Configuring a Network Policy Server Infrastructure

THE BOTTOM LINE

Remote Authentication Dial-In User Service (RADIUS) is a networking and client/server protocol that provides centralized ***authentication, authorization, and accounting (AAA)*** management for computers that connect and use a network service. It can be used in wireless and remote access connection technologies, 802.1x switches, and Remote Desktop Services Gateway.

RADIUS is defined in the Internet Engineering Task Force (IETF) RFCs 2865 and 2866. Microsoft's RADIUS server is ***Network Policy Server (NPS)***. By installing and configuring RADIUS, you can create and enforce wide network access policies for client health, connection request authentication, and connection request authorization.

As mentioned before, RADIUS is used for authentication, authorization, and accounting. ***Authorization*** is the process that determines what a user is permitted to do on a computer system or network. After a client or device is authenticated, the client or device must be authorized to access any type of network resource. The authorization controls what resources an authenticated user can and cannot access. Finally, accounting keeps track of what resources a user has accessed or attempted to access.

When you implement RADIUS, Windows computers running Routing and Remote Access and/or wireless access points can forward access requests to a single RADIUS server (see Figure 12-1). The RADIUS server then queries the domain controller for authentication and applies NPS Network Policies to the connection requests. NPS Network Policies are discussed in the next two lessons.

Figure 12-1

Looking at RADIUS servers and clients

TAKE NOTE *

RADIUS clients (also referred to as access servers) are servers (such as servers running RRAS) and devices (such as wireless access points and 802.1X switch) that forward RADIUS requests to a RADIUS server. An ***access client*** is a computer or device that contacts or connects to a RADIUS client, which requires authentication and authorization to connect.

When NPS is used as a RADIUS server, authentication, authorization, and accounting follow these steps:

1. When an access client accesses a VPN server or wireless access point, a connection request is created that is sent to the NPS server.
2. The NPS server evaluates the Access-Request message.
3. If required, the NPS server sends an Access-Challenge message to the access server. The access server processes the challenge and sends an updated Access-Request to the NPS server.
4. The user credentials are checked and the dial-in properties of the user account are obtained by using a secure connection to a domain controller.
5. When the connection attempt is authorized with both the dial-in properties of the user account and network policies, the NPS server sends an Access-Accept message to the access server. If the connection attempt is either not authenticated or not authorized, the NPS server sends an Access-Reject message to the access server.
6. The access server completes the connection process with the access client and sends an Accounting-Request message to the NPS server, where the message is logged.
7. The NPS server sends an Accounting-Response to the access server.

RADIUS has been officially assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting by the Internet Assigned Numbers Authority (IANA). However, before IANA officially allocated ports 1812 and 1813, ports 1645 and 1646 were used for authentication and accounting. Although Microsoft RADIUS servers default to port 1812 and 1813, others can still use 1645 an 1646. Therefore, if the RADIUS server is separated by a firewall, you should open all four ports.

Installing and Configuring a RADIUS Server

Installing NPS—Microsoft's RADIUS server—is a simple process, which is done with Server Manager. After NPS is installed, you then use the Network Policy Server console to configure NPS.

INSTALL NETWORK POLICY SERVER (NPS)

GET READY. To install NPS, follow these steps:

1. Click the Server Manager button on the task bar to open *Server Manager*.
2. At the top of Server Manager, select Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation, and then click Next.
5. Click Select a server from the server pool, click the name of the server to install Network Policy and Access Services to, and then click Next.
6. On the *Server Roles* page (see Figure 12-2), select Network Policy and Access Services.

Figure 12-2

Installing Network Policy and Access Services

7. When it asks you to add features that are required for Network Policy and Access Services, click Add Features.
8. Back on the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Network Policy and Access Services* page, click Next.
11. On the *Select role services* page, with the NPS selected, click Next.
12. On the *Confirm installation* page, click Install.
13. When the installation is complete, click Close.

After the NPS is installed, it can be configured using the Network Policy Server console.

Configuring RADIUS Clients

To configure NPS as a RADIUS server, you can use either standard configuration or advanced configuration in the NPS console or in Server Manager.

The standard configuration includes:

- RADIUS server for dial-up or VPN connections
- RADIUS server for 802.1X wireless or wired connections
- NAP policy server (The NAP policy server is discussed in Lesson 14)

When you configure NPS as a RADIUS server for dial-up or VPN connections, you create a network policy.

CONFIGURE NPS FOR RADIUS SERVER FOR VPN CONNECTIONS

GET READY. To configure NPS for RADIUS server for VPN connections, perform the following steps:

1. Open the Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens.
3. In the main pane, select RADIUS server for Dial-Up or VPN Connections under the *Standard Configuration*.
4. Click Configure VPN or Dial-Up. The *Configure VPN or Dial-Up Wizard* opens.
5. On the *Select Dial-up or Virtual Private Network Connections Type* page, select Virtual Private Network (VPN) Connections. Click Next.
6. On the *Specify Dial-Up or VPN Server* page, click Add.
7. When the *New RADIUS Client* dialog box opens, type a friendly name for the RADIUS client in the *Friendly name* text box.
8. In the *Address (IP or DNS)* text box, type the address of the remote access server.
9. At the bottom of the dialog box, type in a shared secret password to be used for RADIUS setup.
10. Click OK to close the *Remote Access Properties* dialog box.
11. Back on the *Specify Dial-Up or VPN Server* page, click Next.
12. On the *Configure Authentication Methods* page, select an authentication method and click Next.
13. On the *Specify User Groups* page, click Add.
14. When the *Select Group* dialog box opens, type a name of the group in the *Enter the object name to select* text box and click OK.
15. Back at the Specify User Groups, click Next.
16. An IP filter enables you to specify what addresses or protocols are allowed or not allowed through the remote servers. If you have an IP Filter template, you can select it on the *Specify IP Filters* page (see Figure 12-3).

Figure 12-3

Specifying IP filters

17. If you do not have an IP filter to choose, you can manually specify what filters you want by clicking the Input Filters or Output Filters for IPv4 or IPv6, which opens the *Inbound or Outbound Filters* dialog box. You then click the New button to open the *Add IP Filter* dialog box. Then specify the source network, destination network, and protocol. Click OK to close the *Add IP Filter* and click OK to close the *Inbound or Outbound Filters* dialog box.
18. Back on the *Specify IP Filters* page, click Next.
19. On the *Specify Encryption Settings* page, deselect the encryption that you don't want to support and click Next.
20. The *Specify a Realm Name* page appears. If you need to specify a realm (a user account location such as a domain name or server name), specify the realm name in the appropriate text box. Click Next.
21. When the wizard is complete, click Finish.

CONFIGURE NPS FOR 802.1X WIRELESS CONNECTIONS

GET READY. To configure NPS for 802.1X wireless or wired connections, perform the following steps:

1. Open the Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens.
3. In the main pane, under *Standard Configuration*, select RADIUS server for 802.1X Wireless or Wired Connections.
4. Click Configure 802.1X. The *802.1X Wizard* opens.
5. On the *Select 802.1X Connections Type* page, select 802.1X Secure Wireless Connections. Click Next.

6. On the *Specify 802.1X Switches* page, click Add.
7. When the *New RADIUS Client* dialog box opens, type a friendly name for the RADIUS client in the *Friendly name* text box.
8. Type the address of the remote access server in the *Address (IP or DNS)* text box.
9. At the bottom of the dialog box, type in a shared secret password to be used for RADIUS setup.
10. Click OK to close the *New RADIUS Client* dialog box.
11. Back on the *Specify 802.1X Switches* page, click Next.
12. On the *Configure Authentication Methods* page, choose the appropriate authentication method (see Figure 12-4), select an authentication method, and click Next.

Figure 12-4

Configuring authentication methods for 802.1X

13. On the *Specify User Groups* page, click Add.
14. When the *Select Group* dialog box opens, type a name of the group in the *Enter the object name to select* text box and click OK.
15. Back at the Specify User Groups page, click Next.
16. On the *Configure Traffic Controls* page, you can specify traffic control attributes, which are sent to the RADIUS server with authentication and authorization requests by clicking the Configure button. When you are done, click Next.
17. When the wizard is complete, click Finish.

If you want more control in the configuration, use NPS Advanced Configuration (see Figure 12-5). In addition to modifying the RADIUS clients, network policies, and accounting, you can configure NAP Health Policy server, and the RADIUS proxy.

Figure 12-5

Looking at NPS Advanced Configuration

To modify a network policy, expand *Policies* in the NPS tree and click *Network Policies*.

Configuring NPS Templates

NPS templates, sometimes referred as RADIUS templates, enable you to create RADIUS configuration elements that can be reused on local NPS servers and can be exported to other NPS servers.

Much like the use of other templates, NPS templates (especially RADIUS clients and Remote RADIUS servers) are designed to reduce the amount of time and cost that it takes to configure RADIUS on one or more servers. Creating an NPS template does not affect the functionality of NPS. It affects only the NPS server when the template is selected and applied when configuring RADIUS. The NPS templates are available (see Figure 12-6) for configuration in Templates Management.

Figure 12-6

Looking at Template Configuration options in the NPS console

To create a template, right-click a template type in the NPS console tree, such as *RADIUS Clients*, and then select *New*. A *New RADIUS Client* dialog box opens that allows you to configure your template. Creating a template does not affect the functionality of NPS. It affects only the NPS server when the template is selected and applied when configuring RADIUS. For example, if you right-click *RADIUS Clients* in the *RADIUS Clients and Servers* group and select *Properties*, you can apply the NPS template that was previously created.

Configuring RADIUS Accounting

NPS supports ***RADIUS accounting***, which you can use to track network usage for auditing and billing purposes.

When configured for accounting, NPS can log accounting data to a text log file and/or a SQL Server database. When accounting is enabled, at the start of the service delivery, the NPS server generates an Accounting-Start message describing the type of service being delivered and the user it is being delivered to, which is sent to the RADIUS Accounting server. The RADIUS Accounting server sends back an acknowledgment to the RADIUS client. At the end of service delivery, the client generates an Accounting-Stop message that describes the type of service that was delivered, and optional statistics, such as elapsed time, input and output octets, or input and output packets. It then sends that data to the RADIUS Accounting server, which sends back an acknowledgment to the RADIUS client.

ENABLE AND CONFIGURE ACCOUNTING IN NPS

GET READY. To enable and configure accounting on NPS, perform the following steps:

1. Open the Server Manager.
2. Click Tools > Network Policy Server. The Network Policy Server console opens.
3. On the NPS tree, click Accounting. The *Accounting* pane opens.
4. In the *Accounting* section, click Configure Accounting.
5. When the *Accounting Configuration Wizard* starts, click Next.
6. On the *Select Accounting Options* page, select the accounting option that you want to use and click Next.
7. If you choose to use the SQL server, the *Configure SQL Server Logging* page appears (see Figure 12-7). To configure the SQL connection, click Configure.

Figure 12-7

Configuring SQL Server logging

8. When the *Data Link Properties* dialog box opens (see Figure 12-8), specify the name of the SQL server in the *Select or enter a server name* text box and click Refresh. Then specify the user name and password that has access to the SQL server database that you want to log to. Select the database using the *Select the database on the server* pull-down menu. To verify the SQL connection, click Test Connection. Click OK to close the *Data Link Properties* dialog box.

Figure 12-8

Configuring the Data Link properties

9. If you select to save the data into a local text file, the *Configure Local File Logging* page appears. Notice the path of the log file is C:\Windows\System32\LogFiles. Click Next.
10. On the *Summary* page, click Next.
11. On the *Conclusion* page, click Close.

After you run the Accounting Wizard, you can click the Change Log File Properties or the Change SQL Server Logging Properties to make changes without rerunning the wizard. The Change Log File Properties dialog box opens the Log File. If you choose the Log Files, make sure that the C drive is large enough to hold the logs or move the log files to a drive that is large enough.

When selecting which RADIUS attributes to record, you should include the RADIUS Class attribute, which will be used to track usage and simplify the identification of which department or user to charge the usage. It should be noted that if a request is lost, a duplicate request may be sent. Therefore, to accurately track usage, you will need to delete duplicate requests.

Understanding NPS Authentication Methods

As already stated throughout the lesson, NPS authenticates and authorizes a connection request before allowing or denying access when a user attempts to connect to a network through a network access server such as a VPN server. NPS must receive proof of the identity of the user or computer.

Authentication is usually broken down into the following categories:

- Password-based credentials
- Certificate-based credentials

When you deploy NPS, you can specify the required type of authentication method for access to your network.

USING PASSWORD-BASED AUTHENTICATION

When a user uses password-based credentials, the network access server passes the username and password to the NPS server, which verifies the credentials against the user account database, either a domain database or a local server database. Unfortunately, password-based authentication is not considered strong security. As a result, certificate authentication or multi-factor authentication is recommended.

However, if you do use password-based authentication, it is processed from the most secure (Microsoft Challenge-Handshake Authentication Protocol v2 or MS-CHAPv2) to the least secure (unauthenticated access) of those enabled options. If you are using only Microsoft clients, you should only allow MS-CHAPv2. However, if you have some non-MS clients, you may need to enable CHAP. Of course, Password Authentication Protocol (PAP) is never recommended because the username and password are sent in plain text.

USING CERTIFICATES FOR AUTHENTICATION

To provide strong security for authenticating users and computers and eliminate the need for less secure password-based authentication methods, you can use certificates with the NPS. Certificates are customized using certificate templates and are issued using a Certificate Authority.

When you customize the template, you specify how certificates are issued (how long a certificate is good for and who can receive a certificate) and their purpose. For example, the Computer template is used to define the template that the CA uses to assign certificates to computers, which, by default, includes the Client Authentication purpose and the Server Authentication purpose in EKU extensions.

If you decide to use smart cards for authentication, you need certificates that include the Smart Card Logon purpose and the Client Authentication purpose. When using NPS, you can configure NPS to check certificate purposes before granting network authorization. NPS can check additional EKUs and Issuance Policy purposes, also known as certificate policies.

If you decide to use Protected Extensible Authentication Protocol Microsoft Challenge-Handshake Authentication Protocol v2 (PEAP-MS-CHAP v2), Protected Extensible Authentication Protocol Transport Layer Security (PEAP-TLS), or Extensible Authentication Protocol Transport Layer Security (EAP-TLS) as the authentication method, the computers need a digital certificate installed, and the NPS server must use a server certificate that meets the minimum server certificate requirements.

AUTOMATICALLY ADD WORKSTATION AUTHENTICATION CERTIFICATES TO ALL WORKSTATIONS

GET READY. To automatically add workstation certificates to all workstations, perform the following steps:

1. On the server that has the Certificate Authority, open the Server Manager.
2. Click Tools > Certificate Authority. The Certificate Authority opens.
3. Expand the server. Then right-click Certificate Templates and select Manage. The *Certificate Templates console* opens.
4. Right-click the Workstation Authentication template and select Duplicate Template. The *Properties of New Template* dialog box opens.
5. Select the General tab.
6. Type a new name for the certificate template in the *Template display name* text box.
7. Select the Security tab.
8. In *Group or user names*, click Domain Computers (see Figure 12-9).

Figure 12-9

Configuring security for a template

9. Under *Allow*, select the Enroll and Autoenroll permission check boxes.
10. Click OK to close the *Properties of New Template* dialog box.
11. Close the *Certificate Templates console*.
12. On the *Certificate Authority console*, right-click Certificate Templates, select New, and select Certificate Template to Issue. The *Enable Certificate Templates* dialog box opens.
13. Click the name of the certificate template you just configured, and then click OK.
14. Close the *Certificate Authority console*.
15. From the Server Manager, click Tools > Group Policy Management console. The *Group Policy Management console* opens.

16. Right-click the Default Domain Policy and select Edit. The *Group Policy Management Editor* opens.
17. Open *Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies*.
18. Double-click Certificate Services Client – Auto-Enrollment. The *Certificate Services Client – Auto-Enrollment* dialog box opens.
19. Select Enabled for the Configuration Model.
20. Select the Renew expired certificates, update pending certificates, and remove revoked certificates check box.
21. Select the Update certificates that use certificate templates check box.
22. Click OK to close the *Certificate Services Client – Auto-Enrollment* dialog box.

AUTOMATICALLY ADD RAS AND IAS SERVER CERTIFICATES TO ALL WORKSTATIONS

GET READY. To automatically add workstation certificates to all workstations, perform the following steps:

1. On the server that has the Certificate Authority, open the Server Manager.
2. Click Tools > Certificate Authority. The *Certificate Authority* opens.
3. Expand the server, right-click Certificate Templates, and then select Manage. The *Certificate Templates console* opens.
4. Right-click the RAS and IAS template and select Duplicate Template. The *Properties of New Template* dialog box opens.
5. Select the General tab.
6. Type a new name for the certificate template in the *Template display name* text box.
7. Select the Security tab.
8. In *Group or user names*, click RAS and IAS Servers.
9. Under *Allow*, select the Enroll and Autoenroll permission check boxes.
10. Click OK to close the *Properties of New Template* dialog box.
11. Close the *Certificate Templates console*.
12. Back on the *Certificate Authority console*, right-click Certificate Templates, select New, and select Certificate Template to Issue. The *Enable Certificate Templates* dialog box opens.
13. Click the name of the certificate template you just configured, and then click OK.
14. Close the *Certificate Authority console*.

Business Case Scenarios

Scenario 12-1: Supporting Multiple VPN Servers

You have two VPN servers. One is located on the main corporate office and the second is located at the backup site. You want to provide centralized authentication and logging. What should you do?

Scenario 12-2: Securing VPN Connections

Your manager approaches you to discuss implementing VPN for the corporate users. However, he is concerned about security. What do you recommend to maintain the best security?

13 LESSON

Configuring NPS Policies

Managing NPS Policies

THE BOTTOM LINE

An ***NPS policy*** is a set of permissions or restrictions that are used by remote access authenticating servers that determine who, when, and how a client can connect to a network. With the remote access policies, connections can be authorized or denied based on user attributes, group membership, time of day, type of connection, and many other variables.

Network Policy Server (NPS) provides three types of policies:

- ***Connection request policies:*** A policy that establishes sets of conditions and settings that specify which RADIUS servers perform the authentication, authorization, and accounting of connection requests received by the NPS server from RADIUS clients. It can also be used to designate which RADIUS servers are used for RADIUS accounting.
- ***Network policies:*** A policy that establishes sets of conditions, constraints, and settings that specify who is authorized to connect to the network and the circumstances under which they can or cannot connect.
- ***Health policies:*** A policy that establishes one or more system health validators (SHVs) and other settings that enable you to define client computer configuration requirements for the Network Access Policy (NAP)-capable computers that attempt to connect to your network. Health policies are used only with NAP. NAP is discussed in Lesson 14.

Figure 13-1 shows the Policies pane in NPS.

Figure 13-1

Looking at NPS policies

Configuring Connection Request Policies

Connection request policies determine which RADIUS servers will perform the authentication and authorization of connection requests of RADIUS clients for servers running NPS. It can also be used to specify RADIUS accounting.

Connection request polices are applied to NPS as a RADIUS server or as a RADIUS proxy. The policies are based on a range of factors such as the following:

- The time of day and day of the week
- The realm name in the connection request
- The type of connection requested
- The IP address of the RADIUS client

When you create a connection request policy, you define the following parameters:

- Type of network access server such as Remote Access server (VPN dial-up)
- Condition that species who or what can connect to the network based on one or more RADIUS attributes
- Settings that are applied to an incoming RADIUS message, such as authentication, accounting, and attribute manipulation

RADIUS Access-Request messages are processed or forwarded by NPS only if the settings of the incoming message match at least one of the connection request policies configured on the

NPS server. If the policy settings match and the policy requires that the NPS server processes the message, NPS acts as a RADIUS server, authenticating and authorizing the connection request.

Connection request policy conditions are one or more RADIUS attributes that are compared to the attributes of the incoming RADIUS Access-Request message (see Table 13-1). If there are multiple conditions, then all the conditions in the connection request message and in the connection request policy must match in order for the policy to be enforced by NPS.

Table 13-1

Conditions Used in Connection Request Policies

Group	Attribute	Description
Username	User Name	Designates the user name (including the realm/domain name and a user account name) that is used by the access client in the RADIUS message.
Connection Properties	Access Client IPv4 Address	Designates the Internet Protocol version 4 (IPv4) address of the Access client that requests access from the RADIUS client.
	Access Client IPv6 Address	Designates the Internet Protocol version 6 (IPv6) address of the Access client that requests access from the RADIUS client.
	Framed Protocol	Designates the type of framing for incoming packets, such as Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Frame Relay, and X.25.
	Service Type	Designates the type of service requested, such as framed (for example, PPP connections) and login (for example, Telnet connections).
	Tunnel Type	Designates the type of tunnel that is created by the requesting client, such as Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP).
Day and Time Restriction	Day and Time Restriction	Designates the day of the week and the time of day a connection can be made.
Identity Type	Identity Type	Used to restrict the policy to only clients that can be identified through the special mechanism, such as NAP statement of health (SoH).
RADIUS Client Properties	Calling Station ID	Designates the phone number used by the caller (the access client). This attribute is a character string. You can use pattern-matching syntax to specify area codes.
	Client Friendly Name	Designates the name of the RADIUS client computer that requests authentication.
	Client IPv4 Address	Specifies the IPv4 address of the RADIUS client that forwarded the connection request to NPS.
	Client IPv6 Address	Specifies the IPv6 address of the RADIUS client that forwarded the connection request to NPS.

(continued)

Table 13-1

(continued)

Group	Attribute	Description
	Client Vendor	Specifies the name of the vendor of the RADIUS client that sends reconnection requests to NPS.
Gateway	Called Station ID	Specifies a character string that is the telephone number of the network access server (NAS).
	NAS Identifier	Specifies a character string that is the name of the NAS.
	NAS IPv4 Address	Designates the IPv4 address of the network access server (the RADIUS client).
	NAS IPv6 Address	Designates the IPv6 address of the network access server (the RADIUS client).
	NAS Port Type	NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, Integrated Services Digital Network (ISDN) tunnels, VPN connection, IEEE 802.11 wireless, and Ethernet switches.

The default connection request policy uses NPS as a RADIUS server and processes all authentication requests locally. If you do not want the NPS server to act as a RADIUS server and process connection requests locally, you can delete the default connection request policy.

To configure a server running NPS to act as a RADIUS proxy and forward connection requests to other NPS or RADIUS servers, you must configure a remote RADIUS server group in addition to adding a new connection request policy that specifies conditions and settings that the connection requests must match.

CREATE A CONNECTION REQUEST POLICY

GET READY. To create a connection request policy, perform the following steps:

1. Open Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens.
3. Double-click Policies in the NPS tree.
4. Right-click Connection Request Policies, and then click New. The *New Connection Request Policy Wizard* appears.
5. In the *Policy name* text box, type a meaningful name to identify the policy.
6. If desired, select the type of network access server, such as Remote Desktop Gateway, Remote Access Server (VPN-Dial up), DHCP Sever, Health Registration Authority, or Host Credential Authorization Protocol (HCAP) Server. Click Next.
7. On the *Specify Conditions* page, click Add.
8. When the *Select condition* dialog box opens (as shown in Figure 13-2), select the desired condition such as Tunnel Type, and then click Add.

Figure 13-2

Selecting a condition

9. If you selected Tunnel Type, a *Tunnel Type* dialog box opens. Select the desired tunnel type and click OK.
10. Repeat the process of adding conditions as desired. After the conditions have been added, click Next.
11. On the *Specify Connection Request Forwarding* page, select Authenticate requests on this server, or Accept users without validation credentials. If you have a remote RADIUS server group, you can select the Forward requests to the following remote RADIUS server group for authentication and specify the group. Click Next.
12. On the *Specify Authentication* page, if you want to override the network policy authentication settings, select the Override network policy authentication settings and select or deselect the authentication methods as desired. Click Next.
13. On the *Configure Settings* page, specify the Realm name or RADIUS attribute. Click Next.
14. On the Completing Connection Request Policy Wizard page, click Finish. When created, the Network Policy is listed in the *Network Policies* pane.

After a connection request policy has been created, you can modify the policy by right-clicking the policy and selecting *Properties*. When the Properties dialog box opens, you then select the *Overview* tab, *Conditions* tab, or the *Settings* tab.

Configuring Network Policies

While the connection request policy specified settings for the RADIUS server, the network policy will allow or disallow the remote access.

An NPS network policy evaluates remote connections based on the following three components:

- Conditions
- Constraints
- Settings

If the conditions and constraints defined by the connection attempt match those configured in the network policy, the remote access server will either allow or deny the connection and configure additional settings, as defined by the policy. Every remote access policy has an Access Permissions setting, which specifies whether connections matching the policy should be allowed or denied.

When a user attempts to connect to a remote access server, the following process takes place:

1. User attempts to initiate a remote access connection.
2. Remote Access server checks the conditions in the first configured NPS network policy.
3. If the conditions of this NPS network policy do not match, the Remote Access server checks the next configured NPS network policies. It keeps checking each policy until it finds a match or reaches the last policy.
4. Once the Remote Access Server finds an NPS network policy with conditions that match the incoming connection attempt, the Remote Access server checks any constraints (such as time of day or minimum encryption level) that have been configured for the policy.
5. If the connection attempt does not match any configured constraints, the Remote Access Server denies the connection.
6. If the connection attempt matches both the conditions and the constraints of a particular NPS network policy, the remote access server will allow or deny the connection, based on the Access Permissions configured for that policy.

Of course, if you have multiple NPS network policies, you have to specify the order in which the policies are evaluated from top to bottom. It is important to place these policies in the correct order, because once the RRAS server finds a match, it will stop processing additional policies. As a best practice, NPS network policies should be ordered so that more specific policies are higher in the list, and less specific policies are lower in the list.

CREATE A NETWORK POLICY

GET READY. To create a network policy, perform the following steps:

1. Open Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens.
3. Double-click Policies in the *NPS tree*.
4. Right-click Network Policies, and then click New. The *New Network Policy Wizard* opens.
5. In the *Policy name* text box, type a meaningful name to identify the policy.
6. If desired, select the type of network access server, such as Remote Desktop Gateway, Remote Access Server (VPN-Dial up), DHCP Sever, Health Registration Authority, or HCAP Server. Click Next.
7. On the *Specify Conditions* page, click Add.
8. When the *Select condition* dialog box opens, select the desired condition such as *Windows Groups* and click Add.

9. If you selected *Windows Groups*, a *Windows Groups* dialog box opens. Click Add Groups. When the *Select Group* dialog box opens, type the name of the desired group and click OK.
10. Repeat the process of adding conditions as desired. After the conditions have been met, click Next.
11. On the *Specify Access Permissions* page, select Access granted, Access denied, or Access is determined by User Dial-in Properties.
12. On the *Configure Authentication Methods* page, select or deselect the authentication methods. If you need to add an EAP type, click Add to specify Microsoft: Smart Card or other certificate, Microsoft: Protected EAP (PEAP), or Microsoft: Secured password (EAP-MSCHAP v2). Click Next.
13. On the *Configure Constraints* page, specify the *Idle Timeout*, *Session Timeout*, *Called Station ID*, *Day and time restrictions*, and *NAS Port Type*. Click Next.
14. On the *Configure Settings* page, specify *RADIUS attributes*, *Network Access Protection* settings, and *Routing and Remote Access* settings. Click Next.
15. On the *Completing New Network Policy* page, click Finish. When created, the network policy is listed in the *Network Policies* pane.

After the network policy has been created, you can modify the network policy by right-clicking the network policy and selecting *Properties*. When the Properties dialog box opens, you can then select the *Overview* tab, *Condition* tab, *Constraints* tab, and *Settings* tab.

MULTILINK AND BANDWIDTH ALLOCATION

When ISDN was introduced, ISDN included multiple channels, which allow simultaneous voice and data communications. With multilink and Bandwidth Allocation Protocol (BAP) settings (see Figure 13-3), you can specify whether multiple connections form a single connection to increase bandwidth. In addition, you can specify how BAP determines when these extra lines are dropped.

Figure 13-3

Configuring Multilink and BAP settings

IP FILTERS

The IP filters (see Figure 13-4) allow you to control which packets are allowed through the network connection based on IP address. By clicking the *Input Filters* or *Output Filters* for IPv4 or IPv6, you can specify to permit or not permit packets. You then use the New button to specify the source network or destination network.

Figure 13-4

Configuring an IPv4 Inbound filter

ENCRYPTION

The Encryption settings (as shown in Figure 13-5) enable you to specify the supported encryption used with network connections. The available encryption options include the following:

- **Basic Encryption (MPPE 40-Bit):** For dial-up and PPTP-based VPN connections, MPPE is used with a 40-bit key. For L2TP/IPsec VPN connections, 56-bit DES encryption is used.
- **Strong Encryption (MPPE 56-Bit):** For dial-up and PPTP VPN connections, MPPE is used with a 56-bit key. For L2TP/IPsec VPN connections, 56-bit DES encryption is used.
- **Strongest Encryption (MPPE 128-Bit):** For dial-up and PPTP VPN connections, MPPE is used with a 128-bit key. For L2TP/IPsec VPN connections, 168-bit Triple DES encryption is used.
- **No Encryption:** This option allows unencrypted connections that match the remote access policy conditions. Clear this option to require encryption.

Figure 13-5

Configuring encryption settings

IP ADDRESSING

The last setting in the Routing and Remote Access is IP settings, which specify how IP addresses are assigned. IP settings include the following options:

- Server Must Supply An IP Address.
- Client May Request An IP Address.
- Server Settings Determine IP Address Assignment (the default setting).
- Assign A Static IP Address.

The assigned IP address is typically used to accommodate vendor-specific attributes for IP addresses.

Importing and Exporting NPS Policies

Network Policy Server templates enable you to create configuration elements that can be reused on the local NPS server and can be exported to other NPS servers.

Much like the use of other templates, NPS templates are designed to reduce the amount of time and cost that it takes to configure NPS on one or more servers. Creating a template does not affect the functionality of NPS. It affects only the NPS server when the template is selected and applied when configuring NPS.

The following NPS template types are available for configuration in Templates Management:

- Shared Secrets
- RADIUS Clients
- Remote RADIUS Servers
- IP Filters
- Health Policies
- Remediation Server Groups

To create a template, right-click a template type in the NPS console tree, such as *IP Filters*, and then select *New*. A new IP Filters Template dialog box opens (as shown in Figure 13-6) that enables you to configure your template. Creating a template does not affect the functionality of NPS. It affects only the NPS server when the template is selected and applied when configuring NPS.

Figure 13-6

Creating a new IP filter template

You can use a template that you've created in Templates Management by navigating to a location in the NPS console where the template can be applied. For example, if you create a new Shared Secrets template that you want to apply to a RADIUS client configuration, expand NPS, expand RADIUS Clients and Servers, and select *RADIUS Clients*. Then right-click the RADIUS client and select *Properties*. To apply the template, select an existing Shared Secrets template, and then select the template you created from the list of templates.

To export and import templates so that they can be used on other NPS servers, perform the following steps:

1. To export NPS templates, right-click *Templates Management* in the NPS console, and then select *Export Templates to a File*.
2. To import NPS templates, right-click *Templates Management* in the NPS console, and then click *Import Templates from a Computer* or *Import Templates from a File*.

EXPORTING AND IMPORTING THE NPS CONFIGURATION INCLUDING NPS POLICIES

You can export the entire NPS configuration, including RADIUS clients and servers, network policy, connection request policy, registry, and logging configuration, from one NPS server for import on another NPS server by using the `netsh` command.

EXPORT AND IMPORT THE NPS CONFIGURATION

GET READY. To export and import the NPS configuration, perform the following steps:

1. Open a command prompt on the source server.
2. Type netsh, and then press Enter.
3. At the *netsh prompt*, type nps, and then press Enter.
4. At the *netsh nps prompt*, type export filename="path\file.xml"exportPSK=YES, where path is the folder location where you want to save the NPS server configuration file, and file is the name of the XML file that you want to save. Press Enter.
5. When the export is complete, close the command prompt.
6. Copy the XML file to the destination NPS server.
7. Open a command prompt on the target server.
8. At a command prompt on the destination NPS server, type netsh nps import filename="path\file.xml", and then press Enter. A message appears indicating whether the import from the XML file was successful.
9. When the import is complete, close the command prompt.

WARNING Do not use this procedure if the source NPS database has a higher version number than the version number of the destination NPS database. You can view the version number of the NPS database from the display of the `netsh nps show config` command.

Business Case Scenarios

Scenario 13-1: Defining Policies

You have two VPN servers. One is located on the main corporate office and the second is located at the backup site. You want to create policies that forward authentication and authorization requests to an NPS server and have the users approved if they are members of the Help Desk, Management, or Sales group. What should you do?

Scenario 13-2: Duplicating Servers

You are an administrator for the Contoso Corporation. You recently had a server failure where the RADIUS server was down for an extended period of time. You need to create a second NPS server for your organization to provide fault tolerance in the DR site. However, the server will only be used when the first server is not available. Describe the easiest way to duplicate all of the settings of the first NPS server on to the second NPS server and how to further configure the server to provide the specified functionality.

Configuring Network Access Protection (NAP)

LESSON 14

Using Network Access Protection (NAP)

THE BOTTOM LINE

You have probably heard the phrase "a chain is as strong as its weakest link." With networking, this can be applied where a network is only as secure as the least-secure computer attached to it. If a computer is not secure and it goes out to web server, the web server can infect the computer. That computer can then be used to attack the network, bypass security, infect other computers, capture and forward confidential information, and so on. As a result, many tools help secure a computer. Ensuring a computer has up-to-date security patches and a reputable anti-virus/anti-malware software package installed is important. Although a corporate desktop computer that is constantly connected to the network is easy to manage and although it is easy to ensure that the computer has an up-to-date security patches and an up-to-date antivirus package, laptops that are rarely on the network or unmanaged computers that are not part of the domain, so they are much more difficult to control. To help solve this problem, Microsoft developed Network Access Protection (NAP) to ensure that all computers connected to your network have the most up-to-date security patches and an up-to-date anti-virus/malware package.

Network Access Protection (NAP) is Microsoft's software for controlling network access for computers based on the health of the host such as if it is the newest security patches and a current anti-virus/anti-malware software package. As a computer connects to the network, the health status of the computer is evaluated to determine whether it should be allowed to connect to the network based on health policies. If a computer is not compliant with the system health requirements, the computer can be denied access to the network or given restricted access to the network. In some situations, automatic remediation can occur, which brings the computer into compliance.

NAP can be used on any computer that runs Windows and supports NAP.

NAP includes a number of built-in enforcement methods that define the mechanisms that NAP can use:

- ***DHCP enforcement:*** This enforcement method uses DHCP configuration information to ensure that NAP clients remain in compliance. If a computer is out of compliance, NAP provides a Dynamic Host Configuration Protocol (DHCP) configuration that limits a person's access to the network until the computer is compliant. DHCP enforcement is considered the weakest form of NAP enforcement because it can be bypassed with the client computer using static IP addresses.
- ***Internet Protocol Security (IPsec) enforcement:*** This enforcement method uses IPsec that has been secured by specially configured PKI certificates known as health certificates, which are issued to clients that meet defined compliance standards. If clients cannot provide the necessary health certificate, they cannot participate in IPsec-secured

traffic. IPsec enforcement is considered the strongest form of NAP enforcement. DirectAccess uses the Internet Protocol Security enforcement.

- ***VPN enforcement:*** This enforcement method restricts the level of network access that a remote access clients can obtain, based on the health information that the client computers present when the VPN connection is made.
- ***802.1x enforcement:*** This enforcement method uses 802.1x-aware network access points, such as network switches or wireless access points, to restrict network access of noncompliant resources.
- ***Remote Desktop Gateway (RD Gateway) enforcement:*** This enforcement method allows authorized remote users to connect to resources on an organization network, from any Internet-connected device. NAP can restrict connection attempts by RD Gateway clients just as with other enforcement methods.

Each of these NAP enforcement methods has its strengths and weaknesses. Although combining enforcement methods enables you to eliminate most of the weaknesses of your NAP deployment, using multiple NAP implementations makes the implementation complex to initiate and manage.

The overall architecture of NAP involves the following components:

- **NAP client-side components:** Windows Server 8, Windows 7, Windows Vista, Windows XP with SP3, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008. Microsoft also provides third-party vendors that can use NAP API to write additional clients for additional operating systems, such as Macintosh and Linux computers.
- **NAP enforcement points:** A server or device that enforces compliance. Depending on the enforcement method in use, a NAP enforcement point can take a number of different forms, such as an 802.1X-capable Wireless Access Point (WAP) for 802.1X enforcement, a Windows Server 2008 DHCP server for the DHCP enforcement method, or a Health Registration Authority (HRA) that can obtain health certificates from client computers when the IPsec enforcement method is used.
- ***NAP health policy server:*** A server running the Network Policy Server (NPS) server role that receives information from NAP enforcement points. The health policy server stores NAP health requirement policies and provides health state validation for NAP clients.
- ***System Health Agents (SHAs):*** A component that maintains information and reporting on one or more elements of the health of a NAP client. Newer versions of Windows have a built-in Windows SHA that monitors the settings configured in the Windows Security Center. Third-party vendors can use the NAP API to write additional SHAs to plug into third-party products.
- ***Statement of Health (SoH):*** Each SHA creates an SoH that transmits to the NAP Agent. Each SHA generates a new SoH whenever the status is updated, such as when an update to the anti-virus package is released but has not been installed on the client.
- ***NAP Agent:*** This maintains information about the health of the NAP client computer and transmits information between the NAP enforcement clients and the SHAs. The NAP Agent combines the SoH from each SHA into a single System Statement of Health (SSOH), which it then passes to the enforcement clients. The enforcement clients then use this SSOH to request network access by passing the SSOH information on to the NAP server components.
- ***Health Registration Authority (HRA):*** A computer that runs Windows Server 2012 R2 and Internet Information Services (IIS) and that obtains health certificates from a certification authority (CA) for compliant computers.
- **Health requirements server*:*** A server that provides the current health state information to NPS health policy server. Examples of health requirements include an anti-virus software management server, or a Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM) server that sends updates to client computers.

- ***Remediation servers:*** An optional component that can be deployed to allow noncompliant client computers to achieve network compliance and gain network access. Examples include anti-virus software or a WSUS server.

Installing Network Access Protection

NAP is provided by NPS. Therefore, to install NAP, you install NPS.

Because NAP is offered through NPS, the installation is similar to installing NPS, as discussed in Lesson 12. However, you want to add HRA, which is used to issue health certificates to NAP client computers that are compliant with network health requirements. For HRA to function, you need to have a CA available.

INSTALL NETWORK POLICY SERVER

GET READY. To install Network Policy Server, perform the following steps:

1. Open Server Manager.
2. At the top of Server Manager, select Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation, and then click Next.
5. Click Select a server from the server pool, click the name of the server to install Network Policy and Access Services to, and then click Next.
6. On the *Server Roles* page, select the Network Policy and Access Services and click Next.
7. When you are asked to add features that are required for Network Policy and Access Services, click Add Features.
8. On the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Network Policy and Access Services* page, click Next.
11. On the *Select role services* page, with the Network Policy Server selected, select Health Registration Authority so that there is a checkmark in the checkbox. Click Next.
12. When the *Add Roles and Features Wizard* dialog box opens, click Add Features.
13. On the *Select role services* page, click Next. The *Certification Authority* page.
14. If the CA is located on the current sever, select Use the local CA to issue health certificates for this HRA server. If the CA is on another server, select Use an existing remote CA and then specify the name of the server. Click Next.
15. On the *Authentication Requirements* page, select the Yes, required requestors to be authenticated as members of a domain (recommended). Click Next.
16. On the *Confirm installation selection* page, click Install.
17. When the installation is complete, click Close.

Configuring NAP Enforcement

To configure NAP, you need to install and configure the server on which you will apply NAP enforcement. You then need to configure NPS and the NAP-related policies. Finally, you need to configure the remediation servers.

Microsoft's TechNet website has several whitepapers, step-by-step guides, and checklists when implementing NAP enforcement. However, if you choose NAP, you need to plan the implementation so that you can minimize problems during the initial implementation until everything is configured properly.

CONFIGURING NAP ENFORCEMENT FOR DHCP

If you are to provide DHCP enforcement, you need a DHCP server. As shown in the 70-410 course, you use Server Manager to install DHCP. Because DHCP enforcement relies on a limited IPv4 address configuration, any user with client administrator access can override the DHCP configuration by assigning IP addresses manually. Therefore, DHCP is considered the weakest NAP enforcement method. Unfortunately, DHCP enforcement is not possible for IPv6 clients.

To control network access, DHCP enforcement sets the following:

- The DHCP Router option is set to 0.0.0.0 so that noncompliant computers do not have a configured default gateway.
- The subnet mask is set to 255.255.255.255 so that there are no routes to the attached subnet.

To allow noncompliant computers to access the restricted network's remediation servers, the DHCP server assigns the Classless Static Routes DHCP option, which contains host routes to the remediation servers, without giving access to the other computers.

To configure DHCP enforcement, you must complete the following:

1. Configure a DHCP server and create the appropriate DHCP scopes.
2. Install NPS on the DHCP server.
3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation servers, which noncompliant clients can access.
4. Enable NAP for individual DHCP scopes.
5. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.

INSTALL THE DHCP SERVER

GET READY. To install DHCP, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, select Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation, and then click Next.
5. Click Select a server from the server pool, click the name of the server to install DHCP Server to, and then click Next.
6. On the *Server Roles* page, select the DHCP Server and click Next.
7. When you are asked to add features that are required for Network Policy and Access Services, click Add Features.
8. Back on the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.

10. On the *DHCP* page, click Next.
11. On the *Confirm installation selection* page, click Install.
12. When the installation is complete, click Close.

CONFIGURE THE DHCP SERVER

GET READY. To configure the DHCP, perform the following steps:

1. Open Server Manager.
2. Click Tools > DHCP. The *DHCP console* opens.
3. Expand the server node, and expand the IPv4 node.
4. Right-click IPv4 node and click New Scope.
5. When the *New Scope Wizard* starts, click Next.
6. On the *Scope Name* page, in the *Name and Description* text box, type a descriptive name and description of the scope.
7. On the *IP Address Range* page, enter the following information:

   Start IP address: 192.168.1.201

   End IP address: 192.168.1.250

   Click Next.
8. On the *Add Exclusions and Delay* page, click Next.
9. On the *Lease Duration* page, click the lease time to 8 hours. Click Next.
10. On the *Configure DHCP Options* page, click Next.
11. For the *Router (Default Gateway)* page, type 192.168.1.1 for the IP address and click the Add button. Click Next.
12. On the *Domain Name and DNS Servers* page, click Next.
13. On the *WINS Servers* page, click Next.
14. On the *Activate Scope* page, with the *Yes, I want to activate the scope now option* already selected, click Next.
15. When the *Completing the New Scope Wizard* page appears, click Finish.
16. At the top of the tree, right-click the server and click Authorize.

CONFIGURE NAP FOR DHCP SERVER

GET READY. To configure NAP for DHCP servers, perform the following steps:

1. Open Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens (see Figure 14-1).

Figure 14-1

Starting the Network Policy Server console

3. In the main pane, click Configure NAP to start the *Configure NAP Wizard*.
4. When the *Select Network Connection Method For Use with NAP Wizard* opens, select the Dynamic Host Configuration Protocol (DHCP) for the network connection method. Click Next.
5. If the server is not running DHCP and is providing NAP for RADIUS clients, you can add the RADIUS clients on the *Specify NAP Enforcement Servers Running DHCP Server* page. Because this server is already running DHCP, click Next.
6. On the *Specify DHCP Scopes* page, click the Add button to open the *MS-Server Class* page. Type NAP DHCP in the text box and click OK. On the *Specify DHCP Scopes* page, click Next.
7. On the *Configure Machine Groups* page, click the Add button to open the *Select Group* dialog box. Type the name of the computer group and click OK. If no computer groups are added, the policy is added to all computers that connect using DHCP. Back at the *Configure Machine Groups* page, click Next.
8. On the *Specify a NAP Remediation Server Group and URL* page, you specify each computer that can be used for remediation, including WSUS, anti-virus management severs, and so on. To add a computer, click the New Group to open the *New Remediation Server Group* dialog box. In the *Group Name* text box, provide a group name, and then click Add to open the *Add New Server* dialog box. Type the name of the server and IP address and click OK to close the *Add New Server* dialog box and click OK to close the *New Remediation Server Group* dialog box.
9. You can also specify the URL in the *Help Web* page dialog box that provides instructions to the user to get his or her computer to be compliant. Click Next.

10. On the *Define NAP Health Policy* page, you can define if a computer is to auto-remediate (if possible) and you can specify if you want to deny or allow access if the computer is not compliant. Click Next.
11. On the *Completing NAP Enforcement Policy and RADIUS Client Configuration* page, click Finish.

When you enable NAP for the individual DHCP scopes, you can enable for all of the DHCP scopes at once or individual scopes. When you are first implement NAP, you should specify individual scopes until you get everything working just right.

ENABLE NAP ON ALL DHCP SCOPES

GET READY. To enable NAP on all DHCP scopes, perform steps:

1. Open Server Manager.
2. Click Tools > DHCP. The *DHCP console* opens.
3. Expand the server node.
4. Right-click the IPv4 node and click Properties. The *IPv4 Properties* dialog box opens.
5. Click the Network Access Protection tab.
6. Click Enable on all scopes.
7. When the message that this will overwrite Network Access Protection settings of all the scopes appears, to continue, click Yes.
8. Specify the appropriate action (Full Access, Restricted Access, Drop Client Packet) if NPS is unreachable.
9. Click OK to close *IPv4 Properties* dialog box.

ENABLE NAP ON AN INDIVIDUAL DHCP SCOPE

GET READY. To enable NAP on a single DHCP scope, perform the following steps:

1. Open Server Manager.
2. Click Tools > DHCP. The *DHCP console* opens.
3. Expand the server node and expand the IPv4 node.
4. Right-click an IPv4 scope and click Properties. A *Scope Properties* dialog box opens.
5. Click the Network Access Protection tab.
6. Click Enable for this scope.
7. Click OK to close *Scope Properties* dialog box.

ENABLE THE NAP DHCP QUARANTINE ENFORCEMENT CLIENT AND START NAP SERVICE ON A DHCP SERVER

GET READY. To enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on a DHCP server, perform the following steps:

1. Click the Start button, right-click the Start button, and select Command Prompt (Admin).
2. At the command prompt, execute the `napclcfg.msc` command. The *NAP Client Configuration console* opens (see Figure 14-2).

Figure 14-2

Opening the NAP Client Configuration console

3. In the left pane, click Enforcement Clients.
4. In the center pane, double-click DHCP Quarantine Enforcement Client to open the *DHCP Quarantine Enforcement Client Properties* dialog box.
5. Select the Enable this enforcement client option. Click OK to close the *DHCP Quarantine Enforcement Client Properties* dialog box.
6. Close the *NAP Client Configuration Client console*.
7. At the command prompt, execute the `services.msc` command.
8. Scroll down and find the Network Access Protection Agent. Then double-click the Network Access Protection Agent service to open the *Network Access Protection Agent Properties* dialog box.
9. Change the Startup type to Automatic.
10. Click the Start button.

11. After the service is started, click OK to close the *Network Access Protection Agent Properties* dialog box.
12. Close the *Services console* and close the command prompt.

Alternatively, you can configure a GPO to enable NAP enforcement clients. Navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Network Access Protection\NAP Client Configuration\Enforcement Clients and enable the DHCP Quarantine Enforcement Client.

CONFIGURING NAP ENFORCEMENT FOR VPN

VPN enforcement provides strong limited network access for all computers that connect to the organization's network through a remote access VPN connection. However, it applies only to remote access VPN connections, which typically do not affect computers connected directly to the organization's network. VPN enforcement uses a set of remote-access IP packet filters to limit VPN client traffic, so that it can reach only the resources on the restricted network.

To configure VPN enforcement, you must complete the following:

1. Install NPS on the VPN server.
2. Configure the VPN server and have them use PEAP-based authentication (either PEAP-MS-CHAP v2 or PEAP-TLS).
3. Run the *NAP Wizard* to configure the connection request policy, network policy, and NAP health policy. Define the remediation severs, which noncompliant clients can access.
4. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.

To configure VPN servers, follow the procedures discussed in Lesson 10 to install a VPN server. Then, use the following procedures to configure NAP for VPN servers. Finally, follow similar steps to enable the NAP VPN Quarantine Enforcement Client as the NAP DHCP Quarantine Enforcement Client service and start the NAP service as you did for the DHCP server.

CONFIGURE NAP FOR VPN SERVERS

GET READY. To configure NAP for VPN servers, perform the following steps:

1. Open Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens (refer to Figure 14-1).
3. In the main pane, click Configure NAP to start the *Configure NAP Wizard*.
4. When the *Select Network Connection Method For Use with NAP* wizard opens, select the Virtual Private network (VPN) for the network connection method. Click Next.
5. By default, NPS already supports Remote Access and Wireless RADIUS clients. If you want to add additional RADIUS clients on the *Specify NAP Enforcement Servers Running DHCP Server* page, click the Add button. For now, click Next.
6. On the *Configure User and Machine Groups* page, you can specify who gets access based on the machine group or the user group, by clicking the appropriate Add button. When the *Select Group* dialog box opens, type the name of the group and click OK. If no computer groups are added, the policy is added to all computers that connect using VPN. On the *Configure User Groups and Machine Groups* page, click Next.
7. On the *Configure an Authentication Method* page, *Secure Password (PEAP-MS-CHAP v2)* is already selected. If you support smart-cards, select Smart Card or other certificate (EAP-TLS). Click Next.

8. On the *Specify a NAP Remediation Server Group and URL* page, specify each computer that can be used for remediation, including WSUS, anti-virus management severs, and so on. To add a computer, click the New Group to open the *New Remediation Server Group* dialog box. In the *Group Name* text box, provide a group name and click Add to open the *Add New Server* dialog box. Type the name of the server and IP address and click OK to close the *Add New Server* dialog box. Click OK to close the *New Remediation Server Group* dialog box.
9. You can also specify the URL in the *Help Web* page dialog box that would provide instructions to the user to get his computer to be compliant. Click Next.
10. On the *Define NAP Health Policy* page, you can define a computer to auto-remediate (if possible) and you can specify if you want to deny or allow access if the computer is not compliant. Click Next.
11. On the *Completing NAP Enforcement Policy and RADIUS Client Configuration* page, click Finish.

Configuring System Health Validators

As mentioned before, the System Health Agents (SHAs) and System Health Validators (SHVs) provide health-state status and validation. Windows 8 includes a Windows Security Health Validator SHA that monitors the Windows Security Center settings. Windows Server 2012 R2 includes a corresponding Windows Security Health Validator SHV.

System Health Validators (SHVs) settings define the requirements for client computers that connect to your network. They are configured using the Network Policy Server console, as shown in Figure 14-3.

Figure 14-3

Managing the Windows SHV

If you double-click a *SHV*, you open the Windows Security Health Validator box. When you configure SHV, there are two sets of configurations:

- Windows 8, Windows 7, Windows Vista
- Windows XP

The settings for each of these include the following options:

- **Firewall Settings:** Specifies if a firewall (Windows Firewall or firewall software that is compatible with Windows Security Center) is enabled for all network connections. If the client computer does not run firewall software or does run a firewall that is not compliant with Windows Security Center, the client computer is restricted to a remediation network until firewall software is installed and running. If you enable NAP autoremediation and WSHA on the client computer reports that no firewall is enabled, then WSHV directs WSHA on the client computer to turn on Windows Firewall.
- **Antivirus Settings:** Specify if a compatible anti-virus application runs on the client computer. If it is up-to-date, the client computer is restricted to a remediation network until the computer becomes compliant.
- **Spyware Protection Settings:** Specify if an antispyware application (Windows Defender or some other spyware protection software that is compatible with the Windows Security Center) runs on the client computer. If it is up-to-date, the client computer is restricted to a remediation network until the computer becomes compliant.
- **Automatic Updates Settings:** When Automatic Updates are on and Microsoft Update Services is not enabled on the client computer, the client computer is restricted to a remediation network until Microsoft Update Services is enabled.
- **Security Updates Settings:** If you select Restrict access for clients that do not have all available security updates installed, the client computer is restricted to a remediation network. However, this option should not be selected unless the computers that have the Windows Update Agent running are registered with a server running Windows Server Update Service (WSUS) or similar server. You can specify the minimum severity of the updates (Critical Only, Important and above, Moderate and above, and Low and above), and the number of hours allowed since the client has checked for security updates (maximum of 72 hours).

Configuring Health Policies

Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for the NAP-capable computers that attempt to connect to your network.

Typically, the health policies are in pairs, one for NAP-compliant and the other for NAP-noncompliant, as shown in Figure 14-4. To use the NAP-compliant policy, the client must pass all SHV checks, and to use the NAP-noncompliant policy, the client just has to fail one or more of the SHV checks.

Figure 14-4

Viewing the health policies

The health policies are connected directly to the network policies and connection Request Policies. As you open the network policies, the Condition tab specifies the health policy that it is connected to.

As you can see in Figure 14-5, for NAP DHCP health policies, the network policies include NAP DHCP-compliant, NAP DHCP-noncompliant, and NAP DHCP nonNAP-capable policies. If you open each policy, you find the following NAP enforcement settings:

- **NAP DHCP-compliant:** Allow full network access.
- **NAP DHCP-noncompliant:** Allow limited access.
- **NAP DHCP nonNAPcapable properties:** Allow full network access.

Figure 14-5

Displaying the network policies

Configuring Isolation and Remediation

It has already been discussed that if a computer is non-compliant, it should be isolated from production network. When you configure NAP, you can configure either a monitor-only policy or an isolation policy.

Although a monitor-only policy cannot prevent PCs from gaining access to your network, the compliance state of each remote PC that attempts a connection will be logged. Typically, you use a monitor-only policy when you first implement NAP so that you can test the implementation to verify which computers are blocked and which are granted access to the production network by viewing the security logs in the Event Viewer on the NAP server. After you have the policies tweaked and NAP is working like it should be, you then switch the policy to isolation mode.

To provide assistance to users of noncompliant computers when requiring NAP health enforcement, you can configure a remediation server group and troubleshooting URL that is available to users if they fail the compliance check. Each organization has its own remediation server depending on the requirements of the SHVs. Remediation servers typically consists of the following:

- DHCP servers to provide IP configuration
- Naming servers, including DNS servers and WINS servers
- Active Directory domain controllers (read-only domain controllers are recommended to minimize security risks)

- Internet proxy servers so that noncompliant NAP clients can access the Internet
- HRAs so that noncompliant NAP clients can obtain a health certificate for the IPsec enforcement method
- Web server that contains the troubleshooting URL server, so users can access information on compliance
- Anti-virus/anti-malware servers to retrieve updated anti-virus/anti-malware updates
- Software update servers so that clients can get Windows updates

CONFIGURE ISOLATION MODE OR THE LIST OF REMEDIATION SERVERS

GET READY. To configure the isolation mode or the list of remediation servers, perform the following steps:

1. Open Server Manager.
2. Click Tools > Network Policy Server. The *Network Policy Server console* opens.
3. Under *Policies*, click Network Policies.
4. In the right pane, double-click the appropriate network policy.
5. Click the Settings tab.
6. To modify the NAP Enforcement, including whether the policy has full network access or limited access, click NAP Enforcement.
7. To change the Remediation Servers Group and Troubleshooting URL, click Configure.

Configuring NAP Client Settings

For clients to use NAP, they must have the Security Center enabled and have the NAP Agent service running.

You can use the Enable Security Center in the Group Policy procedure to enable Security Center on NAP-capable clients using Group Policy. Some NAP deployments that use Windows Security Health Validator require Security Center. In addition, you need to open the Services console to start and set the startup type to Automatic the Network Access Protection Agent service.

ENABLE THE SECURITY CENTER AND START THE NETWORK ACCESS PROTECTION AGENT SERVICE

GET READY. To enable the Security Center and start the NAP Agent service using Group Policy, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Navigate to a GPO, right-click the GPO, and then click Edit. The *Group Policy Management Editor* opens.
4. In the console tree, navigate to Computer Configuration\Administrative Templates\Windows Components\Security Center.
5. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.
6. Navigate to Computer Configuration\Policies\Windows Settings\Security Settings\System Services.

7. Double-click the Network Access Protection Agent service. The *Network Access Protection Agent Properties* dialog box.
8. Select Automatic and click OK to close the *Network Access Protection Agent Properties* dialog box.
9. Close the *Group Policy Management Editor* and close the *Group Policy Management console*.

To verify a client's configuration, you can run the following command:

```
netsh nap client show state
```

Business Case Scenarios

Scenario 14-1: Implementing NAP

You have a network with around 1,000 clients that connect to it. In addition, you have an additional 50 consultants and vendors that connect to your network each week directly and through the VPN. How can you ensure that all computers connecting to your network have an updated antivirus software package, an updated anti-spyware package, and the newest security patches, and if they don't, how can they get an updated antivirus software package, an updated anti-spyware package, and the newest security patches?

Scenario 14-2: Configuring Remediation Servers

You have implemented NAP with DHCP enforcement so that you make sure you have an updated antivirus software package, an updated anti-spyware package, and the newest security patches. Which servers do you need to set up as remediation servers and why?

15 LESSON

Configuring Service Authentication

Configuring Server Authentication

THE BOTTOM LINE

Authentication is the act of confirming the identity of a user or system and is an essential part used in authorization when the user or system tries to access a server or network resource. Because authentication is such a key component in security, you need to choose the appropriate authentication method. Two types of authentication that Windows supports are NT LAN Manager (NTLM) and Kerberos.

Although Kerberos is the default authentication protocol for today's domain computers, NTLM is the default authentication protocol for Windows NT, standalone computers that are not part of a domain, and situations in which you authenticate to a server using an IP address. NTLM also acts as a fallback authentication protocol if Kerberos authentication cannot be completed, such as when it is blocked by a firewall.

Managing Service Principal Names

A service or application that is secured by Kerberos must have an identity (a user account or computer account) within the realm (in this case, the domain) that the system exists on. Although Active Directory can identify an account using a simple username, the Kerberos standard includes information such as the service class, host name, and port that the account can use.

A ***service principal name (SPN)*** is the name by which a client uniquely identifies an instance of a service. The client locates the service based on the SPN, which consists of three components:

1. The service class, such as HTTP (which includes both the HTTP and HTTPS protocols) or SQLService
2. The host name
3. The port (if port 80 is not being used)

To establish an SPN for https://portal.contoso.com on port 443, you use HTTP/portal.contoso.com:443. Kerberos authentication service then uses the SPN to authenticate a service.

When a domain controller's KDC receives the service ticket request from a client, it looks up the requested SPN. The KDC then creates a session key for the service and encrypts the session key with the password of the account with which the SPN is associated. The KDC

issues a service ticket, containing the session key, to the client. The client presents the service ticket to the service. The service, which knows its own password, decrypts the session key and authentication is complete.

If a client submits a service ticket request for an SPN that does not exist in the identity store, no service ticket can be established and the client throws an access denied error. For this reason, each component of a SharePoint infrastructure that uses Kerberos authentication requires at least one SPN. For example, the intranet web application app pool account must have an SPN of HTTP/intranet.contoso.com.

The SPN is associated with the application pool, not the server. In addition, for each web application, you should assign two SPNs, one with the fully qualified domain name for the service and one with the NetBIOS name of the service.

You can use ADSI Edit to add SPNs to an account. To configure an SPN for a service or application pool account, you must have domain administrative permissions or a delegation to modify the `ServicePrincipalName` property. In addition, you must run ADSI Edit from a domain controller or from a computer that has the remote server administration tools installed.

CONFIGURE AN SPN FOR A SERVICE OR APPLICATION POOL ACCOUNT

GET READY. To configure an SPN for a Service or Application Pool Account, perform the following steps:

1. Open Server Manager.
2. Click Tools > ADSI Edit. The *ADSI Edit console* opens.
3. Right-click ADSI Edit in the console tree, and then click Connect To.
4. When the *Connection Settings* dialog appears, click OK.
5. Expand Default Naming Context in the console tree, expand the domain, and then expand the nodes representing the OUs in which the account exists. Click the OU in which the account exists.
6. In the *Details* pane, right-click the service account and then click Properties.
7. In the *Attributes* list, double-click servicePrincipalName to display the *Multi-valued String Editor* dialog box (see Figure 15-1).

Figure 15-1

Managing the SPNs for an object

8. In the *Value to add* field, type the SPN and then click Add.
9. Click OK twice.

Configuring Kerberos Delegation

Kerberos delegation allows a Kerberos ticket to be created for another service on the originating user's behalf. This can be done with full delegation or with constrained delegation. Constrained delegation is when you specify that the Kerberos delegation can be executed only against a limited set of services.

To configure Kerberos delegation, you simply open *Active Directory Users and Computers*, go to the account that has an SPN, open the account's properties, and click *Delegation*. Figure 15-2 shows the Delegation tab.

Figure 15-2

Configuring the Kerberos delegation

To allow full delegation, select the *Trust this user for delegation to any service (Kerberos only)*. To allow for constrained delegation, select the *Trust this user for delegation to specified services only*. You can then select to use only for Kerberos, or you can specify *Use any authentication protocol*, and then click the *Add* button, to specify which services to be delegated for a user or computer and specify the user or computer.

Managing Service Accounts

THE BOTTOM LINE

A ***service account*** is an account under which an operating system, process, or service runs. A service account can allow the application or service specific rights and permissions to function properly while minimizing the permissions required for the users using the application server. Service accounts are used to run Microsoft Exchange Microsoft SQL Server, Internet Information Services (IIS), and SharePoint.

On a local computer, you can configure an application run the Local Service, Network Service, or Local System. Although these service accounts are simple to configure and use, they are typically shared among multiple applications and services, and they cannot be managed on a domain level. In addition, often you need to use accounts that have domain administrative rights and/or permissions. Besides the traditional service account, Microsoft has introduced Managed Service Accounts and group Managed Service Accounts.

Creating and Configuring Service Accounts

The traditional service account is a standard user account. Therefore, it is created with the Active Directory Users and Computers console.

Typically with user accounts, you specify how often a password gets changed. When a user logs on and a password is due to be changed, the user will be prompted to change the password. With service accounts, there is no interactive login. Therefore, you will configure the password not to expire. Unfortunately, anytime you have an account that does not expire, the password is more vulnerable because more time is available for cracking a password.

To reduce the risk of using service accounts, you should follow these guidelines:

- Require a unique account to run the service on each server.
- If possible, set up the account as a local account rather than a global domain account.
- Use a strong password for the service account.
- Make sure that the password changes often. Of course, when you change the password for the account, you will have to change the password for the services or applications that use the service account simultaneously.
- Give the account the least amount of access (user rights, NTFS permissions, and share permissions) it needs to perform its necessary tasks.
- Do not share the password, and store the password in a safe location.

CREATE A SERVICE ACCOUNT

GET READY. To configure a forwarding computer to forward events, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Users and Computers.
3. In the console tree, double-click the Domain node to expand the node.
4. In the *Details* pane, right-click the organizational unit where you want to add the service account, click New, and then click User. The *New Object – User Wizard* starts.
5. In the *First name* text box, type a first name for the service account.
6. In the *Last name* text box, type a last name for the service account.
7. Modify *Full name* as desired.
8. In the *User logon name* text box, type the name in which the service account will log on. Click Next. The password options appear.
9. In the *Password* and *Confirm password* dialog boxes, type a password for the service account.
10. If you don't want the password to expire, select the Password never expires option. When a dialog box opens saying that the password should never expire and that the user will not be required to change the password at next logon, click OK.
11. Click Next.
12. Click Finish to complete creating a service account.

After the service account is created, you can double-click the service account in Active Directory Users and Computers console to open the account properties. You can then add the account to groups, using the Member Of tab.

Creating and Configuring Managed Service Accounts

Managed Service Accounts (MSAs), introduced with Windows Server 2008 R2, are used to improve the use of the traditional service account in Windows. They are an Active Directory `msDS-ManagedServiceAccount` object class that enables automatic password management and SPN management for service accounts.

Rather than manually changing the account password and the password for the service or application, you use the MSA where the password will automatically change on a regular basis.

As mentioned previously, MSAs are stored in Active Directory Directory Services (AD DS) as `msDS-ManagedServiceAccount` objects in Windows Server 2008 and `MSDS-GroupManagedServiceAccount` on Windows Server 2012 R2. This class inherits structural aspects from the Computer class (which inherits from the User class). This enables an MSA to fulfill user-like functions such as providing authentication and security context for a running service, while it uses the same automatic password update mechanism used by Computer objects in AD DS. However, a standard MSA cannot be shared between multiple computers or be used in server clusters where the service is replicated between nodes.

Similar to computer accounts, a Managed Service Account establishes a complex, cryptographically random, 240-character password and changes that password when the computer changes its password. By default, this occurs every 30 days. An MSA cannot be locked out and cannot perform interactive logons.

MSAs provide the following benefits to simplify administration:

- Automatic password management
- Simplified SPN management

MSAs are stored in the `CN=Managed Service Accounts, DC=<domain>, DC=<com>` container, which can be used if you enable the Advanced Features option in the View menu within Active Directory Users and Computers. In addition, you can also see the container using the Active Directory Administrative Center.

To have MSAs, you must have the following:

- Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 domain controller
- .NET Framework 3.5.x
- Active Directory module for Windows PowerShell

When you create a Managed Service Account, you must specify a short account name of fewer than 15 characters. The dollar sign suffix lengthens the name; the resulting SAM Account Name must be 15 characters or less. Although you can create a Managed Service Account with a longer name in Active Directory, you will be unable to install or use the managed account on a computer.

For example, to create the testsvc account on the domain controller, perform the following command at the Active Directory Module for Windows PowerShell:

1. `new-adserviceaccount -name testsvc –dnshostname win2012srv.contoso.com`
2. `add-adcomputerserviceaccount –identity win2012srv -serviceaccount testsvc`

Then go to the win2012srv and execute the following command using Windows PowerShell:

```
Install-ADServiceAccount -Identity testsvc
```

After you install the Managed Service Account, you can configure a service to use the account as its logon identity. When you specify the logon account, be sure that the name includes the dollar sign ($).

USE THE MSA WITH A SERVICE

GET READY. To configure a forwarding computer to forward events, perform the following steps:

1. Open Server Manager.
2. Click Tools > Services. The *Services console* opens.
3. Double-click the desired service. The services *Properties* dialog box opens.
4. Click the Log On tab.
5. Select This account option and type the name of the service account in the *This account* text box.
6. Clear the password in the *Password and Confirm password* text boxes.
7. Click OK.
8. When it says that the account has been granted the Log On As Service, click OK.
9. When it states that the new logon name will not take effect until you stop and restart the service, click OK.

After you install the Managed Service Account, you can configure a service to use the account as its logon identity. In the Services console, open the properties of a service and click the *Log On* tab. Select *This Account*, and then click *Browse*. Type the name of the Managed Service Accounts, and then click *OK*. On the Log On tab, confirm that the name appears with a dollar sign ($). The account will be given the Log On As Service right.

If you move a service to another computer and you want to use the same Managed Service Accounts on the target system, you must first use the `Uninstall-ADServiceAccount` cmdlet to remove the Managed Service Account from the current computer and then use the `Install-ADServiceAccount` cmdlet on the new computer.

If necessary, when you create the new MSA, you can also specify the SPN by using the `-ServicePrincipalNames <SPN_string>`.

```
New-ADServiceAccount -Name svcaccount
-DNSHostname win2012srv.contoso.com
-ServicePrincipalNames
HTTP/portal.contoso.com,HTTP://portal
```

To change the parameter for a service account, you use `Set-ADServiceAccount`. To delete a group service account using a Windows PowerShell command, you use the `Remove-ADServiceAccount`. To display a list of the service accounts, use the `Get-ADServiceAccount`.

Creating and Configuring Group Managed Service Accounts

The one limitation of Managed Service Accounts is that it can only be used on one server. Therefore, if you have a cluster or farm where you need to run the system or application service under the same service account, you cannot use Managed Service Accounts. ***Group Managed Service Accounts*** are similar to Managed Service Accounts, but they can be used on multiple servers at the same time.

To use group Managed Service Accounts, you must have one domain controller that is running Windows Server 2012 R2 so that it can store managed password information. Similar to MSAs, you have to create a KDS root key.

Configuring Virtual Accounts

Virtual accounts were introduced with Windows 7 and Windows Server 2008 R2. A ***virtual account*** is an account that emulates a Network Service account that has the name NT Service*servicename*. The virtual account has simplified service administration, including automatic password management, and simplified SPN management.

The Local System account has full local system privileges on a local machine, but it does not have access to the network. The Network Service account can access the network using the computer account credentials, but it has limited local privileges. In addition, when using the Network Service account, it becomes difficult to track which services are accessing resources and performing actions when all of the services are using the Network Service account.

Virtual accounts are accounts that emulate Network Service accounts, but they can be assigned unique names, usually the same name as the service. Virtual accounts use a single account for a single service. If you have multiple service accounts that use virtual accounts, there will be a different account for each service.

Service accounts are not created or deleted. To configure a service to use a virtual service account, when you configure the properties of a service, configure the account to use NT SERVICE*servicename* (where *servicename* matches the name of the service).

USE A VIRTUAL ACCOUNT

GET READY. To use a virtual account, perform the following steps:

1. Using Server Manager, click Tools > Services.
2. Double-click the service that you want to modify. The *Properties* dialog box for the service will open.
3. Click the Log on tab.
4. Select This account. In the *This account* text box, type NT Service*servicename*.
5. Ensure the Password text box and the Confirm Password text box is empty.
6. Click OK to close the *Properties* dialog box.
7. When the *Services* dialog box opens, indicating that the new logon name will not take effect until you stop and restart the service, click OK.
8. Right-click the service and choose Restart.

Business Case Scenarios

Scenario 15-1: Creating and Using a Service Account

You are an administrator of the Contoso Corporation. You installed a cluster of computers that need to use the same service account for the Widget application/services. What solution would you use?

Scenario 15-2: Using Kerberos

You have a client application/service placed on Server1. When a user accesses the application/service, you want the server to send a Kerberos request on behalf of the user who is running the application.

16 LESSON

Configuring Domain Controllers

Understanding Domain Controllers

THE BOTTOM LINE

The domain controllers are the servers that store and run the Active Directory database. Active Directory is a major component in authentication, authorization, and auditing. Therefore, you need to know how the different types of domain controllers and how they are used to create the Active Directory environment.

You can look at Active Directory from two sides: logical and physical. First, when you hear Active Directory, you most likely focus on the logical components that make up Active Directory. The logical components (which administrators create, organize, and manage) include:

- **Organization units:** Containers in a domain that allow you to organize and group resources for easier administration, including providing delegating administrative rights.
- ***Domains*:** An administrative boundary for users and computers, which are stored in a common directory database. A single domain can span multiple physical locations or sites and can contain millions of objects.
- **Domain trees:** Collection of domains that are grouped together in hierarchical structures and that share a common root domain. A domain tree can have a single domain or many domains. A domain (known as the parent domain) can have a child domain. A child domain can have its own child domain. Because the child domain is combined with the parent domain name to form its own unique Domain Name System (DNS) name, the domains with a tree have a contiguous namespace.
- **Forests:** A collection of domain trees that share a common Active Directory Domain Services (AD DS). A forest can contain one or more domain trees or domains, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. A forest can be a single domain tree or even a single domain. The first domain in the forest is called the *forest root domain*. For multiple domain trees, each domain tree consists of a unique namespace.

The physical components that make up Active Directory include the following:

- ***Domain controllers*:** The servers that contain the Active Directory databases. A domain partition stores only the information about objects located in that domain. All domain controllers in a domain receive changes and replicate those changes to the domain partition stored on all other domain controllers in the domain. As a result, all domain controllers are peers in the domain and manage replication as a unit.

- **Global catalog servers:** A domain controller that stores a full copy of all Active Directory objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest. Applications and clients can query the global catalog to locate any object in a forest. A global catalog is created automatically on the first domain controller in the forest. Optionally, other domain controllers can be configured to serve as global catalogs.
- **Operations Masters:** Specialized domain controllers that perform certain tasks so that multi-master domain controllers can operate and synchronize properly.
- **Read-only domain controllers:** Specialized domain controllers that are intended for use in branch offices and servers in a low physical security environment that holds only a non-writable copy of Active Directory.

When a user logs on, Active Directory clients locate an Active Directory server (using the DNS SRV resource records) known as a domain controller in the same site as the computer.

Each domain has its own set of domain controllers to provide access to the domain resources, such as users and computers. For fault tolerance, a site should have two or more domain controllers. That way, if one domain controller fails, the other domain controller can still service the clients. Note that whenever an object (such as a username or password) is modified, it is automatically replicated to the other domain controllers within a domain.

A domain controller is a Windows server that stores a replica of the account and security information for the domain and defines the domain boundaries. To make a computer running Windows Server 2012 R2 a domain controller, you must install the Active Directory Domain Services (AD DS) role and then promote the computer to a domain controller.

Managing Operations Masters

Operations masters, sometimes referred to as *Flexible Single Master Operations (FSMO)*, are specialized domain controllers that perform certain tasks that can be handled only by a single domain controller in a multi-master environment.

TAKE NOTE*

Since 2005, the term *FSMO* has been deprecated in favor of *operations masters*.

With Active Directory, domain controllers follow a multi-master replication model that ensures copies of all domain objects are found on each domain controller within a domain so that they can be quickly and easily accessed and to provide fault tolerance. To help resolve conflicts and such, all transactions use version IDs and timestamps. However, some critical functions need to have the assurance of little or no risk of error.

For example, when you add attributes to an Active Directory object, you change the schema of the domain database. Although it is relatively easy to make those changes, it is considered a big deal when you modify the schema because it affects all objects for that object type you are about to change and it can corrupt the database. Luckily, making changes in a controlled way provides a virtually 100% success rate. However, if two administrators attempt to make similar changes at the same time from two different locations (and two different domain controllers), the chances of problems significantly rise. Therefore, to prevent this type of problem, there is only one specific domain controller that can handle this type of function. In this particular case, it is the Schema Master, which is discussed next.

The five operations master roles are shown in Table 16-1. When you install a domain, the first domain controller installed for a domain has the Primary Domain Controller, RID Master, and Infrastructure Master. Similarly, the first domain controller in the root domain has the Domain Naming and Schema Master roles.

Table 16-1

Operations Master Roles

Operations Master Roles	Description	Affect of Failure
Primary Domain Controller (PDC) Emulator (*one per domain*)	Originally created to provide backward compatibility with Windows NT 4.0 domains. It also coordinates password changes, account lockouts, and time synchronization; manages edits to Group Policy Objects (GPOs); and acts as a domain master browser (provides a list of workgroups and domains when you browse). When a password is changed, the domain controller that initiates a password change will send the change to the PDC Emulator, which in turn updates the global catalog server and provides immediate replication to other domain controllers in the domain.	Because the PDC emulator is the most heavily one used, and by the tasks that it does, it can affect users when it is down. For example, if a password is changed, it might not be immediately replicated, which can cause problems when a user tries to access resources. If the system clocks drift too much, users might not be able to log on as Kerberos fails. Account lockout will not work and you will not be able to raise the functional level of a domain.
Infrastructure Master (*one per domain*)	Used to track which objects belong to which domain because it is responsible for reference updates from its domain objects to other domains. When you rename or move a member of a group (and the members that reside in different domain from the group), the infrastructure master is responsible for updating the group so that it knows the new name or location of the member.	Typically, the loss of the infrastructure master will not be visible to users. However, it might be seen if you recently moved or renamed a large number of accounts.
Relative Identifier (RID) Master (*one per domain*)	When a domain controller creates a user, group, or computer object, it assigns the object a unique security ID (SID). The SID consists of a domain security ID that identifies the domain to which the object belongs and a relative ID that identifies the object within the domain. The RID master is responsible for assigning relative identifiers to domain controllers in the domain. The RID master assigns a block of 500 identifiers to each domain controller. When 50% of the supply of RIDs is used, it contacts the RID to request a new supply.	Although the loss of the RID master will not be seen by users, it can be seen when administrators are creating objects and the domain runs out of relative IDs to assign. In addition, you will not be able to move objects between domains.
Schema Master (*one per forest*)	Controls all the updates and modifications to the schema. To update the schema of a forest, you must have access to the Schema Master.	Although the loss of the Schema Master will not affect the users, you cannot modify the schema or install any applications, such as Microsoft Exchange, that would modify the schema. You will also not be able to raise the functional level of the forest.
Domain Naming Master (*one per forest*)	Holds the Domain Naming Master role that controls the addition or removal of domains in the forest.	Although the loss of the Domain Naming Master will not affect users, you will not be able to add or remove domains from the forests

According to Microsoft, when you place the Operations Master roles, you should follow these guidelines:

- Place the domain-level roles on high-performance domain controllers.
- Do not place the infrastructure master on a global catalog server unless you have only one domain or all the domain controllers in your forest are also global catalogs.
- The Schema Master and Domain Naming Master should be on domain controllers in the forest-root domain.
- If the Primary Domain Controller (PDC) Emulator becomes overworked, you should offload non-AD DS roles to other servers, upgrade the PDC Emulator, or move the PDC Emulator to a more powerful computer.

TAKE NOTE*

To activate the necessary DLL files for Active Directory Schema, you need to register the schmmgmt.dll DLL file using the following syntax: `regsvr32 schmmgmt.dll`.

TRANSFERRING THE OPERATIONS MASTERS ROLE

From time to time, you might need to move the operation master roles to other domain controllers. If you are planning to do maintenance where a domain controller that holds the Operations Master will be down for an extended period of time, you are going to retire a domain controller that holds a role of Operations Master or you need to move the role to a domain controller with more resources, you will need to transfer the Operations Master. Transferring a FSMO role requires that the source domain controller and the target domain controller be online.

TRANSFER THE HOLDERS OF RID MASTER, PDC EMULATOR, OR INFRASTRUCTURE MASTER

GET READY. To transfer the holders of RID Master, PDC Emulator, and Infrastructure Master, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Users and Computers. The *Active Directory Users and Computers* console opens.
3. In the console tree, right-click the Active Directory Users and Computers node and select Change Domain Controller.
4. When the *Change Directory Server* dialog box opens, select the domain controller that you want to transfer the role to and click OK.
5. Right-click the domain, and select Operations Masters.
6. Select the tab that reflects the role you are transferring.
7. Click Change.
8. In the *confirmation message* box, click Yes to confirm the change in roles. In the next message box, click OK.
9. When done, click Close to close the *Operations Masters* dialog box.
10. Close the *Active Directory Users and Computers console*.

TRANSFER THE HOLDERS OF DOMAIN NAMING OPERATIONS MASTER ROLE

GET READY. To transfer the holder of the Domain Naming Operations Master role holder, perform the following steps:

1. Open Server Manager.
2. Right-click the Active Directory Domains and Trusts node and select Connect To Domain Controller.

3. When the *Change Directory Server* dialog box opens, select the domain controller that you want to transfer the role to and click OK.
4. In the console tree, right-click Active Directory Domains and Trusts and select Operations Master.
5. In the *Change Operations Master* dialog box, click Change.
6. In the confirmation message box, click Yes to confirm the change in roles. In the next message box, click OK.
7. Click Close to close the *Operations Master* dialog box.
8. Close the *Active Directory Domains and Trusts console*.

TRANSFER THE HOLDERS OF SCHEMA MASTER OPERATIONS MASTER ROLE

GET READY. To transfer the holder of the Schema Master Operations Master role holder, perform the following steps:

1. Right-click the start button and select Command Prompt (Admin). The command prompt opens.
2. Execute the mmc command. The *MMC console* opens.
3. Open the File menu and select Add/Remove Snap-in. The *Add or Remove Snap-ins* dialog box opens.
4. Select Active Directory Schema (second option) and click Add. Then click OK to close the *Add/Remove Snap-ins* dialog box.
5. Right-click Active Directory Schema and select Change Domain Controller.
6. Select the Specify Name option and select the domain controller that you want to switch to. Click OK.
7. In the console tree, right-click Active Directory Schema and select Operations Master.
8. In the *Change Schema Master* dialog box, click Change.
9. Click OK to close the *Change Schema Master* dialog box.
10. Close the *MMC console* and command prompt.

SEIZING THE OPERATIONS MASTERS ROLE

If a domain controller that holds an Operations Master role has an unrecoverable failure, you cannot transfer roles because the current domain controller is not online. Therefore, you need to size the role. Seizing a FSMO role is a drastic measure that should be performed only in the event of a permanent role holder failure.

To seize a role of an Operations Master, you use the ***ntdsutil.exe*** utility. The ntdsutil.exe is a command-line tool that allows you to manage Active Directory including performing maintenance on the Active Directory database, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

SEIZE THE ROLE OF AN OPERATIONS MASTER HOLDER

GET READY. To seize the holder of the Schema Master Operations Master role holder, perform the following steps:

1. Right-click the start button and select Command Prompt (Admin). The command prompt opens.
2. From the command prompt, execute the ntdsutil command.

3. At the ntdsutil prompt, execute the roles command.
4. At the fsmo maintenance prompt, execute the connections command.
5. At the server connections prompt, execute the following command:

   connect to server <FQDN_of_desired_role_holder>

   An example of this would be:

   connect to server server1.contoso.com
6. At the server connections prompt, execute the quit command.
7. At the fsmo maintenance prompt, type one of the following commands:

   seize schema master

   seize naming master

   seize RID master

   seize PDC

   seize infrastructure master

Figure 16-1 shows the commands to seize the PDC Emulator role.

Figure 16-1

Seizing the PDC Emulator role

8. If an *"Are you sure?"* dialog box appears, click Yes to continue.
9. At the fsmo maintenance prompt, execute the quit command.
10. At the ntdsutil prompt, execute the quit command.
11. Close the command prompt.

Installing and Configuring an RODC

THE BOTTOM LINE

Windows Server 2008 introduced the ***read-only domain controller (RODC)***, which contains a full replication of the domain database. It was created to be used in places where a domain controller is needed but the physical security of the domain controller could not be guaranteed. For example, it might be placed in a remote site that is not very secure and that has a slower WAN link. Because it has a slow WAN link, a local domain controller would benefit the users at that site.

An RODC does not perform any outbound replication and accepts only inbound replication connections from writable domain controllers. Because the RODC has only a read-only copy of the Active Directory database, the administrator needs to connect to a writable domain controller to make changes to Active Directory.

To deploy an RODC, you need the following:

- Ensure that the forest functional level is Windows Server 2003 or higher.
- Deploy at least one writable domain controller running Windows Server 2008 or higher.

If any domain controllers run Windows Server 2003, you need to configure permissions on DNS application directory partitions to allow them to replicate to RODCs by running the `ADPrep /RODCPrep` command. The `adprep.exe` command is located on the \support\adprep folder on the Windows Server 2012 R2 installation disk.

When you install an RODC, you need to define a delegated administrator that has local administrative permission to the RODC, even though the account is not a member of the Domain Admin or domain built-in Administrators group.

Because RODCs need to be as secure as possible, you can configure each RODC to have its own Password Replication Policy (PRP). On writable domain controllers, Active Directory passwords are stored locally within the ntds.dit file. Because the RODC is put in a place where the security cannot be guaranteed, you can specify a particular list of user or group accounts whose password information should be stored (or cached) on a particular RODC.

For example, if you have a Site1 branch, you can configure the RODC to cache only passwords for those users who are members of the Site1 security group. In addition, you can configure specific users or groups whose password information should not be cached on an RODC such as administrative accounts.

To allow enterprise-wide configuration of the RODC Password Replication Policy, Windows Server 2012 R2 creates the following security groups:

- **Denied RODC Password Replication Group:** Members of this group are placed in the Deny list of the Password Replication Policies of all RODCs by default. Some of the groups include Administrators, Server Operators, Backup Operators, Account Operators, and Denied RODC Password Replication Group.
- **Allowed RODC Password Replication Group:** Members of this group are placed in the Allow list of the Password Replication Policies of all RODCs by default. By default, this group does not have any members.

INSTALL A READ-ONLY DOMAIN CONTROLLER

GET READY. To install a Read-only domain controller, perform the following steps:

1. Open Server Manager.
2. On the left pane, click AD DS. On the right-pane, click More in the yellow bar (see Figure 16-2).

Figure 16-2

Installing AD DS on a new computer

3. When the *All Servers Task Details* window opens, click Promote this server to a domain controller. The *Active Directory Domain Services Configuration Wizard* starts.
4. On the *Deployment Configuration* page, with the Add a domain controller to an existing domain already selected, click Next.
5. On the *Domain Controllers Options* page, select Read only domain controller (RODC). Select the correct site name. Type a Directory Service Restore Mode (DSRM) password in the *Password and Confirm password* text boxes. Click Next.
6. On the *RODC Options* page, click Select in the *Delegated administrator account* section. When the *Select User or Group* dialog box opens, type the name of the account to be used as a delegated administrator in the *Enter the object names to select* text box and click OK. Click Next.
7. On the *Additional Options* page, click Next.
8. On the *Paths* page, click Next.
9. On the *Review Options* page, click Next.
10. On the *Prerequisites Check* page, click Install.
11. When the installation is complete, restart the domain controller.

To modify the Password Replication Policy, after the RODC was installed, just open the Active Directory Users and Computers console, navigate to the Domain Controllers OU, right-click the RODC, and select *Properties*. The Password Replication Policy is shown in the Password Replication Policy (see Figure 16-3). To add new entries, click the *Add* button. To modify the current entries, click the *Advanced* button.

Figure 16-3

Configuring the Password Replication Policy

Cloning a Domain Controller

THE BOTTOM LINE

Starting with Windows Server 2012, you can safely virtualize a domain controller and rapidly deploy virtual domain controllers through cloning. It allows you to quickly restore domain controllers when a failure occurs and to rapidly provision a test environment when you need to deploy and test new features or capabilities before you apply the features or capabilities to production.

Because domain controllers provide a distributed environment, you could not safely clone an Active Directory domain controller in the past. However by following the steps in the next exercise, you will be able to make a copy of a Server 2012 domain controller that can be used over and over.

Before, if you cloned any server, the server would end up with the same domain or forest, which is unsupported with the same domain or forest. You would then have to run sysprep, which would remove the unique security information before cloning and then promote a domain controller manually. When you clone a domain controller, you perform safe cloning, which a cloned domain controller automatically runs a subset of the sysprep process and promotes the server to a domain controller automatically.

The four primary steps to deploy a cloned virtualized domain controller are as follows:

1. Grant the source virtualized domain controller the permission to be cloned by adding the source virtualized domain controller to the Cloneable Domain Controllers group.
2. Run `Get-ADDCCloningExcludedApplicationList` cmdlet in Windows PowerShell to determine which services and applications on the domain controller are not compatible with the cloning.

3. Run `New-ADDCCloneConfigFile` to create the clone configuration file, which is stored in the C:\Windows\NTDS.
4. In Hyper-V, export and then import the virtual machine of the source domain controller.

DEPLOY A CLONED VIRTUALIZED DOMAIN CONTROLLER

GET READY. To deploy a cloned virtualized domain controller, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Users and Computers. The *Active Directory Users and Computers console* opens.
3. Navigate to and click the Domain Controllers OU.
4. Right-click the source virtualized domain controller and select Properties. The domain controller *Properties* dialog box opens.
5. Click the Member Of tab.
6. Click Add. When the *Select Groups* dialog box opens, type Cloneable Domain Controllers in the *Enter the object names to select* text box and click OK.
7. Close the *Active Directory Users and Computers console*.
8. To display the list of services and programs installed that are not compatible with cloning of the AD server on the source virtualized domain controller, run the following command from Windows PowerShell:

   Get-ADDCCloningExcludedApplicationList
9. Review the list and remove any services and applications that you believe are not safe to clone. The others need to be tested or verified from the vendor.
10. After the list has been cleaned up and you still have items that you want to be included in the cloning, create a CustomDCCloneAllowList.xml file by running the following command:

    Get-ADDCCloningExcludedApplicationList

    -GenerateXml
11. Click the Windows PowerShell icon on the task bar. The *Windows PowerShell* command prompt opens.
12. Run the `New-ADDCCloneConfigFile` cmdlet on the source virtual DC while specifying the configuration settings for the clone domain controller, such as the name, the IP address, and DNS resolver. For example:

    New-ADDCCloneConfigFile –Static -IPv4Address

    “192.168.3.125” -IPv4DNSResolver “192.168.3.120”

    -IPv4SubnetMask “255.255.255.0” -CloneComputerName

    “VServer2” -IPv4DefaultGateway “192.168.3.1”

    -SiteName “Site1”

    Make sure the site exists. A DCCloneConfig.xml file is created in the C:\Windows\NTDS folder.
13. Go back to the *Server Manager Dashboard*.
14. Click Tools > Hyper-V Manager. The *Hyper-V Manager console* opens (see Figure 16-4).

Figure 16-4

Opening the Hyper-V Manager

15. Right-click the source virtual domain controller and click Turn Off. If you asked if you are sure, click Turn Off.
16. Right-click the source virtual domain controller in Hyper-V Manager and select Export. Specify the folder where you want to export to in the *Location* text box (such as d:\clone) and click Export. Exporting the image will take several minutes.
17. Right-click the source virtual domain controller and click Start.
18. In Hyper-V, open the Action menu and click Import Virtual Machine.
19. When the *Import Virtual Machine Wizard* starts, click Next.
20. On the *Locate Folder*, specify the exported folder (such as D:\Clone\DC02) in the *Folder* text box and click Next.
21. On the *Select Virtual Machine* page, click Next.
22. On the *Choose Import Type* page, select copy the virtual machine (create a new unique ID) and click Next.
23. On the *Choose Folders for Virtual Machine Files* page, select Store the virtual machine in a different location. Then specify the following locations:

    Virtual machine configuration folder: D:\Hyper-V\

    Snapshot store: D:\Hyper-V

    Smart paging folder: D:\Hyper-V

    Click Next.

24. On the *Choose Folders to Store Virtual Hard Disks* page, type D:\Hyper-V in the *Location* text box. Click Next.
25. On the *Completing Import Wizard* page, click Finish. Importing will take several minutes.
26. When the import is complete, right-click the new server and click Start.

Business Case Scenario

Scenario 16-1: Establishing a Help Station in an Information Lobby

You work for the Contoso Corporation. At a car show, you need to establish a Sales station that needs to record information for potential users to a system that requires access to a domain controller. However, you want only the sales people to be able to log in to the application and domain controller. What should you do?

17 LESSON

Maintaining Active Directory

Backing Up and Restoring Active Directory

THE BOTTOM LINE

When working with servers, there is no good time for a failure. Active Directory is a complicated database that stores information about your users, computers, groups, and other objects. Just like any other database, it can become corrupt, or objects might be accidentally or maliciously deleted. No matter what happens, the best method to data recovery is using backup.

A ***backup*** or the process of backing up refers to making copies of data so that these additional copies can be used to restore the original after a data-loss event. They can be used to restore entire systems following a disaster or to restore small sets of files or objects that are accidentally deleted or corrupted.

Traditionally, magnetic tapes have been the most commonly used medium for bulk data storage, backup, and archiving. Tape is a sequential access medium, so even though access times might be poor, the rate of continuously writing or reading data can actually be fast.

For larger organizations, you might use multiple tape drives connected together with a tape library that can automatically swap and manage tapes. Recently because of increased capacity at lower cost, hard drives have become a viable option for backups. Hard disks can be included in the SAN, NAS, internal hard drives, and external hard drives. Some disk-based backup systems, such as virtual tape libraries, support data de-duplication, which can dramatically reduce the amount of disk storage capacity consumed by daily and weekly backup data.

Usually hard disks are used to provide backup of recent data, and the data is copied to tape and taken off site for longer term storage and archiving. If a failure occurs, you can quickly restore from the disks. If you need to recover or read data from the past, you will then have to retrieve the tapes from off site and read the tapes.

Another media that is becoming more popular for backups is to use recordable optical disks, such as CDs, DVDs, and even Blu-ray. Unfortunately, the newer formats tend to cost more, which might prohibit their use for backups. There is also some concern about the lifetime of a selected optical disk because some optical disks degrade and lose data within a couple of years.

More recently, cloud computing (sometimes just referred to as the *cloud*) can be used for backups. Cloud computing is the use of computing resource (hardware and software) that is delivered as a service over the network, such as the Internet. As far as the client of cloud computing is concerned, cloud computing looks like a "black box." The client does not need to know what makes the computer resources work. As far as they are concerned, it just works and the vendor of the cloud computing is concerned with providing the managing and maintenance of the computing resources.

Using Windows Backup

Windows includes ***Microsoft Windows Backup***, which allows you to back up a system. However, third-party backup software packages usually offer more features and options.

To access the backup and recovery tools for Windows Server 2012 R2, you must install the Windows Server Backup feature using the Add Roles and Features Wizard. To run the Windows Server Backup, you must be a member of the Backup Operators or Administrators group.

You can create a backup by using the Backup Schedule Wizard or by using the Backup Once option. You can back up to any local drive or to a shared folder on another server.

Finally, you perform a backup using wbadmin.exe, which is the Backup command-line tool. To find more information about the wbadmin.exe, you can use `wbadmin.exe /?` from a command prompt or search the Microsoft TechNet website.

PERFORMING A BACKUP OF ACTIVE DIRECTORY AND SYSVOL

You can create a backup by using the Backup Schedule Wizard or by using the Backup Once option. You can back up to any removable local drive or to a shared folder on another server.

INSTALL WINDOWS SERVER BACKUP

GET READY. To install Windows Server Backup, perform the following steps:

1. Open Server Manager.
2. Click Manage and click Add Roles and Features.
3. When the *Add Roles and Features Wizard* starts, click Next.
4. On the *Select installation type* page, click Next.
5. On the *Select destination server pack*, click Next.
6. On the *Select server roles* page, click Next.
7. Click to select the Windows Server Backup and click Next.
8. On the *Confirm installation selections* page, click Install.
9. When the installation is complete, click Close.

PERFORM A BACKUP OF THE SYSTEM STATE INCLUDING ACTIVE DIRECTORY

GET READY. To perform a backup of the system state including Active Directory, perform the following steps:

1. Open Server Manager.
2. Click Tools > Windows Server Backup. The *Windows Server Backup console* opens (see Figure 17-1).

Figure 17-1

Starting Windows Server Backup

3. Under *Actions*, click Backup Once.
4. When the *Backup Once Wizard* starts, if this is the first time you have run the Backup Once Wizard, click Different Options and click Next.
5. On the *Select Backup Configuration* page, click Custom and click Next.
6. On the *Select Items for Backup* page, click Add Items. The *Select Items* dialog box opens.
7. Select System state and click OK.
8. On the *Select Items for Backup* page, click Next.
9. On the *Specify Destination Type* page, select Remote shared folder. Click Next.
10. On the *Specify Remote Folder* page, type the path of the remote folder (such as \\win2012srv2\backups) and click Next.
11. On the *Confirmation* page, click Backup. The backups will take a few minutes.
12. When the backup is completed, click Close.

Windows Server Backup stores the details about your backups in a file called a backup catalog. The catalog is stored in the same place that you store your backups. Because the catalog specifies what is within a backup, you need the backup catalog to use a Windows backup file.

PERFORMING AN ACTIVE DIRECTORY RESTORE

There are two types of restores that you can perform with Active Directory:

- A nonauthoritative restore
- An authoritative restore

With a ***nonauthoritative restore***, you restore a backup of Active Directory as of the date of the backup. The AD DS restarts on the domain controller, and the domain controller contacts the other domain controllers to get updates since the backups were completed. The other domain controllers replicate the information to the restored domain controller so that they are the same. So if there are problems (such as corrupt data or missing objects) within the database that is stored in all of the domain controllers, the same information is sent to the restored domain controller and the same problem still exists. You use only a nonauthoritative restore if the problem has not spread to the other domain controllers (highly unlikely) or you want to restore the domain controller so that it is functional again.

TAKE NOTE*

Of course, if you perform a complete authoritative restore of Active Directory, any changes to Active Directory since the backup will be lost.

An ***authoritative restore*** is an override type restore that the information on the restored domain controller will be replicated to the other domain controllers. To restore an object or container within Active Directory that has been inadvertently deleted, you need to perform an authoritative restore. To accomplish this, when an authoritative restore is performed, Windows increments the version number is higher than any version number used in the other domain controllers.

TAKE NOTE*

If an object is inadvertently deleted, you might consider using the Active Directory Recycle Bin before performing an authoritative restore. The Active Directory Recycle Bin is discussed later in the lesson.

To perform an authoritative restore, you need to reboot the computer into the ***Directory Services Restore Mode (DSRM)***, which is a mode of Windows that takes the Active Directory offline. You access this mode from the Advanced Boot menu, which is accessed before Windows completes booting by pressing the F8 key.

PERFORM A RESTORE OF THE SYSTEM STATE

GET READY. To perform a restore of the System State, perform the following steps:

1. Restart the domain controller. After the *BIOS POST* screen but before the Windows log appears, press the F8 key repeatedly to access the *Windows Advanced Options* menu.
2. When the *Windows Advanced Options* menu is displayed (see Figure 17-2), use the arrow keys to select Directory Services Restore Mode and press the Enter key.

Figure 17-2

Accessing the Advanced Options menu

```
                    Advanced Boot Options

Choose Advanced Options for: Windows Server 2012
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video
    Last Known Good Configuration (advanced)
    Directory Services Repair Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement
    Disable Early Launch Anti-Malware Driver

    Start Windows Normally

Description: View a list of system recovery tools you can use to repair
             startup problems, run diagnostics, or restore your system.
 ENTER=Choose                                                ESC=Cancel
```

3. Log in as the local administrator (DSRM), not the domain administrator.
4. Open Server Manager.
5. Click Tools > Windows Server Backup. The *Windows Server Backup console* opens.
6. Under *Actions*, click Recover.
7. When the *Recovery Wizard* starts, select A backup stored on another location and click Next.
8. On the *Specify Location type* page, click Remote shared folder and click Next.
9. On the *Specify Remote Folder* page, type the path (such as \\win2012srv2\backups) and click Next.
10. On the *Select Backup Date* page, select the date of the backup that you want to restore from and click Next.
11. On the *Select Recovery Type* page, click System state. Click Next.
12. On the *Select Location for System State Recovery* page, select Perform an authoritative restore of Active Directory files and click Next.
13. When the warning appears that this recovery option will cause all replicated content on the local server to re-synchronize after recovery, click OK.
14. When it asks for you to continue, click OK.
15. Click the Confirmation page, and click Recover.
16. When it asks if you want to continue gain, click Yes.
17. When the backup is completed, click Restart.

To perform an authoritative restore of an object or subtree, you need to know the distinguished name of the object. For example, the user object for jsmith in the Sales OU of the contoso.com domain has a distinguished name of cn=jsmith,ou=Sales,dc=contoso,dc=com.

When you do an authoritative restore process, a back-links file is created. A back-link is a reference to an attribute within another object that also needs to be restored with the object. For example, if you have authoritatively restored a user object that was a member of five Active Directory groups, a backlink to each of those groups need to be restored so that the user is added again to each group appropriately. The authoritative restore process creates an LDIF file containing each back-link that needs to be restored; after the authoritative restore completes, you need to use the LDIFDE command-line utility to restore the back-links contained within that file. For more information about the LDIFDE, search the Microsoft TechNet website.

PERFORM AN AUTHORITATIVE RESTORE

GET READY. Before you reboot the computer, you need to mark items as an authoritative restore. To perform an authoritative restore, perform the following steps:

1. Open a command prompt window.
2. Execute the ntdsutil command.
3. From the *Ntdsutil* menu, execute the activate instance NTDS command.
4. Execute the authoritative restore command.
   a. To restore a single object, execute the restore object <ObjectDN> command.
   b. To restore a container and the objects it contains, execute the restore subtree <ContainerDN> command. The *Authoritative Restore Confirmation Dialog* window opens.
5. When the *Authoritative Restore Confirmation* dialog box opens, click Yes to perform the authoritative restore. When the record or records have been updated, the names of the back-link files are displayed.
6. Be sure to write down the name of the back-link files.
7. Execute the quit command.
8. Press the Enter key to return to the command prompt.
9. Restart the domain controller in normal mode.
10. If back-links need to be restored, right-click the Start button and execute the ldifde –i –f <LDIF file name> -s <FQDN of the local DC> command.
11. Close the command prompt window.
12. Reboot the domain controller.

Configuring Active Directory Snapshots

Another tool used in recovery of Active Directory is the ***Active Directory database mounting tool*** to create and view Active Directory snapshots. An ***Active Directory snapshot*** is a shadow copy, created by the Volume Shadow Copy Service (VSS), of the volumes that contain the Active Directory database and log files.

To create and use snapshots, perform the following steps:

1. Create a snapshot with ntdsutil.exe.
2. Mount the snapshot with the Active Directory database mounting tool.
3. View the objects within the snapshot.
4. When done with the snapshot, dismount the snapshot.

By default, only members of the Domain Admins group and the Enterprise Admins group are allowed to view the snapshots.

CREATE AN ACTIVE DIRECTORY SNAPSHOT

GET READY. To create an Active Directory snapshot, perform the following steps:

1. Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.
2. At the command prompt, execute the ntdsutil command.
3. At the ntdsutil prompt, execute the snapshot command.
4. At the snapshot prompt, execute the activate instance ntds command.
5. Execute the create command.
6. Execute the quit command twice.
7. Close the command prompt window.

MOUNT AN ACTIVE DIRECTORY SNAPSHOT

GET READY. To mount an Active Directory snapshot, perform the following steps:

1. Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.
2. At the command prompt, execute the ntdsutil command.
3. At the ntdsutil prompt, execute the activate instance ntds command.
4. Execute the snapshot command.
5. To return a list of all snapshots, at the snapshot prompt, execute the list all command.
6. Execute the mount {GUID} command, where GUID is the GUID returned by the create snapshot command or displayed with the list all command.
7. Execute the quit command twice to exit ntdsutil.
8. To mount the snapshot, execute the dsamain -dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit -ldapport 50000. You need to specify the date-time as shown on the list. The port number, 50000, can be any open and unique TCP port number.
9. A message indicates that Active Directory Domain Services startup is complete. Do not close the command prompt window and leave the command you just ran, Dsamain.exe, running while you continue to the next step.

After the snapshot, you can view the snapshot using multiple tools, including Active Directory Users and Computers (as shown in the next procedure), LDP.exe, or ADSIEDIT.exe. You can also use LDIFDE and CSVDE to export the information from the snapshot and import the data into production. When you use the CSVDE or LDIFDE, you use the `-s <servername>` and `-t <port number>`.

MORE INFORMATION

For more information on using the **CSVDE** command or **LDIFDE** command, search for these commands at the Microsoft's TechNet website.

Unfortunately, the snapshots are read-only and you cannot modify the contents of a snapshot. Moreover, there are no direct methods with which to move, copy, or restore objects or attributes from the snapshot to the production instance of Active Directory.

VIEW AN AD DS SNAPSHOT

GET READY. To view an AD DS Snapshot, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Users and Computers. The *Active Directory Users and Computers console* opens.
3. Right-click the root node, and then click Change Domain Controller. The *Change Directory Server* dialog box appears.
4. Click <Type a Directory Server name[:port] here> and replace the <Type a Directory Server name[:port] here> text with the name of the domain controller and port number using the DCservername:port# format and press Enter.
5. Click OK.

When you are done with the snapshot, you should unmount the snapshot. Of course, when you need to free up disk space or to do regular maintenance, you will want to delete the snapshot as well.

UNMOUNT AN AD DS SNAPSHOT

GET READY. To unmount an Active Directory Domain Service snapshot, perform the following steps:

1. Switch to the command prompt in which the snapshot is mounted.
2. Press Ctrl+C to stop DSAMain.exe.
3. Execute the ntdsutil command
4. Execute the activate instance ntds command.
5. Execute the snapshot command.
6. Type unmount <GUID>, where GUID is the GUID of the snapshot, and then press Enter.
7. Execute the quit command twice.
8. Close the command prompt window.

DELETE AN AD DS SNAPSHOT

GET READY. To delete an Active Directory Domain Service snapshot, perform the following steps:

1. Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.
2. Execute the ntdsutil command
3. Execute the snapshot command.
4. Execute the list all command.
5. Execute the delete <number of snapshot> command. For example, if the second entry is the one that you want to delete, you use the delete 2 command.
6. Type unmount <GUID>, where GUID is the GUID of the snapshot, and then press Enter.
7. Execute the quit command twice
8. Close the command prompt window.

Performing Object- and Container-Level Recovery

Starting with Windows Server 2008 R2, Windows offers the Active Directory Recycle Bin. Similar to the Recycle Bin found in Windows that is used to undelete deleted files, the ***Active Directory Recycle Bin*** can be used to undelete deleted Active Directory containers and objects.

When an object or OU in AD DS is deleted, it is moved to the Deleted Objects container. As long as the object has not been scavenged by the garbage collection process after reaching the end of the object tombstone lifetime, you can restore the deleted object. However, when the item is deleted, certain attributes are removed such as group membership. By default, the garbage collection occurs every 12 hours.

The LPD.exe tool allows users to perform operations against any LDAP-compatible directory, including Active Directory. LDP is used to view objects stored in Active Directory along with their metadata, such as security descriptors and replication metadata.

RESTORE A DELETED OBJECT WITHOUT USING THE RECYCLE BIN

GET READY. To restore a deleted object without using the Recycle Bin, perform the following steps:

1. Click the Start button, type ldp, and press Enter. LDP opens.
2. Click Connection > Connect. When the *Connect* dialog box opens, type the name of the domain controller in the *Server* text box, and click OK.
3. Click Connection > Bind. When the *Bind* dialog box opens, click OK.
4. Click the Options > Controls. When the *Controls* dialog box opens, click Return Deleted Objects in the *Load Predefined* list, and then click OK.
5. Click View > Tree, and then click OK.
6. Expand the domain, and then double-click CN=Deleted Objects,DC=contoso,DC=com to display the deleted objects (see Figure 17-3).

Figure 17-3

Showing deleted objects

7. Right-click the deleted object, and then click Modify. The *Modify* dialog box opens.
8. In the *Attribute* box, type isDeleted. In the *Operation* section, click the Delete option, then click Enter.
9. In the *Attribute* box, type distinguishedName.
10. In the *Values* box, type the distinguished name of the object in the parent container or the organizational unit into which the object should be restored. For example, type the distinguished name of the object before it was deleted.
11. In the *Operation* section, click Replace. Click Enter.
12. Select the Extended checkbox.
13. Click Run.
14. Click Close to close the *Modify* dialog box.
15. Close LDP.

After the account has been undeleted, you need to reset the password (for a user object), and enable the object (if disabled). You then need to add the account to the appropriate groups.

Configuring and Restoring Objects by Using the Active Directory Recycle Bin

With Windows Server 2008 R2, Windows introduced an Active Directory Recycle Bin that can be used to undelete an object. Different from the manual restore, all of the object's attributes are maintained, including group membership. Starting with Windows Server 2012, you can use the Active Directory Administrative Center to recover objects from the Recycle Bin. By default, the deleted object stays in the Recycle Bin for 180 days.

Before you can use the Active Directory Recycle Bin, you need to have the forest functional level set to Windows Server 2008 R2 or higher. You also need to manually enable the Active Directory Recycle Bin. In Windows Server 2012 R2, you can enable the Recycle Bin by performing one of the following actions:

- From the Active Directory module for Windows PowerShell prompt, use the `Enable-ADOptionalFeature` cmdlet.
- From Active Directory Administrative Center, select the domain, and then click *Enable Active Directory Recycle Bin* in the Tasks pane.

Only items deleted after the Active Directory Recycle Bin is turned on can be restored from the Active Directory Recycle Bin.

ENABLE THE ACTIVE DIRECTORY RECYCLE BIN

GET READY. To enable the Active Directory Recycle Bin, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Administrative Center. The *Active Directory Administrative Center* opens (see Figure 17-4).

Figure 17-4

Opening Active Directory Administrative Center

3. Click the domain. The domain options appear (see Figure 17-5).
4. Click Enable Recycle Bin. When it says that once the Recycle Bin has been enabled, it cannot be disabled and asks if you want to continue, click OK.
5. When it says to refresh the AD Administrative Center now, click OK.

Figure 17-5

Selecting the domain options

6. Press the F5 key on the keyboard to refresh the *Active Directory Administrative Center*.
7. Close *Active Directory Administrative Center*.

After the Active Directory Recycle Bin has been enabled, you can access the Deleted Objects container using the Active Directory Administrative Center. You can choose to restore the objects to their original location or to an alternate location within AD DS.

RESTORE AN OBJECT USING THE ACTIVE DIRECTORY RECYCLE BIN

GET READY. To restore an object using the Active Directory Recycle Bin, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Administrative Center. The *Active Directory Administrative Center* opens.
3. Click the small arrow next to the domain and select Deleted Objects.
4. Click the deleted object that you want to restore and click the Restore under *Tasks*.
5. Close *Active Directory Administrative Center*.

Managing Active Directory Offline

THE BOTTOM LINE

In previous versions of Windows, to perform certain tasks such as defrag the Active Directory database, you need to reboot the domain controller in DSRM, so that the Active Directory Domain Services will not be running. Starting with Windows Server 2012, Windows servers include ***Restartable Active Directory Domain Services***, which allows you to stop and start AD DS without restarting the domain controller and stopping other services that might be on the server. As a result, you can perform these tasks quicker than you could before.

Restartable AD DS is available by default on all domain controllers that run Windows Server 2012 R2. There are no functional-level requirements or any other prerequisites for using this feature.

TAKE NOTE*

To perform state restore of a domain controller while AD DS is stopped, you must reboot the domain controller into DSRM. You can perform an authoritative restore of Active Directory objects while AD DS is stopped by using Ntdsutil.exe.

To start or stop the AD DS, you open the Services console to control the service. There are three domain controller states:

- **AD DS Started:** In this state, AD DS is started.
- **AD DS Stopped:** This is a unique mode that combines the characteristics of both a domain controller in DSRM and a domain-joined member server.
- **DSRM:** This mode (or state) allows standard AD DS administrative tasks.

Optimizing an Active Directory Database

THE BOTTOM LINE

As mentioned previously, certain tasks that you must take the domain services offline first. One common task is to perform an offline defragmentation of the Active Directory database.

Similar to running the Optimize and defragment drive tool in Windows to defragment a hard drive, you can use `ntdsutil` to defragment the Active Directory database to free up disk space. To perform an offline defragmentation procedure, you create a new, compacted version of the database file in a different location. When the new defragmented database is created, the procedure copies the compacted ntds.dit file back to the original location.

You can also use the `ntdsutil` command to look for errors in Active Directory. The `integrity` command is used to detect low level (binary level) database corruption, which reads every byte of the data file and makes sure that the correct headers exist in the database itself and that all of the tables are functioning and are consistent. You can also use the semantic checker to check the integrity of the contents of the Active Directory database.

DEFRAGMENT AND CHECK THE INTEGRITY OF THE ACTIVE DIRECTORY DATABASE

GET READY. To defragment and check the integrity of the Active Directory Database, perform the following steps:

1. Open Server Manager.
2. Click Tools > Services. The *Services console* opens.
3. Right-click the Active Directory Domain Services service and click Stop. When it asks if you want to stop other services, click Yes.
4. Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.
5. Execute the ntdsutil command.
6. At the ntdsutil prompt, execute the activate instance NTDS command.
7. Execute the files command.
8. At the file maintenance prompt, execute the compact to C:\ command. The database is compacted.
9. To check the integrity of the offline database, execute the integrity command.
10. At the file maintenance prompt, execute the quit command.
11. To perform a semantic database consistency check, execute the semantic database analysis command.
12. At the semantic checker prompt, execute the go command.
13. Execute the quit command twice.
14. Close the command prompt.
15. Go back to the *Service console*. Right-click the Active Directory Domain Services service and click Start.
16. Close the *Services console*.

Cleaning Up Metadata

THE BOTTOM LINE

To retire a domain controller, the proper method to demote a domain controller is to remove the Active Directory Domain Services. However, if the demotion fails or the server itself fails where you cannot recover the system, you need to clean up the metadata, which means you must manually remove the domain controller from Active Directory. The ***metadata*** is the data that identifies the domain controllers.

There are several ways to clean up the server metadata. Today, the most common method to remove the metadata is to use Active Directory Users and Computers and ntdsutil. Other methods include using the Active Directory Sites and Services and ADSIEdit. During the next procedure, the server metadata is removed using Active Directory Users and Computers.

CLEAN UP SERVER METADATA USING ACTIVE DIRECTORY USERS AND COMPUTERS

GET READY. To clean up server metadata using the Active Directory Users and Computers console, perform the following steps:

1. Open Server Manager.

2. Click Tools > Active Directory Users and Computers. The *Active Directory Users and Computers console* opens.
3. Expand the domain, and click Domain Controllers.
4. Right-click the computer object of the domain controller that you want to clean up and click Delete.
5. When asked if you are sure, click Yes.
6. In the *Deleting Domain Controller* dialog box, select This Domain Controller is permanently offline and can no longer be demoted using the *Active Directory Domain Services Installation Wizard (DCPROMO)*, and then click Delete.
7. If the domain controller is a global catalog server, in the *Delete Domain Controller* dialog box, click Yes to continue with the deletion.
8. If the domain controller currently holds one or more operations master roles, click OK to move the role or roles to the domain controller that is shown.
9. Close the *Active Directory Users and Computers* console.

The following procedure shows how to use ntdsutil.exe to remove the server metadata from Active Directory. Compared to using the ntdsutil.exe on Windows Server 2003 or earlier, the process of removing server metadata is simplified.

CLEAN UP SERVER METADATA USING NTDSUTIL

GET READY. To clean up server metadata using `ntdsutil`, perform the following steps:

1. Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.
2. Execute the ntdsutil command.
3. At the ntdsutil, execute the metadata cleanup command.
4. At the metadata cleanup prompt, execute the remove selected server <servername> command. When a warning appears, click Yes to remove the server object and metadata.
5. Execute the quit command twice.
6. Close the command prompt.

Business Case Scenarios

Scenario 17-1: Recovering Objects from Active Directory

You are an administrator at the Contoso Corporation. Just before you got hired, the company had an incident where a lot of information was removed from Active Directory and it could not be recovered. What would you do to make sure that you have the best chance to recover deleted accounts with minimal disruption.

Scenario 17-2: Recreating a Domain Controller

You are an administrator at the Contoso Corporation. You have three domain controllers for your organization. Unfortunately, one of the domain controllers suffered a catastrophic failure and you do not have a backup of the domain controller. What should you do to replace the domain controller?

Configuring Account Policies

LESSON 18

Working with Account Policies

THE BOTTOM LINE

Group Policies are one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policies provide centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment. For example, you can use Group Policy to specify how often a user has to change his or her password, what the background image on a person's computer is, or whether spell checking is required before a user can send an e-mail.

Thousands of settings can be used to restrict certain actions, make a system more secure, or standardize a working environment. A setting can control a computer registry, NTFS security, audit and security policy, software installation, folder redirection, offline folders, or logon and logoff scripts. Group Policies is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy (see Figure 18-1) provides the centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment. As each server version is released, Microsoft usually adds more parameters.

Group Policy Objects (GPOs) are collections of user and computer settings including the following:

- **System settings:** Application settings, desktop appearance, and behavior of system services.
- **Security settings:** Local computer, domain, and network security settings.
- **Software installation settings:** Management of software installation, updates, and removal.
- **Scripts settings:** Scripts for when a computer starts or shuts down and for when a user logs on and off.
- **Folder redirection settings:** Storage for users' folders on the network.

Account policies Computer Configuration\Windows Settings\Security Settings\Account Policies (as shown in Figure 18-1) are domain level policies that define the security-related attributes assigned to user objects. Account policies contain three subsets:

- **Password Policy:** Determine settings for passwords, such as enforcement and lifetimes.
- **Account Lockout Policy:** Determine the circumstances and length of time that an account is locked out of the system.
- **Kerberos Policy:** Determine Kerberos-related settings, such as ticket lifetimes and enforcement. Kerberos Policy settings do not exist in local computer policies.

Figure 18-1

Accessing the account policies

Unlike the other policies, there is only one account policy per domain, which is usually defined in the Default Domain Policy. If you do not want to use the Default Domain Policy, you can link a new policy to the root of the domain and give it precedence over the Default Domain Policy. The domain level account policies are enforced by the domain controllers.

Traditionally, if you needed to have different password policies for different people, you would have to create different domains for those people. However, starting with Windows Server 2008, fine-grained password policies were created that override the domain-wide policy.

Configuring Domain User Password Policy

As the name indicates, a ***password policy*** defines the password parameters that a user uses.

Much of today's data protection is based on the password. Think about your life. You use passwords to secure your voice mail, your ATM access, your e-mail account, your Facebook account, and a host of other things. To keep these accounts secure, you need to select strong passwords and you need to enforce users to choose strong passwords.

CONFIGURING PASSWORD POLICY SETTINGS

Password policies is the first folder under Account Policies (see Figure 18-2). The settings include:

- **Enforce password history:** Defines the number of unique, new passwords that must be associated with a user account before an old password can be reused. The default setting is 24 previous passwords.
- **Maximum password age:** Defines the number of days that a password can be used before the user must change it. The default setting is 42 days.
- **Minimum password age:** Defines the number of days that a password must be used before the user can change it. The default value is one day, which is appropriate if you also enforce password history.
- **Minimum password length:** Defines the minimum number of characters that a user's password must contain. The default value is seven.
- **Complexity requirements:** Defines a default password filter that is enabled by default. A complex password defines the following characteristics:

- Does not contain your name or your username.
- Contains at least six characters.
- Contains characters from three of the following four groups: uppercase letters [A…Z], lowercase letters [a…z], numerals [0…9], and special, non-alphanumeric characters (such as !@#)(*&^%).

Figure 18-2

Viewing the Password Policy settings

The length of a password is a key component of its strength. Password length is the number of characters used in a password. A password with two characters is considered highly insecure, because there is a limited set of unique passwords that can be made using two characters. Therefore, a two-character password is considered easy to guess.

On the other side of the spectrum is the 14-character password. Although a relative to a secure 2-character password, a 14-character password is difficult for most users to remember. When passwords become long, users often require writing down their passwords, which defeats any security benefits you might have from requiring a 14-character password in the first place.

As these scenarios illustrate, the trick to setting a minimum password length is balancing usability with security. Microsoft permits you to set a minimum password length ranging from 1 to 14 (a setting of 0 means no password is required, which is never appropriate in a production environment). The generally accepted minimum password length is eight characters.

The password history is the setting that determines the number of unique passwords that must be used before a password can be re-used. This setting prevents users from recycling the same passwords through a system. The longer the period of time a password is used, the greater the chances it can be compromised.

Microsoft allows you to set the password history value between 0 and 24. Ten is a fairly common setting in standard environments, although Windows Server 2012 R2 defaults to 24 on domain controllers.

The minimum password age setting controls how many days users must wait before they can reset their password. This setting can be a value from 1 to 998 days. If set to 0, passwords can be changed immediately. Although this seems to be a fairly innocent setting, too low a value can allow users to defeat your password history settings. For example, if you set this value to 0 and your password history is set to 10, all users have to do is reset their password 10 times in a

row, and then they can go back to their original password. This setting must be set to a lower value than the maximum password age, unless the maximum password age is set to 0, which means passwords never expire. Ten days or greater is usually a good setting, although this can vary widely depending on administrator preferences.

The maximum password age setting controls the maximum period of time that can elapse before you are forced to reset your password. This setting can range from 1 to 999 days, or it can be set to 0 if you never want passwords to expire. A general rule for this setting is 90 days for user accounts; although for administrative accounts, it's generally a good idea to reset passwords more frequently. In high security areas, 30 days is not an uncommon setting. We discussed the different settings you can use to ensure the best password security for your environment. Now, let's look at how to review those settings on a Windows 7 workstation.

CONFIGURE PASSWORD POLICIES

GET READY. To configure password policies, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Find and right-click Default Domain Policy and click Edit. The *Group Policy Management Editor* opens.
4. In the left window pane, expand the Computer Configuration node, expand the Policies node, and expand the Windows Settings folder. Then, expand the Security Settings node. In the *Security Settings* node, expand Account Policies and select Password Policy.
5. To modify a setting, double-click the setting in the right window pane to open the *Properties* dialog box for the setting. Then, make the desired value changes.
6. Click OK to close the setting's *Properties* dialog box.
7. Close the *Group Policy Management Editor* window for this policy.

Configuring Account Lockout Settings

To help prevent hacking, Windows uses ***account lockout settings*** that specify when an account is locked when there are too many incorrect logon attempts.

If a hacker has enough time, he or she can crack any password. To help prevent the cracking of a password, you can limit how many times a hacker can guess a password before the account is locked. Account lockout refers to the number of incorrect logon attempts permitted before a system locks an account.

Each bad logon attempt is tracked and added to the bad logon counter. When the counter exceeds the account lockout threshold, the account is locked and no further logon attempts are permitted.

Group policies include the following account lockout settings:

- **Account lockout duration:** Determines the length of time a lockout will remain in place before another logon attempt can be made. This can be set from 0 to 99,999 minutes. If set to 0, an administrator will need to manually unlock the account.

- **Account lockout threshold:** Determines the number of failed logons permitted before account lockout occurs. This can be set from 0 (no account lockouts) to 999 attempts before lockout.
- **Reset account lockout counter after:** Determines the period of time, in minutes, that must elapse before the account lockout counter is reset to 0 bad logon attempts.

CONFIGURE ACCOUNT LOCKOUT SETTINGS

GET READY. To configure account lockout settings, follow these steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Find and right-click Default Domain Policy and click Edit. The *Group Policy Management Editor* opens.
4. In the left window pane, expand the Computer Configuration node, expand the Policies node, and expand the Windows Settings folder. Then, expand the Security Settings node. In the *Security Settings* node, expand Account Policies and select Account Lockout Policy.
5. To modify a setting, double-click the setting in the right window pane to open the *Properties* dialog box for the setting. Then, make the desired value changes.
6. Click OK to close the setting's *Properties* dialog box.
7. Close the *Group Policy Management Editor* window for this policy.

Configuring and Applying Password Settings Objects

If you need to use different password policies for different sets of users, you can use fine-grained password policies, which are applied to user objects or global security groups.

Fine-grained password policies allow you to specify multiple password policies within a single domain so that you can apply different restrictions for password and account lockout policies to different sets of users in a domain. To use a fine-grained password policy, your domain functional level must be at least Windows Server 2008. To enable fine-grained password policies, you first create a ***Password Settings Object (PSO)***. You then configure the same settings that you configure for the password and account lockout policies. You can create and apply PSOs in the Windows Server 2012 R2 environment by using the Active Directory Administrative Center (ADAC) or Windows PowerShell.

CREATE AND CONFIGURE PASSWORD SETTINGS CONTAINER

GET READY. To create and configure the Password Settings Container, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Administrative Center. The *ADAC* opens.
3. In the ADAC navigation pane, click the arrow next to the domain and select the System folder. Then scroll down and double-click Password Settings Container. The *Password Settings Container* opens.
4. In the *Tasks* pane, click New, and then click Password Settings. The *Create Password Settings* window opens.
5. In the *Name* text box, type a name of the Password Settings Container.
6. In the *Precedence* text box, type a Precedence number. Passwords with a lower precedence number overwrite Password Settings Containers with a higher precedence number.

7. Fill in or edit the appropriate fields for the settings that you want to use.
8. Under *Directly Applies To*, click Add. When the *Select Users or Groups* dialog box, opens specify the name of the user or group that you want the Password Settings Container to effect and then click OK.
9. Click OK to submit the creation of the PSO.
10. Close the *ADAC*.

Configuring Local User Password Policy

If you have a standalone computer that is not part of a domain, you can still configure password policies and/or account lockout policies using the local policies.

The easiest method to access the account policies is to execute the secpol.msc from a command prompt, which opens the Local Security Policy (see Figure 18-2). The password-policy and account-policy settings can be located within the Local Security Policy console by expanding Security Settings, and then expanding Account Policies.

Figure 18-2

Opening the Local Security Policy

Delegating Password Settings Management

By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users.

By default, the Domain Admins group has Read and Write capabilities to the Default Domain Policy. If you want to give access to others to manage the Default Domain Policy, you need to add the user to the access list and assign the permissions as described in the next procedure.

MANAGE GPO PERMISSIONS

GET READY. To manage GPO permissions, perform the following steps:

1. Open Server Manager.
2. Open Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Click Default Domain Policy. If you get a warning saying that you selected a link, click OK.

4. Click the Delegation tab. The groups and users that have access to manage the GPO are displayed (see Figure 18-3).

Figure 18-3

Displaying the Delegation tab

5. Click Add. When the *Select User, Computer, or Group* dialog box opens, type the name of the user or group in the *Enter the object name to select* text box and click OK.
6. When the *Add Group or Users* dialog box appears, select the appropriate permissions in the *Permissions* list and click OK.
7. Click OK to submit the creation of the PSO.
8. Close the *Group Policy Management console*.

To assign a PSO to a user, it is best to assign the PSO to a global security group and then add the user to the global security group. If you need a support person to assign the PSO to a user, he or she needs to have the ability to add the user account to the group that the PSO is assigned to. To assign management permissions to the PSO, follow the next procedure.

MANAGE PASSWORD SETTINGS OBJECT PERMISSIONS

GET READY. To manage permissions to a PSO:

1. Open Server Manager.
2. Open Tools > Active Directory Administrative Center. The *ADAC* opens.
3. Navigate to the System\Password Settings Container.
4. Right-click the Password Settings Container and click Properties. The *Password Settings Object Settings* window opens.
5. Under the *Extensions* section, click Add. When the *Select Users, Computers, Service Accounts, or Groups* dialog box opens, type the name of the user account or group and click OK.
6. Click to assign the appropriate permissions under the Allow or Deny column.

7. Click OK.
8. Close the *ADAC*.

Configuring Kerberos Policy Settings

Kerberos is the default authentication mechanism in an Active Directory Domain services (AD DS) environment and plays a critical role in authorization and auditing. Because Kerberos is used as part of the Active Directory domain, Kerberos settings can be configured only at the domain level with a GPO.

The Kerberos version 5 authentication protocol provides the default mechanism for authentication services, which will also be used with the authorization of resources. You can reduce the lifetime of Kerberos tickets, which reduces the risk of a legitimate user's credentials being stolen or replayed. However, by decreasing the ticket lifetime, you will increase the authorization overhead.

The Kerberos Policy settings are located at *Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy*. From there, you can configure the following:

- **Enforce user logon restrictions**: Determines whether the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. The default is Enabled.
- **Maximum lifetime for service ticket**: Determines the maximum number of minutes that a granted session ticket can be used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the Maximum lifetime for user tickets. The default is 600 minutes.
- **Maximum lifetime for user ticket**: Determines the maximum amount of time (in hours) that a user's ticket-granting ticket can be used. The default is 10 hours.
- **Maximum lifetime for user ticket renewal**: Determines the period of time (in days) during which a user's ticket-granting ticket can be renewed. The default is 7 days.
- **Maximum tolerance for computer clock synchronization**: Determines the maximum time difference (in minutes) that the Kerberos V5 protocol tolerates between the time on the client clock and the time on the domain controller that provides Kerberos authentication. The default is 5 minutes.

Business Case Scenarios

Scenario 18-1: Making Passwords Compliant

You are an administrator at the Contoso Corporation. You have the responsibility to make sure that the passwords for all users are at least eight characters and that are changed every 90 days. You must ensure that each password is a strong password. You also have users who are on the road. Because these users use laptops that contain confidential information, you must ensure that each password is 10 characters and that get changed every 30 days. What should you do?

Scenario 18-2: Preventing Intrusion

Recently, you have had a couple accounts where the password has been compromised. You need to take extra steps in preventing the intrusion. What are the steps you can take?

Configuring Group Policy Processing

LESSON 19

Understanding Group Policy Processing

THE BOTTOM LINE

Group policies are defined using ***group policy objects (GPOs)***, which are the collection of configuration instructions that the computer processes. To assign a group policy, it is linked to an Active Directory container (site, domain, or organizational unit). However, you can take steps to control which group policy affects a computer or user.

You can use several mechanisms to scope a GPO, including:

- A GPO link to a site, domain, or organizational unit (OU)
- The GPO link enabled or disabled
- Enforce option of the GPO
- The Block Inheritance option of an OU
- Security group filtering
- WMI filtering
- Loopback policy processing
- Preferences targeting (discussed in Lesson 22, "Configuring Group Policy Preferences")

Configuring Processing Order and Precedence

To understand how group policies are applied, you must first look at the order in which group policies are applied.

When configuring group policies, the settings are applied to the computer or the user. Computer configuration settings are processed when a computer starts, and user configuration settings are processed when a user logs on. Group policies are processed in the following way:

1. When a computer first starts up, it establishes a secure link between the computer and a domain controller.
2. The computer obtains a list of GPOs that are applied to the computer.
3. Computer configuration settings are applied synchronously (one by one) during computer startup before the Logon dialog box is presented to the user. If any startup scripts are configured through GPOs, the scripts are processed synchronously and have a default timeout of 600 seconds (10 minutes) to complete. Because the user has not logged on yet, the process is hidden.
4. When the computer configuration settings have been applied and the startup scripts have been applied, users have the Ctrl+Alt+Del option to log on.

5. A user is authenticated and the user profile is loaded.
6. The computer obtains a list of GPOs that are applied to the user. Again, GPO processing is hidden from the user.
7. After the user policies run, any logon scripts defined by GPOs run, which are executed asynchronously (multiple scripts to be processed at the same time).
8. The login script defined for the user in Active Directory user properties is executed.
9. The user's desktop is displayed.

UNDERSTANDING GROUP POLICY INHERITANCE

A computer and user can be affected by multiple GPOs. GPOs are processed in the following order:

1. Local group policy
2. Site
3. Domain
4. OU

Although the domain and OU are used to deploy GPOs based on the location of the user and computers within Active Directory hierarchy, the Site is used to define GPOs based on physical location.

By default, a Group Policy uses ***inheritance*** in which settings are inherited from the container above. In other words, group policy settings flow down into the lower containers and objects. Generally speaking, the settings are cumulative, unless there is a conflict with a setting defined in a previous GPO. By default, if there is a conflict between settings, the domain controller that is processed later overwrites the setting that was established previously.

If a site, domain, or OU has multiple GPOs, the group policies are processed in order as stated by its precedence. A GPO with higher precedence (lower number) prevails over a GPO with lower precedence (higher number).

When Active Directory is installed, two domain GPOs are created by default:

- ***Default Domain Policy:*** Linked to the domain. It affects all users and computers in the domain, including domain controllers. It specifies the password, account lockout, and Kerberos policies. These policies can be configured only at the domain level. To configure other settings at the domain level, you should create additional GPOs linked to the domain.
- ***Default Domain Controller Policy:*** Linked to the Domain Controllers organization unit, which then affects the domain controllers. It contains the default user rights assignments. You should also use it for auditing policies. It has a security filter to include only Authenticated Users.

Let's say that you have the contoso.com domain that has the Sales OU, which contains the West OU (see Figure 19-1). You create GPO1 and GPO2 GPOs and link them to the domain.

Figure 19-1

Displaying GPOs for a domain

You create GPOSales1 and GPOSales2 and link them to the Sales OU. You create WESTGPO1 and WESTGPO2 and link them to the WEST OU. The policies are processed in the following order:

1. Local group policy
2. GPO2
3. GPO1
4. Default Domain Policy
5. GPOSales2
6. GPOSales1
7. WESTGPO2
8. WESTGPO1

If all the GPOs configure the same setting, the setting defined with the GPO with the highest precedence (lowest number) will be used. Of course, if you configure settings defined in the password, account lockout, or Kerberos policy, only the Default Domain Policy would be used because these can be set only at the domain level. If you need to change the precedence, use the following procedure.

CHANGE THE PRECEDENCE OF A GPO

GET READY. To change the precedence of a GPO for a container, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Navigate to and click the container (site, domain, or OU) that has GPOs that you want to modify.
4. Click the Linked Group Policy Objects tab.
5. Click the GPO that you want to modify. Then, use the arrow icons (Up, Down, Move To Top, and Move To Bottom) to move the GPO up or down on the list (see Figure 19-2).

Figure 19-2

Changing the precedence

6. Close the *Group Policy Management console*.

Using Filtering with Group Policies

As mentioned previously, group policies flow down from the upper containers to the lower objects. However, you might want to define a group policy and not want them to be overwritten by other GPOs, or you might not want the GPO to flow down to lower containers.

The exceptions to the processing of group policies can be modified with the following options:

- Block policy inheritance
- Enforce option

CONFIGURING BLOCKING OF INHERITANCE

By default, group policies flow down to the lower containers and objects. You can prevent the inheritance of policy settings by blocking all Group Policy settings from the GPOs linked to parent containers in the Group Policy hierarchy. GPOs linked directly to the container and GPOs linked to lower containers are unaffected.

BLOCK THE INHERITANCE OF GPOs

GET READY. To block the inheritance of GPOs, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Navigate to and click the container (site, domain, or OU) that you want to stop inheritance from above.
4. Right-click the container and select Block Inheritance. An exclamation point inside a blue circle appears for the container, and the checkmark indicates inheritance is blocked in the context menu.
5. Close the *Group Policy Management console*.

You should use block inheritance sparingly. Instead, you can use security group filtering to control what group policies.

CONFIGURING ENFORCED POLICIES

Let's say that you want to apply a GPO, and you do not want that GPO to be overridden by a GPO that is executed later. By enforcing a GPO link, the GPO takes the highest precedence, which will prevail over any conflicting policy settings in other GPOs. In addition, an enforced link applies to child containers even when those containers are set to Block Inheritance.

ENFORCE A GPO

GET READY. To enforce a GPO, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Navigate to and click the GPO in the desired container.
4. Right-click the GPO and click Enforced.
5. When you right-click a lower container, you will see that the enforced GPO has a high precedence (low number).
6. Close the *Group Policy Management console*.

Configuring Security Filtering and WMI Filtering

By default, Group Policy settings are applied to all child objects within the container to which they are linked to. Although you need to organize your OUs to help you manage your resources, you sometimes need to have granular control that allows you to specify which clients (computers and users) that the group policy applies to.

To give you granular control of whom or what receives a group policy, you can use the following filters:

- **Security group filtering:** Uses a security access list (ACL) to determine who can modify or read a policy and who or what a GPO is applied to.
- **WMI filtering:** Uses the WMI Query Language (WQL) to control who or what a GPO is applied to.

USING SECURITY FILTERING

Security group filtering specifies which users, computers, or groups based on ACL receive a GPO. For example, let's say you have a GPO that locks down a computer so that the user cannot access certain Control Panel applets on his or her computer. However as an administrator, or technical support person, a user might need to have access to those applets to perform his or her job, reconfigure a system, or troubleshoot a problem. Therefore, you can use security group filtering to apply to some and not others.

For a user to receive GPO settings, a user must have Allow Read and Allow Apply Group Policy permissions to the GPO. By default, the Authenticated Users give the Apply Group Policy permissions. To all new GPOs, this means that all users and computers are affected by the container that the GPO is linked to and the user and computer is a member of.

The ways to filtering GPO scopes are to perform one of the following:

- Remove the Allow Apply group policy permissions to a group such as Authenticated Users.
- Remove the Authenticated Users group access control entry (ACE), add other groups or user, and assign the Allow Apply group policy permissions.
- Add ACE for another group, user, or computer assign the Deny Apply group policy permissions. Similar to NTFS permissions, the Deny settings always supersede any Allow settings that are granted to a user through member to another group or the user directly.

Although the Domain Admins group has Full Control permissions to a GPO, the Domain Admins are not directly assigned the Apply group policy permission. Instead, the Domain Admins receive the Allow Apply group policy that is assigned to the Authenticated Users group. The Allow Full Control permission for a GPO allows the group or user to manage the GPO.

CONFIGURE A SECURITY GROUP FILTERING

GET READY. To configure a security group filtering, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Navigate and click the GPO you want to modify.
4. Click the Delegation tab and click Advanced. The *GPO Security Settings* dialog box opens (see Figure 19-3).

Figure 19-3

Showing the ACL for a GPO

5. If the Administrators group is not listed in the *Group or User Names* window, click Add and type Administrators in the *Enter Object Names to Select* dialog box. Click OK.
6. Make sure that Administrators is selected. Then click the Deny checkbox for the Apply Group Policy permission.
7. Click OK to close the *GPO Security Settings* dialog box. When it states that Deny entries take precedence and asks whether you want to continue, click Yes.
8. Close the *Group Policy Management console*.

Unfortunately, when you exclude a group, the exclusion is not shown in the Security Filtering section of the Scope tab. Instead, you need to use the Advanced options to see the Deny permissions. Because it cannot be easily seen, it is recommended to use the Deny permissions sparingly.

USING WMI FILTERING

Windows Management Instrumentation (WMI) is a component that extends the Windows Driver Model to provide an interface to the operating system to provide information and notification on hardware, software, operating systems, and services. ***WMI filtering*** configures a GPO to be applied to certain users or computers based on specific hardware, software, operating systems, and services. For example:

- Computers running Windows XP Professional only (`Select * from Win32_OperatingSystem where Caption = " Microsoft Windows XP Professional"`)
- Computers running Windows XP Professional with SP3 only (`Select * from Win32_OperatingSystem WHERE Caption="Microsoft Windows XP Professional" AND CSDVersion="Service Pack 3"`)
- Computers that are 32-bit machines only (`Select * from Win32_Processor where AddressWidth ='32'`)
- Computers that have 500 MB free item installed (`SELECT * FROM Win32_LogicalDisk WHERE (Name = " C:") AND DriveType = 3 AND FreeSpace > 500000000 AND FileSystem = " NTFS"`)
- A certain type of computer, such as a Toshiba Tecra 800 or 810 (`Select * from Win32_ComputerSystem where manufacturer = "Toshiba" and Model = "Tecra 800" OR Model = "Tecra 810"`)
- A certain software package (MSIPackage1 or MSIPackage2) installed (`Select * from Win32_Product where name = "MSIPackage1" OR name = "MSIPackage2"`)
- A mobile computer based on the presence of a battery (`Select * from Win32_Battery WHERE (BatteryStatus <> 0)`
- A computer that has a ping low round trip delay, such as less than 3 ms (`Select * from PingProtocolStatus where address = 'Server1' AND hops < 3`)

The filter is evaluated at the time the policy is processed.

To use WMI filters:

- You need to have one domain controller running Windows Server 2003 or higher.
- WMI filters will be applied only to computers running Windows XP Professional or newer, or Windows Server 2003 or newer.
- All filter criteria must have an outcome of true for the GPO to be applied. Any criteria with an outcome of false after evaluation will negate the application of the GPO.
- Only one WMI filter can be configured per GPO. After a WMI filter has been created, it can be linked to multiple GPOs.

USE WMI WITH GPOs

GET READY. To use WMI with a GPO, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management console* opens.
3. Navigate to and click the WMI filters.

4. Right-click the WMI Filters node and click New. The *New WMI Filter* dialog box opens.
5. In the *Name and Description* fields, enter a name and description for the new WMI filter.
6. In the *Queries* section, click Add. The *WMI Query* dialog box opens.
7. Enter the desired query information and click OK to close the *WMI Query* dialog box.
8. Click Save to create the WMI filter.
9. Navigate to the *Group Policy Objects* node and click the GPO to be assigned the WMI filter.
10. On the Scope tab, select the name of the WMI filter you just created from the WMI Filtering drop-down box. Click Yes to confirm your changes.
11. Close the *Group Policy Management console*.

Configuring Loopback Processing

As you recall, GPO computer configuration settings are applied when a computer starts up, and GPO user configuration settings are applied when a user logs on. Group Policy ***loopback processing*** is used to assign user policies to computer objects. Therefore, no matter who logs on to a computer, the user policies are applied to the computer.

As the name implies, loopback processing allows the Group Policy processing order to circle back and reapply the computer policies after all user policies and logon scripts run. It is intended to keep the configuration of the computer the same regardless of who logs on.

The loopback policy is enabled using the Group Policy Management Editor, specifically the Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure user Group Policy Loopback processing mode (see Figure 19-4). After you enable the setting, you have two modes to choose from that specify the loopback processing mode:

Figure 19-4

Configuring the Group Policy loopback processing mode

- ***Replace mode:*** The user settings defined in the computer's GPO replace the user settings normally applied to the user. The Replace mode is useful in a situation such as a kiosk, classroom, or public library, where users should receive a standard configuration.
- ***Merge mode:*** The user settings defined in the computer's GPOs and user settings normally applied to the user are combined. If the settings conflict, the user settings in the computer's GPO take precedence over the user's normal settings. This mode is useful to apply additional settings to users' typical configurations, such as mapping additional printers, replacing the wallpaper on a computer, or disabling certain applications or devices in a conference room or reception area.

For computers that are shared by more than one user (such as a kiosk, classroom, or public library), you can use the Replace option to reduce the need to undo actions that are applied by the settings for the user logging on.

Configuring Client-Side Extension Behavior

Group policies are client driven, which means that the Group Policy client pulls the GPOs from the domain, which triggers processes called ***client-side extensions (CSEs)*** that interrupt the settings in a GPO and make the changes to the local computer or the currently logged-on user.

Each major category of policy setting has CSEs. For example, the Security CSE applies security changes, while the script CSE applies startup and logon scripts. Each version of Windows has added CSEs to extend the functional reach of Group Policy.

You can configure the behavior of CSEs by using Group Policy, specifically \Computer Configuration\Policies\Administrative Template\System\Group Policy\. Most CSEs apply settings in a GPO only if that GPO has changed, which reduces the processing that needs to be done. Settings managed by the Security CSE are an important exception to the default policy processing settings. Security settings are reapplied every 16 hours even if a GPO has not changed.

If you open the Configure a particular CSE processing, you can configure the CSE to process the group policies even if the GPO has not changed by selecting the Process even if the Group Policy objects have not changed (see Figure 19-5).

Figure 19-5

Configuring scripts policy processing

To manually refresh a group policy, you use the GPUpdate command. The `gpupdate /force` command causes the system to reapply all settings in all GPO s scoped to the user or computer, because some policies settings require a logoff or a reboot. For these settings, you can use the `gpupdate /force /logoff /boot`.

Starting with Windows 8 and Windows Server 2012, you can remotely refresh Group Policy settings for all computers in an OU using the Group Policy Management console or by using the Windows PowerShell `Invoke-GPUpdate` cmdlet. To refresh Group Policy settings using the Group Policy Management console, right-click the OU and select *Group Policy Update*. While you will not able to refresh policies on the Computer OU, you can refresh policies with the `Invoke-GPUpdate` cmdlet.

LOOKING AT GPOs AND DISCONNECTED COMPUTERS

If a computer is disconnected from the network, the settings previously applied by Group Policies continue to take effect. If you are not connected to the network, logon, logoff, and shutdown scripts will not run, because they might rely on other servers to execute.

CONFIGURING AND MANAGING SLOW-LINK PROCESSING AND GROUP POLICY CACHING

Sometimes when using group policies to perform certain tasks, group policies being executed over slow network links can affect the performance of the client computer or between a site and the corporate office of a site or the computer being configured via a GPO. By default, a link is considered slow if the link is less than 500 kilobits per second (kbps). You can change the slow-link policy processing behavior of each client-side extension by using policy settings located in Computer Configuration\Policies\Administrative Templates\System\Group Policy. The Configure Group Policy slow-link detection (see Figure 19-6) is used to define what is

considered a slow-link connection. You can then use other settings with the Group Policy folder to modify the behavior of client-side extensions such as scripts or software installation so that it does or does not process policies over a slow link.

Figure 19-6

Defining the maximum speed of a slow link

Starting with Windows 8.1 and Windows Server 2012 R2, you can cache GPOs to improve performance when processing synchronous policy settings. When Group Policy gets the latest version of a policy from the domain controller, it writes that policy to a local store (c:\windows\system32\GroupPolicy\Datastore). If Group Policy is running in synchronous mode, it reads the most recently downloaded version of the GPO from the local store when the system is rebooted. As a result, the GPOs are processed faster and the boot time is shorter, particularly if the system is off the premises or you have a slow connection.

To configure and manage Group Policy caching settings, open a GPO and navigate to the *Computer Configuration\Policies\Administrative Templates\System\Group Policy* node and then enable and configure the *Configure Group Policy Caching* settings.

Forcing Group Policy Update

As you recall, GPOs are updated every 90 minutes with a random offset of 0 to 30 minutes. Of course, you can manually refresh settings for the current PC by using the `GPUpdate` command.

Starting with Windows 8 and Windows Server 2012, you can remotely refresh Group Policy settings for all computers (Windows Vista or higher; or Windows Server 2008 or higher) in an organizational unit (OU) by using the Group Policy Management Console. To force

the refresh of GPOs, open the Group Policy Management Console, right-click the OU, and then choose Group Policy Update. You can also use the `Invoke-GPUpdate` Windows PowerShell cmdlet.

As a result, each computer will run the `GPUpdate.exe /force` command for each signed-in user and once for the computer Group Policy refresh. The task will occur with a random delay of up to 10 minutes to decrease the load of network traffic.

■ Business Case Scenarios

Scenario 19-1: Placing the GPOs

You are an administrator of the Contoso Corporation. The Contoso Corporation has a domain called *contoso.com*. At the top level, you have the following OUs:

- Sales
- Marketing
- Support
- Manufacturing
- Engineering

Under each OU, you have additional OUs: North, South, East, and West. You need to implement the following GPO settings:

- Have strong passwords and a minimum of eight characters.
- The Sales team should have passwords with a minimum of 10 characters.
- All computers should have the company logo desktop picture, without exception.
- All computers in the Sales OU should have the widget.msi program installed.
- All computers in the Manufacturing and Engineering departments should have the widget2.msi program installed.
- All computers except Support should have the screen saver enabled.

What do you recommend?

Scenario 19-2: Configure a Library Computer

You are setting up a library for the Contoso University. You want to configure the library computer to have a standard desktop screen, color scheme, programs available, and proxy settings. You need to ensure that no matter who logs on, the computer will have the same settings. What should you do?

Configuring Group Policy Settings

LESSON 20

Configuring Group Policy Settings

THE BOTTOM LINE

One of the most powerful tools available with Active Directory is Group Policy that allow you to control the working environment of the computers and users of the organizations. It provides the centralized management and configuration of operating systems, applications, and user settings.

There are thousands of settings available with Group Policy. In addition, as each version of Windows is released, new settings are added to allow administrators to configure new technology that has been added to Windows, give control that was not available previously, or to give more granular control.

As discussed, Group Policy settings are broken down to computer settings (contained in the Computer Configuration node) and user settings (contained in the User Configuration node). The ***Computer Configuration*** node contains settings that are applied to the computer regardless of who logs on to the computer. By default, computer settings are applied when the computer is started. ***User Configuration*** node contains settings that are applied when the user logs on. Group policy settings are refreshed every 90 minutes with a random delay of 30 minutes (giving a random range between 90 minutes and 120 minutes). On domain controllers, Group Policy settings get refreshed every five minutes.

Starting with Windows Server 2008, the Computer Configuration and User Configuration nodes are divided into Policies and Preferences nodes (see Figure 20-1). Policies include the traditional settings that were available with earlier versions of Windows, but also have many new settings that were not available previously. Preferences allow you to configure additional Windows settings that were not available previously and they allow more control on how the settings are applied to the clients. Preferences are discussed in Lesson 22, "Configuring Group Policy Settings."

Figure 20-1

Viewing the Group Policy Object (GPO) node structure

Computer Configuration\ Policies can be divided into the following nodes:

- ***Software Settings:*** Contains only one node, Software installation, which allows you to install and maintain software within your organization.
- ***Windows Settings:*** Allows you to configure Windows settings, including Name Resolution Policy, Scripts (Startup/Shutdown), Security Settings, and Policy-Based QoS nodes.
- ***Administrative Templates:*** Contains registry-based Group Policy settings that are used to configure the computer environment, such as the Control Panel, Printers, System, and Windows components.

Software Configuration\Policies can be divided into the following nodes:

- **Software Settings:** Contains only one node, Software installation, which allows you to install and maintain software within your organization.
- **Windows Settings:** Allows you to configure Windows settings, including Scripts (Logon/Logoff), Security Settings, Folder Redirection, and Policy-Based QoS nodes.
- **Administrative Templates:** Contains registry-based Group Policy settings that are used to configure the user environment, such as the Control Panel, Printers, System, and Windows components.

Performing Software Installation Using Group Policy

Most experienced Windows users know how to install an application. You insert a CD or DVD in a drive and the application installation automatically starts, or you double-click an installation file (such as file that has an .exe or .msi filename extension). If you need to deploy software to hundreds of computers within your organization can be a chore. However, if all of the computers are connected to a network, you can use Group Policy to install, manage, and maintain software for your organization.

The ***Windows Installer*** is a software component used for the installation, maintenance, and removal of software on Windows. The installation information for software is stored in a ***Microsoft Software Installation (MSI) file*** in a database installation file that has an .msi filename extension. Besides performing installation, msi files can be used in self-healing for damaged applications and to remove an application cleanly.

Besides installing MSI files with Group Policy, you can also install MSI transform files (.mst) and MSI patch files (.msp). ***MSI Transform files*** are used to deploy customized MSI files. For example, you can install Microsoft Office, which consists of multiple applications. You can create a transform file using the Custom Installation Wizard that is included with Microsoft Office so that you can install all the applications except Microsoft Access.

MSI Patch files are used to apply service packs and hot fixes to installed software. Rather than having a complete database found with MSI files, a patch file contains a minimum of a database transform procedure that adds patching information to the target installation package database.

Windows Installer cannot install .exe files. To distribute a software package that installs with an .exe file, you must convert the .exe file to an .msi file by using a third-party utility or you will need to define a ZAP file (file with a .ZAP filename extension). ZAP files are created with a text editor, such as Notepad and they can be only published (not assigned).

ASSIGNING OR PUBLISHING A PACKAGE

To deploy software with Group Policy, you need to take the following steps:

1. Create a distribution point on the publishing server.
2. Create a GPO to use to distribute the software package.
3. Assign or publish a package to a user or computer.

To create a distribution point on a server, you first create a shared network folder where you will put the Microsoft Windows Installer package and any related files that you need for the installation to succeed. Next, you set permissions on the share to allow access to the distribution package. Then copy or install the package to the distribution point. For most packages, you just copy the installation files to the shared folders. For other packages such as Microsoft Office, you install the software to the distribution point (sometimes referred to as an administrative install), which allows for faster installations and customization. You need to contact the vendor or search the vendor's website to determine whether you should perform an administrative install.

You should next create a separate GPO to deploy the software. By using a separate GPO, you can disable the GPO or delete the GPO, and only the deployment of the software will be affected.

When you deploy the installation via Group Policy, you can deploy the software to the user or the computer. Software that is installed for a user is not available for other users unless the software is also installed for the other users. When you install to a computer, the software is available to all users.

When you install to a user or computer, you have the option to assign software or publish software:

- ***Assign software to a user:*** The software is available on the user's Start menu when the user logs on. However, the installation does not occur unless the user clicks the application icon on the Start menu or a file that is associated with the application (for example, .docx then installs Microsoft Word) is opened.
- ***Assign software to a computer:*** The application is installed the next time that the computer starts.
- ***Publish software to a user:*** A program shortcut will be available in the Control Panel's Programs applet, or you can configure the application to be installed when a file that is associated with the application is opened.

An application cannot be published to a computer.

When configuring Group Policy to deploy applications, they must be mapped to UNC paths. If you use local paths, the deployment will fail. In addition, you need to be careful where you place the deployment servers and when the deployment will actually occur. Large applications can generate a lot of network traffic, which might affect local traffic and can greatly affect slower WAN links for remote sites. Lastly, assuming that slow link is enabled (which is enabled by default), the CSE will not deliver the software over a slow link.

When the software is installed using Group Policy, which uses the Windows Installer service, the service runs with elevated privileges. Therefore, no matter who is logged onto the system, the software will still be installed as long as the user has read access to the software distribution point.

When software is installed with Group Policy, the applications are resilient. If an application becomes corrupted, the installer will detect and reinstall or repair the application.

CREATE A NEW SOFTWARE INSTALLATION PACKAGE

GET READY. To create a new Windows Installer Package within a GPO, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to Software Settings under the *Computer Configuration or User Configuration* node, and open \Policies\Software Settings.
3. Right-click the Software Installation node, select New, and then click Package. The *Open* dialog box opens.
4. Navigate to the UNC path of the software distribution point for the Windows Installer packages (.msi file), and then click Open.
5. When the *Deploy Software* dialog box opens, select one of the following:
   - Published
   - Assigned
   - Advanced

   The Advanced option is used to set properties for the Windows Installer package, including published or assigned options and modifications.
6. Click OK.
7. If you selected *Published* or *Assigned*, the Windows Installer package is added to the GPO. If you selected *Advanced*, the *Properties* dialog box for the Windows Installer package opens to permit you to set properties for the Windows Installer package, including deployment options and modifications. Make the necessary modification and click OK.
8. Close the *Group Policy Management Editor* window.

If you selected the Advanced options when you created the installation package or if you right-click the package and select *Properties*, the Properties dialog box opens (see Figure 20-2).

Figure 20-2

Opening the Properties dialog box for a software package

You can further configure the package with the following tabs:

- **General:** Allows you to change the default name of the package, and to specify a URL that points to a support web page.
- **Deployment:** Allows you to change the Deployment Type, Deployment Options, and Installation User Interface Options (Basic or Maximum). The Advanced button contains additional deployment information, such as advanced deployment options and diagnostics information.
- **Upgrades:** Allows you to configure any upgrades that are applied to a package.
- **Categories:** Configures software categories in the Add/Remove Programs option of Control Panel.
- **Modifications:** Specifies the transform (.mst) files or patch (.msp) files that are to be applied to the package and order in which they will be applied.
- **Security:** Specifies who has permissions to install the software using this package.

Using Folder Redirection

Folder redirection allows you to redirect the content of a certain folder to a network location or to another location on the user's local computer. For example, the Documents folder can be redirected to the user's home folder on a centralized server. By having the Documents folder on a centralized server, you can perform a centralized backup of all user's personal files and the personal files can be available no matter what client computer they log on to. By redirecting a folder and folder to a separate drive on the locating computer, you can separate the data files from the operating system files, so that when you have to reinstall a computer, you need to reinstall only the operating system drive without touching the data file drive.

Folder Redirection is found under \User Configuration\Policies\Windows Settings. It can be used to redirect the Desktop, Start Menu, Documents, Picture, Music, Videos, Favorites, Downloads, and other related folders (see Figure 20-3).

Figure 20-3

Viewing the Folder Redirection folders

CONFIGURE FOLDER REDIRECTION

GET READY. To configure folder redirection, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to the \User Configuration\Policies\Windows Settings\Folder Redirection node.
3. Right-click the Documents folder in the left window pane and select Properties. The *Documents Properties* dialog box opens.
4. In the *Setting* drop-down, select one of the following options:
   - **Basic—Redirect everyone's folder to the same location:** Redirects the Documents folder to the location you specify.
   - **Advanced—Specify locations for various user groups:** Redirects the Documents folder to a different place depending on a particular user's group membership.
   - **Not configured**—The folder will not be redirected.
5. If you chose Basic–Redirect Everyone's Folder To The Same Location, specify the Target folder location using a UNC in the *Settings* dialog box. Choose from the following options:

- **Redirect to the user's home directory:** Redirects the Documents folder to the user's home directory, specified in their Active Directory account tab for the user. This option is available only if you are redirecting the Documents folder. By allowing the system to create the subfolder structure automatically, the system will automatically create assign appropriate permissions on the shared folder.
- **Create a folder for each user under the root path:** Allows you to specify the path to a folder, whereas the group policy creates a subfolder for each user based on the %username% variable and the folder name of the redirected folder (such as Documents or Music), and redirects the appropriate folder there.
- **Redirect to the following location:** Allows you to redirect a folder to a specific folder, which is the same for all users. You might use this if you want the same items to appear for every user.
- **Redirect to the local userprofile location:** Redirects to the user's local profile located on the local computer and copies the contents of the redirected folder back to the user profile location. The redirected folder contents are not deleted.

6. If you chose Advanced–Specify Locations For Various User Groups, you specify the target folder location for each group that you add in the *Settings* dialog box. You will then select one of the options listed in the previous step. Click Add to select the groups and choose the target folder location for redirected files. The *Specify Group and Location* dialog box opens. Click OK to close the *Specify Group and Location* dialog box.
7. Click the Settings tab.
8. Click to enable the Grant the user exclusive rights to Documents checkbox, to automatically configure the permissions for the user to access the folder.
9. Click to enable the Move the contents of Documents to the new location checkbox if you need to move the current content of the Documents to the new location.
10. If you will be supporting down-level clients such as Windows XP, select Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems.
11. To configure the Policy Removal settings, select one of the following options:
    - Leave the folder in the new location when policy is removed.
    - Redirect the folder back to the local userprofile location when policy is removed.
12. Click OK to close the *Documents Properties* dialog box.
13. Close the *Group Policy Management Editor* window.

Using Scripts with Group Policy

A ***script*** is a list of commands that can be executed within a single file, which can perform repetitive tasks. You can use Group Policy to execute login/logoff scripts and startup/shutdown scripts. Some of the uses include cleaning up desktops when users log off and shut down computers, deleting the contents of temporary directories, mapping drives and printers, and setting environment variables.

The ***Microsoft Windows Script Hosts (WSH)*** is the component that provides scripting capabilities to Windows. Besides running batch files, it can also run JScripts and VBScripts. When creating scripts for the computer or user that are implemented through GPOs, you can execute batch files, JScripts, VBScripts, and Windows PowerShell scripts.

To use scripts, perform the following steps:

1. Create the login script.
2. Execute the script manually to make sure that the script runs and performs as planned.

3. Copy the script to the c:\Windows\Sysvol\Sysvol\Domain Name\Scripts folder on a domain controller. The content of SYSVOL volume is automatically replicated to the other domain controllers within the domain.
4. Configure a GPO to execute the script during startup, shutdown, logon, or logoff.

For computers, you can assign a ***startup scripts*** and ***shutdown scripts***. These are configured using the GPOs Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown). For users, you can assign a ***logon scripts*** and ***logoff scripts***. These are configured using the GPOs User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff) as shown in Figure 20-4.

Figure 20-4

Viewing the user scripts

IMPLEMENT A LOGIN SCRIPT USING GROUP POLICY

GET READY. To implement a login script using Group Policy, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff).
3. Double-click Logon to open the *Logon Properties* dialog box.
4. Click Add to open the *Add a Script* dialog box.
5. In the *Script Name* text box, type the path to the script, or click Browse to navigate to the script file in the *Netlogon* shared folder on the domain controller.
6. If necessary, type any parameters that are required by the script.
7. Click OK to close the *Logon Properties* dialog box.
8. Close the *Group Policy Management Editor* window.

You use the *Edit* button to edit a selected script. You can use the *Remove* button to remove the script from the GPO. You can use the *Show Files* button to open the \SysVol\.*domain name*,\Policies\{*GPO_GUID*}\User\Scripts\Logon folder to see a list of all scripts associated with the GPO.

If you assign multiple scripts, the scripts are processed in the order that you specify. To change the order, click to select the script and use the Up and Down buttons.

Using Administrative Templates

Windows Server 2012 R2 includes thousands of Administrative Template policies, which contains registry-based policy settings that are used to configure the user and computer environment. For example, to configure the user's desktop image or a default screen saver, you use an Administrative Template policy.

Traditionally, ***ADM files*** have been used to define the settings that an administrator can configure through Group Policy. ADM files use their own markup language, which made it difficult to customize ADM files. The ADM templates are located in the %SystemRoot%\Inf folder.

Windows Vista and Windows Server 2008 introduced ***ADMX files***, which are based on eXtensible Markup Language (XML). ADMX files can be stored in a single location called the *Central Store* in the SYSVOL directory. Unlike ADM files, ADMX files are not stored in individual GPOs. The Group Policy Management Editor automatically reads and displays settings from the local ADMX file store. By default, ADMX files are stored in the Windows\PolicyDefinitions folder, but they can be stored in a central location in the SYSVOL label.

ADMX files are language neutral. The descriptions of the settings are not part of the ADMX files. Instead, they are stored in language-specific ***ADML files***. ADML files are stored in a subfolder of the PolicyDefinitions folder. By default, only the ADML language files for the language of the installed operating system are added.

MANAGING ADMINISTRATIVE TEMPLATES

Administrative Templates appear under both Computer Configuration and User Configuration. The requirements for an Administrative Template setting, such as which operating system supports the setting and the description of the feature, are displayed:

- On the Extended tab when you click to select an Administrative Template setting (see Figure 20-5)

Figure 20-5

Selecting an Administrative Template

- When you double-click an Administrative Template setting (see Figure 20-6)

When configuring Administrative Templates, there are three states:

- **Not Configured:** The registry key is not modified or overwritten.
- **Enabled:** The registry key is modified by this setting.
- **Disabled:** The Disabled settings undo a change made by a prior Enabled setting.

If you want to undo the group policy, removing the group policy does not necessarily remove the setting from a computer that has the setting configured with a GPO. In these cases, you need to change the policy to Disabled (or create a second policy) and is applied to the computer and/or user. After the policy is applied, the policy can be removed. The policy can also be manually removed using the registry editor (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies).

Some Administrative Templates will be used to configure a setting, such as specifying a desktop image or specifying a screen saver. Although these settings are configured with GPOs, some of these

Figure 20-6

Viewing the Settings dialog box

settings can be changed while the computer is running. However, when the group policy is reapplied, the setting will revert back to the setting defined with the GPO. Other settings will be used to lock down a computer so that users cannot modify a setting or hide the setting from the user.

CONFIGURE THE DESKTOP BACKGROUND IMAGE WITH GROUP POLICY

GET READY. To configure the desktop background image with Group Policy, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to User Configuration\Policies\Administrative Templates\Desktop\Desktop.
3. Double-click Desktop Wallpaper. The *Desktop Wallpaper* dialog box opens.
4. Click Enabled.
5. In the *Wallpaper Name* text box, type the path and name of an image file.
6. Click OK to close the *Desktop Wallpaper* dialog box. The *Desktop Wallpaper* shows as *Enabled*.
7. Close the *Group Policy Management Editor* window.

CREATING A CENTRAL STORE

The ***Central Store*** is a folder structure created in the SYSVOL directory on the domain controllers in each domain in your organization. You have to create only the Central Store on a single domain controller for each domain, because the content of the SYSVOL will be replicated to the other domain controllers.

When there is no Central Store, the Group Policy Management Editor reads the local versions of the ADMX files used by the GPO on the Windows machine stored in the %systemroot%\PolicyDefinitions\ folder (which is typically the C:\Windows\PolicyDefinitions folder).

To create the Central Store, follow these steps:

1. Create a PolicyDefinitions folder in the %systemroot%\sysvol\domain\policies\ folder.
2. The PolicyDefinitions folder stores all of the language-neutral ADMX files. Therefore, copy all files from the %systemroot%\PolicyDefinitions* folder to the %systemroot%\sysvol\domain\policies\ folder.
3. Copy all the language folders and files to the %systemroot%\sysvol\domain\policies\PolicyDefinitions. For example, if you use the US English files, you copy the files from the %systemroot%\PolicyDefinitions\EN-US* folder to the %systemroot%\sysvol\domain\policies\PolicyDefinitions\EN-US\ folder.

The Group Policy Management Editor automatically reads all ADMX files stored in the Central Store.

Using Security Templates

GPOs are often used to make a computer more secure. By using security templates, you can implement security settings quickly and efficiently, you can copy and apply security settings from one computer to another, and you can check the security settings based on a security template.

Each computer running Windows 7 and 8 and any computer running Windows Server 2008 R2 and Windows Server 2012 R2 maintains a collection of security settings that can be managed by using the local GPO. These settings can be configured using the Group Policy Management Editor snap-in with the Local Computer object selected, or the Local Security Policy console (see Figure 20-7) found in Administrative Tools. Of course, if you want to configure all computers for your organization, you should use non-local GPOs.

Figure 20-7

Using the Local Security Policy console

A ***security template*** is a collection of configuration settings stored in a text file with the .inf extension. They can be used for the following:

- Save the security configuration to a file.
- Deploy the security settings to a computer or group policy.
- Analyze compliance of a computer's current configuration against the desired configuration.

The Security template allows you to configure the following policies and settings:

- **Account Policies Specify:** Allows you to configure password restrictions, account lockout policies, and Kerberos policies.
- **Local Policies:** Allows you to configure audit policies, user rights assignments, and security options policies.
- **Event Log Policies:** Allows you to configure maximum event log sizes and rollover policies.
- **Restricted Groups:** Allows you to specify users who are allowed to be added to a specific group such as domain administrators.
- **System Services:** Allows you to specify the startup types and permissions for system services.
- **Registry Permissions:** Allows you to set access control permissions for specific registry keys.
- **File System Permissions:** Allows you to specify access control permissions for NTFS files and folders.

You can deploy security templates using the following:

- Active Directory group policy objects
- Security Configuration And Analysis snap-in

To manage security templates, you can use the Security Templates snap-in. Unfortunately, this snap-in is not included in Administrative Tools. Therefore, you need to open Microsoft Management Console (MMC) and manually add the snap-in.

OPEN THE SECURITY TEMPLATES SNAP-IN

GET READY. To open the security template snap-in, perform the following steps:

1. Right-click the Start menu and select Command Prompt (Admin).
2. At the command prompt, execute the mmc command. An empty console opens.
3. Open the File menu, and click Add/Remove Snap-in.
4. When the *Add or Remove Snap-ins* dialog box opens, scroll down to and click Security Templates. Click Add. Click OK. The Security Templates snap-in is available (see Figure 20-8).

Figure 20-8

Viewing the Security Templates console

5. To create a new security template, right-click the node where you want to store the security template, and click New Template.
6. When the dialog box opens, type a descriptive name in the *Template name* text box. Click OK. The security template is added in the console.

You configure settings the same way you configure a GPO. The only exception is when you add registry settings that are not already listed in the Local Policies\Security Option portion of the template. After you make your changes, right-click the template and click *Save*.

After a security template is created and saved, you can deploy those settings by importing the security template into the GPO for a domain, site, organization unit object, or a local computer. To import a security template into a GPO, open the GPO and right-click the *Security Settings* node and click *Import Policy*. If you select the *Clear This Database Before Importing* checkbox, all security settings in the GPO will be erased prior to importing the template settings, so the GPO's security settings will match the template's settings.

Using Custom Administrative Template Files

Although new settings are added to each new release of Windows, and the settings included with Windows are quite comprehensive, it does not support applications, such as Microsoft Office. Therefore, you need to add custom administrative template files that are provided by vendors.

As mentioned previously, Administrative Templates for Windows Server 2012 R2 are ADMX files. To make those settings available to a GPO, you need to add the Administrative Templates file to the GPO.

ADD A CUSTOM ADM ADMINISTRATIVE TEMPLATE FILES

GET READY. To add custom ADM Administrative Template files, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click either Computer Configuration\Policies\Administrative Templates or User Configuration\Policies\Administrative Templates.
3. Right-click Administrative Templates and Add/Remove Templates. The *Add/Remove Templates* dialog box opens.

4. Click Add. The *Policy Templates* dialog box opens.
5. Navigate to the custom Administrative Templates and click Open. Click Close to close the *Add/Remove Templates* dialog box.
6. Close the *Group Policy Management Editor* window.

Configuring Property Filters for Administrative Templates

By default, all policy settings are displayed. To narrow down the displayed list of settings, you can use ***Administrative Templates Property Filters***.

To filter the settings displayed, you can select or deselect the following filter options:

- Managed or Non-Managed settings
- Configured or Not Configured
- Keyword Filters
- Requirements Filters

To configure the Filters, right-click *Administrative Templates* under Computer Configuration or User Configuration and click *Filter Options*.

Administrative Templates can be divided into managed and non-managed and configured and not-configured. Managed policy settings and remove a policy setting when it is no longer within the scope of the user or computer. To display only the Managed settings, you select *Yes* under the Managed section. The default option is Yes.

When opening a GPO, most settings are not configured. Therefore, if you want to show only the Configured settings, select *Yes* in the Configured section. The default setting is Any.

There are hundreds of settings located within the Administrative Templates. Therefore, to help you find a setting, you can select the Enable keyword filters and then specify a keyword.

Lastly, if you want to show only settings that will run on a certain operating system or other component such as a certain version of Internet Explorer, you will enable the *Enable Requirements Filters* option and specify which settings based on the requirement you want to display.

Business Case Scenario

Scenario 20-1: Standardizing a User's Work Environment

Many computers are shared among users and people often use different computers based on where they work. Therefore, you need to configure the following:

- Users must be able to access all documents that he or she stores in the Documents and Desktop folders.
- The users should also have the TimeClock.msi file installed so that he or she can clock in and out.

How can you accomplish this?

21 LESSON

Managing Group Policy Objects

Managing Group Policy Objects

THE BOTTOM LINE

So far, we have discussed how to create Group Policy Objects (GPOs) and manage the settings within a GPO. But so far, managing of the GPOs themselves has not been discussed.

Although Group Policy settings are configured using GPOs, GPOs are made of two components: ***Group Policy Container (GPC)*** and ***Group Policy Template (GPT)***. The GPC is an Active Directory object stored in the Group Policy Objects container with the domain naming content of the directory. The GPC defines basic attributes of the GPO, but it does not contain any of the settings.

The settings are contained in the GPT, a collection of files stored in the SYSVOL (%SystemRoot%\SYSVOL\<*Domain*>\Policies\<*GPOGUID*>) of each domain controller. Of course, as mentioned previously, this folder is replicated from one domain controller to another. The version of the GPO on a domain controller can be determined by looking at the \\{*servername*}\SYSVOL\{*domain*}\Policies\{*GUID*}\gpt.ini.

Backing Up and Restoring GPOs

For most organizations, GPOs is an essential tool to help manage the user environment and to ensure security. If you back up a domain controller including the System State, you back up all GPOs. However, you can back up and restore GPOs using the Group Policy Management Console.

With the Group Policy Management Console, you can back up all GPOs or individual GPOs. Every time a backup is performed, a new backup version of the GPO is created.

BACK UP GPOs

GET READY. To back up GPOs, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. To back up all GPOs, right-click Group Policy Objects container and click Back Up All. The *Back Up Group Policy Object* dialog box opens.
5. To back up a single GPO, right-click the GPO and click Back Up. The *Back Up Group Policy Object* dialog box opens.

6. In the *Location* text box, specify the location of where you want to store the backups and click Back Up.
7. When the backup is complete, click OK.
8. Close the *Group Policy Management Console*.

If a GPO gets deleted or corrupted, you can restore any of the historical versions of the GPO. The restore interface provides the ability for you to view the settings stored in the backed-up version before restoring it.

RESTORE A GPO

GET READY. To restore a GPO, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. To restore a GPO, right-click a GPO and click Restore from Backup.
5. When the *Restore Group Policy Object Wizard* opens, click Next.
6. On the *Backup location* page, specify the location of the backup folder in the *Backup folder* text box. Click Next.
7. On the *Source GPO* page, click the GPO that you want to view and click the View Settings button to view the settings within the backed up GPO.
8. Select the GPO that you want to restore and click Next.
9. When the wizard is complete, click the Finish button.
10. When the restore is complete, click OK.
11. Close the *Group Policy Management Console*.

The Group Policy Management Console also has a Manage Backups feature. By using this feature, you can restore from backup, delete a backup, and view settings. To open the Manage Backups dialog box, right-click *Group Policy Objects* container and click *Managed Backups*.

You can import settings of a backed up GPO into an existing GPO. When you import a GPO, it imports only the GPO settings. It does not transfer the security links or security principals assigned to the GPO. If you import settings into a GPO with settings, the imported settings will overwrite the existing settings.

IMPORT GPO SETTINGS

GET READY. To import a GPO setting, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. Right-click the target GPO and click Import Settings.
5. When the *Welcome* screen opens, click Next.
6. On the *Backup GPO* page, you can click Backup to back up the GPO before you import the settings. Click Next.
7. If you want to restore from a backup location, specify the location of the backups in the *Backup folder* text box and click Next.
8. Click the GPO that you want to copy from and click Next.
9. On the *Scanning Backup* page, click Next.

10. On the *Migrating References* page, with the *Copying them identically from the source* selected, click Next.
11. When the wizard is complete, click Finish.
12. When the import is complete, click OK.
13. Close the *Group Policy Management Console*.

Lastly, you can copy GPOs by using the Group Policy Management Console in the same domain and across domains. Similar to copy and paste used with files, the copy option copies the existing GPO. When you paste it to the Group Policy Objects container, it is named *copy of old_name*. You just have to rename a GPO to a more meaningful name. If you copy between domains, security principals will need to be redefined.

COPY A GPO

GET READY. To copy a GPO, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. Right-click a GPO and click Copy.
5. Right-click Group Policy Objects container and click Paste.
6. When the *Copy GPO* dialog box appears, click Use the default permissions for the new GPOs or Preserve the existing permissions. Click OK.
7. When the copy is complete, click OK.
8. Right-click the new GPO and click Rename. Type a new name and press the Enter key.
9. Close the *Group Policy Management Console*.

Using a Migration Table

When migrating GPOs from one domain to another, the GPO is specific to the domain where the GPO is defined. Therefore, when you transfer a GPO to a different domain, you might not want the same settings. You can use migration tables to modify these references in the GPO during the import or copy operation.

A ***migration table*** is a file that maps references to users, groups, computers, and UNC paths in the source GPO to new values in the destination GPO. A migration table consists of one or more mapping entries. When you specify a migration table while performing an import or copy, each reference in the source GPO will be replaced with a target reference. You can open the migration table when you import GPO settings or you can right-click *Domains* in the Group Policy Management Console and click *Open Migration Table Editor*.

USE A MIGRATION TABLE

GET READY. To use a migration table while importing GPO settings, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. Right-click a GPO and click Import.

5. When the *Import Settings Wizard* starts, click Next.
6. On the *Backup GPO* page, click Next.
7. On the *Backup location* page, specify the location of the backups in the *Backup folder* text box, click Next.
8. Click the GPO that you want to import and click Next.
9. On the *Scanning Backup* page, click Next.
10. On the *Migrating References* page, click Using this migration table to map them in the destination GPO option.
11. To create a new migration table, click New. The *Migration Table Editor – New* opens.
12. Click Tools > Populate from Backup. Alternatively, you can also choose Populate from GPO.
13. On the *Select Backup* dialog box, click the GPO that you want to populate the migration table with and click OK. The migration table will populate (see Figure 21-1).

Figure 21-1

Populating the migration table

Source Name	Source Type	Destination Name
Everyone	Free Text or SID	<Same As Source>
Pre-Windows 2000 Compatible Access	Free Text or SID	<Same As Source>
Authenticated Users	Free Text or SID	<Same As Source>
LOCAL SERVICE	Free Text or SID	<Same As Source>
IIS_IUSRS	Free Text or SID	<Same As Source>
NETWORK SERVICE	Free Text or SID	<Same As Source>
Administrators	Free Text or SID	<Same As Source>
Backup Operators	Free Text or SID	<Same As Source>
ENTERPRISE DOMAIN CONTROLLERS	Free Text or SID	<Same As Source>
group1	Free Text or SID	<Same As Source>
Server Operators	Free Text or SID	<Same As Source>
Account Operators	Free Text or SID	<Same As Source>
Print Operators	Free Text or SID	<Same As Source>
Performance Log Users	Free Text or SID	<Same As Source>

14. Review the Source Name. If you want the values to change for the target, type the new name in the *Destination Name* column.
15. Click File > Save. Specify a name in the *File name* text box and click Save.
16. Close the migration table.
17. On the *Migrating References* page, click Next.
18. When the wizard is complete, click Finish.
19. When the import is succeeded, click OK.
20. Close the *Group Policy Management Console*.

Resetting the Default GPOs

When you create a new domain, you start with the Default Domain Policy and Default Domain Controller Policy. If either of these gets deleted, corrupted, or you just want to start over, you can use the DCGPOFix.exe command.

The ***DCGPOFix.exe*** command can restore either or both the Default Domain Policy and the Default Domain Controllers Policy to their default settings. Of course, you must be a domain administrator to perform this task.

RESTORE THE DEFAULT GPOs

GET READY. To restore the Default Domain Policy and the Default Domain Controllers Policy, perform the following steps:

1. Right-click the Start menu and select Command Prompt (Admin).
2. At the prompt, execute the `DcGPOFix` command.
3. When it warns that you are about to restore the Default Domain Policy and Default Domain Controller Policy, type Y for Yes and press the Enter key.
4. When it says that it will replace all User Rights Assignments, type Y for Yes and press the Enter key.
5. Close the command prompt.

Delegating Group Policy Management

In Active Directory, domain administrators are automatically granted permissions for performing Group Policy Management tasks. If you need to give other users permissions to manage GPOs you grant those permissions through ***delegation***.

When you grant a person or group to create GPOs, they also are granted permissions to manage the GPOs that they created. To delegate GPO permissions, you use the Group Policy Management Console.

SPECIFY WHO CAN CREATE GPOs

GET READY. To specify who can create GPOs, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. Click the Delegation tab.
5. To add a user or group, click Add.
6. When the *Select User, Computer, or Group* dialog box opens, type the name of the user or group in the *Enter the object name to select* text box and click OK.
7. Close the *Group Policy Management Console*.

To give someone permission to manage a particular GPO, you use the Delegate tab of the individual GPO. When you add a user, you can then specify one of the following permissions:

- Read
- Edit settings
- Edit settings, delete, and modify security

SPECIFY WHO CAN MANAGE AN INDIVIDUAL GPO

GET READY. To specify who can manage an individual GPO, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management. The *Group Policy Management Console* opens.
3. Navigate to and click the Group Policy Objects container.
4. Right-click an individual GPO.
5. Click the Delegation tab.
6. To add a user or group, click Add.
7. When the *Select User, Computer, or Group* dialog box opens, type the name of the user or group in the *Enter the object name to select* text box and click OK.
8. When the *Add Group or User* dialog box opens, assign the appropriate permission and click OK.
9. Close the *Group Policy Management Console*.

To give more granular control of users and groups who can manage, read, or are affected by a GPO, you click the *Advanced* button from the Delegation tab, which opens the GPO Security Settings dialog box (see Figure 21-2). For permissions to be applied to a user, the user must have the Allow Read and Allow Apply group policy permissions. If you don't want a GPO to apply, you can assign the Disallow Apply group policy permission to a user or group.

Figure 21-2

Managing security settings for a GPO

Business Case Scenarios

Scenario 21-1: Copying GPOs to a Test Domain

You have multiple domains in your organization forest. In the primary corporate domain, you have created the multiple GPOs. You want to copy the GPOs to the test domain. However, you need to modify the primary corporate user groups to the primary test user groups and to change the production UNCs to the test UNC. What should you do?

Scenario 21-2: Allowing Others to Create GPOs

The developers need to create GPOs while allowing the developers to manage the GPOs that they create. In addition, you need to give administrative access to the Windows administrator team for all GPOs except the Default Domain Policy and Default Domain Controller Policy. What should you do to accomplish this while maintaining security?

Configuring Group Policy Preferences

LESSON 22

Using Group Policy Preferences

THE BOTTOM LINE

Group Policy features were expanded in Windows Server 2008 with the introduction of Group Policy Preferences. ***Group Policy Preferences (GPP)*** are made up of more than 20 new Group Policy client-side extensions (CSEs) that expand the range of configurable settings in a Group Policy object (GPO) that were not available before. Examples of the new GPP extensions include Folder Options, Drive Maps, Printers, Scheduled Tasks, Services, and Start Menu.

The key difference between preferences and policy settings is enforcement. Although Group Policies settings cannot be modified, GPP writes preferences to the same locations in the registry that the application or operating system feature uses to store the setting. Although the group policy setting interface is usually disabled or grayed out, preference settings can still be changed.

By default, Group Policy refreshes preferences using the same interval as Group Policy settings. However, you can chose to prevent Group Policy from refreshing individual preferences by choosing to apply them only once. This allows you to assign a default value but allows the user to change to his or her liking.

GPP can be configured on domain controllers running Windows Server 2008 or higher. By default, GPP are supported by client computers running Windows Vista SP2, Windows 7 or higher, or Windows Server 2008 or higher. To support Windows XP SP3, Windows Vista SP1, or Windows Server 2003 client computers, you must install GPP Client Side Extensions from Microsoft Downloads or Windows Updates.

Configuring Preference Settings

When you create a GPO with preferences, the preferences options are configured much like you would in Windows such as using the Control Panel and Windows Explorer options. So when you need to configure Internet Options, the options that you configure will look exactly like the Internet Options found in the Windows Control Panel (see Figure 22-1).

Figure 22-1

Viewing GPP

For most preferences settings, you right-click the option that you want to configure, select *New* and select the preference item that you want to create. For example, if you right-click Internet Settings, you have the option to configure the following:

- Internet Explorer 5 and 6
- Internet Explorer 7
- Internet Explorer 8 and 9
- Internet Explorer 10

If you have some users using Internet Explorer 8 and 9 and some users using Internet Explorer 10, you will have to add entries for each one.

Configuring Windows Settings

GPP are divided into two sections: Windows Settings and Control Panel Settings. Windows Settings are commonly used configuration settings that are performed in Windows, but are not done in the Control Panel.

Preference extensions under Windows Settings include:

- **Applications Extension:** Configure settings for applications.
- **Drive Maps Extension:** Create, modify, or delete mapped drives, and configure the visibility of all drives.
- **Environment Extension:** Create, modify, or delete environment variables.
- **Files Extension:** Copy, modify, or delete files or change the attributes of the files.
- **Folders Extension:** Create, modify, or delete folders.

- **Ini Files Extension:** Add, replace, or delete sections or properties in configuration settings (.ini) or setup information (.inf) files.
- **Network Shares Extension:** Create, modify, or unshare shared folders.
- **Registry Extension:** Copy registry settings and apply them to other computers. Create, replace, or delete registry settings.
- **Shortcuts Extension:** Create, modify, or delete shortcuts.

Some of the more popular settings are discussed in the next few subsections.

CONFIGURING NETWORK DRIVE MAPPINGS

Network drive maps allow you to create dynamic drive mappings to network shares, modify mapped drives, delete a mapped drive, or hide or show drives.

For Drive Map extensions, the type of preference item provides a choice of four actions: Create, Replace, Update, and Delete. The behavior of the preference item varies with the action selected and whether the drive letter already exists:

- **Create:** Create a new mapped drive for users.
- **Replace:** Delete and recreate mapped drives for users. If the drive mapping already exists, the drive mapping will be deleted. If the drive mapping does not exist, then the Replace action creates a new drive mapping.
- **Update:** Modify settings of an existing mapped drive for users. Only updates settings defined within the preference item. All other settings remain as configured on the mapped drive. If the drive mapping does not exist, then the Update action creates a new drive mapping.
- **Delete:** Remove a mapped drive for users.

CREATE A MAPPED DRIVE PREFERENCE ITEM

GET READY. To create a mapped drive preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Windows Settings\Drive Maps or User Configuration\Preferences\Windows Settings\Drive Maps.
3. Right-click the Drive Maps node, click New, and select Mapped Drive. The *New Drive Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify the location of the remote drive using a Universal Naming Convention (UNC), the drive mapping, and the Connect as and the Hide/Show options.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

PERFORMING FILE AND FOLDER DEPLOYMENT

There might be times when you want to make sure that users have certain files available to them. Therefore, you can use the Files and Folders nodes under Windows Settings to copy, delete, or move files and folders.

File Preference item provides a choice of four actions: Create, Replace, Update, and Delete. The behavior of the preference item varies with the action selected and whether the file already exists:

- **Create:** Copy a file or files from a source location to a destination location if it does not already exist at the destination, and then configure the attributes of those files for computers or users.

- **Replace:** Delete a file or files, replace it with another file or files, and configure the attributes of those files for computers or users. If the file already exists, it will overwrite the file. If the file does not exist at the destination, then the Replace action copies the file from the source location to the destination.
- **Update:** Modify settings of an existing file or files for computers or users. Different from Replace, this option updates only the file attributes for the specified file or files. If the file does not exist, then the Update action copies the file from the source location to the destination.
- **Delete:** Remove a file or files for computers or users.

To copy, replace, update, or delete files, you can use the wildcard (* and ?) characters.

COPY, REPLACE, UPDATE, OR DELETE FILES

GET READY. To copy, replace, update, or delete files, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Windows Settings\Files or User Configuration\Preferences\Windows Settings\Files.
3. Right-click the Files node, click New, and select File. The *New File Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. If you are copying, replacing, or updating files, specify the source files that you want to copy or replace in the *Source file(s)* text box. This option will be grayed out if you select the Delete action.
6. If you are copying, replacing, or updating files, specify the destination files in the Destination File.
7. If you are copying, replacing, or updating files, specify the file attributes.
8. If you are deleting files, specify the files in the *Delete file(s)* text box.
9. To allow multiple files to transfer even if one or more individual files fail to transfer, select the Suppress errors on individual file actions check box.
10. Click the Common tab, and configure any of the Common options.
11. Click OK. The new preference item appears in the details pane.
12. Close the *Group Policy Management Editor*.

Folder preference items provide a choice of four actions: Create, Replace, Update, or Delete folders and their contents:

- **Create:** Create a new folder for computers or users.
- **Replace:** Delete and recreate a folder for computers or users. If the folder does not exist, then the Replace action creates a new folder.
- **Update:** Modify an existing folder for computers or users. This action differs from Replace in that it updates only settings defined within the preference item. All other settings remain as configured on the folder. If the folder does not exist, then the Update action creates a new folder.
- **Delete:** Remove a folder for computers or users.

CREATE, REPLACE, UPDATE, AND DELETE FOLDERS AND THEIR CONTENT

GET READY. To create, replace, update, or delete a folder, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.

2. Navigate to and click Computer Configuration\Preferences\Windows Settings\Folders or User Configuration\Preferences\Windows Settings\Folders.
3. Right-click the Folders node, click New, and select Folder. The *New Folder Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify the path of the folder in the *Path* text box.
6. If you need to delete folders that are not empty, enable the Delete this folder (if emptied) option.
7. If you need to delete all subfolders within the folder you are trying to delete, enable the Recursively delete all subfolders is selected option.
8. If you need to delete read-only file and folders, enable the Allow deletion of read-only files/folders option. If this option is selected, it also clears the read-only attribute of files and folders that this Folder item attempts to delete.
9. If you need to delete items within the folder that you are attempting to delete, you must enable the Delete all files in the folder(s) option.
10. If you want to suppress errors if the folder is not empty, a file that is open in the folder, a file or folder for which the user does not have permission, or any other file or folder that cannot be deleted, enable the Ignore errors for files/folders that cannot be deleted option.
11. Click the Common tab, and configure any of the Common options.
12. Click OK. The new preference item appears in the details pane.
13. Close the *Group Policy Management Editor*.

PERFORMING SHORTCUT DEPLOYMENT

Shortcut preference items allow you to configure a shortcut to a file system object (such as a file, folder, drive, share, or computer), a shell object (such as a printer, desktop item, or control panel item), or a URL (such as a web page or an FTP site).

This type of preference item provides a choice of four actions: Create, Replace, Update, and Delete. The behavior of the preference item varies with the action selected and whether the shortcut already exists.

- **Create:** Create a new shortcut for computers or users.
- **Replace:** Delete and recreate a shortcut for computers or users. If the shortcut already exists, it will be overwritten. If the shortcut does not exist, then the Replace action creates a new shortcut.
- **Update:** Modify settings of an existing shortcut for computers or users. If the shortcut does not exist, then the Update action creates a new shortcut.
- **Delete:** Remove a shortcut for computers or users.

CREATE A SHORTCUT ITEM

GET READY. To create a mapped drive preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Windows Settings\Shortcuts or User Configuration\Preferences\Windows Settings\Shortcuts.
3. Right-click the Shortcuts node, click New, and select Shortcut. The *New Shortcut Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. In the *Name* textbox, type in the name of the shortcut.

6. Using the *Target Type* pull-down menu, select File System Object, URL, or Shell Object.
7. Using the *Location* pull-down menu, select the location of the object such as Desktop, Start Menu, or Explorer Favorites.
8. In the *Target Path* text box, type a local path, UNC path, or drive letter that the shortcut will point to.
9. In the *Start in* text box, specify the working directory that contains files required by the target.
10. In the *Shortcut key* text box, type the key combinations to activate the shortcut. To remove the keyboard shortcut, press Delete or Backspace. This option is not available for Delete.
11. In the *Run* text box, select the size of the window on which to open the target of the shortcut.
12. In the *Comment* text box, which will be displayed as a tooltip, enter text describing the shortcut.
13. In the *Icon file path* text box, specify an icon for the shortcut.
14. Click the Common tab, and configure any of the Common options.
15. Click OK. The new preference item appears in the details pane.
16. Close the *Group Policy Management Editor*.

Configuring Control Panel Settings

The Control Panel Preferences allow you to configure the popular settings found within the Control Panel.

Preference extensions under Control Panel Settings include:

- **Data Sources Extension:** Create, modify, or delete Open Database Connectivity (ODBC) data source names.
- **Devices Extension:** Enable or disable hardware devices or classes of devices.
- **Folder Options Extension:** Configure folder options, such as creating, modifying, or deleting filename extension associations.
- **Internet Settings Extension:** Modify user-configurable Internet settings.
- **Local Users and Groups Extension:** Create, modify, or delete local users and groups.
- **Network Options Extension:** Create, modify, or delete virtual private networking (VPN) or dial-up networking connections.
- **Power Options Extension:** Modify power options and create, modify, or delete power schemes.
- **Printers Extension:** Create, modify, or delete TCP/IP, shared, and local printer connections.
- **Regional Options Extension:** Modify regional options.
- **Scheduled Tasks Extension:** Create, modify, or delete scheduled or immediate tasks.
- **Services Extension:** Modify services.
- **Start Menu Extension:** Modify Start Menu options.

CONFIGURING PRINTER SETTINGS

Similar to adding a printer to Windows, you can add a shared printer, a TCP/IP printer, or a local printer.

The Printers preference extension allows you to create, configure, and delete local printers, TCP/IP printers, and Shared Printers Printer preference item. The next three exercises show you how to create these printers.

CREATE A NEW LOCAL PRINTER PREFERENCE ITEM

GET READY. To create a new local printer preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Control Panel Settings\Printers or User Configuration\Preferences\Control Panel Settings\Printers.
3. Right-click the Printers node, click New, and select Local Printer. The *New Local Printer Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify the Name, port (Comx, LPTx, or USBx), and printer path for the printer. Then type a location and comments if desired.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

CREATE A NEW TCP/IP PRINTER PREFERENCE ITEM

GET READY. To create a new TCP/IP printer preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Control Panel Settings\Printers or User Configuration\Preferences\Control Panel Settings\Printers.
3. Right-click the Printers node, click New, and select TCP/IP Printer. The *New TCP/IP Printer Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify the IP Address, Local Name, and Printer Path for the printer. Then type a location and comments if desired.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

CREATE A NEW SHARED PRINTER PREFERENCE ITEM

GET READY. To create a new shared printer preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Control Panel Settings\Printers or User Configuration\Preferences\Control Panel Settings\Printers.
3. Right-click the Printers node, click New, and select Shared Printer. The *New Shared Printer Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify the Share path and the optional Local port for the printer.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

CONFIGURING CUSTOM REGISTRY SETTINGS

Registry preference extension allows you to copy registry settings from one computer to another, and to create, replace, or delete an individual registry value. It also allows you to create an empty key, delete a key, or delete all values and subkeys in a key. Lastly, it allows you to create collections or folders to organize the Registry preference Items.

CREATE A NEW REGISTRY PREFERENCE ITEM

GET READY. To create a new registry preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Windows Settings\Registry or User Configuration\Preferences\Windows Settings\Registry.
3. Right-click the Registry node, click New, and select Registry Item. The *Registry Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify the Hive such as HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE. Then specify the value name, value type, and value data.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

To help you organize the registry settings, you can use collections, which act as folders to hold the registry settings. To create a collection, you just right-click *Registry* in the Group Policy Management Editor and select *Collection Item*. You then rename the collection to the desired name. After the collection is created, you can then add Registry items.

The last option under the Registry is the Registry Wizard, which allows you to create multiple Registry preference items based upon registry settings that you select on a computer. After you select the settings, you can modify the permissions after the entries are created. Lastly, the wizard organizes the registry items in a collection folder that mimics the structure of the registry.

CONFIGURING POWER OPTIONS

The Power options extension allows you to create and configure Power Plan, Power Options, and Power Scheme preference items. The Power Options and Power Schemes are used with Windows XP and Windows Vista and Power Plan with Windows Vista and later.

CREATE A NEW POWER OPTIONS PREFERENCE ITEM

GET READY. To create a new power options preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Control Panel Settings\Power Options or User Configuration\Preferences\Control Panel Settings\Power Options.
3. Right-click the Power Options node, click New, and select Power Options (Windows XP). The *New Power Options (Windows XP) Properties* dialog box opens.
4. Select an Action for Group Policy to perform.

5. Specify whether the power icon shows on the taskbar, whether a password is required to resume from standby, and whether hibernation is enabled. You can also specify what happens when the laptop lid is closed, when the power button is pressed, and when the sleep button is pressed.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

CREATE A NEW POWER SCHEME PREFERENCE ITEM

GET READY. To create a power scheme preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Control Panel Settings\Power Options or User Configuration\Preferences\Control Panel Settings\Power Options.
3. Right-click the Power Options node, click New, and select Power Scheme (Windows XP). The *New Power Scheme (Windows XP) Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify when to turn off the monitor or hard disk or when the system goes into standby or when the system hibernates.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

CREATE A NEW POWER OPTIONS PREFERENCE ITEM

GET READY. To create a power options preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click Computer Configuration\Preferences\Control Panel Settings\Power Options or User Configuration\Preferences\Control Panel Settings\Power Options.
3. Right-click the Power Options node, click New, and select Power Plan (At least Windows 7). The *New Power Scheme (At least Windows 7) Properties* dialog box opens.
4. Select an Action for Group Policy to perform.
5. Specify which power plan to configure and modify the appropriate power options.
6. Click the Common tab, and configure any of the Common options.
7. Click OK. The new preference item appears in the details pane.
8. Close the *Group Policy Management Editor*.

CONFIGURING INTERNET EXPLORER SETTINGS

Group Policy includes the Internet Settings preference extension, which allows you to configure specific configuration of Internet settings or to configure an initial configuration of Internet settings, but allow end users to make changes.

CREATE AN INTERNET EXPLORER PREFERENCE ITEM

GET READY. To create an Internet Explorer preference item, perform the following steps:

1. Open the Group Policy Management Editor for the GPO you want to configure.
2. Navigate to and click User Configuration\Preferences\Control Panel Settings\Internet Settings.
3. Right-click the Internet Settings node, click New, and select Internet Explorer 10. The *New Internet Explorer 10 Properties* dialog box opens.
4. Under the General tab, specify a home, specify how tabs are displayed, and specify if Delete browsing history on exist.
5. On the Security tab, specify the security level for each zone Internet, Local intranet, Trusted sites, and Restricted sites. You can also enable or disable Protected Mode. If necessary, click Custom Level to change individual settings for a zone.
6. On the Privacy tab, you can specify to turn on Pop-up blocker, configure the Pop-up Blocker by clicking Settings, or to configure InPrivate option.
7. On the Content tab, you configure the AutoComplete settings and the Feeds and Web Slices settings.
8. On the Connections tab, you can configure dial-up and Virtual Private Network settings and to configure LAN settings, which are necessary if your organization is using a proxy server.
9. On the Programs tab, you can specify how Internet Explorer is open (on the desktop, in Internet Explorer, or let Internet Explorer decide). You can also specify whether you want to open Internet Explorer tiles on the desktop.
10. On the Advanced tab, select individual Advanced settings for Internet Explorer.
11. Click the Common tab, and configure any of the Common options.
12. Click OK. The new preference item appears in the details pane.
13. Close the *Group Policy Management Editor*.

Configuring Item-Level Targeting

Item-level targeting is used to change the scope of individual preference items so that the preference items apply to only selected users or computers.

Targeting items are items that you can specify as qualifiers for item-level targeting. Some of the targeting items (see Figure 22-2) that can be used include:

Figure 22-2

Using item-level targeting

- Computer name
- CPU speed
- Date match
- Disk space
- Domain
- IP address range
- Network connection
- Operating system
- Portable computer
- RAM
- User
- Terminal session
- LDAP query
- Time range
- WMI query

Each targeting item results in a value of either true or false. You can apply multiple targeting items to a preference item and select the logical operation (AND or OR) by which to combine each targeting item with the preceding one (see Figure 22-3). If the combined value is false, then the settings in the preference item are not applied to the user or computer.

Figure 22-3

Using the targeting editor

Business Case Scenarios

Scenario 22-1: Saving Power

You are an administrator for the Contoso Corporation. Your manager says that there is a need to save money when possible and he notices that at night, many computers are still on. He started to realize how much power all of these computers consume when they are not in use. Therefore, he wants you to come up with a solution to automatically put the computers to sleep when they are not being used. What do you propose?

Scenario 22-2: Adding Registry Settings

You are an administrator for the Contoso Corporation. You have a mix of Windows XP, Windows 7, and Windows 8 computers. For the Windows 8 computers, you need to add a registry setting. You do not want to add the registry settings for the Windows XP and Windows 7 clients. What should you do?

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.

Microsoft

Microsoft Official Academic Course

Configuring Advanced Windows Server 2012 R2 Services

EXAM 70-412

Microsoft® Official Academic Course

Configuring Advanced Windows Server® 2012 R2 Services Exam 70-412

Patrick Regan

WILEY

VP & PUBLISHER	Don Fowley
EXECUTIVE EDITOR	John Kane
EXECUTIVE MARKETING MANAGER	Chris Ruel
MICROSOFT PRODUCT MANAGER	Natasha Chornesky of Microsoft Learning
EDITORIAL PROGRAM ASSISTANT	Jessy Lentz
TECHNICAL EDITOR	Brian Svidergol
ASSOCIATE MARKETING MANAGER	Debbie Martin
ASSOCIATE PRODUCTION MANAGER	Joyce Poh
COVER DESIGNER	Thomas Nery
SENIOR PRODUCT DESIGNER	Thomas Kulesa
CONTENT EDITOR	Wendy Ashenberg

This book was set in Garamond by Aptara, Inc.

Copyright © 2014 by John Wiley & Sons, Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc. 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, (201) 748-6011, fax (201) 748-6008. To order books or for customer service, please call 1-800-CALL WILEY (225-5945).

Microsoft, Active Directory, AppLocker, Bing, BitLocker, DreamSpark, Hyper-V, Internet Explorer, SQL Server, Visual Studio, Win32, Windows Azure, Windows, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

The 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, John Wiley & Sons, Inc., Microsoft Corporation, nor their resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

ISBN 978-1-118-88299-3

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

www.wiley.com/college/microsoft *or*
call the MOAC Toll-Free Number: 1+(888) 764-7001 (U.S. & Canada only)

Foreword from the Publisher

Wiley's publishing vision for the Microsoft Official Academic Course series is to provide students and instructors with the skills and knowledge they need to use Microsoft technology effectively in all aspects of their personal and professional lives. Quality instruction is required to help both educators and students get the most from Microsoft's software tools and to become more productive. Thus, our mission is to make our instructional programs trusted educational companions for life.

To accomplish this mission, Wiley and Microsoft have partnered to develop the highest-quality educational programs for information workers, IT professionals, and developers. Materials created by this partnership carry the brand name "Microsoft Official Academic Course," assuring instructors and students alike that the content of these textbooks is fully endorsed by Microsoft, and that they provide the highest-quality information and instruction on Microsoft products. The Microsoft Official Academic Course textbooks are "Official" in still one more way—they are the officially sanctioned courseware for Microsoft IT Academy members.

The Microsoft Official Academic Course series focuses on *workforce development*. These programs are aimed at those students seeking to enter the workforce, change jobs, or embark on new careers as information workers, IT professionals, and developers. Microsoft Official Academic Course programs address their needs by emphasizing authentic workplace scenarios with an abundance of projects, exercises, cases, and assessments.

The Microsoft Official Academic Courses are mapped to Microsoft's extensive research and job-task analysis, the same research and analysis used to create the Microsoft Certified Solutions Associate (MCSA) exam. The textbooks focus on real skills for real jobs. As students work through the projects and exercises in the textbooks and labs, they enhance their level of knowledge and their ability to apply the latest Microsoft technology to everyday tasks. These students also gain resume-building credentials that can assist them in finding a job, keeping their current job, or in furthering their education.

The concept of life-long learning is today an utmost necessity. Job roles, and even whole job categories, are changing so quickly that none of us can stay competitive and productive without continuously updating our skills and capabilities. The Microsoft Official Academic Course offerings, and their focus on Microsoft certification exam preparation, provide a means for people to acquire and effectively update their skills and knowledge. Wiley supports students in this endeavor through the development and distribution of these courses as Microsoft's official academic publisher.

Today educational publishing requires attention to providing quality print and robust electronic content. By integrating Microsoft Official Academic Course products, MOAC Labs Online, and Microsoft certifications, we are better able to deliver efficient learning solutions for students and teachers alike.

Joseph Heider

General Manager and Senior Vice President

Preface

Welcome to the Microsoft Official Academic Course (MOAC) program for becoming a Microsoft Certified Solutions Associate for Windows Server 2012 R2. MOAC represents the collaboration between Microsoft Learning and John Wiley & Sons, Inc. Microsoft and Wiley teamed up to produce a series of textbooks that deliver compelling and innovative teaching solutions to instructors and superior learning experiences for students. Infused and informed by in-depth knowledge from the creators of Windows Server 2012 R2, and crafted by a publisher known worldwide for the pedagogical quality of its products, these textbooks maximize skills transfer in minimum time. Students are challenged to reach their potential by using their new technical skills as highly productive members of the workforce.

Because this knowledgebase comes directly from Microsoft, architect of Windows Server 2012 R2 and creator of the Microsoft Certified Solutions Associate exams, you are sure to receive the topical coverage that is most relevant to students' personal and professional success. Microsoft's direct participation not only assures you that MOAC textbook content is accurate and current; it also means that students will receive the best instruction possible to enable their success on certification exams and in the workplace.

■ The Microsoft Official Academic Course Program

The Microsoft Official Academic Course series is a complete program for instructors and institutions to prepare and deliver great courses on Microsoft software technologies. With MOAC, we recognize that because of the rapid pace of change in the technology and curriculum developed by Microsoft, there is an ongoing set of needs beyond classroom instruction tools for an instructor to be ready to teach the course. The MOAC program endeavors to provide solutions for all these needs in a systematic manner in order to ensure a successful and rewarding course experience for both instructor and student—including technical and curriculum training for instructor readiness with new software releases; the software itself for student use at home for building hands-on skills, assessment, and validation of skill development; and a great set of tools for delivering instruction in the classroom and lab. All are important to the smooth delivery of an interesting course on Microsoft software, and all are provided with the MOAC program.

Conventions and Features Used in This Book

This book uses particular fonts, symbols, and heading conventions to highlight important information or to call your attention to special steps.

Convention	Meaning
THE BOTTOM LINE	This feature provides a brief summary of the material to be covered in the section that follows.
WARNING	*Warning* points out instances when error or misuse could cause damage to the computer or network.
A ***shared printer*** can be used by many individuals on a network.	Key terms appear in bold italic.
`[cd\windows\system32\ ServerMigrationTools]`	Commands that are to be typed are shown in a special font.
Click Install Now.	Any button on the screen you are supposed to click on or select will appear in blue.

Instructor Support Program

The Microsoft Official Academic Course programs are accompanied by a rich array of resources that incorporate the extensive textbook visuals to form a pedagogically cohesive package.

- **Instructor's Guide.** The Instructor's Guide contains chapter summaries and lecture notes.
- **Test Bank.** The Test Bank contains hundreds of questions organized by lesson in multiple-choice, best answer, build a list, and essay formats. A complete answer key is provided.
- **PowerPoint Presentations.** A complete set of PowerPoint presentations is available to enhance classroom presentations. Tailored to the text's topical coverage, these presentations are designed to convey key Windows Server 2012 R2 concepts addressed in the text.
- **MOAC Labs Online.** MOAC Labs Online is a cloud-based environment that enables students to conduct exercises using real Microsoft products. These are not simulations but instead are live virtual machines where faculty and students can perform any activities they would on a local virtual machine. MOAC Labs Online relieves the need for local setup, configuration, and most troubleshooting tasks. This represents an opportunity to lower costs, eliminate the hassle of lab setup, and support and improve student access and portability. Contact your Wiley rep about including MOAC Labs Online with your course offering.

About the Author

Patrick Regan has been a PC technician, network administrator/engineer, design architect, and security analyst for the past 23 years since graduating with a bachelor's degree in physics from the University of Akron. He has taught many computer and network classes at Sacramento local colleges (Heald Colleges and MTI Colleges) and participated in and led many projects (Heald Colleges, Intel Corporation, Miles Consulting Corporation, and Pacific Coast Companies). For his teaching accomplishments, he received the Teacher of the Year award from Heald Colleges and he has received several recognition awards from Intel. Previously, he worked as a product support engineer for the Intel Corporation Customer Service, a senior network engineer for Virtual Alert supporting the BioTerrorism Readiness suite and as a senior design architect/engineer and training coordinator for Miles Consulting Corporation (MCC), a premiere Microsoft Gold partner and consulting firm. He is currently a senior network engineer and consultant supporting a large enterprise network at Pacific Coast Companies, which is also a Microsoft Gold Partner and consulting firm. As a senior system administrator, he supports approximately 120 servers and 1,500 users spread over 5 subsidiaries and 70 sites. He has designed, implemented, and managed systems running Exchange Server 2010, SharePoint 2010, and SQL Server 2008 R2. To manage the servers and client computers, Pat and his team use group policies, SCOM, SCCM, and Symantec server.

He has earned several certifications, including Microsoft's MCSE, MCSA, and MCT; CompTIA's A+, Network+, Server+, Linux+, and Security+; Cisco's CCNA; and Novell's CNE and CWNP Certified Wireless Network Administrator (CWNA). Over the past several years, he has written several textbooks for Prentice Hall, including Troubleshooting the PC, Networking with Windows 2000 and 2003, Linux, Local Area Networks, Wide Area Networks, and the Acing Series (Acing the A+, Acing the Network+, Acing the Security+, and Acing the Linux+). For Que Publishing he has written several Exam Cram books for Windows Server 2008 certification tracks. For Wiley Publishing, he has written books on SharePoint 2010, Windows 7, and Window Server 2012.

Brief Contents

1 Configuring Network Load Balancing 1
2 Configuring Failover Clustering 9
3 Managing Failover Clustering Roles 27
4 Managing Virtual Machine Movement 35
5 Configuring Advanced File Services 49
6 Implementing Dynamic Access Control 63
7 Configuring and Optimizing Storage 73
8 Configuring and Managing Backups 83
9 Recovering Servers 94
10 Configuring Site-Level Fault Tolerance 107
11 Implementing an Advanced Dynamic Host Configuration Protocol (DHCP) Solution 116
12 Implementing an Advanced DNS Solution 129
13 Deploying and Managing IPAM 139
14 Configuring a Domain and Forest 148
15 Configuring Trusts 156
16 Configuring Sites 172
17 Managing Active Directory and SYSVOL Replication 184
18 Implementing Active Directory Federation Services 196
19 Installing and Configuring Active Directory Certificate Services (AD CS) 209
20 Managing Certificates 220
21 Installing and Configuring Active Directory Rights Management Services 234

Contents

Lesson 1: Configuring Network Load Balancing 1

Configuring Network Load Balancing 1
- Configuring NLB Prerequisites 2
- Installing NLB Nodes 2
- Configuring Port Rules 5
- Configuring Filtering Mode and Affinity 6
- Configuring Cluster Operation Mode 7
- Upgrading an NLB Cluster 8

Business Case Scenario 8

Lesson 2: Configuring Failover Clustering 9

Understanding Failover Clustering 9
- Installing and Configuring Failover Clustering 10
  - Configuring Cluster Networking 11
  - Installing and Creating a Failover Cluster 11
  - Configuring Cluster Storage 14
- Configuring and Optimizing Clustered Shared Volumes (CSVs) 15
- Configuring Quorum 16
- Configuring Storage Spaces 18
- Configuring Clusters Without Network Names 20
- Implementing Cluster-Aware Updating 21
- Upgrading a Cluster 23
- Backing Up and Restoring Failover Cluster Configuration 24

Business Case Scenarios 26

Lesson 3: Managing Failover Clustering Roles 27

Managing Failover Clustering Roles 27
- Configuring Role-Specific Settings 27
  - Understanding SMB 3.0 28
  - Deploying the General Use File Server Role 28
  - Deploying Scale-Out File Server 30
  - Configuring Guest Clustering 30
- Configuring Failover and Preference Settings 32
- Configuring VM Monitoring 34

Business Case Scenarios 34

Lesson 4: Managing Virtual Machine Movement 35

Understanding Virtual Machine Movement 35

Understanding Live Migration 36
- Performing LM 36
  - Configuring LM Prerequisites 36
  - Moving VMs Using LM 39

Performing Quick Migration 41

Performing Storage Migration 41

Configuring Virtual Machine Network Health Protection 43

Configuring Drain on Shutdown 44

Importing, Exporting, and Copying Virtual Machines 45
  - Understanding Importing, Exporting, and Copying Virtual Machines 45

Business Case Scenarios 48

Lesson 5: Configuring Advanced File Services 49

Configuring NFS Data Store 49
- Obtaining User and Group Information 49
- Creating an NFS Share 52
- Installing and Configuring the NFS Data Store 53

Configuring BranchCache 54

Configuring File Classification Infrastructure 58

Configuring File Access Auditing 61

Business Case Scenarios 62

Lesson 6: Implementing Dynamic Access Control 63

Using Dynamic Access Control 63
Configuring User and Device Claim Types 64
Creating and Configuring Resource Properties and Lists 66
Configuring File Classification 66
Creating and Configuring Central Access Rules and Policies 68
Implementing Policy Changes and Staging 69
Performing Access-Denied Remediation 71
Business Case Scenarios 72

Lesson 7: Configuring and Optimizing Storage 73

Using iSCSI 73
Configuring iSCSI Target 74
Configuring iSCSI Initiator 76
Configuring Internet Storage Name Server 77
Configuring Tiered Storage 79
Implementing Thin Provisioning and Trim 80
Managing Server Free Space Using Features on Demand 81
Business Case Scenarios 82

Lesson 8: Configuring and Managing Backups 83

Configuring and Managing Backups 83
Installing the Windows Server Backup Feature 83
Configuring Windows Server Backups 84
Reviewing Backup Configuration Options 84
Exploring Your Scheduling Options 85
Selecting Where to Store Your Backups 85
Optimizing Your Backups (Full versus Incremental) 85
Configuring Microsoft Azure Backup 87
Configuring Role-Specific Backups 89
Backing Up DHCP and DNS 89
Backing Up WINS 90
Backing Up Certificate Services 90
Managing VSS Settings Using VSSAdmin 91
Creating System Restore Snapshots 92
Enabling Shadow Copies for Shared Volumes 92
Business Case Scenarios 93

Lesson 9: Recovering Servers 94

Preparing For Windows Server 2012 R2 Restore 94
Restoring Files and Folders 95
Restoring Volumes 96
Restoring the System State 98
Restoring the System State on a Member Server 98
Performing a Bare Metal Recovery Restore 99
Recovering Servers Using WinRE and Safe Mode 100
Booting into Safe Mode 101
Configuring the Boot Configuration Data Store 103
Using Bcdedit to Modify Settings in the BCD Store 104
Using Bootrec with Bcdedit to Repair a Corrupted/Missing BCD Store 105
Business Case Scenario 106

Lesson 10: Configuring Site-Level Fault Tolerance 107

Configuring Hyper-V Replica 107
Configuring Hyper-V Replica Between Two Servers 107
Configuring Hyper-V Replica Extended Replication 111
Configuring Multi-Site Clustering 111
Configuring Multi-Site Storage and Network Settings 112
Configuring Quorum and Failover Settings 113
Configuring Multi-Site Failure Cluster 113
Configuring Global Update Manager 114
Recovering a Multi-Site Failover Cluster 115
Business Case Scenarios 115

Lesson 11: Implementing an Advanced Dynamic Host Configuration Protocol (DHCP) Solution 116

Implementing Advanced DHCP Solutions 116
Understanding DHCP Basics 116
Creating and Configuring DHCP Policies 117
Configuring DNS Registration 118
Creating and Configuring Superscopes 119
Creating and Configuring Multicast Scopes 121
Implementing DHCPv6 Scopes 122
Configuring High Availability for DHCP 124
Configuring Split Scopes 124

Configuring DHCP Failover 125
Configuring DHCP Name Protection 127
Business Case Scenarios 128

Lesson 12: Implementing an Advanced DNS Solution 129

Configuring Security for DNS 129
Configuring DNSSEC 129
Configuring DNS Socket Pool 132
Configuring DNS Cache Locking 132
Configuring DNS Logging 133
Configuring Delegated Administration 134
Configuring Recursion 134
Configuring Netmask Ordering 135
Configuring A GlobalNames Zone 136
Analyzing Zone Level Statistics 137
Business Case Scenarios 138

Lesson 13: Deploying and Managing IPAM 139

Configuring IPAM 139
Configuring an IPAM Server 140
Configuring IPAM Database Storage 142
Configuring Server Discovery 143
Creating and Managing IP Blocks and Ranges 143
Monitoring Utilization of IP Address Space 145
Migrating to IPAM 146
Delegating IPAM Administration 146
Managing IPAM Collections 147
Business Case Scenario 147

Lesson 14: Configuring a Domain and Forest 148

Implementing Complex Active Directory Environments 148
Implementing Multi-Domain Active Directory Environments 148
Implementing Multi-Forest Active Directory Environments 150
Upgrading Existing Domains and Forests 151
Understanding Functional Levels 152
Raising Domain Functional Levels 152
Raising Forest Functional Levels 153
Upgrading Windows Server 2008 and Windows Server 2008 R2 to Windows Server 2012 Domain Controllers 153
Configuring Multiple UPN Suffixes 154
Business Case Scenarios 155

Lesson 15: Configuring Trusts 156

Configuring Trusts 156
Understanding Trusts 156
Creating External Trusts 157
Creating Forest Trusts 159
Creating Shortcut Trusts 161
Creating Realm Trusts 163
Configuring Trust Authentication 165
Configuring Selective Authentication 166
Configuring Domain-Wide Authentication 167
Configuring Forest-Wide Authentication 167
Configuring SID Filtering 168
Configuring Name Suffix Routing 169
Business Case Scenarios 170

Lesson 16: Configuring Sites 172

Configuring Sites and Subnets 172
Configuring Sites 172
Configuring Subnets 173
Creating and Configuring Site Links 175
Site Link Bridges 175
Site Link Costs 178
Replication Interval 179
Replication Schedule 179
Managing Site Coverage 180
Automatic Site Coverage 180
Disable Automatic Site Coverage 180
Managing Registration of SRV Records 181
NETLOGON Service 181
NETLOGON.DNS 181
Moving Domain Controllers between Sites 182
Preparing the Domain Controller, DNS, and Environment 182
Business Case Scenarios 183

Lesson 17: Managing Active Directory and SYSVOL Replication 184

Managing Active Directory Replication 184
Controlling Active Directory Replication 184
Using the REPADMIN Command to Control Active Directory Replication 185
Using the Active Directory Sites and Services Tool to Control Active Directory Replication 185
Configuring Read-Only Domain Controllers 185
Configuring Replication to a Read-Only Domain Controller 186
Configuring Password Replication Policy for RODCs 188
Read-Only Domain Controller Security 188
Monitoring Replication 190
Monitoring Replication with REPADMIN 190
Monitoring Replication with Active Directory Replication Status Tool (ADREPLSTATUS) 191
Upgrading SYSVOL Replication to Distributed File System Replication (DFSR) 192
Understanding the FRS to DFSR Migration Process 192
Global States 192
Preparing the Domain for Migration 193
Business Case Scenarios 195

Lesson 18: Implementing Active Directory Federation Services 196

Understanding Active Directory Federation Services 196
Implementing AD FS 197
Installing AD FS 198
Creating a Standalone Federation Server 198
Implementing Claims-Based Authentication 200
Implementing Relying Party Trusts 203
Configuring Authentication Policies 204
Configuring Multi-Factor Authentication 205
Configuring Workplace Join 207
Business Case Scenarios 208

Lesson 19: Installing and Configuring Active Directory Certificate Services (AD CS) 209

Understanding the Active Directory Certificate Services 209
Installing an Enterprise Certificate Authority 209
Configuring AIA and CRL Distribution Points 213
Installing and Configuring Online Responder 215
Implementing Administrative Role Separation 217
Configuring CA Backup and Recovery 218
Business Case Scenarios 219

Lesson 20: Managing Certificates 220

Managing Digital Certificates 220
Managing Certificate Templates 221
Implementing and Managing Certificate Deployment, Validation, and Revocation 225
Using Manual Enrollment 225
Using CA Web Enrollment 226
Enrolling Using Enrollment Agents 226
Using Autoenrollment 228
Managing Certificate Renewal 228
Managing Certificate Enrollment and Renewal Using Group Policies 229
Configuring and Managing Key Archival and Recovery 230
Business Case Scenarios 233

Lesson 21: Installing and Configuring Active Directory Rights Management Services 234

Understanding Active Directory Rights Management 234
Understanding the Rights Management Processes 235
Installing a Licensing or Certificate AD RMS Server 236
Managing AD RMS Service Connection Point 240
Managing RMS Templates 241
Configuring Exclusion Policies 244
Backing Up and Restoring AD RMS 245
Business Case Scenarios 246

Configuring Network Load Balancing

LESSON 1

Configuring Network Load Balancing

THE BOTTOM LINE

Network Load Balancing (NLB) transparently distributes traffic across multiple servers by using virtual IP addresses and a shared name. With NLB, you gain fault tolerance and enhanced performance. It is often used with mission-critical web servers but can also be found with other types of servers.

A cluster has two or more servers, known as nodes. Each ***node*** runs a separate copy of the desired service application such as a web server, an FTP server, or a Secure Shell (SSH) / Remote Desktop Server. NLB is a scalable, high availability feature found in Windows Server 2012 and Windows Server 2012 R2. It is considered scalable because you add additional servers to meet increasing demand.

Windows Sever 2012 NLB clusters can have between 2 and 32 nodes. When you create an NLB cluster, you create a virtual network address and adapter that is assigned to the entire cluster. As network requests are sent to the virtual network address, the requests are distributed across the nodes in the cluster. Based on your needs, you can configure the cluster to even out the requests or you can configure one node to be preferred over another node.

All hosts in the NLB cluster receive the incoming traffic. However, only one node in the cluster accepts the traffic and the other nodes drop the traffic. The node that accepts the traffic is determined by the configuration of port rules and affinity settings, which is configured later in this lesson.

If a node fails, the node will no longer be able to accept requests. However, no service is lost because the other nodes are available to accept the request. When the node comes back online, it will start accepting requests and the traffic will be distributed among the nodes.

NLB can detect the failure of cluster nodes by sending packets known as ***heartbeats***. NLB cluster heartbeats are transmitted every second between nodes in the cluster. If a node misses five consecutive heartbeats, the node is automatically removed from the NLB cluster.

When a node is added or removed from a cluster, a process known as ***convergence*** occurs, in which the cluster determines its current configuration by building a membership of nodes and mapping clients requests based on the available nodes. Convergence can occur only if each node is configured with the same port rules.

Configuring NLB Prerequisites

Although editions of Windows Server 2012 R2 support NLB and NLB supports running different editions of Windows Server 2012 R2, it is best practice to use computers with similar hardware specifications that run the same version and edition of the Windows Server 2012 R2 operating system. However, if you are mixing Windows Server 2012 and Windows Server 2012 R2, you will need to manage the cluster from Windows Server 2012 R2 or administrative tools for Windows Server 2012 R2.

To support NLB, your systems must use the following requirements:

- All hosts in the cluster must reside on the same subnet.
- Within each cluster, all network adapters must be either multicast or unicast. You cannot have some nodes configured as multicast while other nodes are configured as unicast within a single cluster. We discuss multicast and unicast configuration later in the lesson.
- If unicast mode is used, the network adapter that is used to handle client-to-cluster traffic must support changing its media access control (MAC) address.
- The IP addresses assigned to the nodes must be static.

Although hosts can span multiple geographical areas, to achieve convergence successfully, the latency between nodes cannot exceed 250 milliseconds. If you need geographical dispersed NLB clusters, you should deploy an NLB cluster at each site and then use Domain Name System (DNS) round-robin to distribute traffic between sites.

Installing NLB Nodes

To install and configure an NLB node, you must first install NLB. Unlike most of the Windows components installed in the 70-410 and 70-411 exam, the NLB is a feature, and not a role. It is used to enhance other roles such as web services or Remote Desktop Services. After NLB is installed on each machine, you then have to create the cluster and add each host to the cluster.

To add the NLB feature to a computer running Windows Server 2012 or Windows Server 2012 R2, you use Server Manager. After the NLB feature is installed, you can then use the NLB Manager to configure the NLB cluster. Because an NLB is made of multiple computers, you need to install NLB on each server that will be part of the cluster.

INSTALL THE NETWORK LOAD BALANCING FEATURE

GET READY. To install the Network Load Balancing feature, perform the following steps:

1. On the task bar, click the Server Manager button to open the *Server Manager*.
2. At the top of *Server Manager*, click Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. On the *Select destination server* page, click Next.
6. On the *Select server roles* page, click Next.
7. On the *Select features* page, click to select the Network Loading Balancing and click Next.

8. When it asks you to add features required for NLB, click Add Features.
9. On the *Select features* page, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When the installation is complete, click Close.

CREATE A WINDOWS SERVER 2012 OR WINDOWS SERVER 2012 R2 NLB CLUSTER

GET READY. To install the Remote Access Role, perform the following steps:

1. On the task bar, click the Server Manager button to open the *Server Manager.*
2. Click Tools > Network Load Balancing Manager. The *Network Load Balancing Manager* opens as shown in Figure 1-1.

Figure 1-1

Opening the *Network Load Balancing Manager*

3. Right-click Network Load Balancing Clusters and click New Cluster. The *New Cluster: Connect* Wizard opens.
4. In the *Host* text box, type the name of the current server and click Connect.
5. The interface hosts the virtual IP address and receives the client traffic to load balance. Select an interface that you want to use for the cluster and click Next.
6. On the *Host parameters* page, you select a value in the *Priority (unique host identifier)* drop-down list. The parameter specifies a unique ID for each host. The host with the lowest priority handles all the cluster's network traffic not covered by a port rule.
7. In the *Dedicated IP addresses* section, verify that the dedicated IP address from the chosen interface is visible in the list and click Next.
8. On the *New Cluster: Cluster IP Addresses* page, click Add to enter the cluster IP address shared by every host in the cluster. NLB adds this IP address to each selected interface of all hosts chosen to be part of the cluster. Click Next.

9. On the *New Cluster: Cluster Parameters* page, type the full Internet name for the cluster. Then in the *Cluster operation mode* section, specify Unicast, Multicast, or IGMP multicast. Click Next.
10. On the *New Cluster: Port Rules* page, click Edit to open the *Add/Edit Port Rule* dialog box, as shown in Figure 1-2. Port rules define which incoming TCP/IP requests are balanced among the hosts in the NLB cluster. You can specify the cluster IP addresses or use the All option. In the *Port range* area, specify a range corresponding to the service you want to provide in the NLB cluster. For web access, use port 80 or 443. For Remote Desktop Services, use 3389.

Figure 1-2

Specifying the port rules

11. In the *Filtering mode* area, select Multiple host if you want multiple hosts in the cluster to handle network traffic for the port rule. If you want a single host to handle the network traffic for the port rule, choose Single host.
12. If you choose *Multiple host*, you can select None, Single, or Network. If you want multiple connections from the same client IP address to be handled by different cluster hosts, select None. If you want NLB to direct multiple requests from the same client IP address to the same cluster host, select Single (which is the default). If you want NLB to direct multiple requests from the local subnet to the same cluster host, click Network. Click OK to close the *Add/Edit Port Rule* dialog box.
13. After you define the port rules, click Finish.

To add additional hosts to the cluster, right-click the cluster in Network Load Balancing Manager and click *Add Host to Cluster*. You then select an interface for the cluster, configure the unique priority, and define port rules. After a host is added, convergence will occur (as shown in Figure 1-3). When convergence is complete, the host will participate in the cluster.

Figure 1-3

Showing a server (Server02) converging

Configuring Port Rules

Often after a cluster is created, you will need to further configure NLB. Most of these options are similar to the configuration that you performed while first creating the cluster. One of the items that you configured previously was the ***port rules***, which specify how NLB directs traffic based on the port and protocol.

With port rules, you can configure how requests to specific IP addresses and ports are directed by the NLB cluster. For example, you can load balance web traffic using TCP port 80 across all nodes in an NLB cluster, while directing all requests to TCP port 3389 to a specific host.

When you configure the port rules, you configure the following:

- The virtual IP address that the rule should apply to.
- The TCP or UDP port range that this rule should apply to.
- The protocols that this rule should apply to, including TCP, UDP, or both.
- The filtering mode that specifies how the cluster handles traffic, which is described by the port range and the protocols. Filtering mode is discussed in the next section.

To modify the port rules (including the filter mode and affinity), right-click the cluster in Network Load Balancing Manager and click *Properties*. When you click the *Port Rules* tab, select the defined port rule and click *Edit* to open the Add/Edit Port Rule dialog box.

Configuring Filtering Mode and Affinity

Affinity determines how the servers are going to balance the load. You use affinity settings when you use multiple hosts filter mode.

When you configure port rules, you first select the filter mode. The ***filter mode*** specifies which hosts can respond to requests. The filter mode includes the following:

- **Multiple hosts:** Permits all cluster hosts to actively respond to client requests. NLB nodes respond according to the weight assigned to each node. Because this allows the customizing of the affinity and load balancing, it is the most common mode used. Multiple host filtering increases availability and scalability, because you can increase capacity by adding nodes, and the cluster continues to function in the event of node failure.
- **Single host:** Allows only one cluster host (the host with the highest priority) in the cluster to actively respond to client requests. If the host fails, the host with the next highest priority takes over for the failed host. It is usually used to configure one host as the primary server and other hosts as backup servers. Single host rules increase availability, but do not increase scalability.
- **Disable:** Prevents the cluster from responding to a specific type of client traffic.

If you choose the multiple host filtering mode, you can then configure the affinity. When you configure affinity, you can choose one of the three options:

- **None:** Any cluster node responds to any client request, even if the client is reconnecting after an interruption. This option is suitable for stateless application, where the server that is servicing the request does not have to remember the previous events to complete the request. As a result, the client can jump from one server to another within the cluster without problem.
- **Single:** A single cluster node handles all requests from a single client. This option is useful for stateful applications where the status of a process or transaction is maintained through the entire connection including when using SSL and e-commerce shopping cart applications.
- **Class C:** A single node responds to all requests from a class C network (a network with a subnet of 255.255.255.0), often found when used with multiple proxy servers. This type of server is often used with cookie-based affinity or when a common database or session state server is used.

Each node in a cluster must have identical port rules. The only exception is the load weight when in multiple-hosts filter mode and handling priority in single-host filter mode. If the port rules are not identical, the cluster will not converge.

To modify the port rules for an individual host, right-click the host in the left pane and click *Host Properties*. Then, click the *Port Rules* and click *Edit* to open the Add/Edit Port Rule dialog box. To specify a different load weight while in multiple host, click to deselect the *Equal* option and then specify the load weight. If you are in Single host, specify the handling priority.

When creating port rules, the number and type of rules must be the same for each host in the cluster. If a host attempts to join the cluster with a different number of rules than the other hosts, it is not accepted as part of the cluster, and the rest of the cluster continues to handle the traffic as before.

Configuring Cluster Operation Mode

On the Cluster Parameters tab, you configure the virtual IP address, subnet mask, and DNS name that the cluster will use. You also can configure the cluster operation mode, which specifies whether a multicast MAC address should be used for cluster operations.

When a host communicates with another host, the host uses unicast or multicast packets. When communicating using ***unicast***, each packet is sent to a single network destination identified by a unique address. In other words, a host sends packets to a single computer.

With ***multicast***, packets are sent to multiple computers simultaneously in a single transmission from the source. In other words, when a host sends packets using multicasting, a single set of packets is sent to all computers at once. Copies are automatically created on routers, when the packet needs to go to different subnets. If you have five hosts on the same subnet, and two hosts on another subnet, one set of packets is sent from the source host. When the packets get to a router where the packets need to be sent through two different pathways, the packets are copied and sent to the two separate subnets. When the first set of packets gets sent to the subnet with five hosts, only one set of packets gets sent to all five hosts. The second set of packets gets sent to the subnet with two hosts, and only one set of packets gets sent to the two hosts.

When you configure an NLB cluster to use ***unicast mode***, NLB replaces the network card's original MAC address and all cluster hosts use the same unicast MAC address. When you use unicast mode with a single network adapter on each node, the computer can communicate only with other computers within the same subnet. If you perform management tasks on the computer, you need to perform these tasks on a computer that is on the same TCP/IP subnet as the node, or you have to use a second network adapter and address. Lastly, if you use unicast mode, you can use separate virtual local area networks (VLANs) for cluster traffic and management traffic.

When an NLB host is in ***multicast mode***, each NLB network adapter has two MAC addresses (the original MAC address and the virtual MAC address). However, when using multicast mode, some routers might see a unicast IP address with a multicast MAC address as an invalid packet and reject the update to the ARP table. If this happens, the network administrators might need to manually add ARP entries to the router.

In summary, if your system has two network cards, you should use unicast. If a server has only a single network card, you should use multicast mode.

Another mode available is the ***Internet Group Management Protocol Multicast mode***, which is a special form of multicast mode that prevents the network switch from flooding with traffic. When you use IGMP multicast mode, traffic is forwarded only through the switch ports that are part of the NLB cluster. However, to use IGMP multicast mode, you need switch hardware that supports IGMP multicast mode.

To modify the cluster operation mode, right-click the cluster in the Network Load Balancing Manager and click *Cluster Properties*. On the Cluster Parameters, you can modify the cluster IP address, subnet mask, full Internet name, and cluster operation mode.

Upgrading an NLB Cluster

There are two ways to upgrade a Windows Server 2008 R2 with SP1 or Windows Server 2012 NLB cluster to Windows Server 2012 R2. It includes upgrading all the hosts at one time or upgrading each host, one at a time.

The quickest upgrade path is to take the entire cluster offline and perform a rolling upgrade. Of course, if you use this method, the cluster is not available. If you require no down-time, you can upgrade each individual cluster host, one at a time. As you upgrade each node, you should first perform a drainstop for the host so that any pending client requests are finished before the upgrade.

■ Business Case Scenario

Scenario 1-1: Upgrading an NLB Cluster

You are the administrator for several web servers that make up the NLB cluster. They run on servers with Windows Server 2008 R2. Explain the best way to upgrade the NLB cluster to Windows Server 2012 R2 without any downtime.

Configuring Failover Clustering

LESSON 2

Understanding Failover Clustering

THE BOTTOM LINE

A ***failover cluster*** is a set of servers that work together to increase the availability of services and applications. The clustered servers (called ***nodes***) are connected through a network connection (physical or virtual) and by software. If one of the nodes fails, another node begins to provide services (a process known as *failover*). Failover clusters can be used for a wide range of network services including database applications such as Exchange Server or SQL Server, file servers, or network services such as Dynamic Host Control Protocol (DHCP) services.

The most common failover cluster is the ***active-passive cluster***. In an active-passive cluster, both servers are configured to work as one, but only one at a time. The active node provides the network services whereas the passive node waits for something to happen to the active node where it cannot provide network services. If the active node goes down, the passive node becomes the active node and resumes providing the network services. When the failed node is restored, it becomes the passive node.

Active-passive clusters provide high availability but do not provide scalability. The only exception to the scalability issue is if you implement file servers on Cluster Shared Volumes (CSV), which are discussed later in this chapter. If you need higher performance, you can typically reduce the load or use more powerful hardware for the individual nodes.

Another type of failover cluster is the active-active cluster that is designed to provide fault tolerance and load balancing. Network services are split into two groups. One cluster node runs one set of network services while the other cluster node runs the other set of network services. Both nodes are active. If one of the nodes fails, the remaining node will take over providing all the network services.

Failover clustering is best suited for stateful applications that are derived from a single set of data. For example, a database is stored in a single location and there can be only one database instance running.

To create a failover using Windows Server 2012 R2 you need a minimum of two servers (physical or virtual) that meet the minimum requirements of Windows Server 2012 R2 and that have identical hardware components. In addition, the servers must run the same version and edition, including the same hardware version, 64-bit, and the servers should have the same software updates and service packs. The servers must also be part of the same domain.

When you create the cluster, you assign network resources to the cluster, which can be enabled or disabled when the node is active or inactive. Every cluster has a ***cluster virtual server*** assigned, which includes the network name, and IP address assigned to it.

Clustered services are services or applications that are made highly available by installing them on a failover cluster. Clustered services are active on one node, but can be moved to another node.

A ***cluster resource*** is the most basic and smallest configurable unit that may provide a service to clients, or is an important component that makes up the cluster. It can be a network application server or hardware device, such as a storage device, that is defined and managed by the cluster server. At any time, a resource can run only on a single node in a cluster, and is online on a node when it provides its service to that specific node.

So if you have an active-passive cluster, the active node will have the cluster virtual server with a virtual IP address, and cluster resources (resources that you are providing and making fault tolerant with the cluster). When the active cluster goes offline, the passive cluster becomes the active passive and the resources switch over to the new active node.

A ***dependent resource*** is a resource that depends on or is required by another resource to operate. For example, because a network name must be associated with an IP address, a network name is considered a dependent resource.

To perform graceful failover from one node to another node, the dependent resources are taken offline before the resources upon which they depend are taken offline. When the resources are brought online, the resources that are required for the other services to function are brought online first. A resource can specify one or more resources on which it is dependent. Resource dependencies also determine bindings. For example, clients are bound to the particular IP address on which a network name resource depends.

A failover cluster consists of the following components:

- **Nodes:** Servers that make up the cluster and that run the Cluster service. They host the resources and applications associated to cluster.
- **Network:** A common network that connects the cluster nodes. Three types of networks can be used in a cluster: public, private, and public-and-private.
- ***Cluster storage*:** A storage system that is shared between cluster nodes and usually connects using fiber channel or iSCSI.
- **Clients:** Computers (or users) that use the Cluster service.
- **Cluster service:** The service that runs on Windows servers that manages and coordinates cluster resources to provide high availability.

Installing and Configuring Failover Clustering

To create a cluster, you first install the Failover Cluster feature. You then validate your hardware configuration, and create a cluster using the Failover Cluster Manager.

TAKE NOTE*

If you have previously installed Network Load Balancing (NLB) and have it running, you should remove this feature. In addition, you should also remove any secondary addresses where the same address is used by the same server.

CONFIGURING CLUSTER NETWORKING

Failover clustering uses only IP-based protocols and is, therefore, suited only to IP-based applications. Failover clustering now supports both IPv4 and IPv6.

When you connect the cluster to the network, you should consider using the following networks:

- ***Private network:*** Used by cluster nodes to communicate with each other.
- ***Public network:*** Used by the clients to access the cluster and its shared resources.
- ***Public-and-private network:*** Used to communicate with external storage systems.

Similar to a Network Load Balancing (NLB) cluster, a failover cluster has full connectivity and communication with the other nodes in the cluster using a private network. In addition, the cluster is aware when a node is added or removed from the cluster. Cluster nodes are kept aware of the status of the other nodes and services through the use of ***heartbeats***. Heartbeats transmit and receive using UDP port 3343 unicast (legacy clusters used UDP broadcast).

Each node of the cluster has a computer name and IP address. In addition, the cluster has a cluster name and cluster IP address. When users connect to the cluster, the users connect using the cluster name and cluster IP address. Therefore, no matter which node is active, users connect to the active node.

Because clusters usually need to access shared storage, the cluster should have a public-and-private network to communicate with the shared storage. If the cluster communicates to shared storage using Fibre Channel, the Fibre Channel will connect using a dedicated network known as a *fabric*. If the cluster connects to shared storage using iSCSI, you can use the public network or use a dedicated public-and-private network to handle iSCSI traffic. Sharing a public network can cause contention and latency issues for the users and the shared resources. However, you can use the public network for a test network.

The Windows Server 2012 R2 Failover Cluster uses a virtual network adapter called ***Microsoft Failover Cluster Virtual Adapter*** to communicate between nodes in the cluster. It is assigned an APIPA address (169.254.0.0/16) and an fe80::/10 prefix. The Microsoft Failover Cluster Virtual Adapter is used as an alternative network if the private network or connection fails.

INSTALLING AND CREATING A FAILOVER CLUSTER

Initially installing a failover cluster is a three-step process:

1. Install the Failover Clustering feature.
2. Validate the cluster configuration.
3. Create the cluster.

You must first install the Failover Clustering feature, which installs the Failover Cluster Manager. You can then use the Failover Cluster Manager to validate the cluster configuration and create the cluster. When you validate the cluster configuration of servers and components that will make up the cluster, you are validating whether everything is compatible with a cluster and that you have the minimum to make a cluster. The four main tests include inventory, network, storage, and system configuration.

INSTALL THE FAILOVER CLUSTERING FEATURE

GET READY. To install the Failover Clustering feature, perform the following steps:

1. On the task bar, click the Server Manager button to open the *Server Manager*.
2. At the top of *Server Manager*, click Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. On the *Select destination server* page, click Next.
6. On the *Select server roles* page, click Next.
7. On the *Select features* page, click to select the Failover Clustering and click Next.
8. When you are asked to add features required for Failover Clustering, click Add Features.
9. Back on the *Select features* page, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When the installation is complete, click Close.

VALIDATE CLUSTER CONFIGURATION

GET READY. To validate the cluster configuration, perform the following steps:

1. Open Server Manager.
2. Click Tools > Failover Cluster Manager. The *Failover Cluster Manager* opens as shown in Figure 2-1.

Figure 2-1

Opening the *Failover Cluster Manager*

3. In the *Actions* pane, click Validate Configuration. The Validate a Configuration Wizard starts.
4. On the *Before You Begin* page, click Next.
5. In the *Enter* name, type the name of the first server in the cluster such as Server01 and then click Add. Repeat for other servers that will be used within the cluster. After the computers have been added, click Next.
6. With *Run all tests (recommended)* selected, click Next.
7. On the *Confirmation* page, click Next.
8. When the testing is done, the *Summary* page appears. Click View Reports. The *Failover Cluster Validation Report* opens.
9. Close the report.
10. After the cluster has been validated, the *Create Cluster Wizard* opens. For now, click Cancel to close the wizard.

CREATE A CLUSTER

GET READY. To create a cluster, perform the following steps:

1. With the Failover Cluster Manager already open, in the *Actions* pane, click Create Cluster. The *Create Cluster Wizard* opens.
2. On the *Before You Begin* page, click Next.
3. On the *Select Servers* page, type the name of the first server of the cluster and click Add. Repeat for the other nodes of the cluster. When done, click Next.
4. On the *Access Point for Administering the Cluster* page, type the name of the cluster such as Cluster1.contoso.com in the *Cluster Name* text box.
   In the *Click here to type an address* text box, type the address that will be assigned to the entire cluster and click Next.
5. When the *Confirmation* page appears, click Next.
6. When the cluster is created, click Finish.

CONFIGURING CLUSTER STORAGE

Most failover clusters use shared storage to provide consistent data to all cluster nodes. There are three shared-storage options for a failover cluster:

- **Shared serial attached SCSI (SAS):** A low-cost option that requires the cluster nodes to be physically close to the drives. Typically, the SAS has a limited number of connections for cluster nodes.
- **Internet SCSI (iSCSI):** A type of storage area network (SAN) that transmits SCSI commands over an IP network. iSCSI drives can be connected to a Windows server using the iSCSI initiator, which is included with Windows Server 2012 R2.
- **Fibre Channel:** A form of SAN technology that is based on fibre optics. It typically offers better performance than iSCSI SANs but is more expensive because it requires specialized equipment.
- **Fibre Channel over Ethernet (FCoE):** A form of SAN technology that uses the Fibre Channel protocol using 10 Gigabit Ethernet networks or higher on a converged network.

To use a shared disk, you must use the following guidelines:

- For the disk type, use basic disks, not dynamic disks.
- For the file system type, format the disk as New Technology File System (NFTS).
- For the partition style of the disk, you can use either master boot record (MBR) or globally unique identifier (GUID) partition table (GPT).
- The storage device must follow the SCSI Primary Commands-3 (SPC-3) standard including supporting Persistent Reservations.
- The miniport driver used for the storage must work with the Storport storage driver.
- A storage device can be assigned to only one cluster. This is usually accomplished with logical unit number (LUN) masking or zoning.

Before you add storage to a cluster, be sure that all nodes can see the storage device and that the storage device has been initialized, partitioned, and formatted and that the same drive letter is assigned to the storage device on all nodes.

ADD A SHARED DRIVE TO THE CLUSTER

GET READY. To add a shared drive to a cluster, perform the following steps:

1. Using Server Manager, open Failover Cluster Manager.
2. In the left pane, expand the cluster, expand Storage, and click Disks. The available shared disks are displayed.

3. Right-click Disks and click Add Disk.
4. When the *Add Disks to a Cluster* dialog box opens, select the disks that you want to include and click OK.

Configuring and Optimizing Clustered Shared Volumes (CSVs)

Traditionally, a single node controls a LUN on the shared storage. However, starting with Windows Server 2008 R2, Windows can use a ***Cluster Shared Volume (CSV)***, which allows multiple nodes to share a single LUN concurrently. Instead of taking control of the entire LUN, a node takes control of an individual file. With CSV, a clustered role can fail over quickly from one node to another node without requiring a change in drive ownership or without dismounting and remounting a volume. After a disk has been added to a CSV, the volumes appear as Cluster Shared Volume File System (CSVFS).

After a disk has been added to a CSV, the volumes appear as Cluster Shared Volume File System (CSVFS). Because volumes appear as CSVFS, applications can quickly see that the volume is a CSV; as a result, the applications know how to handle the volume. To make the volumes available to all cluster nodes, the volumes use a single file namespace, using the same name and path on any node in a cluster.

To use CSV:

- The disk or storage space must be a basic disk.
- If you want to use storage space for a CSV, Windows Server 2012 supports simple space or a mirror space, while Windows Server 2012 R2 can also be configured as a parity space. Storage spaces are discussed in the "Configuring Storage Spaces" section later in this lesson.
- On all nodes, the drive letter for the system disk must be the same.
- The NTLM protocol must be enabled on all nodes. This is enabled by default.

A CSV cannot be used as a quorum witness disk and you cannot use disk compression.

To add storage to the CSV, you must make the LUN available as shared storage to the cluster and add the shared disk to the cluster. When you add a disk to CSV, the LUN's drive letter or mount point is removed. It should also be noted that you cannot add shared storage to CSV if it is in use.

ADD A VOLUME TO CSV

GET READY. To add a volume to CSV, perform the following steps:

1. Open Failover Cluster Manager.
2. Expand the Storage node and click the Disks node.
3. Right-click the volume that you want to convert to a Cluster Shared Volume and choose Add to Cluster Shared Volumes. To convert a volume from Cluster Shared Volumes, right-click the CSV and choose Remove from Cluster Shared Volumes.
4. When prompted to confirm this action, click Yes.

With Windows Server 2012, one node is the coordinator node or owner for CSV. The coordinator node owns the physical disk resources associated with a LUN, including all I/O operations. With Windows Server 2012 R2, the CSV ownership is automatically distributed and rebalanced across the failover cluster nodes based on the number of CSVs that each node owns. Ownership is automatically rebalanced when a CSV failover occurs, a node rejoins the cluster, a new node is added to the cluster, a cluster node is restarted, or failover is started after being shut down.

In Windows Server 2012, there was only one instance of the Server service per node. With Windows Server 2012 R2, there are multiple Server service instances per failover cluster node so that the default instance can handle incoming traffic from Server Message Block (SMB) clients that access regular file shares and another CSV instance can handle the inter-node CSV traffic.

Problems with the Server service will impact the CSV coordinator node to accept I/O requests from other nodes and to perform the orchestration of metadata updates. In Windows Server 2012 R2, if the Server service becomes unhealthy on a node, CSV ownership will be automatically transitioned to another node.

In Windows Server 2012 R2, you can view the state of a CSV on a per-node basis, including where I/O is direct or redirected or whether the CSV is unavailable. If the CSV is in I/O redirected mode, you can view the reason. To view the state information and the redirection reason, use the Windows PowerShell cmdlet `Get-ClusterSharedVolumeState`.

In Windows Server 2012, the CSV cache (which is a write-through cache) was disabled by default. Also, you could allocate only 20 percent of the total physical RAM to the CSV cache. In Windows Server 2012 R2, however, you can allocate up to 80 percent. Increasing the CSV cache limit is more beneficial for Scale-Out File Server scenarios.

To control the CSV cache, use the following configuration properties:

- `CsvEnableBlockCache`: Allows you to enable CSV Cache on an individual disk. The default setting is 0 for disabled. Setting to a value of 1 enables CSV Block Cache on that disk.
- `SharedVolumeBlockCacheSizeInMB`: Defines how much memory (in megabytes) you wish to reserve for the CSV Cache on each node in the cluster. Configuring a value of 0 disables CSV Block Cache.

To change the CSV cache, use the following Windows PowerShell command:

```
(Get-Cluster).BlockCacheSize = XXX
```

whereby *XXX* is the number in MB.

Configuring Quorum

A ***quorum*** is used with a failover cluster to determine the number of failures that the cluster can sustain. If a quorum (the majority of the votes) is not reached, the cluster will stop running. Each voting element contains a copy of the cluster configuration, and the Cluster service works to keep all copies synchronized at all times.

For example, if a cluster has five nodes, it needs three nodes running to have a majority. Therefore, two nodes can fail and the cluster will still continue to function. If there is an even number of nodes, then the cluster needs to have a witness assigned to the cluster to break the tie. The witness can be either a disk or a file share.

A cluster protects against only hardware failure such as a server with a faulty power supply, motherboard, or processor. A quorum will not protect if a remaining cluster node does not have the resources to run properly such as sufficient disk space, processing power, random access memory (RAM), or network bandwidth.

For a simple failover cluster that has only two nodes, you want to configure a quorum drive. Therefore, you will need to add a shared drive that is seen by all nodes.

When you configure the quorum, there are four possible quorum configurations:

- **Node Majority:** Recommended for clusters with an odd number of nodes. It can sustain failures of half the nodes (rounding up) minus one.
- **Node and Disk Majority:** Recommended for clusters with an even number of nodes. It can sustain failures of half the nodes (rounding up) if the disk witness remains online.
- **Node and File Share Majority:** Used for clusters with special configurations. Instead of using a disk witness, it uses a file share witness.
- **No Majority (Disk Only):** Allows the cluster to function as long as one node is available and the disks are online. However, this configuration is not recommended because the disk might be a single point of failure.

If you use a witness disk, the disk must be at least 512 MB. It must be dedicated for cluster use and not assigned to a clustered role. It cannot be a volume that is a CSV.

In Windows Server 2012, you had to configure a witness and manually adjust the quorum configuration if node membership changed so that you would keep the total number of votes as an odd number. With Windows Server 2012 R2, to reduce the risk that a cluster will go down because of the witness failure, by default, the cluster determines quorum management options, including the quorum witness. Therefore, if you have an odd number of votes, the quorum witness does not have to vote; if you have an even number of votes, the quorum witness has a vote. In addition, if the witness resource is offline or has failed, the cluster sets the witness vote to "0".

In Windows Server 2012, you had to run the Validate Quorum Configuration validation report or use Windows PowerShell to view the vote status. In Windows Server 2012 R2, you can view the assigned quorum vote and the current quorum vote for each cluster node in the Failover Cluster Manager user interface (UI) by clicking the Nodes node. However, the quorum mode terminology–such as node majority (no witness), node majority with witness (disk or file share) or no majority (disk witness only)–are not longer being used.

A value of "0" indicates that the witness does not have a vote. A value of "1" indicates that the witness has a vote.

CONFIGURE THE CLUSTER QUORUM SETTINGS USING TYPICAL SETTINGS

GET READY. To configure the Cluster Quorum settings using typical settings, perform the following steps:

1. Open Server Manager, and then open Failover Cluster Manager.
2. In the left pane, right-click the cluster, click More Actions, and click Configure Cluster Quorum Settings.
3. When the *Configure Cluster Quorum Wizard* starts, click Next.
4. On the *Select Quorum Configuration Option* page, verify that Use typically settings (recommended) is already selected. Click Next.
5. On the *Confirmation* page, click Next.
6. On the *Summary* page, click Finish.

ADD OR CHANGE THE QUORUM WITNESS

GET READY. To add or change the Cluster Quorum settings, perform the following steps:

1. Open Server Manager, and then open Failover Cluster Manager.
2. In the left pane, right-click the cluster, click More Actions, and then click Configure Cluster Quorum Settings.

3. When the *Configure Cluster Quorum Wizard* starts, click Next.
4. On the *Select Quorum Configuration Option* page, click Add or change the quorum witness and click Next.
5. On the *Select Quorum Witness* page, click Configure a disk witness, and click Next.
6. On the *Configure Storage Witness* page, click the drive to be used as a storage witness and click Next.
7. On the *Confirmation* page, click Next.
8. On the *Summary* page, click Finish.

In Windows Server 2012, when a partition failed, and you manually restarted any partitioned nodes that were not part of the forced quorum subset by using the /pq switch to prevent quorum. With Windows Server 2012 R2, if you manually force quorum to start the cluster (such as when you start the Cluster service with the /fq switch), the partition that you started with force quorum is considered authoritative. However, when the partition nodes are brought back online, the partitioned nodes automatically restart the Cluster service and the partitions are joined back to the cluster.

In Windows Server 2012 R2, when a node fails, you can now specify which node is removed for a quorum vote (by specifying the `LowerQuorumPriorityNode` ID property).

To set the property, run the following Windows PowerShell command (whereby node 1 is considered less critical):

```
(Get-Cluster).LowerQuorumPriorityNodeID = 1
```

Configuring Storage Spaces

As you recall from the 70-410 exam, you can group local disks–USB, Serial ATA (SATA) or Serial Attached SCSI (SAS)–into storage pools and then create virtual disks called ***Storage Spaces*** from the available capacity in the storage pools. Storage Spaces can also provide resiliency (such as using mirroring or parity) and scalability. You can deploy clustered storage spaces by using Storage Spaces and Failover Clustering to provide solutions that are resilient, highly available, and cost efficient.

Although you cannot use a storage space to host the Windows system drive, you can use clustered storage spaces to help protect against the following:

- Physical disk failures
- Data access failures
- Data corruptions and volume unavailability
- Server node failures

By using CSVs, you can combine the storage access into a single namespace, which all cluster nodes can access at the same time, and you can easily take a server offline for maintenance.

To deploy clustered storage spaces, you will need a small collection of servers and a set of shared Serial Attached SCSI enclosures, which must be connected to all servers with redundant paths. All physical disks used to create a clustered pool must pass the failover cluster validation tests. Clustered storage spaces must use fixed provisioning. Simple and mirror storage spaces are supported, but Parity Spaces are not supported. Storage spaces formatted with ReFS cannot be added to the CSV.

CONFIGURE A CLUSTERED STORAGE SPACE

GET READY. To configure a Clustered Storage Space, perform the following steps:

1. Using *Server Manager*, click Manage > Add Roles and Features.
2. On the *Before You Begin* page, click Next.
3. On the *Select installation type* page, click Next.
4. On the *Select destination server* page, click the server to which you want to install and then click Next.
5. On the *Select server roles* page, click the File Server role and then click Next.
6. On the *Select features page*, click Next.
7. On the *Confirm installations selections* page, click Install.
8. When the installation is complete, click Close.
9. Using *Server Manager*, click Tools > Failover Cluster Manager.
10. In the left pane, expand the cluster node, expand the Storage node, and then click the Pools node (see Figure 2-2).

Figure 2-2

The Pools node

11. Right-click Pools and choose New Storage Pool.
12. On the *Before You Begin* page, click Next.

13. On the *Storage Pool Name* page, in the *Name* text box, type the name of the storage pool. Then select the storage subsystem that is available to the cluster and click Next.
14. Select a minimum of three physical disks and then click Next.
15. On the *Confirmation* page, click Create.
16. Once the storage pool is created, click Close.
17. Right-click the storage pool and choose New Virtual Disk.
18. On the *Before You Begin* page, click Next.
19. On the *Storage Pool* page, select the server and storage pool for the virtual disk and then click Next.
20. On the *Virtual Disk Name* page, in the *Name* text box and the *Description* text box, provide a name and description for the virtual disk and then click Next.
21. On the *Storage Layout* page, specify the desired *Storage Layout* (Simple or Mirror). Remember, parity is not supported in a failover cluster. Click Next.
22. On the *Size* page, specify the size of the virtual disk and then click Next.
23. On the *Confirmation* page, click Create.
24. Once the virtual disk is created, the *Create a volume when this wizard closes* option is already selected. Click Close.
25. On *Before You Begin* page, click Next.
26. On the *Server and Disk* page, verify the correct selection of the disk and server that must be provisioned and then click Next.
27. On the *Size* page, specify the size of the volume and then click Next.
28. On the *Drive Letter or Folder* page, select the desired drive letter and then click Next.
29. On the *File System Settings* page, select the file system settings and then click Next.
30. On the *Confirmation* page, click Create.

    The new volume will be created on the virtual disk and will be added to the failover cluster.

Configuring Clusters Without Network Names

Windows Server 2012 R2 introduced ***Active Directory-detached cluster***, which allows you to deploy a failover cluster without any dependencies in Active Directory Domain Services (AD DS) for network names. When you create an Active Directory-detached cluster, you register the cluster network names with the network names of the clustered roles to your DNS servers without creating computer objects in AD DS.

Active Directory-detached clusters simplifies the process of deploying, managing, and maintaining your failover cluster. Because the hosts of an Active Directory-detached cluster are joined to an Active Directory domain, Kerberos authentication is used when performing inter-node cluster communications, However, when accessing the cluster network name—which does not have an Active Directory account—NT LAN Manager (NTLM) authentication is used when communicating with the cluster as a whole.

If the cluster applications require Kerberos authentication, it is not recommended to use Active Directory-detached clusters. Therefore, you should consider the following:

- Since the Server Message Block (SMB) traffic recommends using Kerberos, you should not use Active Directory-detached clusters.
- If you require live migration, which requires Kerberos authentication, you should not use Active Directory-detached cluster for Hyper-V.

- Since Message Queuing stores properties in AD DS, you cannot use Active Directory-detached clusters.
- If you have an Active Directory-detached cluster with a SQL server, you should use SQL Server authentication.
- BitLocker Drive Encryption is not supported with Active Directory-detached clusters.
- Cluster-Aware Updating (CAU) in self-updating mode is not supported with Active Directory-detached clusters. However, CAU is supported in remote-updating mode.
- If you deploy a highly available file server by using this deployment method, you cannot use Server Manager to manage the file server. Instead, you must use Windows PowerShell or Failover Cluster Manager.
- After you create the cluster, you cannot change the cluster to an Active Directory-detached cluster or an Active Directory-attached cluster.

Before you create the failover cluster, you must ensure that all servers that you want to add as cluster nodes meet the following prerequisites:

- All servers must be running Windows Server 2012 R2.
- All servers must be joined to the same Active Directory domain.
- All servers must have the Failover Clustering feature installed.
- All servers must use supported hardware and the collection of servers must pass all cluster validation tests.

To deploy an Active Directory-detached cluster, you must create the failover cluster with the Windows PowerShell `New-Cluster` cmdlet with the

`-AdministrativeAccessPoint` parameter set to a value of `Dns`.

For example, to create a failover cluster called Cluster1 using the two nodes (Node1 and Node2) and using an administrative access point of type DNS (Active Directory-detached), use the following command:

```
New-Cluster Cluster1 –Node Node1,Node2 –StaticAddress 192.168.1.16
-NoStorage –AdministrativeAccessPoint Dns
```

To verify the type of administrative access point for a failover cluster, use the following Windows PowerShell command:

```
(Get-Cluster).AdministrativeAccessPoint
```

Implementing Cluster-Aware Updating

Applying Windows updates to nodes in a cluster always needs more attention and planning because having one update on one node and not on the other node can cause problems or corruption of data. If you don't want downtime, you must move resources manually from the node that you are updating, perform the updates on the first node, and then change the resources to another node and perform the updates on the next node. Starting with Windows Server 2012, ***Cluster-Aware Updating (CAU)*** lets administrators update cluster nodes automatically, with little or no downtime, particularly if you use Hyper-V with live migration.

You can use CAU in one of the following two modes:

- Remote-updating mode
- Self-updating mode

With remote-updating mode, you install the failover clustering administrative tools on a CAU orchestrator (a remote computer running Windows 8.1 or Windows Server 2012 R2 that is not a member of the cluster). The CAU is included in the Remote Server Administration Tool (RSAT). The administrator triggers the update process on the orchestrator computer. Remote-updating mode is useful for monitoring real-time progress during the Updating Run, and for clusters that run on Server Core installations of Windows Server 2012 R2.

With self-updating mode, the CAU (installed on a node on the cluster) updates the cluster at scheduled times by using a default or custom Updating Run profile. During the Updating Run, the CAU orchestrator process starts on the node that currently owns the CAU clustered role, and the process sequentially performs updates on each cluster node. You can use a self-updating mode, which allows the CAU to update the failover cluster by using a fully automated, end-to-end updating process, or you can trigger the updates manually. When using self-updating mode, you can check the progress of updates by connecting to the cluster and running the `Get-CauRun` Windows PowerShell cmdlet.

UPDATE THE SERVER USING CLUSTER-AWARE UPDATING

GET READY. To update the server using Cluster-Aware Updating, perform the following steps:

1. Open Server Manager, and then open Cluster-Aware Updating. The *Cluster–Aware Updating* dialog box opens.
2. Click the Connect to a failover cluster option and select your cluster. Click Connect. The cluster nodes appear.
3. To install the cluster-aware role on the cluster, click Configure cluster self-updating options.
4. When the *Configure Self-Updating Options Wizard* starts, click Next.
5. Click the Add the CAU clustered role, with self-updating mode enabled, to this cluster and click Next.
6. On the *Specify self-updating schedule* page, specify how often it should do self-updating and when it should occur. Click Next.
7. On the *Advanced Options* page (see Figure 2-3), you can modify the options that define how self-updating runs. Click Next.

Figure 2-3

Modifying advanced options

8. If you want recommended updates, click Give me recommended updates the same way that I receive important updates option and click Next.
9. On the *Confirmation* page, click Apply.
10. On the *Completion* page, click Close.
11. To manually apply updates, click Apply updates to this cluster.
12. When the *Cluster-Aware Updating Wizard* starts, click Next.
13. On the *Confirmation* page, click Update.
14. When the scheduling of the immediate updating is successful, click Close.

Upgrading a Cluster

If you have a cluster running on Windows Server 2008 or Windows Server 2008 R2, and you want to upgrade Windows to Windows Server 2012 or Windows Server 2012 R2, upgrading a cluster is more difficult if you want little or no downtime. Therefore, in these situations, you need to plan your upgrade.

To replace cluster nodes or upgrade to a newer version of Windows, you need to migrate cluster roles or services from one cluster to another. You can migrate clusters running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. You can migrate these roles and configuration in one of the two ways:

- Migrate from an existing cluster to a new cluster that is running Windows Server 2012 or Windows Server 2012 R2
- Perform an in-place migration on a two-node cluster

When you migrate from an existing cluster to a new cluster, you create a new cluster consisting of two cluster nodes running Windows Server 2012 R2. You then migrate from the existing cluster to the new cluster.

To perform an in-place migration on a two-node cluster, you actually perform a migration when you don't have extra computers to form a new cluster. Instead of migrating to a new cluster, you basically upgrade to Windows Server 2012 R2. To accomplish this, perform the following:

1. Remove resources from one node and evict that node from a cluster.
2. Perform a clean installation of Windows Server 2012 R2 on the evicted server.
3. Create a one-node failover cluster.
4. Migrate the clustered services and applications from the old cluster node to the new one-node failover cluster.
5. Remove the old node from the cluster.
6. Install Windows Server 2012 R2 on the second cluster node and configure the failover cluster features.

To perform the actual migration, use the Cluster Migration Wizard. Because the Cluster Migration Wizard does not copy data from one storage location to another, you must copy or move data or folders (including shared folder settings) during a migration. Although you can migrate physical disk resource settings to and from disks that use mount points, you cannot migrate mount-point information that do not use drive letters, and are mounted in a folder on another hard disk drive.

RUN THE MIGRATE A CLUSTER WIZARD

GET READY. To run the Migrate a Cluster Wizard, perform the following steps:

1. On a node of the new cluster, use Server Manager to open the *Failover Cluster Wizard*.
2. Right-click the cluster, click More Actions, and click Migrate Roles.
3. When the *Migrate a Cluster Wizard* starts, click Next.
4. On the *Specify Old Cluster* page, type the name of the cluster or a name of one of the cluster nodes in the *Cluster or cluster node to migrate from* text box and click Next.
5. On the *Select Services and Applications* page, select the resources that you want to migrate and click Next.
6. On the *Customize Virtual Machine Networks*, select the virtual network switch and click Next.
7. On the *Confirmation* page, click Next.
8. When the wizard is complete, click Finish.

At this point, the target cluster is ready to take over. So during a scheduled maintenance window, you need to shut down all servers on the old cluster, configure the storage, and start the servers on the Windows Server 2012 R2 cluster.

Backing Up and Restoring Failover Cluster Configuration

Because configuring a cluster is time-consuming and sometimes complex, it is important that you back up the cluster configuration. You can back up the cluster configuration and restore using Windows Server Backup or a non-Microsoft Backup tool.

Before you put a cluster into production, you should test failover to make sure it is functioning properly. In addition, be sure that each node runs with the necessary resources. Lastly, you should test the backup and recovery process so that if a disaster occurs, you will know the steps to bring the cluster back in a timely manner.

Assuming that you have installed the Windows Server Backup feature, before you can perform a backup, the cluster needs to be running and you must have quorum. The Cluster service keeps track of the cluster configuration. When a change is made, it replicates the configuration to all cluster nodes. If the cluster has a witness disk, the Cluster service also replicates the configuration to the witness disk. Therefore, be sure to back up the System State, Cluster folders, and the witness disk.

You still have to back up the individual applications running the server and the associated data such as SQL databases, Exchange databases, or shared files. To back up application data, you can install backup software on the cluster node that owns the disk resource, or you can run the backup against the clustered resource over the network. If you use CSV volumes, you can run backup from any node that is attached to the CSV volume.

To restore the cluster, you can perform one of the two types of restores:

- ***Non-authoritative restore:*** A type of restore that restores the information that was performed when originally backed up but is overwritten by current information stored on other cluster nodes.
- ***Authoritative restore:*** A type of restore that restores the information that was performed when originally backed up but is marked as the current and authoritative configuration, which will then overwrite the configuration on the other nodes.

If you have a single cluster node that has failed, you can perform the non-authoritative restore. After fixing or replacing the failed node, perform a non-authoritative restore including the system state. When you restart the node, the restored node will join the cluster and automatically receive the latest cluster configuration from the other nodes or the witness disk.

Alternatively, you can remove a node and add a new node to the cluster. The new node will automatically receive the cluster information.

If an administrator accidently removed clustered resources or modified other cluster settings and you need to restore the cluster back to a specific point in time before the changes were made, you will perform an authoritative restore. To perform an authoritative restore, you will need to stop the cluster restores on all nodes. You then perform a system state recovery on a single node. After the restore, restart the cluster service so that the cluster service will mark the current configuration as the most recent configuration. As you bring the remaining cluster nodes online and start the cluster service, the other nodes will receive the restored configuration.

Business Case Scenarios

Scenario 2-1: Configuring a Redundant Server

You work for the Contoso Corporation. You have a server that acts as a file server for clients. You must make sure that the server is up at all times. What would you recommend?

Scenario 2-2: Upgrading a Cluster to Windows Server 2012 R2

You work for the Contoso Corporation. You have a cluster used as a file server that is running Windows Server 2008 R2. You do not have any other free servers. How would you upgrade the cluster to Windows Server 2012 R2?

Managing Failover Clustering Roles

LESSON 3

Managing Failover Clustering Roles

THE BOTTOM LINE

Failover clusters provide high availability and scalability to many server applications such as Microsoft Exchange, Microsoft SQL, and Hyper-V. You can use the High Availability Wizard to configure a *clustered role* (formerly called a *clustered service* or *application*), which is a service or application that you make highly available.

Similar to storage, if a server has a problem, a clustered role can fail over to another server. Clustered roles are divided into the following two types:

- Cluster-aware
- Generic

A ***cluster-aware clustered role*** is designed to work with Windows Server 2012 and Windows Server 2012 R2 fail-over clusters. Examples include the File Server clustered role and the Virtual Machine clustered role.

A ***generic clustered role*** provides high availability for a service, application, or script that is not originally designed to run in a cluster. As a result, the cluster cannot detect the state of the generic application, script, or service as it can with a cluster-aware role.

- ***Generic application:*** The cluster software starts the generic application, and then periodically queries the operating system to see whether the application still runs.
- ***Generic script:*** You create a script that runs in Windows Script Host, which monitors and controls an application. The state of the application is determined by the script.
- ***Generic service:*** The cluster software starts the service. Similar to generic applications, the cluster services periodically queries the Service Controller to determine whether the service is still running.

Depending on the cluster role or application that you try to run, one or more server roles or applications on each node might be required. In addition, some applications, such as mail and database applications might require additional configuration to work properly in a clustered environment. Microsoft provides thorough documentation to configure Microsoft Exchange or Microsoft SQL to run on a failover cluster on the technet.microsoft.com website.

Configuring Role-Specific Settings

Clusters can be used for a wide range of applications to provide high availability. However, popular uses of clustering include file services and VMs.

When you deploy high-available file services and VMs, you use a shared disk to store data files or VM files. Therefore, you need to choose a shared disk that is highly available and has high performance.

UNDERSTANDING SMB 3.0

Server Message Block (SMB) 3.0 (previously named *SMB 2.2*) is the newest version of the SMB protocol, which was introduced with Windows 8 and Windows Server 2012. It brings significant changes to add functionality and improve performance, particularly in virtualized data centers.

SMB 3.0 has the following additional features:

- **SMB Transparent Failover:** Provides Continuously Available properties that allow SMB 3 clients to not lose an SMB session when failover occurs. Both the SMB client and SMB server must support SMB 3.0 to take advantage of the SMB Transparent Failover functionality.
- **SMB Scale Out:** Allows users to scale shared bandwidth by adding cluster nodes. Both the SMB client and SMB server must support SMB 3.0 to take advantage of the SMB Scale Out feature. SMB 1.0 clients do not contain the required client functionality to access SMB scale-out file shares and will receive an "Access Denied" error message when they try to connect to a scale-out file share. SMB 2.x clients will be able to connect to SMB scale-out file shares but will not benefit from the SMB Transparent Failover functionality.
- **SMB Multichannel:** Uses multiple network interfaces to provide both high performance through bandwidth aggregation and network fault tolerance through the use of multiple network paths to data on an SMB share. SMB 1.0 and SMB 2.x clients will use a single SMB connection.
- **SMB Direct (SMB over Remote Direct Memory Access [RDMA]):** Enables direct memory-to-memory data transfers between servers, with minimal CPU utilization and low latency, using standard RDMA-capable network adapters (iWARP, InfiniBand, and RoCE). It also minimizes the processor utilization when performing large file I/O operations. SMB Direct Functionality requires that the SMB client and SMB server support SMB 3.0.
- **SMB Encryption:** Performs encryption by selecting a check box. Both the SMB client and SMB server must support SMB 3.0 to take advantage of the SMB Encryption functionality.
- **VSS for SMB file shares:** Extends the Windows Volume Shadow Copy Service infrastructure to enable application-consistent shadow copies of server application data stored on SMB file shares, for backup and restore purposes. Both the SMB client and SMB server must support SMB 3.0 to take advantage of the Volume Shadow Copy Service (VSS) for SMB file shares functionality.
- **SMB Directory Leasing:** Reduces the latency when accessing files over slow WAN links by caching directory and file meta-data for longer periods, which reduces the associated round-trips to fetch the meta-data from the server. Both the SMB client and SMB server must support SMB 3.0 to take advantage of the SMB Directory Leasing functionality.
- **SMB PowerShell:** SMB PowerShell management cmdlets were introduced in Windows Server 2012 and in Windows 8.

DEPLOYING THE GENERAL USE FILE SERVER ROLE

File servers in a cluster can be configured for general use—***General Use File Server***—which is almost the same as it was in Windows Server 2008 R2. It provides a central location for users to share files or for server applications that open and close files frequently. It also supports SMB, Network File System (NFS), Data Deduplication, File Server Resource Manager, DFS Replication, and other File Services role services. The only significant difference between Windows Server 2008 R2 and Windows Server 2012/Windows Server 2012 R2 is that Windows Server 2012/Windows Server 2012 R2 supports SMB 3.0.

Before you install and configure the File Server role, be sure that you install the appropriate file server roles for Windows Server 2012 and Windows 2012 R2 such as File Server or Server for NFS. Then when you deploy the General Use File Server role, you will first add the File Server role, and then create the file shares.

DEPLOY THE GENERAL USE FILE SERVER ROLE

GET READY. To deploy the General Use File Server role, perform the following steps:

1. Open Server Manager and click Tools > Failover Cluster Manager. The *Failover Cluster Manager* opens.
2. Right-click Roles and click Configure Roles. Alternatively, you can click the cluster and under *Actions,* click Configure Role.
3. When the *High Availability Wizard* opens, click Next.
4. On the *Select Role* page, click File Server and then click Next.
5. On the *File Server Type* page, click File Server for general use, and then click Next.
6. On the *Client Access Point* page, type a NetBIOS name that the clients will access for the clustered role in the Name text box. Next, type an IP address in the *Address* column.
7. On the *Select Storage* page, enter a storage location for the data and click Next. The disk cannot be assigned as a Cluster Shared Volume (CSV).
8. On the *Confirmation* page, click Next.
9. On the *Summary* page, click Finish.
10. To create a file share, right-click the File Server Role, and click Add File Share.
11. When the *New Share Wizard* opens, select the appropriate file share profile. Click SMB Share – Quick and click Next.
12. On the *Share Location* page, be sure that the File Server cluster role is selected. Then with the Type a custom path selected, type a path (such as E:\Data) in the text box. Click Next.
13. On the *Share Name* page, type a name in the *Share name* box and click Next.
14. On the *Other Settings* page (see Figure 3-1), select or deselect the desired options and click Next.

Figure 3-1

Select other settings

15. On the *Permissions* page, configure the NTFS and Share permissions as necessary by clicking Customize permissions. When done, click Next.
16. On the *Confirmation* page, click Create.
17. When the installation is complete, click Close.

DEPLOYING SCALE-OUT FILE SERVER

The type of file server that you can use with a cluster is the Scale-Out File Server (introduced in Windows Server 2012), which is intended for application data, such as Hyper-V VM files, file shares that require reliability, manageability, and high performance. Different from a General Use File Server cluster, the ***Scale-Out File Server*** cluster is an active-active failover cluster where all file shares are online on all nodes simultaneously. Although the Scale-Out File Server supports SMB, it does not support NFS, Data Deduplication, DFS Replication, or File Server Resource Manager.

To support multiple nodes to access the same volume at the same time, the Scale-Out File Server uses a CSV. It also uses a CSV cache, which reads cache that significantly improves performance in certain scenarios, such as Virtual Desktop Infrastructure.

DEPLOY A SCALE-OUT FILE SERVER

GET READY. To deploy a Scale-Out File Server, perform the following steps:

1. Open Server Manager and click the Tools > Failover Cluster Manager. The *Failover Cluster Manager* opens.
2. Right-click Roles and click Configure Roles. Alternatively, you can click the cluster and under *Actions*, click Configure Role.
3. When the *High Availability Wizard* opens, click Next.
4. On the *Select Role* page, click File Server and click Next.
5. On the *File Server Type* page, click Scale-Out File Server for application data, and click Next.
6. On the *Client Access Point* page, type the name that clients will use to access the file server. Click Next.
7. On the *Confirmation* page, click Next.
8. On the *Summary* page, click Finish.
9. Click Roles. Right-click the file server role, and click Add File Share.
10. When the *New Share Wizard* opens, click SMB Share – Quick, and then click Next.
11. On the *Share Location* page, click the file server name, and click Select by volume. Click Next.
12. On the *Share Name* page, type the name of the share and click Next.
13. On the *Other Settings* page, verify that Enable continuous availability is selected, and then click Next.
14. On the *Permissions* page, configure the NTFS and Share permissions as necessary by clicking Customize permissions. When done, click Next.
15. When the installation is complete, click Close.

CONFIGURING GUEST CLUSTERING

One popular use of failover clusters is to have Hyper-V provide highly available virtual machines. A failover cluster that is made up of two or more virtual machines is typically referred to as a ***guest cluster***, which is used to provide ***highly available virtual machines***.

Highly available virtual machines can be migrated to another physical host in a failover cluster to provide continuing service when the current host goes down or needs maintenance. Different from the other types of clusters, the Hyper-V nodes must be composed of physical hosts. You cannot run Hyper-V on a VM. In addition, to avoid losing network connectivity, you must create the same virtual networks on all physical hosts that participate in the cluster.

To make a VM highly available, all the VM storage location must be on shared storage that all nodes can access. In addition, the storage needs to be configured as a CSV.

In addition to the network and storage requirements, to deploy Hyper-V on a failover cluster, you must meet the following hardware requirements:

- Physical hosts should have similar hardware.
- Physical hosts require an x64-based processor with hardware-assisted virtualization, and hardware-enforced Data Execution Prevention (DEP).
- The processors should be the same architecture and version.
- To provide network redundancy, you can connect cluster nodes to multiple networks and/or use teamed network adapters, redundant switches, and redundant routers.
- To provide inter-host communications, you need one network adapter for each host to form the private network.
- If you use a Serial Attached SCSI (SAS) or Fibre Channel, the mass-storage device controllers in all physical hosts should be identical and should use the same firmware version.
- If you use iSCSI, each physical host should have one or more network adapters that are dedicated to the cluster storage.
- The network adapters that you use to connect to the iSCSI storage target should be identical, and you should use a gigabit Ethernet or faster network adapter.
- When creating shared storage, use basic disks, not dynamic disks.
- Format the disks with the NTFS file system.
- Use either master boot record (MBR) or GUID partition table (GPT).
- If you use a storage area network (SAN), the miniport driver that the storage uses must work with the Microsoft Storport storage driver.
- If you use a SAN, consider using multipath I/O software.
- To protect against host failure, it is recommended that you place virtual machines that are part of the same guest cluster on different physical hosts.

To deploy Hyper-V on a failover cluster, you must meet the following software requirements:

- All physical hosts must run the Windows Server 2012 R2 Standard Edition or Windows Server 2012 R2 Datacenter Edition. In addition, you must have the same edition.
- All physical hosts must be either Full installation or Server Core installations.
- All physical hosts should have the same Windows updates and service packs.
- Network settings such as speed, duplex mode, flow control, and media type settings are the same.
- Make sure that the private network uses a unique subnet.
- Use DNS Dynamic update protocol.
- All servers must be in the same Active Directory Domain Services (AD DS) domain.
- When you first create a cluster or add servers to a cluster, you must be logged on to the domain with an administrator's account on all the cluster's servers. If the account is not a domain administrator, the account must have the Create Computer Objects permission in the domain.

DEPLOY A GUEST CLUSTER

To deploy a guest cluster, perform the following steps:

1. Connect both host computers to the network and storage.
2. Install and configure the required versions of Windows Server 2012 R2.
3. Configure the network settings and join the computers to the AD DS domain.
4. Configure the connection to the shared storage and partition and format the disks with Disk Manager.
5. Install the Hyper-V role.
6. Create the necessary virtual switches.
7. Install the failover clustering features on the host servers.
8. Validate the cluster configuration using the Validate This Cluster Wizard.
9. Create the cluster.
10. Enable Clustered Shared storage for the cluster.
11. Create a VM on one of the cluster nodes. Be sure that the virtual hard disk and VM configuration files are stored on the shared CSV volume.
12. Using the High Availability Wizard, select the *Virtual Machine role* and select the VMs that you want to make highly available.
13. Install the guest operating system on the VM.
14. Test VM failover.

Configuring Failover and Preference Settings

Usually, in a cluster, one node is the same as another. However, you do have some control over which server is the preferred node, and whether a server fails back when the server is brought back online.

You have multiple nodes in a cluster. To specify that one node is the ***preferred node***, you can right-click a role and click *Properties*. When the Properties dialog box opens, select the *General* tab (see Figure 3-2). You can then click the server that you prefer and click the *Up* button to make it first in the list.

The default value for the maximum number of failures is $n - 1$, where n is the number of nodes. Although you can change this value, it is recommended that you keep the value relatively low or the application or service will keep bouncing between nodes.

If a cluster has multiple roles, you can categories the priority for each role. Roles with higher priorities are started before roles with lower priorities. If you don't want a role to start, you select *No Auto Start*.

Figure 3-2

Specifying the preferred owner

When you click the *Failover* tab (see Figure 3-3), you can specify the number of times the Cluster service will attempt to restart or failover. In the Failback option, you can specify not to failback to the preferred owner after the preferred owner is brought back online and when the failback will occur.

Figure 3-3

Specifying Failover and Failback options

Configuring VM Monitoring

With Windows Server 2012 R2, you can use ***VM monitoring***, which is used to monitor specific services within the VM and reacts if there is a problem with a service.

Lesson 2, "Configuring Failover Clustering," discusses how you can use the Failover Cluster Manager, Event Viewer, and Performance and Reliability Monitors to verify that a cluster runs and how well the cluster is doing. However, you cannot monitor the health of applications running inside the guest operating systems of a Hyper-V VM.

Before you can set up VM monitoring on the Failover Cluster Manager, you must have the following:

- The Hyper-V Host operating system must be Windows Server 2012 R2 or Microsoft Hyper-V Server 2012 R2.
- The guest operating system of the VM must be Windows Server 2012.
- The VM guest operating system needs to be on the same domain as the Hyper-V host.
- The administrator of the Hyper-V Cluster needs to have local administrator rights on the VM guest.
- The VM guest firewall needs to allow VM monitoring.

To enable VM monitoring, right-click the *VM* in the Failover Cluster Manager, choose *More Actions*, and click *Choose Configure Monitoring*. When the Select Services dialog box opens, select the services that you want to monitor and click *OK*. You can also enable VM monitoring with the following Windows PowerShell command:

```
Add-ClusterVMMonitoredItem –VirtualMachine
"VM_Name" –Service Name_of_Service
```

When the service is determined to be unhealthy, the Event ID 1250 will be shown in the System Logs. VM monitoring will then restart the VM gracefully on the host that it's currently running on. If the VM fails again, VM monitoring will move the VM to another node and start the VM. Virtual Machine monitoring gives you a finer granularity of the kind of monitoring you want to have for your VMs. It also brings the added benefit of additional health-checking and availability. Without "VM monitoring", if a particular service has a problem, you will have to recognize the problem and then manually restart the service or move the VM to another host.

Business Case Scenarios

Scenario 3-1: Deploying a Clustered File Server

You are an administrator for the Contoso Corporation. You have client software that receives its configuration from a shared folder. Therefore, you need to make sure that this shared folder is highly available. Because it is used by hundreds of users, many at the same time, you want to make sure that performance is high. What would you do?

Scenario 3-2: Deploying a High Availability Virtual Machine

You are an administrator for the Contoso Corporation. You have an enterprise database application that has to be highly available. The application currently runs on a VM. What do you need to make the VM highly available?

Managing Virtual Machine Movement

LESSON 4

Understanding Virtual Machine Movement

THE BOTTOM LINE

Because of the ease with which virtual machines (VMs) can be created and the speed with which the services they provide grow, VM management can quickly become a problem. When this happens, you need a way to move the VM and its storage quickly and with as little inconvenience to your users as possible.

As a server administrator, VMs are one of the best tools to use for providing functionality on demand. With relative speed and ease, you can deliver additional applications as soon as they are needed rather than waiting for the purchase of new hardware.

However, there comes a time when that new application grows from being hardly used to being a mission-critical application that everyone in your organization relies on daily or even hourly. When that happens, inevitably, the server with which you started is no longer powerful enough to handle the load.

In these growth scenarios—when a more powerful server or more storage space is required—because the application started as a VM, it can be moved to that more powerful server or larger disk with relative ease and no server downtime. The challenge, however, is to move the existing VM from one physical computer to another *and* not impact your users.

In prior versions, moving VMs required either a cluster or powering the VM down and moving the files manually. Starting with Windows Server 2012, Live VM movement is no longer limited to a cluster. You can now move an entire VM and its storage to another physical machine with ease while it is online and being used. Three processes are used to move an entire VM or its parts while it runs:

- ***Live Migration (LM):*** The process of moving an entire VM or parts of a VM to another physical server without a cluster.
- ***Quick Migration:*** The process of moving an entire VM or parts of a VM to another physical server using a cluster.
- ***Storage Migration:*** The process of moving the storage of a VM from one physical server to another without a cluster.

■ Understanding Live Migration

THE BOTTOM LINE

LM is the process of moving a VM or its storage from one physical server to another without turning off the VM and without any perceived or actual downtime. In prior versions, the process of performing LM required the VM to be hosted within a clustered environment. In Windows Server 2012 and Windows Server 2012 R2, although that is still possible, it is no longer a requirement.

LM allows you to move the entire VM or its storage from one physical host to another without interrupting your users. This process is sometimes referred to as a *shared nothing* migration because the storage is mirrored over the network to the destination server while the VM continues to run and provide network services

Performing LM

LM requires four steps performed in order to properly move a running VM.

To perform an LM, your systems must perform the following steps:

1. Configure LM prerequisites.
2. Configure LM security (constrained delegation, if needed).
3. Configure the source and destination computers for LM.
4. Move a running VM or VM storage.

CONFIGURING LM PREREQUISITES

To support LM, you need two or more Windows Server 2012 and Windows Server 2012 R2 servers with the Hyper-V Role enabled, and they must meet the following requirements:

- They must use processors from the same manufacturer (for example, all Intel or all AMD).
- All hosts must support hardware virtualization.
- They must belong to the same Active Directory domain or two domains that trust one another; LM does not work with servers that are in a workgroup.
- The VMs must be configured to use ***virtual hard disks (VHD)***, which is the older VM file format, or ***VHDX***, the new VM file format, or virtual Fibre Channel disks.
- It is recommended they use a private network dedicated to LM traffic.
- Membership in one of the following groups on both the source and destination machines or in Active Directory for both domains (if using trusted domains) is required:
  - **a.** Administrators
  - **b.** Domain Admins
  - **c.** Hyper-V Administrators

In addition, you need to ensure the following is configured and available:

- Windows 8.1 computer
- Hyper-V Remote Management tools installed and configured to remotely manage both Hyper-V servers

Finally, you need to consider how you will perform the actual migration and from where you can or need to sign in to perform it. Will you perform the LM via a Keyboard, Video, and Monitor switch (KVM), through an attached monitor session, a Remote Desktop, Remote Management tools, or a Windows PowerShell session?

The answer to this consideration determines whether you will utilize ***Credential Security Support Provider (CredSSP)*** protocol, which enables you to securely delegate a user's credentials from a client to a target server, or Kerberos to authenticate LM traffic.

If you are not using remote management tools to perform a LM, you must sign on to the source server and use CredSSP to authenticate the LM.

If you are using remote management tools, you need to configure constrained delegation and select Kerberos as the authentication protocol.

CONFIGURE CONSTRAINED DELEGATION

GET READY. To configure constrained delegation, perform the following steps:

1. Open the Active Directory Users and Computers snap-in.
2. In the navigation pane, expand the *domain name* and select the Computers folder.
3. In the *Computers* folder, identify the two (or more) servers you will use in this process: *Server01* and *Server02*.
4. Right-click the account of Server01, (the server you are moving from), and then select Properties.
5. In the *Properties dialog box,* click the Delegation tab.
6. On the *Delegation tab,* select Trust this computer for delegation to the specified services only, and then select Use Kerberos only.
7. Click Add.
8. In the *Add Services* dialog box, click Users or Computers. The *Select Users or Computers* dialog box opens.
9. Type the name Server02 (the server you are moving to).
10. Click Check Names to verify that you typed the name correctly, and then click OK. The *Add Services* dialog box opens.
11. The *List of Available Services* dialog box opens. Select both of the following, and then click OK.
    - To move VM storage, select CIFS. This is required for moving the VM storage either with or without the VM.
    - To move VMs, select Microsoft Virtual System Migration Service.
12. Verify your selections on the *Delegation* tab of the *Properties* dialog box, and then click OK (see Figure 4-1).

Figure 4-1

Verifying selections on the Delegation tab

13. For the next part of the process, repeat steps 3 through 12, substituting the appropriate server names where needed.

CONFIGURE THE SOURCE AND DESTINATION COMPUTERS FOR LM

GET READY. To prepare both the source and destination computers for an LM, perform the following steps:

1. Click Server Manager, click Tools, and then select the Hyper-V Manager.
2. In the navigation pane, select the first server you want to configure for LMs.
3. In the *Action* pane, select Hyper-V Settings.
4. In *Hyper-V Settings* dialog box, click Live Migrations.
5. In the *Live Migrations* pane, select Enable incoming and outgoing live migrations (see Figure 4-2).

Figure 4-2

Enabling Live Migrations pane

6. In the *Authentication protocol*, select Use Kerberos if you are using the Hyper-V Remote Management Tools and have configured constrained delegation; otherwise, leave Use Credential Security Support Provider (CredSSP) selected.
7. In *Simultaneous live migrations*, specify a different number if you don't want to use the default of 2.
8. In *Incoming live migrations*, if you have configured dedicated network connections to accept LM traffic, select Add to type the IP address information. If you have not configured a dedicated network for LM, select Use any available network for live migration, and then click OK.
9. Select the second server in Hyper-V Manager and repeat steps 3 through 8.

MOVING VMS USING LM

The machines are now ready for the LM.

In the sixth step of the following exercise, you are presented with three options for moving virtual machines. These options allow you the flexibility to either move the entire VM to one location or allow you to selectively move the various pieces to different locations.

The three options for moving VMs are:

- **Move the VM's data to a single location:** This is simplest because it moves all of the files of the VM to one location at one time.

- **Move the VM's data by selecting where to move the items:** This provides the most options on where you can store the various components.
- **Move only the VM:** This requires shared storage and allows you to move the VM without moving the virtual hard disk.

MOVE A RUNNING VM TO A SINGLE LOCATION

GET READY. To move a running VM to a single location, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the VM and, from the popup menu, select Move to launch the *Move Wizard*.
3. On the *Before You Begin* page, click Next.
4. On the *Choose Move Type* page, select Move the virtual machine.
5. On the *Specify Destination* page, browse to or type the name of the destination computer, and then click Next.
6. On the *Choose Move Options* page, select Move the virtual machine's data to a single location; this is the default and moves everything. Click Next.
7. On the *Choose a new location for virtual machine* page, in the *Destination location Folder* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the VM, and then click Next.
8. On *the Completing Move Wizard*, verify that your selections are correct, and then click Finish.

MOVE A RUNNING VM'S DATA BY SELECTING WHERE TO MOVE THE ITEMS

GET READY. To move a running VM's data by selecting where to move the items, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the virtual machine and, from the popup menu, select Move to launch the *Move Wizard*.
3. On the *Before You Begin* page, click Next.
4. On the *Choose Move Type* page, select Move the virtual machine.
5. On the *Specify Destination* page, browse to or type the name of the destination computer, and then click Next.
6. On the *Choose Move Options* page, select Move the virtual machine's data by selecting where to move the items, and then click Next.
7. On the *Choose Advanced Options for the Move* page, select Move the virtual machine's data automatically. This maintains the file and folder structure of the source on the destination.
8. On the *Completing Move Wizard*, verify that your selections are correct, and then click Finish.

MOVE A RUNNING VIRTUAL MACHINE

GET READY. To move a running VM's data, you select where to move the items. To do this, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.

2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the VM and, from the popup menu, select Move to launch the *Move Wizard*.
3. On the *Before You Begin* page, click Next.
4. On the *Choose Move Type* page, select Move the virtual machine.
5. On the *Specify Destination* page, browse to or type the name of the destination computer, and then click Next.
6. On the *Choose Move Options* page, select Move only the virtual machine, and then click Next.
7. On the *Completing Move Wizard*, verify that your selections are correct, and then click Finish.

Performing Quick Migration

THE BOTTOM LINE

Windows Server 2012 and Windows Server 2012 R2 includes a way to move a running VM that is hosted in a cluster called a Quick Migration.

Quick Migration is another process of moving a running VM from one physical host to another. However, Quick Migration occurs within the confines of a cluster.

Quick Migration allows you to:

- Consolidate physical servers.
- Maintain availability of a production VM during host maintenance.
- Quickly restore services after service outages.

The process by which Quick Migration works is as follows:

- Quick Migration saves the state of the running guest VM to disk or shared storage.
- It moves the storage connection from the source physical server to the destination server.
- It restores the state of the running guest VM to the destination server.

The speed of the Quick Migration is dependent upon how much memory needs to be written to disk and the speed of the network connection between the source and destination servers.

Performing Storage Migration

THE BOTTOM LINE

As VMs grow, they can outgrow their initial storage. ***Storage Migration*** is yet another way to move live VM data without disrupting users.

Storage is the heart of the VM. As long as you have the VHD/VHDX file, you can rebuild the configuration and the VM. It is a powerful file.

Whether facing a server or storage hardware maintenance, upgrades, or other performance issues, during the course of normal operations, there may be times when the VM storage needs to be moved.

Just as there are three options for moving VMs, there are also three options for moving storage. These options give you the flexibility to either move the entire VM to one location or to selectively move the various pieces to different locations.

The three options for moving storage are:

- **Move the VM's data to a single location:** This is simplest because it moves all of the files of the VM to one location at one time.
- **Move the VM's data by selecting where to move the items:** This provides the most options on where you can store the various components.
- **Move only the VM:** This requires shared storage and allows you to move the VM without moving the virtual hard disk.

MOVE THE VM'S DATA TO A SINGLE LOCATION

GET READY. To move a running VM's data to a single location, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the VM and, from the popup menu, select Move to launch the *Move Wizard*.
3. On the *Before You Begin* page, click Next.
4. On the *Choose Move Type* page, select Move the virtual machine's storage, and then click Next.
5. On the *Choose Options for Moving Storage* page, select *Move the virtual machine's data to a single location*. This is the default and moves everything. Click Next.
6. On the *Choose a new location for virtual machine* page, in the *Destination location Folder* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the VM storage. Click Next.
7. On *the Completing Move Wizard*, verify that your selections are correct, and then click Finish.

MOVE A RUNNING VM'S DATA TO DIFFERENT LOCATIONS

GET READY. To move a running VM's data to different locations, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the VM and, from the popup menu, select Move to launch the *Move Wizard*.
3. On the *Before You Begin* page, click Next.
4. On the *Choose Move Type* page, select Move the virtual machine's storage, and then click Next.
5. On the *Choose Options for Moving Storage* page, select Move the virtual machine's data to different locations, and then click Next.
6. On the Select Items to Move page, select any or all of the items you want to move, and then click Next.
7. On the *Chose a new location for attached virtual hard disk* page, in the *Destination location Folder:* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the VM storage. Click Next.

8. On the Chose a new location for current configuration page, in the *New location Folder:* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the current configuration, and then click Next.
9. On the *Chose a new location for snapshot* page, in the *New location Folder:* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the current configuration, and then click Next.
10. On the *Chose a new location for smart paging* page, in the *New location Folder:* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the Smart Paging files, and then click Next.
11. On *the Completing Move Wizard*, verify that your selections are correct, and then click Finish.

MOVE ONLY THE VM'S HARD DISKS

GET READY. To move a running VM's virtual hard disks, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the VM and, from the popup menu, select Move to launch the *Move Wizard*.
3. On the *Before You Begin* page, click Next.
4. On the *Choose Move Type* page, select Move the virtual machine's storage, and then click Next.
5. On the *Choose Options for Moving Storage* page, select Move only the virtual machine's virtual hard disks, and then click Next.
6. On the *Select Items to Move* page, select the disk(s) you want to move, and then click Next.
7. On the *Choose a new location for attached virtual hard disk* page, in the *Destination location Folder:* box, specify the path of the folder on the destination computer or browse to it and select the folder where you wish to place the VM storage, and then click Next.
8. On the *Completing Move Wizard*, verify that your selections are correct, and then click Finish.

Configuring Virtual Machine Network Health Protection

THE BOTTOM LINE

Starting with Windows Server 2012 R2, the network health detection and recovery option called ***Protected network*** is available at the virtual machine level for a Hyper-V host cluster. When a virtual machine becomes disconnected from the network, a live migration will occur to a host where the external virtual network is available. Of course, for this to occur, you must have multiple network paths between cluster nodes.

In Windows Server 2012, if a virtual machine was disconnected from the network, the virtual machine continued to run on the host computer (but the virtual machine might not be available to users). In Windows Server 2012 R2, if the virtual machine has the Protected network option enabled, the availability of the machine is increased. If live migration occurs, there

is no downtime because live migration maintains the session state of the virtual machine. If there are no available networks, the cluster removes the node from the cluster, transfers ownership of the virtual machine files, and then restarts the virtual machines on another node. Protected network option is enabled by default.

ENABLE THE PROTECTED NETWORK OPTION

GET READY. To enable the protected network option, perform the following steps:

1. Using *Server Manager,* open the Tools menu and click Hyper-V Manager.
2. In *Hyper-V Manager*, right-click a virtual machine and choose Settings.
3. In the *Settings* dialog box, in the left pane, expand the Network Adapter node and then click Advanced Features.
4. To enable the *Protected network* option, make sure the Protected network check box is selected. To disable the Protected network, deselect the Protected network option.
5. Click OK to close the Settings dialog box.

Configuring Drain on Shutdown

THE BOTTOM LINE

A Hyper-V host will typically have multiple virtual machines. If you need to shut down or reboot a Hyper-V host, and want those virtual machines to continue to run, you need to migrate those virtual machines to another Hyper-V host. Starting with Windows Server 2012 R2, you can configure Hyper-V to automatically migrate or drain the virtual machine to another host.

When you shut down a cluster node in Windows Server 2012 without draining the node, the virtual machines were put into a saved state, moved to other nodes, and resumed. If the process took too long, there was the potential for an interruption in service.

In Windows Server 2012 R2, the cluster automatically live-migrates all running virtual machines before shutdown. To enable or disable this functionality, configure the `DrainOnShutdown` cluster common property. By default, this property is enabled (set to a value of 1).

To view the property value, execute the following Windows PowerShell command:

```
(Get-Cluster).DrainOnShutdown
```

To enable `DrainOnShutdown` cluster common property, execute the following Windows PowerShell command:

```
(Get-Cluster).DrainOnShutdown = 1
```

To disable `DrainOnShutdown` cluster common property, execute the following Windows PowerShell command:

```
(Get-Cluster).DrainOnShutdown = 0
```

Importing, Exporting, and Copying Virtual Machines

THE BOTTOM LINE

VMs are easy to create. By leveraging the exporting, importing, and copying functions of Hyper-V, you significantly reduce the time spent creating duplicate VMs.

UNDERSTANDING IMPORTING, EXPORTING, AND COPYING VIRTUAL MACHINES

Exporting a VM is the process by which you take a partially or completely configured VM and create other VMs without having to perform the installation and configuration from scratch.

Importing and copying are related in that to do either, you must use the Import Virtual Machine Wizard.

- Importing is the process by which you take an existing set of VM files and recreate the exact same VM.
- Copying is the process of using an exported VM like a template to create as many additional VMs as you need.

In Windows Server 2012 and Windows Server 2012 R2, there are three options available when you select the Import Virtual Machine Wizard:

- **Register the virtual machine in place (use the existing unique ID):** Used when you have manually placed the VM files where you want them, there is no other VM on the machine that has the same unique ID, and you just want Hyper-V to register the VM.
- **Restore the virtual machine (use the existing unique ID):** Used when you have VM files on other media (external drive, file server, and so on), there is no other VM on the machine that has the same unique ID, and you want Hyper-V to organize the files and register the VM.
- **Copy the virtual machine (create a new unique ID):** Used when you have an exported VM that you are using as a template and want to import many times.

TAKE NOTE*

If you want to use an exported VM as a template to create multiple VMs, you should run Sysprep on the VM prior to performing the export.

EXPORT A VM

GET READY. To export a VM, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Virtual Machines* section of *Hyper-V Manager*, right-click the GM and, from the popup menu, select Export to launch the *Move Wizard*.
3. In the *Export Virtual Machine* dialog box, in the *Location* box, specify the path of the folder or browse to it and select the folder where you wish to place the exported VM, and then select Export.
4. In the *Virtual Machines* section of *Hyper-V Manager*, scroll to the right to view the status of the export.

COPY A VM

GET READY. To copy a VM, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Actions s* section of *Hyper-V Manager*, click Import Virtual Machine. The *Import Virtual Machine Wizard* opens.
3. On the *Before You Begin* page, click Next.
4. On the *Locate Folder* page, specify the path of the folder or browse to it and select the folder of the exported VM, and then click Next.
5. On the *Select Virtual Machine* page, select the name of the VM to import, and then click Next.
6. On the *Choose Import Type* page, select from the following choices:
   - **Register the virtual machine in-place (use the existing ID):** This takes the existing VM and corresponding files and folder structure as it is and registers the VM with the host.
   - **Restore the virtual machine (use the existing ID):** This is similar to registering; however, it enables you to specify different paths for the files and folders.

   Click Next.
7. If you selected the *Register* option, you are presented with the *Completing Import Wizard* box. Verify that your selections are correct, and then click Finish.
8. If you selected the *Restore* option, you are presented with the *Choose Folders for Virtual Machine Files* box. Select the Store the virtual machine in a different location checkbox.
9. In the *Virtual machine configuration folder* box, specify the path of the folder or browse to it and select the folder where you wish to place the current configuration.
10. In the *Snapshot store* box, specify the path of the folder or browse to it and select the folder where you wish to place the current configuration.
11. In the *Smart Paging Folder* box, specify the path of the folder or browse to it and select the folder where you wish to place the Smart Paging files.
12. Click Next.
13. On the *Chose Folders to Store Virtual Hard Disks* page, in the *Location:* box, specify the path of the folder or browse to it and select the folder where you wish to place the VM hard disk, and then click Next.
14. On *the Completing Move Wizard*, verify that your selections are correct, and then click Finish.

TAKE NOTE*

This should be the same name as the VM you are replacing.

IMPORT A VIRTUAL MACHINE

GET READY. To import a VM, perform the following steps:

1. Open *Hyper-V Manager* and in the navigation pane, select the name of the source server.
2. In the *Actions s* section of *Hyper-V Manager*, click Import Virtual Machine. The *Import Virtual Machine Wizard* opens.
3. On the *Before You Begin* page, click Next.
4. On the *Locate Folder* page, specify the path of the folder or browse to it and select the folder of the exported VM, and then click Next.
5. On the *Select Virtual Machine* page, select the name of the VM to import, and then click Next.

6. On the *Choose Import Type* page, select Copy the virtual machine (create a new unique ID), and then click Next.
7. In the *Choose Folders for Virtual Machine Files* box (see Figure 4-3), if you want to move the files from their current location, select the Store the virtual machine in a different location checkbox. Then, choose one of the following:
   - In the *Virtual machine configuration folder* box, specify the path of the folder or browse to it and select the folder where you wish to place the current configuration.
   - In the *Snapshot store* box, specify the path of the folder or browse to it and select the folder where you wish to place the current configuration.
   - In the *Smart Paging Folder* box, specify the path of the folder or browse to it and select the folder where you wish to place the Smart Paging files.
   - Then, click Next.

Figure 4-3

The Choose Folders for Virtual Machine Files page

8. On the Choose Folders to Store Virtual Hard Disks page, if you want to move the files from their current location, in the Location box, specify the path of the folder or browse to it and select the folder where you wish to place the VM hard disk, and then click Next.
9. On *the Completing Move Wizard*, verify that your selections are correct, and then click Finish.

■ Business Case Scenarios

Scenario 4-1: Exporting and Importing a VM

Management has decided to migrate all servers to Windows Server 2012 R2 and all users to Windows 8. As the senior administrator for Contoso, management has tasked you with preparing a lab quickly so that the new features of both operating systems can be tested along with the current set of standard corporate applications and division-specific applications for three divisions. In a virtual environment, you need to create a simple Active Directory domain with DNS and DHCP, LOB application servers and workstations to test each configuration. How many servers and workstations do you need and what do you do?

Scenario 4-2: Using Live Migration

Server01 is in need of maintenance. You use LM to move a VM from Server01 to Server02. When the maintenance is complete, you try to move the VM back to Sever01 from the Hyper-V Manager on Server01 and encounter the following error: `Virtual machine migration operation failed at migration Source. Failed to establish a connection with host Server01: No credentials are available in the security package (0x8009030E.`

Why does this occur?

Configuring Advanced File Services

LESSON 5

Configuring NFS Data Store

THE BOTTOM LINE

Network File System (NFS) is a distributed file system protocol that is used to access files over a network, similar to accessing a file using a shared folder in Windows (which uses Server Message Block (SMB). It is used with UNIX and Linux file server clients and VMware. Therefore, to support these clients, Windows Server 2012 and Windows Server 2012 R2 supports NFS.

NFS was originally developed by Sun Microsystems in the 1980s. NFS was later released to the public, and by 1995, the Internet Engineering Task Force (IETF) standardized it as RFC 1813, "NFS Version 3 Protocol Specification." Virtually all UNIX and Linux distributions available today include both NFS client and server support.

By installing the Network File System role service, you can provide NFS Server and NFS Client capabilities. Different from using a Universal Naming Convention (UNC), which uses a \\servername\sharename, or mounting a UNC to a drive letter, NFS takes part of a remote file system and mounts it or connects to a local file system. The client can then access the server's files as if they were a local resource.

Obtaining User and Group Information

Natively UNIX and Linux machines have their own user accounts, which are not part of Windows or Active Directory. As Active Directory is common among corporations, there are several technologies that can be used to link or add the Unix/Linux machines to Active Directory. To prevent NFS clients running on UNIX or Linux systems from having to perform a separate logon when accessing NFS shares, the Windows Server 2012 R2 NFS Server implementation can look up the user information sent by the client and the associated UNIX/Linux account with a particular Windows account.

Similar to Windows, with UNIX and Linux, you log in and authenticate with an account name and password. The user is identified with a ***user identifier (UID)*** value and a ***group identifier (GID)***. Whenever a file is accessed using NFS, the UID and GID are sent to the NFS server to see whether the user has the proper permissions to access.

For the Windows Server 2012 and Windows Server 2012 R2 NFS server to grant the UNIX user access to the requested file, it must associate the UID and GID with a Windows or Active Directory account and use that account to authenticate the client. NFS uses Active Directory lookup and User Name Mappings to obtain user and group information when accessing NFS shared files.

Identity Management for UNIX enables you to integrate Windows users into an existing UNIX or Linux environment, including managing user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS), and enables you to automatically synchronize passwords between Windows and UNIX operating systems. To use this method, you must install the Identity Management for UNIX using the Deployment Image Servicing and management command-line tool, Dism.exe.

INSTALL THE IDENTITY MANAGEMENT FOR UNIX USING DISM.EXE

GET READY. To install the Identity Management for UNIX using Dism.exe, on a Windows Server 2012 R2 domain controller, perform the following steps:

1. Click Windows PowerShell on the taskbar to open the *Windows PowerShell* window.
2. To install the administration tools for Identity Management for UNIX, execute the following command:

   ```
   Dism.exe /online /enable-feature /featurename:adminui /all
   ```

   When you are asked to restart the computer, type N.
3. To install the Server for NIS, execute the following command:

   ```
   Dism.exe /online /enable-feature /featurename:nis /all
   ```

   When you are asked to restart the computer, type N.
4. To install Password Synchronization, execute the following command:

   ```
   Dism.exe /online /enable-feature /featurename:psync /all
   ```
5. When you are asked to restart the computer, type Y.

When you use Active Directory lookup, NFS searches the Active Directory database for the UID and GID values in the NFS file access request and uses the accounts associated with those values to authenticate the client.

When you install the ***Server for NFS role***, it extends the Active Directory schema by adding UNIX attributes. These attributes can be set with Active Directory Users and Computers (see Figure 5-1).

Figure 5-1

Setting UNIX attributes

INSTALL THE SERVER AND CLIENT FOR NFS

GET READY. To install the Server for NFS and Client for NFS, perform the following steps:

1. On the task bar, click the Server Manager button to open the *Server Manager*.
2. At the top of *Server Manager*, click Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. On the *Select destination server* page, click Next.
6. On the *Select server roles* page, expand File and Storage Services, expand File and iSCSI Services, and click to select Server for NFS. Click Next.
7. When you are asked to add features required for Server for NFS, click Add Features.
8. On the *Select features* page, click to select Client for NFS and click Next.
9. Back on the *Select features* page, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When the installation is complete, click Close.

CONFIGURE ACCOUNT LOOKUPS

GET READY. To configure Account Lookup for NFS, perform the following steps:

1. Using Server Manager, open the Tools menu and click Services for Network File System (NFS). The *Services for Network File System* console opens.
2. Right-click the Services for NFS node and, click Properties. The *Services for NFS Properties* dialog box opens.
3. Select one of the following check boxes to choose an identity mapping source:

   Active Directory domain name: Specify the name of the domain that Services for NFS should use to look up user UIDs and GIDs.

   User Name Mapping: Specify the name or IP address of the User Name Mapping server that Services for NFS should use to look up user UIDs and GIDs.
4. Click OK to close the *Server for NFS Properties* dialog box.

Creating an NFS Share

When you install the Services for NFS role service, an NFS Sharing tab is added to the properties of every volume and folder on the computer's drives.

To make a volume or folder available to NFS clients, you need to open the properties for the volume or folder and configure the appropriate values.

CREATE AN NFS SHARE

GET READY. To create an NFS share, perform the following steps:

1. Browse to a volume or folder on a local NTFS drive, right-click it, and click Properties. The *Properties* dialog box opens.
2. Click the NFS Sharing tab.
3. Click Manage NFS Sharing (see Figure 5-2). The *NFS Advanced Sharing* dialog box appears.

Figure 5-2

Sharing an NFS folder

4. Select the Share this folder check box.
5. In the *Share Name* text box, type the name that you want NFS clients to use when accessing the folder and select one of the encoding schemes from the Encoding drop-down list.
6. If you want NFS clients to be able to access the share without authenticating, click to select the Allow anonymous access, and modify the *Anonymous UID* and *Anonymous GID* values, if necessary.
7. Click Permissions. The *NFS Share Permissions* dialog box appears.
8. By default, all NFS clients have read-only access to the share. If you want clients to have Read-Write, change the type of access. You can also grant root access by clicking the Allow root access option.
9. You can click Add to select users or groups and create new permission assignments.
10. Click OK to close the *NFS Share Permissions* dialog box.
11. Click OK to close the *NFS Advanced Sharing* dialog boxes.
12. Click OK to close the *Properties* dialog box.

Installing and Configuring the NFS Data Store

Starting with Windows Server 2012, Server for NFS can be used with failover clustering so that you can deploy NFS while providing fault tolerance. The shared folder within a cluster is known as a ***NFS Data Store***.

To create an NFS shared folder on a cluster, you need to install the following on each cluster node:

- The File Services role
- The Server for NFS role service
- The Failover Clustering feature

After you install these prerequisites and create a cluster, you can configure the cluster to provide high availability for NFS and create an NFS share.

CONFIGURE THE CLUSTER FILE SERVER ROLE

GET READY. To configure the cluster file server role, perform the following steps:

1. In *Server Manager*, click the Tools > Failover Cluster Manager. The *Failover Cluster Manager* opens.
2. Under *Actions*, click Configure Role.
3. When the *High Availability Wizard* starts, click Next.
4. When it asks you to click Select Role, click File Server and click Next.
5. On the *File Server Type* page, with the File Server for general use already selected, click Next.
6. For the *Client Access Point* page, type a name for the cluster in the *Name* text box.
7. In the Click here to type an address box, type an address for the cluster.
8. On the *Select Storage* page, click the available storage and click Next.
9. On the *Confirmation* page, click Next.
10. On the *Summary* page, click Finish.

To create an NFS share to be used with the cluster, you need to choose an *NFS Share–Quick or NFS Share–Advanced*. The NFS Share–Quick is the quickest way to create an NFS file share. The Advanced profile allows you to set the folders' owners for access-denied assistance, configure default classification of data in the folder for management and access polices, and enable quotas. If you want to use the NFS Share–Advanced, you need both the Server for NFS and File Server Resource Manager role servers installed.

CREATE A REDUNDANT NFS SHARE

GET READY. To create a redundant NFS share, perform the following steps:

1. In *Failover Cluster Manager*, click Roles in the left pane.
2. Right-click the cluster under *Roles* and click Add File Share.
3. When the *New Share Wizard* opens, it will ask to select a profile. Click NFS Share – Quick and click Next.
4. On the *Share Location* page, select the volume and click Next.
5. On the *Specify share name* page, type a share name in the *Share name* text box. In the *Local path to share* text box, specify the local path to share. If the folder does not exist, it will create the folder.
6. On the *Authentication* page, click the desired authentication method and click Next.
7. To specify the share permissions, click the Add button.
8. When the *Add Permissions* dialog box opens, *Host* will already be selected. In the text box, type the name of the host that can access the NFS share. Then specify the language encoding and specify the Share permissions. If desired, you can click Allow root access. Click Add.
9. Repeat step 8 as necessary to add additional hosts or groups.
10. On the *Share Permissions* page, click Next.
11. On the *Permissions* page, you can customize the permissions by clicking the Customize permissions. When done, click the Next button.
12. On the *Confirmation* page, click Create.
13. When the share has been created, click Close.

Configuring BranchCache

THE BOTTOM LINE

Branch offices typically have slow connectivity to the central office and typically have limited infrastructure for security servers. When users access files over the slower WAN links, there might be a delay when opening files and when opening large files or many files at the same time, which can cause other programs to be slow or delayed. When using ***BranchCache***, you are essentially creating a WAN accelerator where information is cached on branch computers or local servers. If the document is cached, it is accessed from the local branch office rather than going across a slower WAN link.

BranchCache improves the performance of applications by reducing the network use on the WAN connection between branch offices and the central office by locally caching frequently used files on computers in the branch office. BranchCache works in the background by retrieving data from the server as the client requests the data.

BranchCache supports the following protocols:

- HTTP or HTTPS
- SMB, including signed SMB traffic
- Background Intelligent Transfer Service (BITS)

BranchCache supports IPv4, IPv6, and end-to-end encryption methods such as SSL and IPsec.

BrancheCache can operate in one of two modes:

- Hosted cache mode
- Distributed cache mode

Although an organization can use both modes, you can configure only one mode per branch office.

The ***hosted cache mode*** uses one or more dedicated servers to host the cache. If the content is not available in the hosted cache, the content will be retrieved over the WAN link and added to the hosted cache so that clients requesting the same content in the future will benefit. By default, BranchCache allocates five percent of the disk space on the active partition for hosting cache data. However, this size can be changed by using Group Policy or the `netsh branchcache set cachesize` command.

Instead of having a centralized cache, ***distributed cache mode*** has the cache distributed among the local Windows 7 or 8/8.1 clients at the local site. Content on an individual client is shared with the other clients at the site. Distributed cache mode is designed for branch offices with fewer than 50 users that do not have a dedicated server in the branch office. BranchCache works across a single subnet only.

Windows 8/8.1, Windows Server 2012, and Windows Server 2012 R2 Clients can be configured through Group Policy as distributed cache mode clients by default. However, the clients will search for a hosted cache server, and if one is found, it will automatically configure itself into hosted cache mode clients so that it can use the local server.

To use BranchCache, you perform the following:

- For each web server that you want to cache, you must install the BranchCache feature.
- For each file server, you must install the BranchCache for Network Files role service on the file server that is hosting the data. In addition, you have to configure a hash publication for BranchCache and create BranchCache-enabled file shares.
- For the clients to use BranchCache, you must configure the clients using Group Policy or the netsh command.
- If you use the hosted cache mode, you just add the BranchCache feature to the computer running Windows Server 2012 R2 that will be holding the hosted cache.

INSTALL AND CONFIGURE THE BRANCHCACHE FEATURE

GET READY. To install and configure the BranchCache feature, perform the following steps:

1. Open Server Manager, and then click Manage > Add Roles and Features.
2. When the *Add Roles and Features Wizard* opens, click Next.
3. On the *Select Installation Type* page, make sure that *Role-based or feature-based installation* is selected, and then click Next.
4. On the *Select destination server* page, make sure that the correct server is selected, and then click Next.

5. In *Select server roles*, click Next.
6. In *Select features*, click BranchCache, and then click Next.
7. When installation is complete, click Close.

INSTALL BRANCHCACHE FOR NETWORK FILES

GET READY. To install BranchCache for Network Files, perform the following steps:

1. With Server Manager, open the Manage menu, and click Add Roles and Features.
2. When the *Add Roles and Features Wizard* opens, click Next.
3. On the *Select Installation Type* page, make sure that *Role-based or feature-based installation* is selected, and then click Next.
4. On the *Select destination server* page, make sure that the correct server is selected, and then click Next.
5. In *Select Server Roles*, under *Roles*, expand File and Storage Services, and expand File and iSCSI Services. Click to select the check boxes for File Server and BranchCache for Network Files. Click Next.
6. In *Select features*, click Next.
7. In *Confirm Installation Selections*, review your selections, and then click Install.
8. When installation is complete, click Close.

Because all the file servers that participate in the BranchCache infrastructure must have the same hash publication policy, it is best to place all of the servers in the same Active Directory OU and then assign the appropriate Group Policy object (GPO).

CONFIGURE THE BRANCHCACHE HASH PUBLICATION GROUP POLICY OBJECT

GET READY. To configure the BranchCache hash publication Group Policy object, perform the following steps:

1. In *Server Manager*, click Tools > Group Policy Management. The *Group Policy Management* console opens.
2. Right-click the GPO that is assigned to the OU that the file servers are in and click Edit. The *Group Policy Management Editor* opens.
3. In the *Group Policy Management Editor* console, expand the following path: Computer Configuration, Policies, Administrative Templates. Click Network, Lanman Server.
4. Double-click Hash Publication for BranchCache. *The Hash Publication for BranchCache* dialog box opens.
5. In the *Hash Publication for BranchCache* dialog box, click Enabled (see Figure 5-3).

Figure 5-3

Configuring Hash Publication for BranchCache using group policies

6. In *Options*, click Allow hash publication for all shared folders, and then click one of the following:
   a. To enable hash publication for all shared folders for all file servers that you added to the OU, click Allow hash publication for all shared folders.
   b. To enable hash publication only for shared folders for which BranchCache is enabled, click Allow hash publication only for shared folders on which BranchCache is enabled.
   c. To disallow hash publication for all shared folders on the computer even if BranchCache is enabled on the file shares, click Disallow hash publication on all shared folders.
7. Click OK to close the *Hash Publication for BranchCache* dialog box.
8. Close *Group Policy Management Editor*.

ENABLE BRANCHCACHE ON A FILE SHARE

GET READY. To enable BranchCache on a File Share, perform the following steps:

1. In *Server Manager*, click Tools > Computer Management. The *Computer Management* console opens.
2. Under *System Tools*, expand Shared Folders and click Shares.
3. In the details pane, right-click a share, and then click Properties. The share's *Properties* dialog box opens.

4. In the *Properties* dialog box, on the *General* tab, click Offline Settings. The *Offline Settings* dialog box opens.
5. Ensure that Only the files and programs that users specify are available offline is selected, and then click Enable BranchCache.
6. Click OK twice.
7. Close Computer Management.

BranchCache is disabled by default on client computers. To enable and configure BranchCache, you need to perform the following steps:

1. Enable BranchCache.
2. Enable the *Distributed Cache* mode or *Hosted Cache* mode.
3. Configure the client firewall to allow BranchCache protocols.

Before the clients can use the BrancheCache, you need to enable BranchCache on the clients. To configure BranchCache settings by using group policy, you open a group policy and navigate to *Computer Configuration* > *Policies* > *Administrative Templates* > *Network*, and then click *BranchCache*. Then Turn on BranchCache and set either the *Distributed Cache* mode or the *Hosted Cache* mode.

■ Configuring File Classification Infrastructure

THE BOTTOM LINE

File Server Resource Manager (FSRM) is a suite of tools that enables you to control and manage the quantity and type of data stored on a file server. It enables you to define how much data a person can store, define what type of files that a user can store on a file server, and generate reports about the file server being used. In this section, you classify files based on defined properties and apply policies based on the classification. You can restrict access to files, encrypt files, and have files expire.

File classification allows you to configure automatic procedures for defining a desired property on a file, based on the conditions specified in classification rules. For example, if the content contains "sales figure," you can automatically set the *Confidentiality* property to *High*. By using file classification, you can automate file and folder maintenance tasks, such as deleting old data or protecting sensitive information.

To use file classification, you perform the following steps:

1. Define classification properties and values, which you can assign to files by running classification rules.
2. Create, update, and run classification rules, which are based assigning a single predefined property and value to files within a specified directory based on installed classification plug-ins.
3. When running a classification rule, reevaluate files that are already classified. You can choose to overwrite existing classification values, or add the value to properties that support multiple values. You can also use classification rules to declassify files that are not in the classification criterion anymore.

To configure file classifications, you use the File Server Resource Manager console to create classification rules that scan files for a standard text string, or a string that matches a pattern. When a match is found, the file is classified as specified in the classification rule.

When planning for file classifications, you should do following:

1. Identify which classification or classifications that you want to apply on documents.
2. Determine the method you to want to use to identify documents for classification.
3. Determine the schedule for automatic classifications.
4. Establish a review of classification success.

After you define the classifications, you can then use Dynamic Access Control to enable control on who can access the classified files. Dynamic Access Control is discussed in Lesson 6, "Implementing Dynamic Access Control."

Similar to the previous Windows server roles, the FSRM is installed with Server Manager as a server role.

INSTALL FILE SERVER RESOURCE MANAGER

GET READY. To install FSRM, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Manage > Add Roles and Features to open the *Add Roles and Feature Wizard*.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install FSRM to, and then click Next.
6. Scroll down and expand File and Storage Services and expand File and iSCSI Services. Select File Server Resource Manager.
7. When you are asked to add features, click Add Features.
8. On the *Select server roles* page, click Next.
9. On the *Select features* page, click Next.
10. On the *Confirm installation selections*, click Install.
11. When the installation is complete, click Close.

CREATE A CLASSIFICATION PROPERTY AND RULE

GET READY. To create a classification property and rule using FSRM, perform the following steps:

1. In *Server Manager*, click Tools > File Server Resource Manager. The *File Server Resource Manager* opens.
2. In *File Server Resource Manager*, under *Classification Management*, click, then right-click Classification Properties and click Create Local Property. The *Create Local Classification Property* dialog box opens (see Figure 5-4).

Figure 5-4

Creating a classification property

3. In the *General* tab, type the name and an optional description for the local classification.
4. You can choose different property types such as Yes/No, Date-time, number, Multiple Choice List, Ordered List, Single Choice, String, or Multi-String. For the *Property* type, select Yes/No, and click OK.
5. Click, then right-click Classification Rules, and click Create Classification Rule. The *Create Classification Rule* dialog box opens.
6. In the *General* tab, type a rule name and description. Make sure the rule is enabled.
7. Click the Scope tab.
8. Click the Add button. When the *Browse For Folder* dialog box opens, navigate to the folder such as C:\Data.
9. Click the Classification tab.
10. In the *Classification method* section, you can use Content Classifier to search for specified content in the file. To select that the classification is based on its location, for the *Choose a method to assign a property to files*, select Folder Classifier.
11. Under *Properties*, select the classification previously created and the Yes value.
12. Click the Evaluation Type tab.
13. Click to select the Re-evaluate existing property values. Aggregate the value should already be selected.
14. Click OK to close the *Create Classification Rule* dialog box.
15. In *File Server Resource Manager*, under *actions*, click Run Classification with All Rules Now.

16. When the *Run Classification* dialog box opens, click Wait for classification to complete. When the classification is complete, the *Automatic Classification Report* opens.
17. Close the Automatic Classification Report.
18. Close File Server Resource Manager.

Configuring File Access Auditing

THE BOTTOM LINE

Security can be divided into three areas: authentication, authorization, and auditing. ***Authentication*** is used to prove the identity of a user. ***Authorization*** gives access to the user who was authenticated. To complete the security picture, you need to enable ***auditing*** so that you can have a record of the users who have logged in, what the users accessed or tried to access, and what action the users performed such as rebooting, shutting down a computer, or accessing a file. When you want to audit files, you must first enable object access auditing. Then you must specify which files you want to audit.

Most audit settings require you to enable only specific audit settings. However, object auditing is more complex. After you enable object access (using standard audit policy settings or using the detailed audit policy (specifically audit file system), you have to enable auditing on the specific object (including a folder or file) that you want to enable.

ENABLE OBJECT AUDITING

GET READY. To audit account logon successes and failures, perform the following steps:

1. Open Server Manager.
2. Click Tools > Group Policy Management to open the *Group Policy Management* console.
3. Expand the Domain Controllers to show the *Default Domain Controllers Policy*. Then right-click the Default Domain Control Default Policy and click Edit. *Group Policy Management Editor* appears.
4. Expand Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, and select Audit Policy.
5. Double-click Audit object access. The *Audit account logon events Properties* dialog box opens.
6. Select Define these policy settings and select both Success and Failure.
7. Click OK to close the *Audit account logon events Properties* dialog box.

CONFIGURE FILE SYSTEM AUDITING

GET READY. To audit files and folders, perform the following steps:

1. Right-click the file or folder that you want to audit, click Properties, and then click the Security tab.
2. Click the Advanced button. The *Advanced Security Settings for Updates* dialog box opens.
3. In the *Advanced Security Settings for Updates* dialog box, click the Auditing tab.
4. To add an auditing entry, click Add. The *Auditing Entry for Data* dialog box opens.
5. To specify a user or group, click Select a principal. When the *Select User, Computer, Service Account, or Group* dialog box opens, type a name for a *username* or *group*, and then click OK. See Figure 5-5.

Figure 5-5

Creating auditing entries for file auditing

6. For *Type*, select Success, Fail, or All.
7. Specify the permissions that you want to audit by selecting or deselecting the appropriate permission.
8. Click OK to close the *Auditing Entry for Updates* dialog box.
9. Click OK to close the *Advanced Security Settings for Updates* dialog box.
10. Click OK to close the *Properties* dialog box.

Business Case Scenarios

Scenario 5-1: Configuring BranchCache for a Remote Site

You have a site (Site1) that has about 20 users. For the last few months, users at Site1 have been complaining about the performance when accessing multiple large files at the corporate office, particularly if the files are relatively large. They have no dedicated server to configure DFS replication. Therefore, what else can you do to improve the performance when accessing these files?

Scenario 5-2: Classifying Human Resource Documents

You have a bunch of files on Server01 that belong to the Human Resources department. You need to classify these documents as confidential so that you can define some auditing and make sure that the documents are secure. What should you do?

Implementing Dynamic Access Control

LESSON 6

Using Dynamic Access Control

THE BOTTOM LINE

Dynamic Access Control (DAC), originally called *claims-based access control*, was introduced with Windows Sever 2012, is used for access management. It provides an automatic mechanism to secure and control access to resources.

Claims-based access control uses a trusted identity provider to provide authentication. The ***trusted identity provider*** issues a token to the user, which the user then presents to the application or service as proof of identity. Identity is based on a set of information. Each piece of information is referred to as a ***claim*** (such as who the user or computer claims to be), and stored as a token, which is a digital key. The ***token*** is digital identification for the user or computer that is accessing a network resource. The token has a digital signature of the identity provider to verify the authenticity of the information stored within the token. As users or computers need access to a resource, the user or computer presents the token to get access to the resource.

In Windows Server 2012 R2 the identity provider is the ***Security Token Service (STS)*** and the claims are the Active Directory attributes assigned to a user or device (such as a computer). The claims, the user's security identifier (SID), and group membership are stored inside the Kerberos ticket. The ticket is then used to access protected resources. Of course, claims authorization relies on the Kerberos Key Distribution Center (KDC).

To use claims-based authorization, you need the following:

- Windows Server 2012 R2 must be installed on the file server that hosts the resources that DAC protects.
- At least one Windows Server 2012 R2 domain controller must be accessible by the requesting client.
- If you use claims across a forest, you must have a Windows Server 2012 R2 domain controller in each domain.
- If you use device claims, clients must run Windows 8.1.

When you enable DAC, you have the option to support claims, compound authentication, and Kerberos armoring. Compound authentication is an extension to Flexible Authentication Secure Tunneling (FAST), which allows Kerberos to create service tickets to devices. The Kerberos armoring fully encrypts Kerberos messages and signs Kerberos errors. Although Kerberos armoring enhances security, it also increases processing time.

ENABLE DAC FOR ACTIVE DIRECTORY DOMAIN SERVICES

GET READY. To enable DAC for Active Directory Domain Services (AD DS), perform the following steps:

1. To enable AD DS for DAC, create a new Group Policy Object (GPO) and link the GPO to the *Domain Controllers* organization unit (OU) or edit the *Default Domain Controllers Policy* GPO. Open Server Manager, and then open Group Policy Management.
2. When the *Group Policy Management* console opens, double-click the GPO assigned to the Domain Controllers OU that you want to use to enable DAC.
3. When the *Group Policy Management Editor* opens, navigate to Computer Configuration\Policies\Administrative Templates\System\KDC and double-click KDC support for claims, compound authentication and Kerberos armoring.
4. Click Enabled.
5. Under *Options*, you can choose one of the following:
   - Not supported: Does not provide support for claims, compound authentication, or armoring.
   - Supported: Supports claims, compound authentication, and Kerberos armoring for DAC.
   - Always provide claims: Provides support for claims.
   - Fail unarmored authentication requests: Rejects unarmored Kerberos requests.
6. Click Close to close the *KDC support for claims, compound authentication and Kerberos armoring* dialog box.
7. Close the Group Policy Management Editor.

Configuring User and Device Claim Types

After you enable support for DAC in AD DS, you must create and configure claims and resource property objects. To create and configure claims, you primarily use the Active Directory Administrative Center.

The most common types of claims are attribute-based claims, which are usually configured with Active Directory Administrative Center, specifically using the Dynamic Access Control node (see Figure 6-1). All claims are stored in the configuration partition in AD DS, which is a forest-wide partition. As a result, all domains in the forest share the claim dictionary.

Figure 6-1

Managing DAC using Active Directory Administrative Center

To create a ***claim type***, you specify a specific attribute from Active Directory. Of course, for DAC to be effective, Active Directory must contain accurate information. By default, the claim name is the name of the selected attribute name. However, you can modify this to give a more meaningful name. Lastly, you have the option to provide suggested values for the claim.

CREATE CLAIM TYPES

GET READY. To create a claim type, perform the following steps:

1. Open Server Manager.
2. Click Tools > Active Directory Administrative Center. The *Active Directory Administrative Center opens.*
3. Navigate to the Dynamic Access Control node and click the Claim Types container.
4. In the *Tasks* pane, under *Claim Types*, click New, and then click Claim Type. The *Create Claim Type* dialog box opens.
5. With *User* already selected on the right side of the dialog box, under *Source Attribute,* scroll down and click department.
6. For the display name, to give a more meaningful name, type Company Department and click OK. An entry for *Company Department* is listed under *Claim types.*
7. In the *Tasks* pane, under *Claim Types,* click New, and then click Claim Type.

8. Click to deselect User and click to select Computer.
9. Under *Source Attribute*, scroll down and for *Source Attribute*, click description.
10. Click OK to close the *Create Claim Type* dialog box. The *description* claim type appears.
11. When the installation is complete, click Close.

After you create the claim types, you must configure the resource property objects such as a folder or a file using the Active Directory Administrative Center. You can create your own resource property, or you can use preconfigured properties, such as Project, Department, or Folder Usage. If you choose to use a preconfigured property, they are disabled by default. Therefore, you have to enable the preconfigure property.

Each resource property must be added to at least one resource property list and each resource property list must then be downloaded to the file servers. The Global Resource Property List is downloaded by all servers.

ENABLE RESOURCE PROPERTIES

GET READY. To enable a resource property, perform the following steps:

1. With Active Directory Administrative Center, navigate to and click the Dynamic Access Control node. Next, double-click Resource Properties.
2. To enable the Department resource property, under *Resource Property*, right-click Department, and click Enable.
3. To enable the *Confidentiality* resource property, under *Resource Property*, right-click Confidentiality, and click Enable.
4. To view the *Confidentiality* settings, double-click Confidentiality. The *Confidentiality* dialog box opens.
5. Click Cancel to close the *Confidentiality* dialog box.
6. Close *Active Directory Administrative Center*.

Creating and Configuring Resource Properties and Lists

When you configure the properties that are downloaded by files servers and used to classify files or directories, you will use DAC rules to compare user attribute values with resource properties, which are assigned to Resource Properties Lists. You can enable existing properties or create new ones.

Configuring File Classification

When planning DAC implementation, you should include file classification. Although file classification is not mandatory for DAC, it can enhance the automation of access control because it can be used to identify documents that you need to protect, and classify them appropriately.

Classification management and file management tasks enable administrators to manage groups of files based on various file and folder attributes. After folders and files are classified, you can automate file and folder maintenance tasks, such as cleaning up stale data or protecting sensitive information. Although classification management can be done manually, you can automate this process with the File Server Resource Manager console.

Classification rules can be created and then scheduled to be applied on a regular basis so that files are automatically scanned and classified based on the content of the file. When you want to perform file classification, you need to determine the following:

- Classifications that you want to apply to documents
- Method that you will use to identify documents for classification
- Schedule for automatic classifications

Of course, to determine the success of the classification, you have to establish periodic reviews.

AUTOMATE THE CLASSIFICATION OF FILES

GET READY. To automate the classification of files, perform the following steps:

1. Open Server Manager, open File Server Resource Manager.
2. Click Classification Properties.
3. To see the new classification property that you created in the previous exercise, right-click Classification Properties and click Refresh. The *Confidentiality* and *Department* properties appear with a *Global* scope (see Figure 6-2).

Figure 6-2

Viewing newly created classification properties

4. Click Classification Rules. Next, right-click Classification Rules and click Create Classification Rule. The *Create Classification Rule* dialog box opens.
5. In the *General* tab, in the *Rule name* text box, type Confidentiality.
6. Click the Scope tab.
7. At the bottom of the dialog box, click Add. Browse to the C:\Data folder and click OK. *C:\Data* is listed under *The following folders are included in this scope* section.
8. Click the Classification tab.
9. The *Classification method* should already be *Content Classifier*, the *Confidentiality* and *High* are set under *Property*. To configure the Classification parameter, under *Parameters*, click Configure. The *Classification Parameters* dialog box opens.
10. Change the Regular expression to String. Under *Expression*, type HR. This means that if any of the documents have the string *HR*, they will be automatically tagged as *High* confidentiality.
11. Click OK to close the *Classification Parameters* dialog box.
12. Click Evaluation Type tab.

13. Click to select Re-evaluate existing property values. Then select Overwrite the existing value.
14. Click OK to close the *Create Classification Rule* dialog box.
15. With *File Server Resource Manager* open, click Run Classification with All Rules Now. When you are asked how you want to run the classification rules, click Wait for classification to complete and click OK.
16. When the *Automatic Classification Report* opens, review the results and close the report.
17. If you have a document that has the *HR* string, right-click the document and click Properties.
18. When the *Properties* dialog box opens, click the Classification tab, and notice that *Confidentiality* has been set to *High*.
19. Click OK to close the *Properties* dialog box.
20. Close the *File Server Resource Manager*.

Creating and Configuring Central Access Rules and Policies

Similar to file classification, a Central Access Policy is not mandatory for DAC. However, it is recommended to implement at least one Central Access Policy.

Files stored in shared folders are data files that need to be accessed by multiple users. However, when you apply shared and NTFS permissions, the permissions apply to all files in a specific folder. Unless you constantly monitor the folder and modify the permissions for the folder or the individual files in the folder, the shared and NTFS permissions might not always be a good fit to keep the files secure.

A ***Central Access Policy*** contains ***Central Access Rules*** that grant permissions to objects for a defined group of resources. By default the rules apply to all resources, but you can limit the resources to which the rule will apply. Once the rule is defined, you can choose to apply it live or you can choose to use a "staging" mode.

Before you implement a Central Access Policy, you should do the following:

1. Identify the resources that you want to protect.
2. Define the authorization policies.
3. Translate the authorization policies into expressions.
4. Break down the expressions that you have created, and determine what claim types, resource properties, and device claims that you must create to deploy the policies.

During the next exercise, you create a Central Access Rule that grants permissions to files in a folder that is classified as Confidentiality – High.

CREATE A CENTRAL ACCESS POLICY

GET READY. To create and apply a Central Access Policy, perform the following steps:

1. In the *Active Directory Administrative Center*, navigate to and click the Dynamic Access Control node. Next, double-click Central Access Policies.
2. Under *Tasks*, click New, and click Central Access Policy. The *Central Access Policy* dialog box opens.
3. In the *name* text box, type a name of the Central Access Policy.
4. Under the *Member Central Access Rules* section, click Add.

5. Because you do not have a Central Access Rule defined, click Add a new central access rule. The *Create Central Access Rule* dialog box opens.
6. In the *Name* text box, type a name to identify the rule.
7. Under *Target Resources*, click Edit. The *Central Access Rule* dialog box opens.
8. For the condition, specify the following:

   Resource > Confidentiality > Equals > Value > High

   Click OK to close the *Central Access Rule* dialog box.
9. Click OK to close the *Create Central Access Rule* dialog box.
10. Back on the *Central Access Rule* dialog box, the rule should be listed in the right pane. Click OK to close the *Add Central Access* dialog box.
11. Click OK to close the *Create Central Access Policy* dialog box.
12. Click Cancel to close the *Confidentiality* dialog box.
13. Close the *Active Directory Administrative Center*.

    You can also take this a step further and specify that access is granted only if the user is part of the Human Resources department:

    Resource > Department > Equals > Value > Human Resources

Implementing Policy Changes and Staging

As you probably already have figured out, DAC can be a powerful tool that helps secure your environment and automates the configuration to make your resources secure. However, if you do not properly plan out DAC, when you first implement DAC or when you make changes, you can either grant more access than desired, or you can restrict access to the files too much, resulting in an increase of help desk calls.

To help you test implementing DAC or making changes, Windows Server 2012 R2 allows you to perform staging, which allows you to verify the proposed policy updates before enforcing them. To use staging, you deploy the proposed polices along with the enforced policies, but you do not actually grant or deny permissions. You then open the Event Viewer on the file server search for Audit Event 4818 in the security logs. The Audit Event 4818 shows the result of the access check that is using the staged policy is different than the access check that is using the enforced policy. However, before the staging appears, you need to first enable *Audit Central Access Policy Staging* using *Group Policies*.

CONFIGURE STAGING OF CENTRAL ACCESS POLICY

GET READY. To configure staging of Central Access Policy, perform the following steps:

1. Open Server Manager, and then open Group Policy Management.
2. Using the *Group Policy Management* console, right-click a group policy that you are using to configure DAC and click Edit. The *Group Policy Management Editor* opens.
3. Navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies and double-click Object Access.
4. Double-click Audit Central Access Policy Staging, select all three check boxes, and then click OK.
5. Double-click Audit File System.
6. When the *Audit Central Access Policy Staging Properties* dialog box opens, click to select Configure the following audit events, Success, and Failure.

7. Click OK to close the *Audit Central Access Policy Staging Properties* dialog box.
8. Close the *Group Policy Management Editor* and the *Group Policy Management* console.

Another way to test DAC changes is to use effective permissions. Of course, you should test for users who should have access and users that do not have access.

VIEW THE EFFECTIVE PERMISSIONS OF A USER ON A FILE RESOURCE

GET READY. To view the effective permissions of a user on a file, perform the following steps:

1. Using *File Explorer*, navigate to a test folder with documents that you are protecting with DAC.
2. Right-click a test document and click Properties. The *Properties* dialog box opens.
3. Click the Advanced button. The *Advanced Security Settings* dialog box opens.
4. Click the Effective Access tab.
5. Click Select a user. If you need to test computer access, you would instead click Select a device. When the *Select User, Computer, Service Account, or Group* dialog box opens, type a name of a test user in the *Enter the object name to select* text box and click OK.
6. Click Include a user claim. Select the resource, and type a value as shown in the Figure 6-3.

Figure 6-3

Viewing effective permissions

7. On the *Confirm installation selections* page, click Install.
8. When the installation is complete, click Close.

Performing Access-Denied Remediation

When a user is denied access to a shared folder or file, Windows Server 2012 R2 provides the ***Access-Denied Assistant***, which helps users determine why they cannot access the folder or file, and directs users to resolve the issue without calling the help desk. At this time, Access-Denied Assistance works only with Windows 8.1 and Windows Server 2012 R2.

When Access-Denied Assistant is combined with DAC, Access-Denied Assistant can inform an administrator so that the administrator can make adjustments to the policy or user attribute. For example, it might help to identify that the department was HR instead of Human Resources.

ENABLE ACCESS-DENIED ASSISTANCE

GET READY. To enable Access-Denied Assistance, perform the following steps:

1. Open Server Manager, and then open Group Policy Management.
2. In the *Group Policy Management* console, right-click a group policy that you are using to configure DAC and click Edit. The *Group Policy Management Editor* opens.
3. Navigate to Computer Configuration\Policies\Administrative Templates\System\Access-Denied Assistance, and double-click Enable access-denied assistance on client for all file types.
4. When the *Enable access-denied assistance on client for all file types* dialog box opens, click Enabled.
5. Click OK to close *the Enable access-denied assistance on client for all file types* dialog box.
6. Double-click Customize message for Access Denied errors. The *Customize message for Access Denied errors* dialog box opens.
7. Click Enabled.
8. Under *Options*, type a message to the users in the *Display the following message to users who are denied access* text box.
9. If desired, click to select the Enable users to request assistance. Then type the text that will be in the e-mail in the *Add the following text to the end of the email* text box.
10. If desired, specify the e-mail recipients. Options include Folder owner, File server administrator, or additional recipients.
11. Click OK to close *the Customize message for Access Denied errors* dialog box.
12. Close the *Group Policy Management Editor*.
13. Close the *Group Policy Management* console.

■ Business Case Scenarios

Scenario 6-1: Controlling Access to Files

You are an administrator for the Contoso Corporation. Many of the HR documents have Social Security numbers, which are considered confidential. What can you do to make sure that only people from HR can access those files and they are labeled as Highly confidential?

Scenario 6-2: Implementing and Testing a Central Access Policy

You are an administrator for the Contoso Corporation. You have just replaced a senior administrator. During your first week, you discover that certain users have access to the HR documents that should not. The HR documents preside on three file servers at the corporate office. Therefore, you want to make sure that only HR personnel have access to the HR documents, and no one else. However, when you make the changes, you need to ensure that the users who need to access them still have access. What would you recommend?

Configuring and Optimizing Storage

LESSON 7

Using iSCSI

THE BOTTOM LINE

iSCSI is an Internet Protocol-based storage network standard that allows servers and other devices to connect to a data storage device or devices. As the name indicates, it carries SCSI commands over IP networks. Different from standard local SCSI drives, iSCSI allows data transfers over intranets and can be used over long distances. iSCSI allows clients, which are called ***iSCSI initiators***, to send SCSI commands to iSCSI storage devices, which are known as ***iSCSI targets***.

Storage devices provided by iSCSI are often used as storage devices that contain sensitive or critical data. Therefore, you need to protect the iSCSI infrastructure. The best approach for security is to use a Defense-in-Depth security strategy consisting of the following:

- Policies, procedures, and awareness that include security best practices, enforcing a strong user password policy and strong administrator password policy for accessing iSCSI storage devices and computers that have iSCSI management software installed.
- Physical security that protects servers and iSCSI storage devices that can be accessed by authorized personnel only.
- Perimeter security that includes firewalls to protect attacks from outside the organization and prevent attacks on the iSCSI devices.
- Network protection including authentication such as target access lists, Challenge-Handshake Authentication Protocol (CHAP), virtual LANs (VLANs), and physical isolation. You might also consider using Internet Protocol security (IPsec).
- Keeping your servers updated with the latest security updates.
- Protecting the data stored on the iSCSI storage devices including encryption (using BitLocker and Encrypted File System (EFS)) and Access Control Lists (ACLs).
- Performing backups on a regular basis and storing the backups in a safe place.

Of these, iSCSI targets and initiators have the following security features built in:

- Limit which iSCSI initiators can connect to an iSCSI target.
- Use CHAP to provide authentication between an iSCSI initiator and an iSCSI target.
- For encryption of traffic between an iSCSi initiator and an iSCSI target, you can use IPsec.

iSCSI Qualified Name (IQN) are unique identifiers that are used to address initiators and targets on an iSCSI network. The IQN uses the following format:

- Literal iqn
- Date (yyyy-mm) that the naming authority took ownership of the domain

- Reversed domain name of the authority
- Optional ":" prefixing a storage target name specified by the naming authority.

An example of an IQN is:

```
iqn.1991-05.com.contoso:storage01-target1-target
```

When you configure an iSCSI target, you define which iSCSI initiators can connect to an iSCSI LUN by the client's IQN. You can also specify which servers can connect to the iSCSI target based on MAC addresses, IP address, and DNS name. The iSCSI initiators use IQNs to connect to the iSCSI targets. If name resolution is possible, you can also use IP addresses to identify initiators and targets.

Configuring iSCSI Target

Starting with Windows Server 2012 R2, you can install the iSCSI Target Server role, so that other Windows servers can provide iSCSI storage to other clients (including other Windows servers). After you install the iSCSI Target Server role, you use Server Manager to create the volumes that will be presented to clients and specify which servers can access the iSCSI LUNs.

The iSCSI Target Server included in Windows Server 2012 R2 provides the following functionality:

- By using boot-capable network adapters or a software loader, you can use iSCSI targets to deploy diskless servers.
- By using virtual disks, you can save up to 90 percent of the storage space for the operating system images by using differencing disks.
- Supports server application storage that requires block storage.
- Supports iSCSI initiators for Windows and non-Windows operating systems.
- Supports lab environments.

When you install iSCSI Target Server, you should install the following two components:

- **iSCSI Target Server:** Provides tools to create and manage iSCSI targets and virtual disks. Enabling iSCSI Target Server can provide application block storage, consolidate remote storage, provide for diskless boots, and run in a failover cluster environment.
- **iSCSI Target Storage Provider:** Enables applications on a server that is connected to an iSCSI target to perform volume shadow copies of data on iSCSI virtual disks. It also enables you to manage iSCSI virtual disks by using older applications that require a Virtual Disk Service (VDS) hardware provider, such as using the DiskRAID command-line tool.

INSTALL iSCSI TARGET SERVER

GET READY. To install the iSCSI Target Server, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Manage > Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. On the *Select destination server* page, select the server that you are installing to and click Next.

6. On the *Select server roles* page, expand File and Storage Services, expand File and iSCSI Services, and click iSCSI Target Server and iSCSI Target Storage Provider (VDS and VSS hardware providers). Click Next.
7. On the *Select features* page, click Next.
8. On the *Confirm installation selections* page, click Install.
9. When the installation is complete, click Close.

Virtual disks or targets are created on an iSCSI disk storage subsystem that is not directly assigned to a server. Targets are created to manage the connections between an iSCSI device and the servers that need to access it. Instead of having its own console, managing iSCSI virtual disks and iSCSI targets are done with Server Manager.

CREATE AN iSCSI VIRTUAL DISK

GET READY. To create an iSCSI virtual disk, perform the following steps:

1. Open Server Manager, click File and Storage Services, and then click iSCSI.
2. Click To create an iSCSI virtual disk, start the New iSCSI Virtual Disk Wizard (see Figure 7-1). Alternatively, you can open the Tasks menu in the *iSCSI Virtual Disks* section and click New iSCSI Virtual Disk.

Figure 7-1

Managing iSCSI virtual disks

3. On the *Select virtual disk location* page, click a drive to store the iSCSI virtual disk, and then click Next.
4. On the *iSCSI Virtual Disk Name* page, in the *Name* text box, type the name of the iSCSI virtual disk. Click Next.
5. In the *iSCSI Virtual Disk Size* page, specify the size in GB of the iSCSI virtual disk. Click Next.
6. On the *iSCSI Target* page, if targets have been defined previously, you can click a target and click Next. To create a new target, click New iSCSI target and click Next.
7. If you chose the *New iSCSI target*, on the *Target Name and Access* page, type the name of the target. Click Next.
8. On the *Access Servers* page, click Add.
9. When the *Add initiator ID* page opens, for the type, select IQN, DNS Name, IP Address, or MAC address. Then in the *Value* text box, type the corresponding value for the initiator that matches the type. Click OK.
10. On the *Access Servers* page, add any additional iSCSI initiators. Then click Next.
11. On the *Enable Authentication* page, if you want to use authentication, click to select the Enable CHAP. Then type a username and password. When done, click Next.
12. On the *Confirmation* page, click Create.
13. When the iSCSI virtual disk is created, click Close.

You can assign a current iSCSI virtual disk to an initiator by right-clicking the virtual disk and clicking *Assign iSCSI Virtual Disk*. You can modify the iSCSI targets by right-clicking an iSCSI target and clicking *Properties*.

Configuring iSCSI Initiator

To connect to an iSCSI target, you use an iSCSI initiator. As mentioned previously, the iSCSI Initiator is already included with Windows.

After the targets are configured and registered, you open the iSCSI initiator, as discussed in the following procedure.

CONFIGURE THE iSCSI INITIATOR

GET READY. To configure the iSCSI initiator, perform the following steps:

1. Click Tools > iSCSI Initiator. The *iSCSI Initiator Properties* dialog box opens. If it is the first time launching, Microsoft iSCSI will not be running. Therefore, when it asks to start automatically each time the computer restarts, click Yes.
2. On the *Targets* tab, the iSCSI target should be listed in the *Discovered targets* section. If you just created one and it does not show up, click Refresh.
3. When the target appears, click the target and click Connect. When the *Connect to Target* dialog box opens, if you need to specify the target portal IP address or a CHAP username, click Advanced to open the *Advanced Settings* dialog box. When you click OK to close the *Advanced Settings* dialog box and *Connect to Target* box, the status should show *Connected*.

TAKE NOTE*

If the target does not show up, verify that the initiator ID is specified correctly in the iSCSI target access server list.

4. Click the Volumes and Devices tab.
5. Click Auto Configure. The available iSCSI targets should appear in the Volume List.
6. If you need to configure CHAP or IPsec to connect to the iSCSI target, click the Configuration tab.
7. Click OK to close the *iSCSI Initiator Properties* dialog box.

After an iSCSI device is attached to a server running Windows Server 2012 R2, you might need to format the volume and assign a drive letter to the new volume. To accomplish this, you use *Computer Management*. After opening Computer Management, if the disk does not show up, right-click *Disk Management* and try to perform a Rescan disk.

Configuring Internet Storage Name Server

The ***Internet Storage Name server (iSNS)*** protocol is used to automatically discover, manage, and configure iSCSI devices on a TCP/IP network. iSNS is used to emulate Fibre Channel fabric services to provide a consolidated configuration point for an entire storage network.

iSNS is installed as a feature. The iSNS provides a registration function to allow entities in a storage network to register a query in the iSNS database. Both targets and initiators can register in the iSNS database. After information is entered in the database, targets and initiators can query information about other initiators and targets. For information to be entered into the database, you specify iSNS server on the iSCSI Initiator's Discovery tab.

INSTALL ISNS

GET READY. To install iSNS, perform the following steps:

1. Open Server Manager.
2. At the top of *Server Manager*, click Manage > Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. On the *Select destination server* page, select the server that you are installing to and click Next.
6. On the *Select server roles* page, click Next.

7. On the *Select features* page, click to select iSNS Server service and click Next.
8. On the *Confirm installation selections* page, click Install.
9. When the installation is complete, click Close.

The iSNS Server can be started from Administrative Tools or the Server Manager Tools menu. Registered iSCSI initiators and targets are listed in the iSNS Server Properties (see Figure 7-2). For more information about the initiator or target, click the iSCSI initiator or target and click *Details*.

Figure 7-2

Viewing registered iSCSI initiators and targets

The ***discovery domain (DD)*** service allows the partitioning of storage nodes into management groupings (called discovery domains) for administrative and logon control purposes. The iSNS Server Properties start with the Default DD (see Figure 7-3). You can create a new discovery domain by using the *Creating* button and typing the name of the discovery domain. Then use the *Add* button to add members.

Figure 7-3

Managing discovery domains

Configuring Tiered Storage

THE BOTTOM LINE

A new feature of Windows Server 2012 R2 is ***storage tiers***, which allow you to use solid-state drives (SSDs) and hard drive storage within the same pool. To get acceptable performance while managing costs, you will store more frequently accessed data on SSD media.

Typically, faster disk drives cost more than slower disk drives. So while you always desire faster disk drives, it might not be cost-effective to use all SSD disks. However, if you use the faster disks for programs that are accessed more often than others, you can realize better performance while still managing costs effectively. Windows Server 2012 R2 offers tiered storage, in which you can combine the two types of disks into one virtual disk and volume. You should keep in mind that you cannot remove storage tiers from a virtual disk after it is created. In addition, storage tiers require fixed provisioning.

CONFIGURE TIERED STORAGE

GET READY. To configure tiered storage, perform the following steps:

1. Open Server Manager.
2. Click File and Storage Services. In the *Volumes* section, click Disks to view the current disks that are available.
3. In the *Volumes* section, click Storage Pools.
4. In the main pane, under *Storage Spaces*, right-click Primordial pool and choose New Storage Pool.

5. On the *Before you Begin* page, click Next.
6. On the *Storage Pool Name* page, in the *Name* text box, type a descriptive name. In the *Description* text box, type a description for the storage pool and then click Next.
7. On the *Physical Disks* page, select the disks that you want to include in the pool and then click Next.
8. On the *Confirmation* page, click Create.
9. When the Storage Pool is created, click Close.
10. Right-click the storage pool and choose New Virtual Disk.
11. In the *New Virtual Disk Wizard*, on the *Before you Begin* page, click Next.
12. On the *Storage Pool* page, select the storage pool that you just created and then click Next.
13. On the *Virtual Disk Name* page, in the *Name* text box, type a descriptive name for the virtual disk. In the *Description* text box, type a description.
14. Click to select Create storage tiers on the virtual disk. Click Next.
15. On the *Storage layout* page, click to select the desired storage layout and then click Next.
16. On the *Provisioning* page, *Fixed* provisioning type is already selected. Click Next.
17. On the *Size* page, for the *Faster Tier (SD)* setting and the *Standard Tier (HDD)* setting, click Maximum size.
18. Click Next.
19. On the *Confirmation* page, click Create.
20. When the virtual disk is created, click Close.
21. In the *New Volume Wizard*, on the *Before You Begin* page, click Next.
22. On the *Server and Disk* page, select the server and virtual disk and then click Next.
23. On the *Size* disk, specify the size of the volume and then click Next.
24. On the *Drive Letter or Folder* page, specify the desired drive letter and then click Next.
25. On the *Select file system settings* page, for the *File system* setting, select NTFS or ReFS. In the *Volume label* text box, type a volume name. Click Next.
26. On the *Confirmation* page, click Create.
27. When the volume is created, click Close.

■ Implementing Thin Provisioning and Trim

THE BOTTOM LINE

The advantage of running virtual machines is to share resources and to make use of wasted or idle resources on a computer. For example, although a physical server might have two processors, much of what the processors do is nothing as it waits for something to do. The same can be said for storage. Therefore, Hyper-V introduces ***thin provisioning*** using ***dynamically expanding disks*** in Windows Server 2012 R2.

With dynamically expanding disks, rather than creating a file equivalent in size of the disk, it creates a small file that grows as data is written to it, up to the limitations set forth in the configured size of the disk. Therefore, if you designate a 100 GB disk but you have only 5 GB of data, the disk will take only 5 GB. When you combine the amount of disk space that is not used with several servers on the LUN, the amount of wasted space is often significant.

When you use thin provisioning, you must make sure that you do not have a disk that suddenly expands a lot causing a disk to run out of disk space on the Hyper-V host. If you run out of space on Hyper-V, virtual machines that use the same storage device and LUN could fail. In addition, you need to monitor disk growth so that if you need to move a VM or virtual disk from the LUN or expand the LUN, you can do so before running of disk space becomes a problem. When you create a disk in Hyper-V, you have a choice of the following:

- **Fixed size:** The virtual hard disk that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
- **Dynamically expanding:** The virtual hard disk file that is created is initially small and grows as data is added.
- **Differencing:** Allows you to build on top of a parent disk. Changes to the virtual disk are written to a child disk. As a result, the parent disk does not change.

After a virtual disk is created, you can change the parameters of the disk by opening the properties of the virtual machine, clicking on the virtual disk, and clicking *Edit* to open the Edit Virtual Hard Disk Wizard dialog box. You can then perform the following actions:

TAKE NOTE*

To perform some of these actions, the VM needs to be powered off. If not, the option may be greyed out.

- **Compact:** Compacts the file size of a virtual hard disk by removing blank space that is left behind when data is deleted from the virtual hard disk. The storage capacity of the virtual hard disk is unchanged.
- **Convert:** Converts a virtual disk by copying the contents to a new virtual hard disk. It can be used to convert from an expanding virtual hard disk to a fixed virtual hard disk or vice versa.
- **Expand:** Expands the capacity of the virtual hard disk.
- **Shrink:** Reduces or ***trims*** the storage capacity of the virtual hard disk.

■ Managing Server Free Space Using Features on Demand

THE BOTTOM LINE

Features on Demand allows administrators to completely remove the installation binaries for roles and features that are not needed for the server. Of course, by using ***Features on Demand***, you save disk space and enhance the security by removing binaries for features that will not be needed.

To view the available features for Windows, you can execute Windows PowerShell command:

```
Get-WindowsFeature
```

or the following command at a command prompt:

```
dism /online /get-features /format:table
```

Then to remove the binaries of a feature, you use the *Uninstall-WindowsFeature PowerShell* cmdlet with the `-Remove` parameter. For example, if you do not need BitLocker, you can perform the following command:

```
uninstall-WindowsFeature Bitlocker -Remove
```

After the binaries are removed, the previous `dism` command shows `Disabled with Payload Removed`.

Business Case Scenarios

Scenario 7-1: Using iSCSI Devices

You are an administrator for the Contoso Corporation. You have a large server that is running Windows Server 2012 R2 and that has about 8 TB of disk space that you can allocate to be used by other servers. What can you do so that two other servers running Windows Server 2012 R2 can use the disk space just as if the disk space was local?

Scenario 7-2: Reducing Disk Space

You are an administrator for the Contoso Corporation. You have several virtual machines running on Hyper-V that get their disk space from a local SAN. The SAN is running out of disk space. What can you do to reduce the space used on the SAN?

Configuring and Managing Backups

LESSON 8

Configuring and Managing Backups

THE BOTTOM LINE

When an organization loses data, the results can range from a loss of productivity to an entire meltdown of the company itself. Having a solid backup strategy along with the systems, processes, and tools to execute the strategy is the key to your ability to recover.

There is an old saying that nothing lasts forever, which means one should live it up, take chances, and never have any regrets. That might be sound advice in some situations, but it's not the approach you want to take when it comes to protecting your data.

Unfortunately, most people and companies take backups seriously only after they've experienced the impact of losing their data. It's inevitable; it will happen sooner or later, and you must be prepared by implementing a backup strategy and executing it when the time comes.

Installing the Windows Server Backup Feature

Windows Server Backup, ***wbadmin***, and Windows PowerShell cmdlets provide the tools you need to back up and restore your critical data and servers.

To prepare for a server backup, you need to first install the Windows Server Backup feature. Once installed, you have access to the following tools:

- Windows Server Backup Microsoft Management Console (MMC) snap-in
- wbadmin command-line tool (wbadmin.exe)
- Windows PowerShell cmdlets for Windows Server Backup

The Windows Server Backup MMC snap-in is not installed on Windows Server 2012 R2 systems running the Server Core installation option only. To run backups on these systems, you need to use either the command-line tool wbadmin or the Windows PowerShell cmdlets, or manage them remotely from another computer using the Windows Server Backup MMC. You can also use the Windows 8 Remote Server Administration Tools (RSAT) for Windows 8.1.

INSTALL THE WINDOWS SERVER BACKUP FEATURE

GET READY. To install the Windows Server Backup feature on Server01, perform the following steps:

1. Log in to Server01 and open Server Manager.
2. Click Manage > Roles and Features.
3. Click Next when the *Add Roles and Features Wizard* appears.

4. Click Next on the *Select installation type* screen.
5. Click Next on the *Select destination server* screen.
6. Click Next on the *Select server roles* screen.
7. Select Windows Server Backup and click Next.
8. Select Restart the destination server automatically if required and click Yes to allow automatic restarts.
9. Click Install and then click Close.

After the installation completes, you can launch the Windows Server Backup Microsoft Management Console (MMC) snap-in by selecting *Server Manager* > *Tools* > *Windows Server Backup*.

Configuring Windows Server Backups

The Windows Server Backup feature provides full server, bare metal recovery, system state, system reserve, and local/remote volume backup capabilities.

Once the Windows Server Backup feature is installed, it's time to refer to your backup strategy to answer several key questions.

REVIEWING BACKUP CONFIGURATION OPTIONS

When configuring your backup, you select either a full server (recommended) or a custom configuration.

The following provides an overview of the configuration options:

- **Full server (recommended):** This option backs up all hard disk volumes (except for the volume where the backup is stored) as well as any critical data required for recovery. This includes your server data, applications, and system state. Full server backups can be used to recover the Active Directory Domain Services (AD DS), bare metal recovery restores, as well as specific files/folders.
- **Custom:** This option allows you to specify the items you want to include in the backup. The options include:
  - ***Bare metal recovery:*** This option allows you to recover your server from a hard drive failure to a machine running the same/different hardware. It does not support cross-architecture (x86 to x64) and requires Windows Server installation media to start the recovery process. Selecting this option automatically includes system state, system reserved, and the critical volumes that are necessary for the operating system to run. Examples of critical volumes include those that hold the boot files (Bootmgr and the Boot Configuration Data [BCD] store), the operating system and registry, the SYSVOL, Active Directory database, and Active Directory database log files. When selecting this option as a substitute for a full backup, keep in mind that it will not automatically back up non-critical volumes that contains data you need.
  - ***System state:*** This option backs up all the files needed to recover Active Directory. The system state includes the registry, boot files, the COM+ class registration database, the Active Directory database (ntds.dit) and its associated log files, the Active Directory Certificate Services database, the SYSVOL folder, and system files under the protection of Windows Resource protection. Additional data can be included if the server performs additional roles.
  - **System Reserved:** This option contains the Windows Recovery Environment (WinRE) files and can be used to boot the server in situations where the operating system becomes corrupted or fails to boot.
  - **Local disk (x:):** This option represents local disks and volumes on the server.

EXPLORING YOUR SCHEDULING OPTIONS

You can run a manual backup (one-time backup) by using the Backup Once Wizard, which can be accessed via the Actions pane in the Windows Server Backup console. These types of backups can also be initiated using wbadmin and Windows PowerShell.

Never use manual backups as a replacement for your regularly scheduled backup. Depending upon the needs of your organization, you have the option to schedule a backup to occur once a day or multiple times during the day at the times you specify.

SELECTING WHERE TO STORE YOUR BACKUPS

Windows Server Backup provides three options to select from when deciding where to store your backups. These options include:

- Backing up to hard disk(s) (recommended)
- Backing up to a volume
- Backing up to a shared network folder

After selecting a storage location for your backups, you are ready to perform the actual backup.

OPTIMIZING YOUR BACKUPS (FULL VERSUS INCREMENTAL)

After you complete the first full backup, you can then automatically run incremental backups, which saves only the data that has changed from the last backup. By default, Windows Server Backup creates incremental backups that function much like full backups allowing you to restore from a single backup. In the past, you had to restore a full backup followed by the necessary incremental backup(s) to complete the restore process.

Windows Server Backup also provides performance enhancements by using block-level technology and Volume Shadow Copy Service (VSS). Block-level backup technology increases performance by bypassing the files and file system. In other words, Windows Server Backup reads the blocks in the order they appear on the disk instead of reading them in the order they appear in files, which are usually fragmented across the disk. ***Volume Shadow Copy Service (VSS)*** takes a snapshot of the volume's current data, which is used by Windows Server Backup to back up the data. The snapshot, or shadow copy, is then deleted when the backup has completed.

If you are backing up full volumes, you have the option to optimize the backup process by selecting *Configure Performance Settings…* under the Actions panel in the Windows Server Backup console.

The following provides a brief overview of each option:

- **Normal backup performance (default):** Indicates you are performing full backups and that you want the volume's contents transferred in their entirety.
- **Faster backup performance:** Indicates you are performing incremental backups; therefore, Windows keeps a shadow copy on the source volume, which it will use to track changes. The next time you perform a backup, only the changes made since the last backup will be transferred. This is accomplished by reading from the "diff" area of the shadow copy. The "diff" area is storage space on a volume that is used to maintain a set of information that represents the differences between the current content and the content from a previous point in time. These differences are called *snapshots* and you look at them closer later in this lesson. To protect against data loss, Windows Server Backup still performs a full backup when you reach 14 incremental backups and more than 14 days have passed since the last full backup.
- **Custom:** Allows you to configure each volume separately.

TAKE NOTE*

A remote share (\\server02\volbackup) needs to be created on Server02 before starting this exercise, and Server01 needs to have a simple volume named *CorpData* mapped to drive (E:) with a few sample folders and files to include in the backup.

PERFORM A MANUAL BACKUP OF A LOCAL VOLUME TO A REMOTE SHARE

GET READY. To complete a backup on a volume on Server01 to a remote share on Server02, perform the following steps:

1. Log in to the Server01 and open Server Manager.
2. Click Tools > Windows Server Backup.
3. Select Backup Once from the *Actions* panel.
4. Select Different Options when prompted to select a Backup option and click Next.
5. Select Custom for the backup configuration and click Next.
6. Select Add Items, select the CorpData (E:) volume, and then click OK.
7. Select Next to continue.
8. On the *Specify Destination type* screen, select Remote shared folder, and then click Next.
9. Enter the location \\server02\volbackup and click the More information link to read and understand the security implications of backing up to a shared folder. Click OK and then click Next to continue.
10. Review the backup items to confirm your settings and then click Backup.
11. Click Close after the backup status changes to completed for the Corpdata volume.

PERFORM A SCHEDULED FULL BACKUP TO A REMOTE SHARE

GET READY. To complete a full backup on Server01 to a remote share on Server02, perform the following steps:

TAKE NOTE*

A remote share (\\server02\fullbackup) needs to be created on Server02 before starting this exercise.

1. Log in to the Server01 and open Server Manager.
2. Click Tools > Windows Server Backup.
3. From the *Actions* panel, select Backup Schedule and click Next when the *Getting Started Wizard* appears.
4. Select Full server (recommended) and click Next.
5. Select Once a day, select a time of day that is closest to your current time, and click Next.
6. Select Backup to a shared network folder and click Next.
7. Click OK after reading the message that each backup will erase the previous backup when using a remote shared folder as a storage destination.
8. Enter the location for the backup \\server02\fullbackup, and then click Next.
9. Enter the user name and password to use for scheduling the backup, and then click Next.
10. Review the settings and click Finish.
11. Click Close.
12. Confirm the backup was successful by viewing the status in Windows Server Backup after the scheduled time has passed.

PERFORM A BARE METAL RECOVERY BACKUP OF A SERVER

GET READY. To complete a bare metal recovery backup on Server01 to a remote share on Server02, perform the following steps:

1. Log in to the Server01 and open Server Manager.
2. Click Tools > Windows Server Backup.

TAKE NOTE*

A remote share (\\server02\BMbackup) needs to be created on Server02 before starting this exercise.

3. From the *Actions* panel, select Backup Once.
4. Select Different Options when prompted to select a Backup option and click Next.
5. Select Custom for the backup configuration and click Next.
6. Select Add Items and select the Bare metal recovery. Notice that a bare metal recovery includes the system state, system reserved, and c: but not data drives. To restore volumes that include data to a new system, you need to include them as part of the backup. Click OK.
7. Click Next.
8. Select Remote shared folder for the storage location, and then click Next.
9. Enter the location for the backup \\server02\BMbackup, and then click Next.
10. Confirm the settings and click Backup.
11. Click Close after the backup has completed successfully.

Configuring Microsoft Azure Backup

Storing your backups in the cloud allows you to retrieve them from any location where you have Internet access as well as provides you with an offsite storage location to protect against disasters.

Microsoft Azure Online Backup is a feature available with Windows Server 2012 R2 that allows you to back up your files and folders to the Microsoft Azure Online Backup service. Microsoft Azure is a cloud-based storage service managed by Microsoft. The backups are compressed, which means the backup is smaller and reduces bandwidth requirements. The backups are also encrypted to protect the data while it's stored. Storing your data in the cloud allows you to recover it from any location that has Internet access and provides offsite protection against disasters (for example, floods, earthquakes, fire, and theft).

A Windows Azure Backup Online Agent, installed on each server and integrated with the Windows Server Backup console, connects to the Microsoft Azure Recovery Services service and transfers file and folder data. Prior to transferring the data, the agent compresses and encrypts it using a passphrase you create during setup. The agent, which is an add-on for Windows Server 2012 or Windows Server 2012 R2, can also be integrated with System Center 2012 (SP1) or System Center 2012 R2 DPM.

When using Microsoft Azure Recovery Services, you need to keep the following in mind:

- It's only used with Windows Server 2012 or Windows Server 2012 R2.
- If BitLocker is enabled to protect your data files, it must be turned off in order for the software agent to back up your data files.
- You can back up only files and folders (data); system state and system drives are not supported.

There are eight steps to get a server up and running with Microsoft Azure Recovery Services.

1. Install and enable the Windows Server Backup feature on each server you want to back up.
2. Generate a digital certificate for the server. The certificate must have at least 2048 bit key, the enhanced key usage is Client Authentication, and the expiration date is not more than 3 years from current date.
3. Export the certificate to a file.
4. Register and set up an account for the Microsoft Azure Recovery Services.

5. Log in to Microsoft Azure with the account.
6. Access Recovery Services, create a New Vault (as shown in Figure 8-1), click Backup Vault, and then click Quick Create. You then specify the name and region of the vault, and then click Create Vault.

Figure 8-1

Creating a new vault

7. After the vault is created, open the vault by clicking the vault.
8. Click Manage certificate to upload the server certificate that you exported in Step 3.
9. Download and install the Windows Azure Online Backup Agent, and then verify the installation.
10. Using the Start button, start Windows Azure Backup.
11. When the Windows Azure Backup opens, click Register Server to register the current server for backup. You will choose the same certificate that you uploaded previously, select the Backup Vault, and then specify a passphase (which will be used with the backups).
12. Set up a backup schedule.

SCHEDULE A MICROSOFT AZURE ONLINE BACKUP

GET READY. To back up a data folder on Server01 using the Microsoft Azure Online Backup service, perform the following steps:

TAKE NOTE*

Before starting this activity, create a folder named *OnlineBackups* on the C: drive and add a text file to the folder.

1. Open the Windows Azure Backup console if it is not already open.
2. Select Schedule Backup under the *Actions* panel.
3. Click Next when the wizard launches.
4. On the *Select Items to Backup* screen, select Add Items.
5. Expand the C: drive, select OnlineBackups, and then click OK.
6. Click Next to continue.
7. Select the current day for your backup.
8. Select an available time that is closest to your current time and click Add to move it to the scheduled time for your backup. Click Next.
9. Confirm the retention period is set to its default (7 days) and click Next. Windows Azure Online also supports retention periods of 15 and 30 days.
10. Review your selections and then click Finish. Windows Azure Online Backup has a limit of 825 GB per volume of data that can be backed up in one backup operation.
11. Select Close when notified that the Online Backup was scheduled successfully.

Upon completion of the backup, you see the message, under the Jobs tab. If you don't want to wait for the scheduled backup to occur, you can right-click *Online Backup* from the Action pane and select *Backup now* from the menu that appears. The Alerts tab provides information regarding problems you need to address as well as a message when there is a new version of the Windows Azure Backup Agent available for download.

Configuring Role-Specific Backups

The roles assigned to a server can dramatically impact its configuration as well as the frequency and type of backup needed to restore it in the future.

As part of your overall backup strategy, take into consideration the roles installed on each of your servers. As you learned, the role performed by the server can have an impact on how you approach the backup and eventually the restore of the server. Let's take a closer look at some of these roles and what can be done to back them up.

BACKING UP DHCP AND DNS

The Dynamic Host Configuration Protocol (DHCP) database contains information about IP address leases, reservations, scopes, scope options, and DHCP registry key settings. It's backed up automatically at 60-minute intervals to the %systemroot%\System32\Dhcp\Backup directory. It is also backed up as part of a system state or full backup, and by using the DHCP Manager console.

You can back up DHCP via the DHCP Manager console by performing the following steps:

1. Open the *DHCP Manager* console.
2. Select the DHCP Server that contains the scopes you want to back up.
3. Select *Action* > *Backup*.
4. Browse to the folder where you want to store the backup and click *OK*. By default this will be the %systemroot%\Windows\System32\Dhcp\Backup.
5. Click *OK*.

Active Directory-integrated DNS zone configuration information is stored in the registry; therefore, it's also backed up as part of the system state and during full backups. In situations where you have a corrupted or failing DNS, you can recover it only by restoring the entire system state, which might or might not be what you want to do. An alternative is to use DNSCMD with the /zoneexport switch to export the Active Directory-integrated zones to a file you can back up. This file can be restored as a primary zone file and then converted into an Active Directory-integrated zone if necessary.

The following command creates a copy of the DNS zone contoso.com in the %systemroot%\system32\dns\backup\contoso.com.dns.bak file.

```
DNSCMD /zoneexport contoso.com \backup\contoso.com.dns.bak
```

The XCOPY command can be used to back up primary and secondary zone files to a backup folder you specify.

```
Example: XCOPY %systemroot%\system32\dns c:\backups\dns /y
```

The command backs up all zone text files into the c:\backups folder.

You can then restore them by using XCOPY to copy the backup to the %systemroot%\system32\Dns folder.

BACKING UP WINS

The Windows Internet Name Service (WINS) maintains a distributed database used to register and query dynamic mappings of NetBIOS names for computers and groups. It maps NetBIOS names to IP addresses. Although the database is backed as part of system state and full backups, you can also back up the WINS database from the WINS console.

Because most of the entries in the database are dynamically entered by the servers and workstations, the only reason to back it up would be if you had created static entries in the WINS database. You can back up the WINS database by performing the following steps:

1. Open the *WINS* console.
2. Right-click the *WINS Server*.
3. Select *Back Up Database*.
4. Browse to the folder where you want to store the backup and click *OK*. By default this will be %systemroot%\Windows\System32\WINS.
5. Click *OK*.

BACKING UP CERTIFICATE SERVICES

Certificate Services stores a database in the C:\Windows\system32\Certlog location by default. When certificates are issued to users and computers, the associated information is maintained in the Certificate Services database.

If this database becomes corrupted or is accidentally deleted, certificates issued by the server will be considered invalid. Although Certificate Services is backed as part of a system state and a full backup, you can also back it up via the Certificate Services console by performing the following steps:

1. Open the *Certificate Service* console.
2. Right-click the server and select *All Tasks >Backup CA …*
3. Select *Next* to start the Certification Authority Wizard.
4. Select *Private Key and CA Certificate* and the *Certificate database and certificate database log* options.
5. Enter *C: \Windows\System32\CABackup* and click *Next*.
6. Click *OK* to create the directory.

7. Enter and confirm a password to gain access to the private key and the CA certificate file and click *Next*.
8. Click *Finish* to back up the Certificate Authority.

Managing VSS Settings Using VSSAdmin

Volume Shadow Copy Administrative Command-line Tool (VSSAdmin) can be used to create and delete volume shadow copies/associations, list shadow copy providers and writers, and resize a volume shadow storage association.

The VSSAdmin is used to manage the VSS. Before you take a closer look at this tool and the information it provides, it's important that you have a good understanding of VSS and its components.

The VSS coordinates several components, which allow you to back up your server without impacting running applications or users. It accomplishes this through the use of shadow copies. A shadow copy (also called a *snapshot*) of a volume is a duplicate of the data on the volume at a specific point in time.

The VSS components communicate with each other via the VSS Framework to both create and restore your shadow copies.

MANAGE VSS SETTINGS USING VSSADMIN

GET READY. To manage VSS settings using VSSAdmin, perform the following steps:

1. Log in to Server01 with administrative privileges.
2. Open a command prompt.
3. Type the following to see a list of commands supported with vssadmin:

   ```
   c:\vssadmin /?
   ```

4. Type the following to see a list of VSS writers on Server01 and their current state.

   ```
   c:\vssadmin list writers
   ```

   If this were a server and you noticed one or more of the VSS writers with a state set to Failed, you can most likely fix them with a quick server reboot. In situations where you cannot reboot the server, you can search the registry or the Internet for the Writer ID to identify the service associated with it. You can then restart that specific service and rerun the list writers command to confirm the fix.
5. Type the following to see a list of VSS providers on Server01:

   ```
   c:\vssadmin list providers
   ```

6. Type the following to see a list of existing volume shadow copies:

   ```
   c:\vssadmin list shadows
   ```

7. To list the volumes that are eligible for shadow copies, enter the following:

   ```
   c:\vssadmin list volumes
   ```

8. To view used, allocated, and maximum shadow copy storage space, type the following:

   ```
   c:\vssadmin list shadowstorage
   ```

After running the command, you see the amount of shadow copy storage space being used, the amount allocated for the future, and the maximum space that can be used. If you notice the amount of storage space that is being used is almost as large as the maximum, you might need to move the VSS storage area to another location. This can be accomplished by accessing the computer's volume that is currently used for the volume shadow copy storage area, right-clicking it, and selecting *Configure Shadow Copies*. Select *Settings* and then choose another volume to store the shadow copies on.

Creating System Restore Snapshots

Shadow Copies for Shared Volumes (SCSV) and Hyper-V checkpoints provide you with the ability to return to a specific point in time.

Although Windows client operating systems support the ability to create system restore points, Windows Server 2012 and Windows Server 2012 R2 don't. What they do provide is the ability to use Shadow Copies for Shared Volumes (SCSV) as well as Hyper-V checkpoints as mechanisms for returning to a specific point in time. You can also utilize the Hyper-V VSS writer and VSS to back up virtual machines (VMs) using Window Server Backup.

ENABLING SHADOW COPIES FOR SHARED VOLUMES

Shadow Copies for Shared Volumes (SCSV) uses the capabilities of the VSS to capture and store copies of folders and files (located on shared network resources) at a specific point in time.

When SCSV is implemented on a volume, both end users and administrators can recover accidentally deleted or overwritten files as well as compare different versions of the same file. Because end users can restore their own files, implementing SCSV can dramatically reduce not only the time but the associated costs of having to recover their folder and files via their IT support desk.

You enable SCSV on a per-volume basis by selecting *Server Manager* > *Tools* > *Computer Management*. The volumes must be formatted using NTFS and should not contain any mounted drives or mount points. If the volume has either, their contents will not be included in the shadow copies. The first shadow copy of the volume is a complete copy of the data; subsequent shadow copies include only the changes made since the last shadow copy was created. The source volume is the volume that contains the data you want to copy. The storage volume is where your shadow copies will be located and if possible should be placed on a separate disk from the one that holds the source volume.

You need at least 300 MB of free space to create a shadow copy on the selected volume. By default, a shadow copy is created at 7:00 AM (Monday-Friday) and at 12:00 PM (Monday-Friday). You can modify the schedule by selecting the *Settings* button. You can also click the *Create Now* button to take a manual snapshot between scheduled times (see Figure 8-5).

ENABLE SHADOW COPIES FOR SHARED VOLUMES

GET READY. To enable Shadow Copies for Shared Volumes on Server01, perform the following steps:

1. Log in to Server01 with administrative privileges.
2. Create a shared folder called CorpDocs on a simple volume (E:) on Server01 and share the folder so that administrators have full access.
3. Create a file in the *CorpDocs* folder named Agenda.txt, enter sample text, and then save and close.
4. Open Server Manager, and select Tools > Computer Management.
5. Expand the Storage item and select Disk Management.
6. Right-click the volume you created the shared folder on and select Properties.
7. Select the Shadow Copies tab.
8. Confirm the volume you selected in Step 4 is highlighted and then click Enabled.
9. Click Yes to confirm you want to enable shadow copies on the volume. A snapshot is taken immediately and the date/time stamp is noted.
10. Click Create Now to create a second snapshot of the selected volume and then click OK to close.

Business Case Scenarios

Scenario 8-1: Recovering the System State of DNS

You are currently running system state backups on a server that has Active Directory-integrated DNS zones. Will this be sufficient to allow you to restore the DNS zones should they become corrupted? What are the restore implications to consider when using this backup approach?

Scenario 8-2: Running Out of Space

After running the `vssadmin list shadowstorage` command, you noticed that the amount of storage space used for shadow copies is almost as large as the maximum configured size. What should you do?

9 LESSON

Recovering Servers

Preparing For Windows Server 2012 R2 Restores

THE BOTTOM LINE

Having a written server recovery plan that outlines roles and responsibilities as well as the steps necessary to recover your servers is critical to reducing the overall downtime and loss of productivity in your organization.

Do you have a written plan that describes how you will recover a server in your organization? If so, when is the last time you reviewed it to make sure it was current and applicable to your existing environment?

If you're like most, you either don't have a plan or the one you do have is probably out of date. You might be thinking, "No problem! I'll figure it out when the time comes." If so, that would be a mistake! When users need access to data that has become corrupted or lost or in situations where a server is no longer functional, you will discover quickly how stressful and hostile those around you can become.

Here are just a few questions to consider when developing a recovery plan for your servers:

1. Who will be on the recovery team from IT and what will each of their recovery responsibilities be?
2. Do you know how many servers you have and where they are located (main office, branch office, and so on)?
3. Do you have a current network topology map that shows all critical servers, roles/features, IP addressing information, and network connections?
4. Do you have the specs on each server (memory, drive space, and volume info)? In other words, the information you need to know to rebuild the server from scratch?
5. Which server(s) will you need to recover first?
6. What is the step-by-step procedure for how the data recovery process will occur on each?
7. How will you know/test that things are back to normal after the restore?
8. When is the last time you performed a test restore to make sure your backups were working correctly?

When the time comes to restore a server, you need to decide whether you want to restore the entire system, restore a single volume, or spend some time trying to troubleshoot the problem and hopefully get the server back into production. The option you choose depends upon the situation you find yourself in at the time.

In this lesson, you look at how to address and perform some of the most common restores you will experience when running Windows Server 2012 R2. The backups that you restore from were created in Lesson 8, "Configuring and Managing Backups."

Restoring Files and Folders

Windows Server provides two options when it comes to restoring files and folders. You can take advantage of the Previous Version option if shadow copies are available or use Windows Server Backup to restore your data.

If a user accidentally deletes or overwrites a file or folder on a network share, you have two options for restoring the data:

- Access the share and restore the previous version.
- Use Windows Server Backup to restore the data.

The simplest approach for restoring files is to access the share and restore the previous version of the file. Of course, this assumes you enabled Shadow Copies for Shared Volumes (SCSV) on the volume prior to the point in time the data was deleted. As you recall from Lesson 8, SCSV uses the capabilities of the Volume Shadow Copy Service (VSS) to capture and store copies of folders and files (located on a shared network resource) at a specific point in time. The previous version of the file, which is read-only until it is restored, comes from shadow copies that are saved automatically on the server.

When working with previous versions of files, you have two options: copy a previous version of the file to a new location or restore a previous version of the file.

If you select *Copy*, you will be prompted to select a new location. The file's permissions will default to those of the directory where you place the file. The following lists the basic steps to copy a previous version of the file:

1. Connect to the shared folder.
2. Right-click the folder and select *Restore previous versions*.
3. Select the version of the file you want to copy from the Previous Versions tab and click *Copy*.
4. Select the place where you want to copy the file to.
5. Select *Copy*.
6. Select *OK* to close.

If you choose restore, you will delete the current version and restore the file to the state it was in at the date and time you selected. This means any changes that were made after that time will be lost, but the file retains its permission settings. The following lists the basic steps to restore a previous version of the file:

1. Connect to the shared folder.
2. Right-click the folder and select *Restore previous versions*.
3. Select the version of the file you want to restore from the Previous Versions tab and click *Restore*.
4. Read the prompt and click *Restore*.

You can store a maximum of 64 copies per volume. Once you reach the limit, the oldest shadow copy will be permanently deleted.

If you did not enable shadow copies on the volume, you can use the Windows Server Backup program to restore the data. Windows Server Backup provides similar options when it comes to restoring your data. You can overwrite the existing data or restore a copy with a different name. You can also determine whether you want to restore permissions to the file or folder that you are recovering.

The following lists the basic steps to restore a previous version of a file previously backed up from the local computer, to its original location overwriting existing versions with the recovered version:

1. Open *Server Manager* and select *Tools* > *Windows Server Backup*.
2. Select *Local Backup*.
3. Click *Recover* under the Actions pane.
4. Select the location of the backup (local server).
5. Select the backup you want to restore by date/time.
6. Select *Files and Folders* on the Select Recovery Type page.
7. Select the files to be restored.
8. Specify that the files will be restored to their original location.
9. Select *Overwrite the existing versions with the recovered versions*.
10. Verify your selections and click *Recover*.

RESTORE A FILE USING SCSV

GET READY. To restore a file using the Copy option, perform the following steps:

1. Log in to Server02 with administrative privileges.
2. Select the Windows logo key + R and enter the following command in the *Run* dialog box, to view the shared folders on Server01:

   `\\server01`
3. Right-click the CorpDocs shared folder and select Restore previous versions.
4. Select the CorpDocs folder with the latest date modified and click Copy.
5. Select Desktop as the place where you want to copy the Agenda.txt file to, and then click Copy.
6. Click OK.

TAKE NOTE*

This exercise uses a folder created on Server01 in Lesson 8.

Restoring Volumes

The approach used to restore a volume depends on the type of volume you need to recover. Data volumes can be restored using Windows Server Backup, whereas system volumes require you to use the WinRE and Windows installation media.

If the volume you lose contains data only and you still have access to the operating system, you can perform the restore using Windows Server Backup.

To restore a system volume, you must restore using the ***Windows Recovery Environment (WinRE)*** and the Windows installation media. WinRE provides a set of utilities that can assist you in troubleshooting and recovering a system that will not boot due to problems with the operating system files, services, and device drivers.

Here are a few things to keep in mind when restoring a system volume:

- The server's hardware must not have changed and your data volumes must still be operational.
- The server's current system volume will be erased and replaced with the restored system volume.
- If there are any data volumes on the same disk that contain the system volumes, they will be erased as part of the restore process.

RESTORE A DATA VOLUME

GET READY. To restore a data volume on Server01, perform the following steps:

TAKE NOTE*

This exercise uses the \\server02\Volbackup created in Lesson 8.

1. Log in to Server01 and open Server Manager.
2. Select Tools > Computer Management.
3. Expand Storage and select Disk Management.
4. Right-click the CorpData volume (E:\) and select Delete Volume.
5. Select Yes after reading the warning message.
6. Create a new volume that is the same size or larger than the previous Corpdata volume, assign it the letter (E:\), and name it CorpData.
7. Expand Windows Server Backup under the *Storage* node and select Local Backup.
8. Select Recover under the *Actions* pane.
9. Select a backup stored on another location and click Next.
10. Select Remote shared folder for the location type and click Next.
11. Enter \\server02\volbackup and click Next.
12. Select the newest available backup (see Figure 9-1) and click Next.

Figure 9-1

Selecting the newest volume backup

13. Select Volumes for the recovery type and click Next.
14. Select CorpData (E:) and click Next.
15. Select Corpdata (E:) as the *Source Volume* and select the drop-down arrow under *Destination Volume* to select the new volume you created in Step 6. Click Next to continue.

16. Select Yes to confirm you want to continue the recovery operation.
17. Click Recover.
18. Click Close once the volume has been recovered.
19. Select Disk Management and confirm the recovered volume shows as healthy.
20. Right-click the recovered volume and select Explore. You should see the sample folder/files you created in Lesson 8.

Restoring the System State

The system state includes the operating system configuration files. What is included in the system state differs depending upon the role(s) performed by the server. This also impacts the process used to restore the system state when the time comes.

The system state is included in the following backup configuration options:

- Full backups (recommended)
- Bare metal recovery backups
- System state backups

In addition to regularly scheduled backups, you should also perform a manual backup prior to installing a new service pack, driver, or program on the server. In either case, you are preparing for the operating system crash that will inevitably happen.

When backing up the system state, the Windows Server Backup program will take care of the details for you. In other words, you don't have to select each component. Of course, this comes at a cost because when the time comes to restore, your only option is to restore the entire system state. This might or might not be what you want to do as discussed in the section, "Configuring Role-Specific Backups" in Lesson 8.

RESTORING THE SYSTEM STATE ON A MEMBER SERVER

Recovering the system state of a member server can be performed via the Windows Server Backup program. The following steps are typically performed after you replace the faulty hardware and install the Windows operating system:

1. Log in to the member server and open *Server Manager.*
2. Select *Tools* > *Windows Server Backup*.
3. Select *Local Backup* and then select *Recover* from the Actions pane.
4. Select the location where the backup is stored.
5. Select the specific backup you want to restore by date/time.
6. Select system state as the recovery type option.
7. Select the location to restore to.
8. Review your selections and select *Recover*.
9. Reboot the server and confirm functionality.
10. Perform a full backup.

Performing a Bare Metal Recovery Restore

A bare metal recovery restore allows you to restore the server without having to load the operating system beforehand. It does require that you have your Windows installation media from which to boot.

When your server suffers a catastrophic failure, Windows Server 2012 R2 provides you with the option to perform a Bare Metal Restore.

Remember that bare metal recovery backup does not include your data volumes unless you specifically included them in your selection when you set up the backup job.

Although most of the steps in the restore process are straight-forward, there is one point in the recovery process that you need to make a critical decision: whether or not you want to format and repartition your disks or only restore your system drives.

If you select to format and repartition disks, the restore process will delete and reformat the existing partitions on the target drive to be the same as the one included in the backup. You have the option to exclude disks if there are disks that you want to omit from the formatting and partitioning process. If you are restoring from a backup on a locally attached disk, it will automatically be excluded. If all disks are not visible when using the exclude disks option, you might need to use the *Install drivers* button to add the drivers for the storage device you are recovering to. To recover only the operating system, you can select the option to only restore system drives option.

The Advanced option allows you to indicate whether you want to automatically restart the server and determine whether you want to check the disks for errors after the recovery process is complete.

For example, if the disk that contains the operating system has failed and you are restoring to a new disk, *Format and repartition disks* will be the appropriate option. If the server is corrupt, refuses to start, and the disk that contains the system partitions is functional, then you should select to restore only system drives.

TAKE NOTE*

You need to set up a VM without an operating system installed and use the *\\server02\BMbackup* you created during Lesson 8 to complete this exercise. The existing VM (Server01) should be shut down before the new VM is started.

PERFORM A BARE METAL RESTORE OF A SERVER

GET READY. To complete a bare metal recovery of Server01 onto another server VM, perform the following steps:

1. Open Hyper-V Manager and create a new virtual machine (VM).
2. Insert a DVD with the Windows Server installation files or configure the appropriate ISO image file to use in the settings for the VM machine.
3. Start the new VM.
4. Select Next after confirming the language, time/currency format, and keyboard or input methods.
5. Select Repair your computer.
6. Select the Troubleshoot tile.
7. Select the System Image Recovery tile.
8. Close the *Re-image your computer* dialog box and click Next.
9. Select the Advanced button and click Search for a system image on the network.

10. Select Yes when asked if you want to connect to the network.
11. Enter the path to the system image: \\server02\BMBackup and click OK.
12. Enter a user name and password to connect to the share on Server02 (for example, Administrator) and its associated password, and click OK.
13. Select the image and click Next.
14. Select the date and time of the system image to restore and click Next.
15. Select Format and repartition disks.
16. Click Next to continue.
17. Review the information provided and click Finish.
18. Select Yes when prompted that all disks to be restored will be formatted and replaced with the layout and data in the system image.
19. Log in with administrative credentials once the server reboots.
20. Confirm the server is operational.

Recovering Servers Using WinRE and Safe Mode

If you experience problems that prevent Windows Server 2012 R2 from booting, you can use the Windows Recovery Environment (WinRE) to troubleshoot and repair the system.

There are several ways to access the Windows Recovery Environment (WinRE) in Windows Server 2012 R2:

- The server enters WinRE in situations after two consecutive failed attempts to start Windows, after two consecutive shutdowns that were unexpected, or due to secure boot errors. Secure boot is a security feature built into Windows Server that captures a signature of the operating system. Windows checks against the signature the last time it booted up. If the signatures don't match, the system enters WinRE.
- Select *Settings* from the Charms bar, choose *Power,* and click *Restart* while holding down the *Shift* key.
- Boot the server from Windows installation media and select *Repair Computer*.
- Enter the command `shutdown /r /o` from a command prompt.

Upon entering the WinRE environment, you have the following options:

- **Continue:** Exits the WinRE environment and continues to the Windows Server 2012 R2 operating system.
- **Turn off PC:** Shuts down the server.
- **Troubleshoot:** Provides access to the following tools.
  - **System Image Recovery:** Restores the entire system to a previous state by using an image created by Windows Backup. This option should be used only after you try other options and assumes you have a current backup of your server to restore from.
  - **Command Prompt:** Provides command-line access with administrator privileges to the Windows Server file system. You can use it for tools such as Diskpart, System File Checker, bootrec, bcdedit, and format.
  - **Startup Settings:** Provides access to the Advanced Boot options menu.

From the Advanced Boot Options menu, you can select from the following:

- **Repair Your Computer:** Provides a list of system recovery tools that you can use to repair your system, run diagnostics, or restore your system (for example, System Image Recovery, Command Prompt, and Startup Settings).

- **Start Safe Mode:** Starts Windows using only the core drivers and services. This option should be used when you cannot boot after the installation of a new driver and/or device.
- **Start Safe mode with Networking:** Similar to safe mode but with networking support. Use this option to create a network connection to gain access to files on servers, connect and compare settings on other computers, and use the Internet to download updates.
- **Start Safe mode with Command Prompt:** Similar to safe mode but opens a command prompt.
- **Enable Boot Logging:** Creates ntbt.log.txt that lists all of the drivers that are loaded during setup. This includes the last driver loaded before the system failed. It's stored in the %systemroot%.
- **Enable low resolution video:** Starts Windows in low resolution display mode; allows you to set or reset the display resolution.
- **Last Known Good Configuration (advanced):** Starts Windows using the settings from the last time that Windows booted successfully.
- **Debugging Mode:** Enables the Windows kernel debugger.
- **Disable automatic restart on system failure:** The settings here prevent Windows from automatically rebooting after a crash.
- **Disable Driver Signature Enforcement:** Allows drivers containing improper signatures to be loaded.
- **Disable Early Launch Anti-Malware Driver:** Allows drivers to initialize without being measured by the anti-malware driver.

BOOTING INTO SAFE MODE

In Windows Server 2012 R2, you can boot into safe mode by using one of the options discussed previously. Starting in ***safe mode*** allows you to troubleshoot situations where you cannot access the system due to faulty hardware, software, device drivers, and virus infections.

Safe mode loads a minimal set of drivers and services; therefore, if you can boot into safe mode but can't boot normally, the system most likely has a conflict with hardware settings, services, drivers, or some type of registry corruption.

Once you can access your system via safe mode, you should check the event viewer (System and Application logs) for errors. You can also run the Windows System Information tool (msinfo32.exe) to gather details about the computer, operating system, and software including drivers. You can also search for problem devices.

You can review the ntbtlog located in the %systemroot% folder. You can open this file using a text editor (Notepad) to review the devices and services that loaded and did not load. The file shows the path of each item and identifies them as BOOTLOG_LOADED or BOOTLOG_NOT_LOADED.

Another option is to run MSConfig and use the process of elimination to identify the source of the problem that is keeping Windows from booting correctly. ***MSConfig*** (also called *System Configuration*) is a tool used to troubleshoot the system startup process (see Figure 9-2). It can be used to disable or enable, software, device drivers, and services that run at startup. MSconfig can also be used to change boot parameters if necessary.

Figure 9-2

Using MSConfig to troubleshoot

The general process for troubleshooting using MSConfig is as follows:

1. Start Windows in Diagnostic startup mode in the General tab. If the problem occurs during a diagnostic startup, files and drivers are suspect. If the problem does not occur, proceed to Step 2.
2. Start Windows in Select startup mode in the General tab.
3. Select the services tab and disable each service one at a time and restart the server. If the problem does not go away, you can eliminate the services as the source.
4. Select the *Startup* tab and turn off all startup items except the first one. Reboot the server. This process can be used to isolate a startup item.

BOOT INTO SAFE MODE

GET READY. To boot into safe mode on Server01, perform the following steps:

1. Log in to Server01 and enter the following at a command prompt:
   shutdown /r /o
2. Select Close when prompted the system will shutdown in less than a minute.
3. Select the Troubleshoot tile.
4. Select the Startup Settings tile.
5. Select Restart.
6. Select Safe Mode and press Enter.
7. Enter the password for the Administrator account and press Enter.
8. Confirm your system is now in safe mode. The word "safe mode" should appear on each corner of your desktop.
9. Select the Windows logo key + R to open the *Run* dialog box.
10. Enter MSConfig and select OK.
11. Review each tab of the *System Configuration* tool for options you can configure and then close the dialog box.
12. Select the Windows logo key + R to open the *Run* dialog box.
13. Enter compmgmt.msc to open the *Computer Management* console.
14. Expand Event Viewer > Windows logs and review the *System and Application* logs. Close the *Computer Management* console.

TAKE NOTE*

The /r switch tells the server to restart; the /o option tells the server to end the current Windows session and open the Advanced Boot options menu.

15. Use File Explorer to navigate to %systemroot% and locate the ntbtlog.txt file.
16. Open the ntbtlog.txt file to view its contents.
17. Restart the computer by running the following from a command prompt (do not use the /o switch):

    shutdown /r

Configuring the Boot Configuration Data Store

The Boot Configuration Data (BCD) store, a replacement for the boot.ini file in previous releases, stores boot configuration information.

The ***Boot Configuration Data (BCD) store*** contains information that controls how your server boots. It replaces the boot.ini text file that was used in Windows Server 2003 to manage the boot configuration information. The BCD store is located in the \Boot\Bcd directory on BIOS-based operating systems and on the Extensible Firmware Interface (EFI) system partition on EFI-based systems.

Windows Boot Manager displays a list of boot loader entries when your server boots. When you select one of these entries, the Windows Boot Manager loads the system specific boot loader for that operating system and passes those parameters for that boot entry to the system-specific boot loader. The boot loader then loads the operating system based on the parameters it finds.

Because the BCD store is a binary file, you can't modify it by using a standard text editor such as Notepad. Instead, you need to use the ***Boot Configuration Data Editor (bcdedit.exe)*** tool from a command prompt.

To see the list of entries in BCD store, you can enter the following command:

```
Bcdedit /enum
```

In Figure 9-3, you can see the boot environment is split into two components:

- Windows Boot Manager
- Boot loaders/applications

Figure 9-3

Viewing the BCD store with only one operating system loaded

The ***Windows Boot Manager*** makes it possible for you to choose which boot loader/application to load. A ***boot loader/application*** is a small program that moves the operating system into memory. In Figure 9-3, you see a computer that is running Windows Server 2012 R2 only; therefore, only one boot loader is listed. In situations where you are running multiple operating systems on the same system, you see more than one, as shown in Figure 9-3.

This is a client computer running both Windows 7 and Windows 8/8.1 in a multi-boot configuration. As you can see from the Figure 9-4, Windows Boot Manager displays two boot loaders.

Figure 9-4

Viewing the BCD store with more than one operating system

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>bcdedit /enum

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=D:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
integrityservices       Enable
default                 {current}
resumeobject            {da59507d-6721-11e2-8537-eb524f47fdcc}
displayorder            {current}
                        {849ab759-2b7d-11e2-9a4d-10bf4879ebe3}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Windows 8
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {da59507f-6721-11e2-8537-eb524f47fdcc}
integrityservices       Enable
recoveryenabled         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \Windows
resumeobject            {da59507d-6721-11e2-8537-eb524f47fdcc}
nx                      OptIn
bootmenupolicy          Standard
hypervisorlaunchtype    Auto

Windows Boot Loader
-------------------
identifier              {849ab759-2b7d-11e2-9a4d-10bf4879ebe3}
device                  partition=D:
path                    \Windows\system32\winload.exe
description             Windows 7
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {849ab75a-2b7d-11e2-9a4d-10bf4879ebe3}
recoveryenabled         Yes
osdevice                partition=D:
systemroot              \Windows
resumeobject            {849ab758-2b7d-11e2-9a4d-10bf4879ebe3}
nx                      OptIn

C:\Windows\system32>
```

USING BCDEDIT TO MODIFY SETTINGS IN THE BCD STORE

`Bcdedit /timeout <value>` can be used to configure the length of time the computer waits until the default operating system loads. For example, in Figure 9-4, the multi-boot system is configured to boot to Windows 8.1 after 30 seconds pass. To change this setting to only wait for 10 seconds, you enter the following command:

```
bcdedit /timeout 10
```

To create a backup of this BCD store to a folder named *BcdStore* on drive D:\, you enter the following command:

```
bcdedit /export D:\BcdStore
```

You can use `bcdedit /import D:\BcdStore\bcdbackup` to import and restore the backup created using the /export switch.

USING BOOTREC WITH BCDEDIT TO REPAIR A CORRUPTED/MISSING BCD STORE

In Windows Server 2012 R2, the boot loader (bootmgr) looks for the BCD store on the active partition. If the BCD store is missing or corrupt, you see the "Boot Configuration Data for your PC is missing or contains errors" message or a similar error during the boot process.

The best approach to take is to rebuild the BCD using the ***Boot Recovery Tool (bootrec.exe)*** by using the following command after booting in to WinRE:

```
Bootrec /rebuildbcd
```

After running the command, you see a message informing you that there is one or more Windows installations identified along with the path to the installation(s) (for example, C:\Windows, D:\Windows). If an installation is found, you have the option to add it to the boot list; reboot the server and you should be up and running again. If the message indicates there are no installations of Windows identified, you need to export the BCD store by using the following bcedit.exe command:

```
Bcdedit /export c:\BCDStore
```

After backing up the BCD store, you need to remove the hidden, read-only, and system attributes from the BCD file so that you can modify it. This can be done by using the attribute command to change the attributes on the file:

```
Attrib c:\boot\bcd -h -r -s
```

After modifying the BCD file's attributes, rename the existing BCD store by using the Ren command:

```
Ren c:\boot\bcd bcd.old
```

Next, rebuild the BCD store by entering the following command:

```
Bootrec /rebuildbcd
```

Once the rebuild of the BCD store is completed successfully, you should see that a Windows installation was identified and be prompted to add the installation to the boot list. After doing so, reboot the server and you should be up and running.

TAKE NOTE*

This exercise simulates a corruption of the BCD store allowing you to take the steps necessary to rebuild it. You need access to Windows Server installation media before starting this exercise.

REBUILD A BCD STORE

GET READY. To rebuild a BCD store on Server01, perform the following steps:

1. Log in to Server01 and enter the following at a command prompt:
   shutdown /r /o
2. Select the Troubleshoot tile.
3. Select the Command Prompt tile.
4. Choose an account to continue.
5. Enter the password for the account you chose in the previous step and click Continue.
6. Type bcdedit /enum to view the boot loaders on Server01.
7. Export your current BCD database by typing the following and press Enter:
   bcdedit /export c:\BCDbkup
8. Remove the hidden, read-only, and system attributes from the BCD store file by typing the following and pressing Enter:
   attrib c:\boot\bcd –h –r –s

TAKE NOTE*

The /r switch tells the server to restart; the /o option tells the server to end the current Windows session and open the Advanced Boot options menu.

9. Rename the existing BCD store by typing the following and pressing Enter:
   Ren c:\boot\bcd bcd.old
10. Reboot the server and you will see an error message.

TAKE NOTE*

By rebooting the server at this point, you are able to simulate a missing BCD store because you renamed the current store to bcd.old. If you don't want to simulate this error, skip to Step 16 and rebuild the store.

11. Boot back into the server using installation media or by pointing your VM to the ISO image of the installation media.
12. Select Next to install the language, time, and keyboard input methods.
13. Select Repair your computer.
14. Select the Troubleshoot tile.
15. Select the Command Prompt tile.
16. Rebuild the BCD store by typing the following command:
    Bootrec /rebuildbcd
17. Select Yes when prompted to add the installation found to the boot list and press Enter.
18. Type Exit after the rebuild operation reports it was successful.
19. Select Continue from the options provided to boot into Windows Server.
20. Log in and confirm the server is operational.

Business Case Scenario

Scenario 9-1: Recovering from a Missing BCD

It's 5:00 PM on a Friday evening and you receive a call that one of your servers has an error message displayed on the screen. The error message is as follows:

```
The Boot Configuration Data for your PC is missing or contains errors

File: \Boot\BCD
Error code: 0xc0000000f
```

How would you resolve this issue?

Configuring Site-Level Fault Tolerance

LESSON 10

Configuring Hyper-V Replica

THE BOTTOM LINE

The reason that you perform backups is to be ready when you need to perform data recovery. Using clustering, you can provide fault tolerance for servers. However, when disasters occur that cause the cluster to fail or the virtual machine (VM) or data that you have on the central storage device becomes corrupted, it takes time to perform any repairs and restore from backup. To help overcome this problem, Hyper-V replica was created.

Hyper-V replica (offline copy) allows you to replicate a Hyper-V VM from one Hyper-V host at a primary site to another Hyper-V host at the Replica site. The Hyper-V replica is used as a spare server, which is stored on another central storage device at another site. To keep the replica updated, Hyper-V replica tracks the write operations on the primary VM and then replicates the changes to the replica over a wide area network (WAN) link. If the primary site goes down, you can then bring up the replica server in minutes. In addition, Hyper-V replica enables you to restore virtualized workloads to a point in time depending on the Recovery History selections for the VM.

Hyper-V replica consists of the following components:

- **Replication engine:** The component that manages the replication configuration details and manages initial replication, delta replication, failover, and test-failover operations.
- **Change tracking:** The component tracks changes on the primary copy of the VM. It tracks the changes regardless of where the VM .vhdx files reside.
- **Network module:** The network module provides a secure and efficient way to transfer VM replicas between primary hosts and replica hosts by using compression and encryption (using HTTPS and certification-based authentication).
- ***Hyper-V Replica Broker server role:*** A new server role (introduced in Windows Server 2012) that redirects all VM specific events to the appropriate node in the replica cluster. It is configured as part of the failover cluster.

Configuring Hyper-V Replica Between Two Servers

Hyper-V replica is part of the Hyper-V server role. It can be used on servers that are not part of a cluster. To replicate servers that are part of a cluster, use the Hyper-V Replica Broker server role.

To deploy Hyper-V replica, perform the following steps:

1. Enable replication between two Hyper-V hosts.
2. Configure replication of one or more VMs.
3. Test the replication deployment.

To enable Hyper-V replica, you configure the Hyper-V server settings, including selecting the authentication and port options and configuring authorization options. In addition, you must configure the location for replica files.

To use encryption for the replication, you need to use certificate-based authentication (HTTPS). You then need to use an existing X.509v3 certificate or create a self-signed certificate. In either case, the certificate needs to meet the following criteria:

- The certificate must not be expired or revoked.
- The certificate must include both client and server authentication extensions for enhanced key usage (EKU) and an associated private key.
- The certificate must terminate at a valid root certificate in the Trusted Root Certification Authorities store on the Replica server.
- If the VM is hosted by a standalone server, the subject common name (CN) contains the fully qualified domain name (FQDN) of the host. If the VM is hosted by a failover cluster, the subject common name (CN) should contain the FQDN of the Hyper-V Replica Broker.

ENABLE HYPER-V REPLICATION

GET READY. To enable Hyper-V replication, perform the following steps on both Hyper-V hosts:

1. Using Server Manager, open Hyper-V Manager. The *Hyper-V Manager* console opens.
2. Right-click the Hyper-V host, and click Hyper-V Settings.
3. When the *Hyper-V Settings* dialog box opens, click Replication Configuration.
4. In the *Replication Configuration* section (see Figure 10-1), click to enable the Enable this computer as a Replica server option.

Figure 10-1

Configuring host replication

5. To enable Kerberos authentication, click to select Use Kerberos (HTTP).
6. To use certificate-based authentication, click to select Use certificate based authentication (HTTPS).
7. In the *Authorization and storage* section, click to select Allow replication from any authenticated server, and then click Browse.
8. Click Computer, double-click Local Disk (E), click New folder, in the *Name* text box, type VMReplica, and then press Enter.
9. Select the E:\VMReplica\ folder, and then click Select Folder.
10. Click OK to close the *Hyper-V Settings* dialog box.
11. When Inbound traffic needs to be allowed in the Firewall, click OK.
12. Open the Control Panel, click System and Security, and then click Windows Firewall.
13. Click Advanced settings.
14. In the *Windows Firewall with Advanced Security* console, click Inbound Rules.
15. In the center pane, in the Inbound Rules list, right-click Hyper-V Replica HTTP Listener (TCP-In), and then click Enable Rule.
16. Close the Windows Firewall with Advanced Security console, and then close Windows Firewall.

If the VM is running in a failover cluster, the replication options in Hyper-V will be greyed out and will not be available. Instead, you have to open the *Failover Cluster Manager*, right-click the host server and click *Hyper-V Settings*. When the Hyper-V Settings dialog box opens, click *Replication Configuration* to open the same options that you see when you open the Hyper-V Settings.

INSTALL AND CONFIGURE THE HYPER-V REPLICA BROKER

GET READY. To configure Hyper-V Replica Broker, perform the following steps:

1. Using Server Manager, open Failover Cluster Manager.
2. Right-click Roles and click Configure Role.
3. When the *High Availability Wizard* opens, click Next.
4. On the *Select Role* dialog box, click Hyper-V Replica Broker and click Next.
5. On the *Client Access Point* page, specify the name and IP address of the client access point and click Next.
6. In the *Confirmation* page, click Next.
7. On the *Summary* page, click Finish.
8. With Failover Cluster Manager, click Roles, right-click Hyper-V Replica Broker, and click Replication Settings.
9. In the *Replication Configuration* section (refer to Figure 10-1), click to enable Enable this computer as a Replica server.
10. To enable Kerberos authentication, click to select Use Kerberos (HTTP).
11. To use certificate-based authentication, click to select Use certificate based authentication (HTTPS).
12. In the Authorization and storage section, click to select Allow replication from any authenticated server, and then click Browse.
13. Click Computer, double-click Local Disk (E), click New folder, in the *Name* text box, type VMReplica, and then press Enter.
14. Select the E:\VMReplica\ folder, and then click Select Folder.
15. Click OK to close the *Hyper-V Replica Broker Configuration* dialog box.

After you enable replication on the host, you need to configure the VMs to replicate. During this configuration, you must specify the replica server name, options for the connection, and the virtual hard disks drives that you want to replicate. Lastly, you can configure the recovery history and the initial replication method.

CONFIGURE REPLICATION FOR A VM

GET READY. To configure replication for a VM, perform the following steps:

1. Using Server Manager, open Hyper-V Manager.
2. Right-click the VM that you want to replicate and click Enable Replication.
3. When the *Enable Replication Wizard* begins, click Next.
4. On the *Specify Replica Server* page, type the name of the Replica server that you want to copy to in the *Replica server* text box. Click Next.
5. On the *Specify Connection Parameters* dialog box, click Next.
6. On the *Choose Replication VHDs* page, the virtual hard disks are already selected. Click Next.
7. On the *Configure Recovery History* page, the *Only the latest recovery point* is already selected. Click Next.
8. On the *Choose Initial Replication Methods* page, *Send initial copy over the network* and *Start replication immediately* are already selected. Click Next.
9. On the *Summary* page, click Finish.

10. If you get an *Enable Replication* dialog box saying that Replication enabled successfully but the network adapters for the Replica VM is not connected to any network, click Settings.
11. When the *Settings* dialog box opens, select the virtual switch that you want to use and click OK. After a period of time, the server will be replicated to the second Hyper-V host.

After you start the replication, you can check on the status of the replication by right-clicking the VM, clicking *Replication*, and clicking *View Replication Health*.

Configuring Hyper-V Replica Extended Replication

Starting with Windows Server 2012 R2, you can use ***Hyper-V Replica extended replication***, which is used create a second replica from another replica. By having an extra replica, you can replicate to one local server and remote site or you can replicate to two remote sites.

Just as the name implies, when you extend the replica, the second replica is created from first replica. Since you are essentially running a second wizard to configure the replica, you can define different replication intervals between the first and second replica.

CONFIGURE HYPER-V REPLICA EXTENDED REPLICATION

GET READY. To configure Hyper-V Replica Extended Replication, perform the following steps:

1. Using *Server Manager*, open Hyper-V Manager.
2. Right-click a virtual machine that is replicated and choose Replication > Extend Replication.
3. In the *Extend Replication* Wizard, on the *Before You Begin* page, click Next.
4. On the *Specify Replica Server* page, in the *Replica server* text box, type the name of a Hyper-V host. Click Next.
5. On the *Specify Connection Parameters* page, *Use Kerberos authentication (HTTP)* and *Compress the data that is transmitted over the network* options are already selected. Click Next.
6. On the *Configure Replication Frequency* page, select the desired frequency (5 minutes or 15 minutes). The default is 5 minutes. Click Next.
7. On the *Configure Additional Recovery Points* page, *Maintain only the latest recovery point* is already selected. Click Next.
8. On the *Choose Initial Replication Method* page, the *Send initial copy over the network* and *Start replication immediately* options are selected. Click Next.
9. On the *Completing the Extend Replication Wizard* page, click Finish.

Configuring Multi-Site Clustering

THE BOTTOM LINE

Many companies have only one office, which is used to define a single site. If the site goes down, such as from a fire or flooding, the company would be at a stand-still until a minimum number of servers were brought up and the data was restored from backups that were stored offsite. For larger companies, this type of solution is unacceptable. Therefore, assuming that the company has the money and resources, a backup site needs to be established so that it can be brought online and allow the company to function while the primary site is fixed and brought back online.

At the beginning of this lesson, using Hyper-V replicas was used to make a backup copy of servers. The replicas can be used to replicate to a second site. However, the Hyper-V replica is a cold server that must be brought online when the primary site is unavailable.

Another solution is to create a ***multi-site failover cluster***. A multi-site failover cluster has the following advantages, as compared to a replica VM:

- When a failure occurs, a multi-site cluster automatically fails over the clustered service or application to another.
- Because a site fails over automatically, a multi-site cluster has less administrative overhead than a cold standby server, which needs to be turned on and configured.

A multi-site failover cluster is similar to a standard failover cluster, however, you must take into account that the two sites are usually connected with a significantly slower WAN link as compared to links found in Local Area Networks (LANs).

Configuring Multi-Site Storage and Network Settings

Because of the slower WAN link, there is no shared storage that cluster nodes on the two sites can use. Therefore, you need to use two separate storage systems, one at each site, and have some method to replicate the data between the two sites.

Because Microsoft Windows does not include a built-in mechanism for data replication, you need to use one of the following three methods:

- Block level hardware-based replication
- Software-based file replication
- Application-based replication

Some SANs have the capability to replicate data between SAN units. If not, you need to purchase another hardware system or software-based replication system to perform the replication. You should also check whether the shared application or service that you are running on the cluster has built-in replication. For example, both Microsoft Exchange and Microsoft SQL server have replication built in to the software. Exchange Server has continuous replication, and SQL Server has several types of replication including log shipping. In some situations, if the data that you replicate are small files that are typically closed, you can use Distributed File System (DFS) replication.

When you configure multi-site replication, the replication is either synchronous or asynchronous. With ***synchronous replication***, data is written to the remote site and then waits for a receive message stating that the data has been written to the remote site properly. If the message is not received, the data will be sent again. Although the synchronous replication keeps both sites the same, any slowness or delays over a WAN link slows the cluster application or service because the application or service waits for the data to be written to the remote site. Therefore, to use synchronous replication, you need high bandwidth between the two sites and low latency.

With ***asynchronous replication***, the data is written to the primary storage device and then is written separately to the remote storage device, typically on its own schedule. However, most of these systems are written only after a short delay. The advantage of asynchronous replication is that it keeps the performance high for the clustered application or service.

Lastly, your network needs basic network services functioning when a site goes down, which includes Active Directory Domain Services (AD DS) and Domain Name System (DNS). Therefore, you need multiple domain controllers through your organization including at least

one at the secondary site. In addition, you should have multiple DNS servers including at least one at the secondary site. Of course, for clients to use DNS at the secondary site, make sure that the secondary DNS server for the clients point to the DNS server at the secondary site.

Configuring Quorum and Failover Settings

Any time you deal with WAN links, you have to take into account that those links will have slower bandwidth and higher latency. Since failover is triggered by missing heartbeats, you may need to tweak the quorum and failover settings so that the failover will work more efficiently if it is a multi-site cluster.

By default, the heartbeat occurs once every second (1,000 milliseconds). If a node misses five heartbeats in a role, another node will initiate failover.

For a cluster to operate properly over multiple sites, you should have have at least one low-latency and reliable network connection between sites to carry the cluster heartbeats. If not, you will need to use the Failover settings (right-click the role, click *Properties*, and click the *Failover* tab) to specify the maximum failures in a specified period, so that a cluster does not failover prematurely or unnecessarily.

You need enough nodes and votes to reach quorum, even if a site is down. Because the sites are geographically dispersed, you cannot use quorum configuration that requires a witness disk. If there is an odd number of nodes, then use the Node Majority quorum. If there is an even number of nodes, which is typical in a geographically dispersed cluster, you can use the Node Majority with File Share Majority quorum.

If you use Node Majority with File Share Majority quorum, you need to place the file share witness at a third site. In a multi-site cluster, a single server can host the file share witness. However, you must create a separate file share for each cluster.

With Windows Server 2012 and Windows Server 2012 R2, you can adjust cluster quorum settings including specifying which nodes can vote and which nodes cannot vote when determining quorum. This might help you implement solutions across multiple sites and tweak settings after a major failure has occurred.

Configuring Multi-Site Failure Cluster

When you set up the multi-site failure cluster, you use much of the knowledge that you learned in Lessons 3 and 4, which discuss failover clusters.

The high level steps that you should perform when configuring a multi-site failover cluster are the following:

1. Ensure that you have enough cluster nodes at each site and that each node has similar hardware configuration and the same version of operating system and service packs.
2. Ensure that sites have stable connections, with sufficient bandwidth and low network latency. Latency validates when you run the Validate Configuration Wizard in Failover Cluster Manager.
3. Ensure that you have a reliable storage replication mechanism between sites.
4. Make sure you have the basic network services available on each site including AD DS, DNS, and DHCP.
5. Run the Validate a Configuration Wizard on all nodes and fix any problems that it might indicate.

6. Create a cluster.
7. Configure the cluster quorum mode.
8. Configure failover/failback settings.
9. Create the clustered role.
10. Test failover and failback.

Configuring Global Update Manager

Global Update Manager is used to coordinate state changes within the cluster, such as when a cluster node is taken offline. Starting with Windows Server 2012 R2, you can configure how the cluster manages global updates.

The Global Update Manager is a cluster component that is used by Failover Manager, Node Manager, and Database Manager to replicate changes to the cluster database nodes. When a Global Update manager update is initiated by a client node, it will first request a global lock. If a lock cannot be initiated, the client will wait until it can be. When the lock is granted, the client issues the updates to the healthy nodes, including itself. If an update fails on a node, the node will be removed from the current cluster membership.

In Windows Server 2012 R2, the Global Update Manager includes the following modes:

- **0 5 All (write) and Local (read):** The default setting in Windows Server 2012 R2 for all workloads besides Hyper-V. All cluster nodes must receive and process the update before the cluster commits a change to the database. Database reads occur on the local node. Because the database is consistent on all nodes, there is no risk of out of date or "stale" data.
- **1 = Majority (read and write):** The default setting in Windows Server 2012 R2 for Hyper-V failover clusters. A majority of the cluster nodes must receive and process the update before the cluster commits the change to the database. For a database read, the cluster compares the latest timestamp from a majority of the running nodes, and uses the data with the latest timestamp.
- **2 = Majority (write) and Local (read):** A new mode available in Windows Server 2012 R2 that improves cluster database performance in scenarios where there is significant network latency between the cluster nodes (for example, with a stretch multi-site cluster). A majority of the cluster nodes must receive and process the update before the cluster commits the change to the database. Database reads occur on the local node. Because the cluster does not compare the latest timestamp on a majority of nodes, the data may be out of date or "stale."

You should not use either of the majority modes (1 or 2) for scenarios that require strong consistency guarantees from the cluster database, such as for Microsoft SQL Server failover cluster that uses AlwaysOn availability groups or for Microsoft Exchange Server.

In Windows Server 2012, you cannot configure the Global Update Manager mode. However, in Windows Server 2012 R2, you can configure the Global Update Manager mode with the DatabaseReadWriteMode property. To view the Global Update Manager mode, start Windows PowerShell as an administrator, and then execute the following command:

```
(Get-Cluster).DatabaseReadWriteMode
```

To change the Global Update Manager Mode to Majority (write) and Local (read), execute the following command:

```
(Get-Cluster).DatabaseReadWriteMode=2
```

Recovering a Multi-Site Failover Cluster

The best method to restore a cluster is to restore from backup. However, because the cluster configuration is replicated between cluster nodes, you can fix and restore a single node and the configuration information will be replicated to the newly restored node. If you have to restore a cluster configuration from backup, you will have to perform an authoritative restore.

To ensure that you can recover a failed cluster is to make sure that you have a backup of the failover cluster including backing up the cluster configuration, and the data on clustered disks. To back up the cluster configuration, the cluster must be running and must have quorum.

When you restore to a failover cluster from backup, you can restore the cluster configuration, the data on clustered disks, or both. The Cluster service keeps track of which cluster configuration is the most recent, and it replicates that configuration to all cluster nodes, including a disk witness.

When you restore a single cluster node from backup, you can perform one of the following:

- **Non-authoritative restore:** Restore the failed node to normal function, which while restore the node to normal function and join the node to the cluster. Cluster configuration will be automatically replicated to the restored node.
- **Authoritative restore:** By restoring the failed node, but marking the configuration as the most recent. The Cluster service will then overwrite the configuration across all nodes.

When you restore data on clustered disk, data can be written only to disks that are online and owned by that cluster node when the backup is being restored.

■ Business Case Scenarios

Scenario 10-1: Replicating a VM to a Secondary Site

You are an administrator at the Contoso Corporation. You have multiple sites within your corporation. At the main office, you have most of the servers for your company. The secondary site is a data recovery site if there is a major problem at the primary site. The primary servers are VMs on Server01 that need to run all the time. What do you need to have a backup copy at the secondary site?

Scenario 10-2: Setting Up a Multi-Site Cluster

You are an administrator at the Contoso Corporation. You have multiple sites within your corporation. At the main office, you have most of the servers for your company. The secondary site is a data recovery site if there is a major problem at the primary site. At the primary site, you have a failover cluster that has two nodes. You want to expand the cluster to the secondary site. What will you need to do and what are some of things that you will need to overcome?

11 LESSON

Implementing an Advanced Dynamic Host Configuration Protocol (DHCP) Solution

Implementing Advanced DHCP Solutions

THE BOTTOM LINE

The ***Dynamic Host Configuration Protocol (DHCP)*** is a network protocol that automatically configures the IP configuration of a device including assigning an IP address, subnet mask, default gateway, and primary and secondary Domain Name System (DNS) servers. Most clients and some servers that connect to a network receive their address from a DHCP server including home routers/modems and office networks. In addition, the DHCP technology and protocol has becomes a necessary component of Windows Deployment Services (WDS) to deploy Windows to a client, and Network Access Protection (NAP), which is needed to limit the connectivity of clients that do not have the current Windows updates and proper antivirus software.

DHCP has been included with Windows for years and is included with Windows Server 2012 and Windows Server 2012 R2 as a server role. Starting with Windows Server 2012, DHCP supports failover capability. It helps administrators distribute the appropriate IP addresses and network configuration information automatically to network devices or hosts, which eliminates a lot of time to automatically configure each host that connects to the network and eliminates human error during configuration. The devices or hosts include computers, mobile devices, printers, network appliances, and switches.

Understanding DHCP Basics

DHCP is based heavily on the ***Bootstrap Protocol (BOOTP)***, which was one of the early network protocols used to obtain an IP address from a configuration server. Although the DHCP server functions as a BOOTP server, DHCP is a more advanced protocol and includes additional functionality including the ability to reclaim allocated addresses that are no longer used. DHCP is an open, industry-standard protocol defined by the Internet Engineering Task Force (IETF) in Request for Comments (RFCs) 2131 and 2132.

You can install the DHCP server role on a stand-alone server, a domain member server, or a domain controller. The components that make up the DHCP technology and protocol consist of the following:

- ***DHCP server service:*** A service that works in the background on a server. It distributes IP addresses and other network configuration information.

- ***DHCP scopes:*** A range of IP addresses that can be allocated to clients. A scope consists of a name and description, range of addresses, and a subnet mask. To ease the allocation of addresses, administrators can define IP addresses that are excluded from distribution. The administrators can also specify the duration of the IP address leases. By the end of the lease, the address needs to be renewed or it is released back into the pool so that it can be reallocated to another host. After a scope is created, the scope has to be activated before it can allocate addresses.
- ***DHCP options:*** Options that are assigned when the addresses are assigned or renewed including the default gateway and the primary and secondary DNS servers. Other options include DNS domain suffix, Windows Internet Name Service (WINS) server, and TFTP addresses. Based on how you configure the DHCP options, you can assign the options globally (all scopes), specific to a particular scope, to specific clients based on a Class ID values), or to clients that have specific IP address reservations configured.
- ***DHCP database:*** A database that contains the configuration for the DHCP server, the IP addresses that it has distributed, their current lease time, and the IP addresses that the server still have to distributed. The database uses the Microsoft Jet Database Engine, which is stored in the %systemroot%\System32\Dhcp folder.
- ***DHCP console:*** The Microsoft Management Console (MMC) that allows you to manage the DHCP server, and the scopes. Figure 11-1 shows the DHCP console.

Figure 11-1

Looking at the DHCP console

Creating and Configuring DHCP Policies

Starting with Windows Server 2012, by using ***DHCP policies***, you can give granular control over scopes to allow you to assign different IP addresses or different options based on the device type, or its role. Policies are applicable for a specific scope with a defined processing order. The options can be configured at the scope or inherited from server-wide policies.

A DHCP policy consists of conditions and settings. A condition allows you to identify and group clients based on whether a specified criteria is equal or not equal to a specified values. The criteria include:

- MAC address
- Vendor Class
- User Class
- Client identifier
- Relay Agent Information such as remote id, circuit id, and subscriber id

Every DHCP client request is evaluated against the conditions in a policy. If a client request matches the conditions in the policy, the specified settings (IP address and options) assigned to the policy will be applied to the DHCP client. For example, you can identify the type of device, so that wired clients are in one group, and mobile computers are in another group. You can also use a trailing wild card with MAC address, Vendor Class, User Class, and Client identifier conditions to perform a partial match. A client that does not match conditions is leased an IP address from the remaining IP addresses of the scope that are not assigned to a policy and are giving options assigned to the scope.

You can configure more than one policy within a scope or server wide. As a client makes a DHCP request, each policy is evaluated and the settings are combined. If there is a conflict for a specific option, the policy higher up in processing order overrides the previous option.

Every policy has an assigned processing order. While processing client requests, the DHCP server evaluates the client requests against the conditions in the different policies based on the processing order of the policy—with processing order 1 policy processed first. Scope level policies are processed first by the DHCP server followed by server-wide policies.

Configuring DNS Registration

With Windows Server 2012 R2, by using the proper FQDN-based condition and a DNS suffix, you can use DHCP policies to fully control DNS registration for computers and devices on the network, including workgroup computers, guest devices, or clients with a specific attribute.

With Windows Server 2012 R2, you can use DHCP policies to allow users to configure conditions based on the fully qualified domain name (FQDN) of the client. In addition, DHCP policies can be configured to register DHCP clients using a specific DNS suffix, overriding the DNS suffix that is already configured on the client.

CONFIGURE A POLICY BASED ON THE FQDN

GET READY. To configure a policy based on the FQDN, perform the following steps:

1. Using *Server Manager*, open the DHCP console.
2. In the *DHCP* console, expand the server, expand IPv4, expand a scope, and then click the Policies node. Right-click the Policies node and choose New Policy.
3. In the *DHCP Policy Configuration Wizard,* on the *Policy based IP address and Option Assignment* page, in the *Policy Name* text box, type a name of the policy. In the *Description* text box, type a description for the policy. Click Next.
4. On the *Configure Conditions for the policy* page, click Add.

5. In the *Add/Edit Condition* dialog box, for *Criteria,* select Fully Qualified Domain Name. The *Operator* is already set to *Equals*.
6. In the *Value* text box, type a domain name, such as adatum.com and click Add. If desired, you can select the Prefix wildcard (*) option or the Append wildcard (*) option. Click OK.
7. On the *Configure Conditions for the policy* page, click Next.
8. On the *Summary* page, click Finish.

Creating and Configuring Superscopes

A ***superscope*** is the grouping of multiple scopes into a single administrative entity. By using superscopes, you can support larger subnets.

A superscope can be used if a scope runs out of addresses and you cannot add more addresses from the subnet. Instead, you can add a new subnet to the DHCP server. You then perform multinetting, where you lease addresses to clients in the same physical network, but the clients will be in a separate network logically by subnet. Once you add a new subnet, you must configure routers to recognize the new subnet so that you ensure local communications in the physical network.

You can also use superscopes to move clients gradually into a new IP number scheme. Having both numbering schemes coexist at the same time allows you to move clients into the new subnet. When you renew all client leases in the new subnet, you can retire the old subnet.

You can create only a superscope if you have two or more IP scopes already created in DHCP. You can use the New Superscope Wizard to select the scopes that you want to combine together to create a superscope.

CREATE A SUPERSCOPE OUT OF TWO SCOPES

GET READY. To create a superscope out of two scopes, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. In the *DHCP* console, click a DHCP server, such as RWDC01.contoso.com. Right-click IPv4, and then click New Scope.
3. When the *New Wizard* opens, click Next.
4. In the *Name* text box, type Scope1, and click Next.
5. In the IP address range, set the *Start IP address* to 172.24.20.50 and *End IP address* to 172.24.20.240. For the Subnet mask, type 255.255.255.0. Click Next.
6. On the *Add Exclusion and Delay* page, click Next.
7. On the *Lease Duration* page, change the duration to 3 days, and click Next.
8. On the Configure DHCP Options page, click Next.
9. On the *Router (Default Gateway)* page, type the address of 172.24.20.20, and click Add. Click Next.
10. On the *Domain name and DNS Servers* page, the *Parent domain* should already be set to contoso.com, and the DNS server should already be defined. Click Next.
11. On the *WINS Servers* page, click Next.
12. On the *Activate Scope* page, click Next.
13. When the wizard is complete, click Finish.
14. Right-click IPv4, and then click New Scope.
15. When the *New Wizard* opens, click Next.

16. In the *Name* text box, type Scope2, and click Next.
17. In the IP address range, set the *Start IP address* to 172.24.21.50 and *End IP address* to 172.24.21.240. For the *Subnet mask*, type 255.255.255.0. Click Next.
18. On the *Add Exclusion and Delay* page, click Next.
19. On the *Lease Duration* page, change the duration to 3 days, and click Next.
20. On the Configure DHCP Options, click Next.
21. On the *Router (Default Gateway)* page, type the address of 172.24.21.20, and click Add. Click Next.
22. On the Domain name and DNS Servers page, the *Parent domain* should already be set to contoso.com, and the DNS server should already be defined. Click Next.
23. On the *WINS Servers* page, click Next.
24. On the *Activate Scope* page, click Next.
25. When the wizard is complete, click Finish.
26. Right-click IPv4, and click New Superscope.
27. When the *New SuperScope Wizard* begins, type Super1 in the *Name* text box, and click Next.
28. On the *Select Scopes* page, press the Control key and hold it down. Then click Scope1 and Scope2. Release the Control key. Click Next.
29. Click Finish. The superscope shows in the DHCP console (see Figure 11-2).

Figure 11-2

Viewing a superscope in the DHCP console

CREATE A SUPERSCOPE FROM SCRATCH

GET READY. To create a superscope from scratch, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.

2. In the *DHCP* console, click the DHCP server, such as RWDC01.contoso.com. Right-click IPv4, and then click New Superscope.
3. When the *New SuperScope Wizard* begins, type Super2 in the *Name* text box, and click Next.
4. In the IP address range, set the *Start IP address* to 172.25.20.50 and *End IP address* to 172.25.21.254. For the subnet mask, type 255.255.255.0. Click Next.
5. When it says that address range is too large for a single scope, click Yes, to create a superscope. Click Next.
6. On the *Lease Duration* page, change the duration to 3 days, and click Next.
7. On the Configure DHCP Options page, click Next.
8. On the *Router (Default Gateway)* page, type the address of 172.25.20.20, and click Add. Click Next.
9. On the *Domain name and DNS Servers* page, the *Parent domain* should already be set to contoso.com, and the DNS server should already be defined. Click Next.
10. On the *WINS Servers* page, click Next.
11. On the *Active Scope* page, click Next.
12. Click Finish. The superscope shows in the *DHCP* console.

Creating and Configuring Multicast Scopes

When a host sends packets to a single host (single point to single point), the communication is ***unicast***. ***Broadcast*** is sent from one host to all other hosts (one point to all other points). ***Multicast*** is when packets are sent from one host to multiple hosts (one point to a set of other points). Multicasting delivers the same packet simultaneously to a group of clients, which results in less bandwidth usage. For example, if you have to send a live video to 100 computers, instead of sending 100 sets of packets (unicast), you would send one set of packets. When multicast packets reach a router, the packets are forwarded only to the networks that have receivers for the packets. Besides live video or audio transmissions, it can also be used in some instances when deploying multiple computers at the same time—you only need to send one set of packets to multiple computers.

Classful networks include Class A, Class B, and Class C networks. The first octet is the following:

- **Class A:** 0-127 with a default subnet mask of 255.0.0.0
- **Class B:** 128-191 with a default subnet mask of 255.255.0.0
- **Class C:** 192-223 with a default subnet mask of 255.255.255.0

Class D addresses are defined from 224.0.0.0 to 239.255.255.255 and used for multicast addresses.

In DHCP, ***multicast scopes*** (commonly known as a *Multicast Address Dynamic Client Allocation Protocol (MADCAP) scopes*) allow applications to reserve a multicast IP address for data and content delivery. Applications that use multicasting request addresses from the scopes need to support the MADCAP application programming interface (API).

Creating and managing a multicast scope is similar to creating and managing a normal scope; however, multicast scopes cannot use reservations and you cannot set additional options such as DNS and routing. In addition, because multicast is shared by groups of computers, the default duration of a multicast scope is 30 days.

CREATE A MULTICAST SCOPE

GET READY. To create a multicast scope, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. In the *DHCP* console, click the DHCP server, such as RWDC01.contoso.com. Right-click IPv4, and then click New Multicast Scope.
3. When the *New Multicast Scope Wizard* opens, click Next.
4. In the *Name* text box, type Multicast Scope1, and click Next.
5. In the IP address range, set the *Start IP address* to 224.0.0.0 and *End IP address* to 224.255.255.255. Click Next.
6. On the *Add Exclusion and Delay* page, click Next.
7. On the *Lease Duration* page, click Next.
8. On the *Activate Scope* page, click Next.
9. When the installation is complete, click Finish.

Implementing DHCPv6 Scopes

IPv6 address utilizes a 128-bit address space to provide addressing for every device on the Internet with a globally unique address. Because the IPv6 addresses uses 128 bits, the addresses are usually divided into groups of 16 bits, written as 4 hex digits. Hex digits include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F. Colons separate the groups. An example of an address is the following:

FE80:0000:0000:0000:02C3:B2DF:FEA5:E4F1

Similar to the IPv4 addresses, IPv6 addresses are divided into network bits and host addresses. In addition, IPv6 supports automatic configuration. However, with a Windows DHCP server, you can perform stateful address autoconfiguration.

The first 64 bits of an IPv6 address define the network address, and the second 64 bits define the host address. Therefore, in the previous example address, FE80:0000:0000:0000 defines the network bits and 02C3:B2DF:FEA5:E4F1 defines the host bits. The network bits are also further divided where 48 bits are used for the network prefix and the next 16 bits are used for subnetting. The remaining host bits are 64-bits.

With IPv6, unicast addressing can be divided into the following:

- **Global unicast addresses:** Public addresses that are globally routable and reachable on the IPv6 portion of the Internet.
- **Link-local addresses:** Private non-routable addresses confined to a single subnet. These addresses are used to communicate with neighboring hosts on the same link and are equivalent to the Automatic Private IP addresses (169.254.x.x) used by IPv4 when a DHCP server cannot be contacted. Although they can be used to set up permanent small LANs, link-local addresses can also be used to create temporary networks or ad-hoc networks. Although routers process packets sent to a link-local address, they do not forward the packets to other links.
- **Unique local addresses:** Intended private addressing, so that you can join two subnets together without creating any addressing problems.

An IPv6 host address can be configured with stateful or stateless mode. Because the two address configuration modes are independent of each other and will not trample over each other, a host can use both stateless and stateful address configuration.

Stateless mechanism is used to configure both link-local addresses and additional non-link-local addresses based on Router Solicitation and Router Advertisement messages with neighboring routers. With stateless autoconfiguration, the MAC address is used to generate the host bits. When using stateless configuration, the address is not assigned by a DHCP server. However, a DHCP server can still assign other IPv6 configuration settings.

Stateful configuration has the IPv6 addresses and additional IPv6 configuration, assigned by a DHCPv6 server.

When you create an IPv6 scopes, you define the following properties:

- **Prefix:** Defines the network portion of the IP address.
- **Preference:** Values assigned to a DHCP scope to indicate which the preferred DHCP server to use when an organization has multiple DHCP servers. The scope with the lowest preference value is used first.
- **Exclusions:** Defines single addresses or blocks of addresses that will not be offered for lease.
- **Valid and preferred lifetimes:** Defines how long leased addresses are valid. The preferred lifetime is the preferred amount of time the lease should be valid. The valid lifetime is the maximum amount of time the lease is valid.
- **DHCP options:** IPv6 options such as DNS servers and default gateway.

CREATE A DHCP IPV6 SCOPE

GET READY. To create a DHCP IPv6 scope, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. Right-click IPv6, and click New Scope.
3. When the New Scope Wizard starts, click Next.
4. Type a name such as IPv6Scope1 in the *Name* text box.
5. In the *Scope Prefix* page, (see Figure 11-3) specify the *Prefix* such as FEC0::. In addition, specify the *Preference* value, such as 0.

Figure 11-3

Specifying the network prefix

6. On the *Add Exclusions* page, click Next.
7. On the *Scope Lease* page, specify the preferred life time, and valid life time for the host. Change the *Preferred Life Time* to 1 day, and the *Valid Life Time* to 10 days. Click Next.
8. When the wizard is complete, *Yes* is already selected to activate the scope. Click Finish.

Configuring High Availability for DHCP

DHCP is an essential service that allows most clients and some servers to communicate on the network. As clients are turned on, or when a client renews a lease, the DHCP server must be available to assign or renew the lease. So you need to take steps to ensure that DHCP services are available.

To make DHCP highly available, you can use one of the following methods:

- ***Split scopes:*** Use two DHCP servers to assign IP addresses. Eighty percent of the available addresses are assigned on the primary server, and 20 percent of the available addresses are assigned to a secondary server. When the primary server is down, the secondary server can assign IP addresses long enough for you to fix or replace the primary server.
- **Server cluster:** Uses a failover cluster to host the DHCP server. For more information on failover clustering, review Lesson 3, "Managing Failover Clustering."
- ***DHCP failover:*** Introduced in Windows Server 2012, replicates lease information between two DHCP servers.
- **Standby server:** Uses a hot standby DHCP server with identical scopes and options as the production DHCP server.

If you restore a DHCP database server from backup, you need to make sure that DHCP clients do not receive IP addresses that are currently in use on the network. This can be accomplished by opening the *Properties* of a scope, clicking the *Advanced* tab, and setting the *Conflict Detection* value to 2.

CONFIGURING SPLIT SCOPES

For years, if you wanted high availability, you would use a split-scope configuration, also known as the *80/20 configuration*. Split-scope configuration, uses two DHCP servers, with the same scopes and options. However, the scopes have complementary exclusion ranges, so that there is no overlap in the addresses that they lease to clients. You do not want the two servers to hand out the same address to different clients.

It is known as the *80/20 configuration* because the primary server is assigned 80 percent of the available addresses, whereas the secondary server is assigned 20 percent of the available addresses. The secondary server is configured to respond after a delay, giving the primary server the first opportunity to hand out addresses. Because the local server responds first, it leases the address to the clients. If the primary server is not available, the secondary server will respond and lease an address.

To simplify the configuring of split-scopes, Windows Server 2012 and Windows Server 2012 R2 includes a Split-Configuration Wizard. To access this wizard, you need to have the two DHCP servers that are authorized. Then after you create a scope, on one of the servers, you can access the DHCP Split-Scope Wizard.

USE THE DHCP SPLIT-SCOPE WIZARD

GET READY. To use the DHCP Split-Scope Wizard, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. Right-click a scope that you created on the DHCP server, click Advanced, and click Split-Scope.
3. When the *DHCP Split-Scope Configuration Wizard* starts, click Next.
4. On the *Additional DHCP Server* page, type the name of the secondary DCHP server, and click Next.
5. On the *Percentage of Split* page, the slider bar is already set at 80. Click Next.
6. On the *Delay in DHCP Offer* page, the host DHCP server and the added DHCP server have a delay of 0 milliseconds. Change the delay of the added DHCP server to 500. Click Next.
7. When the wizard is complete, click Finish.
8. On the *Summary of Split-Scope* page, click Close.

CONFIGURING DHCP FAILOVER

In the past, DHCP failover was not possible because each DHCP server had its own database. So when a lease was granted to a client, the other DHCP server would not be aware of the other lease. So if you assign the same pool of addresses, you would have the same address assigned to two different hosts, causing an IP address conflict. You can use cluster, which requires some manual configuration and monitoring.

Starting with Windows Server 2012, DHCP can replicate lease information between two DHCP servers for IPv4 scopes and subnets. If one DHCP server fails or becomes overloaded, the other server services the clients for the entire subnet.

DHCP failover establishes a failover relationship between the two DHCP servers. Each relationship has a unique name, which is exchanged during configuration. A single DHCP server can have multiple failover relationships with other DHCP servers as long as each relationship has a unique name.

DHCP failover is time sensitive. The time between partners must be no greater than one minute. If the time is greater, the failover process will halt with a critical error.

DHCP failover supports two modes:

- **Load Sharing:** Both servers simultaneously supply IP configuration to clients. By default, the load is distributed evenly, 50:50. However, you can adjust the ratio if you prefer one server over another. Load Sharing is the default mode.
- **Hot Standby:** One server is the primary server that actively assigns IP configuration for the scope or subnet, and the other is the secondary server that assumes the DHCP role if the primary server becomes unavailable. Hot Standby mode is best suited when the disaster recovery site is located at a different location. Because the failover is defined for a scope, you can have one server act as the primary for one scope or subnet, and be the secondary for another.

When using Hot Standby mode, you configure a percentage of the scope addresses to be assigned to the standby server (5% is the default). If these addresses are used, the secondary server takes control of the IP scope after the Maximum Client Lead Time (MCLT) interval has passed.

To provide better security, Windows Server 2012 and Windows Server 2012 R2 can be used to authenticate the failover message traffic between the replication partners using a shared secret in the Configuration Failover Wizard for DHCP failover.

DHCP uses the same two ports for BOOTP: destination UDP port 67 for sending data to the server, and UDP port 68 for data to the client. DHCP uses TCP port 647 to listen for failover traffic. The DHCP installation automatically creates the following inbound and outbound firewall rules:

- Microsoft-Windows-DHCP-Failover-TCP-In
- Microsoft-Windows-DHCP-Failover-TCP-Out

CONFIGURE DHCP FAILOVER

GET READY. To configure DHCP failover, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. Expand IPv4.
3. To configure a single scope, right-click the scope, and click Configure Failover. To configure failover for all scopes, right-click IPv4, and click Configure Failover.
4. When the *Configure Failover Wizard* starts, all scopes will be selected. To select only one scope, deselect the Select all option and click the scope that you want to configure. Click Next.
5. On the *Specify the partner server to use for failover* page, type the name of the partner DHCP server and click Next.
6. On the *Create a new failover relationship* page (see Figure 11-4), specify the maximum client lead time, the mode, the load balance percentage, and the state switch over interval.

Figure 11-4

Creating a new failover relationship

7. By default, *Enable Message Authentication* is enabled. Type a shared secret such as Password01. Click Next.
8. To complete the wizard, click Finish.
9. When the configuration is done, click Close.

Configuring DHCP Name Protection

If an organization uses only Windows systems that are part of an Active Directory domain, each computer will have its own unique computer name, which DHCP registers in DNS on behalf of the client. Name squatting is when a non-Windows based computer registers a name in DNS that is already registered to a Windows-based computer. To prevent non-Microsoft systems from overwriting systems that use static addresses, Windows Server 2012 introduced ***DHCP Name Protection*** to prevent these conflicts.

When one client registers a name with DNS, but the name is already used by another client, the original machine can become inaccessible. DHCP Name Protection addresses uses a resource record known as a *Dynamic Host Configuration Identifier (DHCID)* to track which machines originally requested which names. When DHCP assigns or renews an address, the DHCP server refers to the DHCID in DNS to verify that the machine that is requesting the name is the original machine that used the name. If it is not the same machine, then the DNS resource record is not updated.

Name Protection can be used for both IPv4 and IPv6 and can be configured at the server level or at the scope level. However, configuring DHCP Name Protection at the server level applies only to newly created scopes.

ENABLE DHCP NAME PROTECTION FOR AN IPV4 OR IPV6 NODE

GET READY. To enable DHCP Name Protection for an IPv4 or IPv6 node, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. Right-click IPv4 or IPv6, and click Properties.
3. When the *Properties* dialog box opens, click the DNS tab.
4. Click the Configure in the Name Protection section. The *Name Protection* dialog box opens (see Figure 11-5).

Figure 11-5

Enabling DHCP Name Protection

5. Click to select the Enable Name Protection option.
6. Click OK to close the *Name Protection* dialog box and click OK to close the *Properties* dialog box.

ENABLE DHCP NAME PROTECTION FOR A SCOPE

GET READY. To enable DHCP Name Protection for scope, perform the following steps:

1. Open Server Manager, open the Tools menu, and click DHCP. The *DHCP* console opens.
2. Right-click the scope and click Properties.
3. When the *Properties* dialog box opens, click the DNS tab.
4. Click Configure in the *Name Protection* section. The *Name Protection* dialog box opens.
5. Click to select the Enable Name Protection option.
6. Click OK to close the *Name Protection* dialog box and click OK to close the *Properties* dialog box.

Business Case Scenarios

Scenario 11-1: Configuring DHCP High Availability

You are the administrator for the Contoso Corporation. Recently, the DHCP server failed. To fix the problem, you had to fix the server and restore from backup. In the future, you want to make the server fault tolerant in case it fails in the future. In addition, you want to ensure that you add additional sites, and you want to allow the servers to handle a bigger load. What would you recommend?

Scenario 11-2: Performing Granular IP Address Leasing on a DHCP Scope

You are the administrator for the Contoso Corporation. You have 15 sites. You want to create one DHCP scope that includes one set of addresses for computers, one set of addresses for printers, and one set of addresses for IP phones. What would you do?

Implementing an Advanced DNS Solution

LESSON 12

Configuring Security for DNS

THE BOTTOM LINE

Windows Server 2012 and Windows Server 2012 R2 include a number of new features for domain naming services (DNS) security. Securing the DNS server and DNS records prevents false records from being added and prevents clients from receiving incorrect DNS query responses, which can lead them to visit phishing sites or worse. To prevent DNS being used to attack systems, DNS Security (DNSSEC), cache locking, and other security measures are implemented.

Having already deployed DNS servers and configured them successfully in the 70-410 and 70-411 courses, the need arises to secure the DNS servers and caches from spoofing, man-in-the-middle, and cache-poisoning attacks. In the modern world, it is a sad fact that securing all areas of functionality is a necessity. DNS is a common area for attack by interception and tampering. A client that uses DNS to connect is always vulnerable to redirection to an attacker's servers unless the zone has been secured using DNSSEC.

The process for securing a zone using DNSSEC is called ***signing the zone***. Once signed, any queries on the signed zone will return digital signatures along with the normal DNS resource records. The digital signatures are verified using the public key of the server or zone from the ***trust anchor***. DNSSEC uses trust anchors represented by public keys that define the top of a chain of trust. The trust anchor verifies that a digital signature and associated data is valid.

Once this public key has been obtained, the resolver or client is able to validate the responses it receives. The trust anchor is the most important link in this chain. The server, resolver, or zone must be configured with this trust anchor. Once this is achieved, the client will be able to confirm that the DNS information it receives came from a valid server, was unchanged, and does or does not actually exist.

Configuring DNSSEC

DNS Security (DNSSEC) is a suite of protocols defined by the Internet Engineering Task Force (IETF) for use on IP networks. DNSSEC provides DNS clients, or resolvers, with proof of identity of DNS records and verified denial of existence. DNSSEC does *not* provide availability or confidentiality information.

DNSSEC can be enabled on an Active-Directory Integrated zone (ADI) or on a primary zone. As with all security measures and particularly advanced implementations, planning is important. Which zones do you want to secure? Who has access to the zone? Who has access to the server and the administration of the server security? The answers to these and lots of other questions always depend on the security requirements of your organization. By the time you are ready to implement DNSSEC on your DNS server, the security documentation should have already been created and approved.

DNSSEC is installed as part of the DNS Server role. To enable DNSSEC, Windows Server 2012 and Windows Server 2012 R2 provides a DNSSEC Zone Signing Wizard. This wizard is run from the DNS console and configures the ***Zone Signing Parameters***—all the settings required for ensuring the zone is signed correctly and securely. Follow the instructions to configure DNSSEC for the ADatum.com ADI zone.

Once a zone is signed, there are a number of new ***DNSSEC Resource records*** available. These records are in addition to the standard A, NS, and SRV records in an unsigned zone. These DNSSEC Resource records include DNSKEY, RRSIG, and NSEC. DNSKEY records are used to sign the records. The RRSIG record is returned to the client in response to a successful query along with the A record. The NSEC record is returned to positively deny that the requested A record exists in the zone.

DNSSEC uses a series of keys to secure the server and the zones. These include the ***Key Signing Key (KSK)*** and the ***Zone Signing Key (ZSK)***. The KSK is an authentication key that signs all the DNSKEY records at the root of the zone, and it is part of the chain of trust. The ZSK is used to sign zone data.

Automated key rollover is the process by which a DNSSEC key management strategy for key management is made easier with automated key regeneration.

CONFIGURE DNSSEC ON AN ACTIVE DIRECTORY INTEGRATED ZONE

GET READY. Log on to the computer where you installed the DNS Server role and the ADatum.com ADI zone, with administrative privileges. To configure DNSSEC on an Active Directory integrated zone, perform the following steps:

TAKE NOTE*

Examine all the options in the Zone Signing Wizard. Test items often require you to know where to set a particular choice.

1. Open Server Manager and click Tools > DNS. This loads the *DNS Manager* console.
2. Expand *DNS Server* by clicking the arrow to the left of the server name.
3. Expand the *Forward Lookup Zones* by clicking the arrow to the left of Forward Lookup Zones.
4. Right-click the ADatum.com zone. Click DNSSEC > Sign The Zone. The DNSSEC Zone Signing Wizard opens. It is possible to choose the default options throughout.
5. Click Next. The wizard displays the signing options.
6. There are three options to define the parameters used to sign the zone. Select Customize zone signing parameters, and then click Next.
7. This screen allows the selection of the DNS server that will manage the keys for the zone. The default is the current server. Click Next.
8. In the *New Key Signing Key (KSK)* dialog box, click Add, and then make the Key Signing Key property selections. Settings include the algorithm, key length, replication, and auto rollover. Click OK when the selections have been made. Click Next, and then click Next again.
9. In the *New Zone Signing Key (ZSK)* dialog box, click Add, and then make the Zone Signing Key property selections. Settings include the algorithm, key length, key storage provider, validity period of the keys, and auto rollover. Click OK when the selections have been made, and then click Next.

10. An NSEC record provides authenticated denial of existence. If a DNS client requests a record that does not exist, the server provides an authoritative denial and the NSEC or NSEC3 record verifies this as genuine. The options are for NSEC or NSEC3. NSEC3 is the default. Click Next.
11. If the DNS server is also a domain controller, when trust anchor distribution is enabled, every other DNS server that is also a domain controller in the forest will receive the trust anchors for the zone. This speeds up the key retrieval. Automated key rollover should be set if trust anchors are required on nondomain-joined computers. Click Next.
12. The final options screen, Signing and Polling Parameters allows for the configuration of the delegation key record algorithm (DS record) and the polling intervals for the delegated zones. Accept the defaults by clicking Next > Next. The wizard signs the zone. Click Finish. The new DNSSEC records can now be seen in the DNS Manager.

Note that the padlock at the root of the Adatum.com zone (see Figure 12-1) shows the zone is signed. Also note the additional records visible in the zone DNSKEY (Public Key for the zone), RRSIG, NSEC3. Indeed, each original entry now has four records: the A, RRSIG for the A, NSEC3, and the RRSIG for the NSEC3 record.

Figure 12-1

Displaying the signed zone

Once the zone is signed, two more options are available on the zone DNSSEC context menu: Properties and Unsign the Zone. The Properties dialog contains the settings you made in the wizard. Unsign the Zone removes all the records and disables DNSSEC for this zone.

The ***Name Resolution Policy Table (NRPT)*** contains a list of rules for DNS client access and response to the DNS server. NRPT is normally set through Group Policy when a zone is signed using DNSSEC.

Configuring DNS Socket Pool

The DNS s***ocket pool*** is a tool used to allow source port randomization for DNS queries, which reduces the chances of an attacker guessing which IP address and port (socket) the DNS traffic uses.

The DNS socket pool protects against DNS spoofing attacks. To be able to tamper with DNS traffic, an attacker needs to know the correct socket and the randomly generated transaction ID. DNS socket pooling is enabled by default in Windows Server 2012 and Windows Server 2012 R2. The default size of the DNS socket pool is 2500, and the available settings range from 0 to 10,000. The larger the number of ports available to the pool, the more secure the communication.

Windows Server 2012 and Windows Server 2012 R2 also allows for an exclusion list to be created. The preferred method to set the socket pool size is through the use of the `dnscmd` command-line tool as shown here:

1. Launch an elevated command prompt.
2. Type the following command:

   ```
   dnscmd /Config /SocketPoolSize <value>
   ```

The value must be between 0 and 10,000.

Configuring DNS Cache Locking

DNS cache locking prevents an attacker from replacing records in the resolver cache while the Time to Live (TTL) is still in force. When cache locking is enabled, records cannot be overwritten.

When a DNS client or server (resolver) has received the DNS record of a requested resource, that entry is stored in the resolver cache until the TTL for that record expires. (The TTL is set on the record itself at the zone level.) It is possible for this information to be altered by an attacker while it sits in the cache. This allows an attacker to divert the client to a different (unsafe) resource.

To prevent this situation, Windows Server 2012 and Windows Server 2012 R2 provides the DNS cache locking feature. This feature prevents any changes being made to the contents of a record in the resolver cache until the TTL has expired. DNS cache locking uses a percentage of the TTL to set the lock. For example, if the cache locking value is set to 75, the record would not be available to be overwritten until at least 75% of the TTL expires. The optimum setting is 100; this prevents any record from being overwritten during the time its TTL is valid.

The preferred method to set the DNS cache locking value is through the use of the `dnscmd` command-line tool as shown here:

1. Launch an elevated command prompt.
2. Type the following command:

   ```
   dnscmd /Config /CacheLockingPercent <percent>
   ```

3. Restart the DNS Service to apply the new settings. From the command prompt enter `net stop DNS`, wait for the service to stop, and then enter `net start DNS`

Configuring DNS Logging

DNS logging is a troubleshooting tool to allow for detailed, file-based analysis of all DNS packets and messages. The full title is DNS ***debug logging***. There is a processing and storage overhead in the use of debug logging.

Event Viewer is an essential tool in the successful management and troubleshooting of a DNS server. Windows Server 2012 and Windows Server 2012 R2 provides a specific DNS server application log. This log records events such as starting and stopping the DNS Service, changes to DNS configurations, warnings, and other events. In addition, the DNSSEC zone signing and zone loading events are recorded. There are, however, many occasions when more detailed logging of events, packets, and protocols is required. To facilitate this, Windows Server provides file-based debug logging.

Debug logging is enabled at the server level and accessed through the DNS Server Properties dialog box.

CONFIGURE DNS DEBUG LOGGING

GET READY. Log on with administrative privileges to the computer where you installed the DNS Server role. Ensure that the ADatum.com ADI zone is present, and then perform the following steps:

1. Open Server Manager and click Tools > DNS. This loads the *DNS Manager* console.
2. Expand the DNS server by clicking the arrow to the left of the server name.
3. Right-click on the LON-DC1 server. Click Properties, click the Debug Logging tab, and then check the Log Packets for debugging check box.

The following DNS debug logging options are available:

- **Direction of packets:** Send packets sent by the DNS server are logged in the DNS server log file. Receive packets received by the DNS server are logged in the log file.
- **Content of packets:** Queries specify that packets containing standard queries (per RFC 1034) are logged in the DNS server log file. Updates specify that packets containing dynamic updates (per RFC 2136) are logged in the DNS server log file.
- **Notifications:** Specifies that packets containing notifications (per RFC 1996) are logged in the DNS server log file.
- **Transport protocol:** UDP specifies that packets sent and received over UDP are logged in the DNS server log file. TCP specifies that packets sent and received over TCP are logged in the DNS server log file.
- **Type of packet:** Request specifies that request packets are logged in the DNS server log file (a request packet is characterized by a QR bit set to 0 in the DNS message header). Response specifies that response packets are logged in the DNS server log file (a response packet is characterized by a QR bit set to 1 in the DNS message header).
- **Enable filtering based on IP address:** Provides additional filtering of packets logged in the DNS server log file. This option allows logging of packets sent from specific IP addresses to a DNS server, or from a DNS server to specific IP addresses.
- **File name:** Lets you specify the name and location of the DNS server log file.
- **Log file maximum size limit:** Lets you set the maximum file size for the DNS server log file. When the specified maximum size of the DNS server log file is reached, the DNS server overwrites the oldest packet information with new information. If left unspecified, the DNS server log file's size can take up a large amount of hard disk space.

Debug logging can be highly resource-intensive and can impact the performance of the DNS server itself. It is recommended that debug logging be used as a temporary measure to gain detailed information regarding DNS server performance, only when it is required. For this reason, the debug logging is disabled by default. The debug logging settings allow for granular control of the types of events or DNS messages that are logged, which reduces the impact to a degree.

■ Configuring Delegated Administration

THE BOTTOM LINE

DNS is a key service within your network. Administration of the service should be restricted to those who really need it. The principle of least privilege should always apply to DNS administration.

Domain Admins have full permissions by default to manage all aspects of the DNS server, but only in the domain where the Domain Admins security group is located. A member of the Enterprise Admins group has similar permissions but throughout the entire forest.

To delegate administration privileges to a specific user or security group, you add that user or group to the DNS Admins security group. Members of this group can view and modify all DNS data, settings, and the configuration of DNS servers within their home domain.

The DNS Admins group is a Domain Local security group. By default, this group is empty.

■ Configuring Recursion

THE BOTTOM LINE

Recursion in DNS is the process by which a client makes a query to a DNS server for an IP address associated with a Fully Qualified Domain Name (FQDN). The server then establishes that IP address through one or many separate queries to other servers and returns the address to the querying client.

In most business networks, the DNS servers are configured to allow recursive queries. That is, the querying client requests the IP address related to an FQDN such as www.adatum.com. The client then makes a recursive query to the configured DNS server.

The local DNS server must either provide an authoritative response (from its own zone) or a positive response (from its cache). If the DNS server has no copy of the namespace requested, it provides an authoritative response (stating the record does not exist).

If the DNS server is configured for recursion, the server makes a recursive query to other DNS servers (usually through root hints on the Internet) and eventually provides the authoritative answer to the querying client.

If recursion is not enabled and no forwarders are configured, the DNS server makes no further queries and responds only from the zones it holds.

The restriction of recursion is a good way of securing a DNS server and maintaining control of DNS query traffic.

To prevent all DNS servers from making recursive queries, forward all external queries to a single server and enable recursion and root hints (or a different forwarder such as an ISP DNS server). This configuration directs all Internet queries through a single internal DNS server, while all local domain or forest DNS queries are resolved locally.

DISABLE RECURSION

WARNING If recursion is disabled and root hints and forwarders are not used on any DNS servers, then *no* external queries will ever be resolved. In short, your network will never be able to connect to named resources on the Internet.

GET READY. Log on with administrative privileges to the computer where you installed the DNS Server role. Ensure that the ADatum.com ADI zone is present, and then perform the following steps:

1. Open Server Manager and click Tools > DNS. This loads the *DNS Manager* console.
2. Expand the DNS server by clicking the arrow to the left of the server name.
3. Right-click the LON-DC1 server. Click Properties, click the Advanced tab under *Server options*, and then check the Disable recursion (also disables forwarders) check box.

WARNING There is a difference between disabling recursion on a server and preventing the server from making recursive queries for a client. If a client can only make iterative queries, then performance will be degraded because every request requires several iterative DNS queries from the client rather than a single recursive one. Recursion and recursive queries are entirely different things!

If the previous option is not set, then the DNS server will try to resolve queries in the following order:

Local Zones, Conditional Forwarders, Forwarders, Root Hints

Configuring Netmask Ordering

THE BOTTOM LINE

Netmask ordering prioritizes DNS responses based on the subnet of the requesting client. If several A records exist for a single name, then the one that exists in the subnet of the client is returned.

It is common for a DNS zone to hold more than one A record for a particular hostname. The netmask ordering feature allows the DNS server to return the record that is most local to the client requesting the IP address.

As an example, the FQDN AddressBook.adatum.com has several instances throughout the network and also has several A resource records associated with it. Each subnet has a copy of this address book that rarely changes.

It makes sense that a DNS server will always provide the most local copy for a client to access. Because the subnet identifies the location or site in which a client resides, it is easy to identify where the query originated and thereby to provide the client with the correct A resource record in response. The alternative to this method is to provide a round-robin type of response each time the FQDN is requested, regardless of the location of the client. This method increases network traffic and is not as efficient.

CONFIGURE NETMASK ORDERING

GET READY. Log on with administrative privileges to the computer where you installed the DNS Server role. Ensure that the ADatum.com ADI zone is present. Then, to configure Netmask ordering, perform the following steps:

1. Open Server Manager and click Tools > DNS. This loads the *DNS Manager* console.
2. Expand the DNS server by clicking the arrow to the left of the server name.
3. Right-click the LON-DC1 server. Click Properties and click the Advanced tab. Under Server options, check the Enable netmask ordering check box.

Configuring A GlobalNames Zone

THE BOTTOM LINE

Windows Server 2012 and Windows Server 2012 R2 DNS provides support for single-label names without the need for NETBIOS or WINS. This allows a large multi-DNS environment to support a single name, such as addressbook, rather than an FQDN, such as addressbook.adatum.com.

In an environment where there are several DNS suffixes such as contoso.com, adatum.com, and fabrikam.net, it is necessary to manually create a GlobalNames zone within DNS to allow a single-label name to be resolved.

As an example, the company address book is accessed throughout the enterprise by entering *addressbook* into an Internet Explorer address bar. Without the use of a GlobalNames zone, in this scenario, the name would not be resolved. In an environment with a single DNS suffix such as contoso.com, the suffix would be appended automatically and the name would be resolved.

The only other method for achieving this would be the use of a Windows Internet Naming Service server (WINS). This is a deprecated technology and GlobalNames zone is now the preferred method for achieving single-label name resolution.

Windows Server 2012 and Windows Server 2012 R2 provides built-in support for a GlobalNames zone; however, it must be manually configured and enabled in several steps, as shown in the following section.

CONFIGURE A GLOBALNAMES ZONE

GET READY. Log on with administrative privileges to the computer where you installed the DNS Server role. Ensure that the ADatum.com ADI zone is present. Then, to configure a GlobalNames zone, perform the following steps:

1. From the start screen, type CMD, right-click the CMD icon, and then click Run As administrator from the bottom of the screen.
2. In the command window, type dnscmd <servername> /Config /EnableGlobalnamessupport 1 and wait for the *Command completed successfully* message.
3. Close the command window, and repeat steps 1 and 2 on every DNS server in the forest.
4. Open Server Manager and click Tools > DNS. The *DNS Manager* console opens.
5. Expand the DNS server by clicking the arrow to the left of the server name.
6. Right-click the LON-DC1 server. Click on New Zone to start the New Zone Wizard. Click Next four times. This creates a new primary forward lookup zone replicated to all DNS servers in the domain.
7. Enter the name GlobalNames (this is not case-sensitive), and then click Next.
8. Select Do not allow dynamic updates. Because all entries in this zone will be manually created, this is not required and would be a security loophole. Click Next > Finish.
9. The GlobalNames zone is visible (see Figure 12-2).

Figure 12-2

Displaying GlobalNames zone—DNS manager

To access the addressbook, create a CNAME record in the GlobalNames zone that points to any records that already exist in the other zones on the Forest DNS servers.

In this instance, a single CNAME record of addressbook in the zone pointing to addressbook.adatum.com would allow any client to resolve this FQDN by entering the label addressbook.

Analyzing Zone Level Statistics

While logging can be used to see what records are being queried and can be used for troubleshooting, logging is not the best tool to determine DNS zone level statistics. Therefore, starting with Windows Server 2012 R2, Microsoft DNS Server provides zone level statistics, which allow you track the usage pattern or monitor DNS server performance.

Statistics that can be retrieved for DNS servers using the Windows PowerShell Get-DnsServerStatistics cmdlet include the following:

- Server wide query statistics
- Zone query statistics
- Zone transfer statistics
- Zone update statistics
- Packet statistics
- Different record statistics
- DNSSEC statistics

To get the complete zone level statistics for the contoso.com domain, execute the following Windows PowerShell command:

```
Get-DnsServerStatistics -ZoneName contoso.com
```

To the current zone level statistics counter execute the following Windows PowerShell command:

```
Get-DnsServerStatistics -ZoneName contoso.com -Clear
```

Business Case Scenarios

Scenario 12-1: Administering a DNSSEC Secured Zone

As a member of the DNS Admins domain local security group of the ADatum.com domain, you have created an ADI zone for the contoso.com domain. You implement DNSSEC for this zone and later realize that you need to delegate the zone to a non-active directory controller DNS server. What must you do first?

Scenario 12-2: Managing Delegation

You are the Enterprise administrator for a multi-domain multi-branch forest. The root domain is contoso.com. You need to provide a number of lower level administrators with privileges to create and modify DNS server and zone settings for the following zones: uk.contoso.com, fabrikam.net, and eu.adatum.com. What must you do?

Deploying and Managing IPAM

LESSON 13

Configuring IPAM

THE BOTTOM LINE

IP Address Management (IPAM) is a new feature in Windows Server 2012 and Windows Server 2012 R2. IPAM provides an administrator with the ability to plan, manage, track, and audit the use of all IP addresses and the DNS services within the network.

IPAM is a new feature within Windows Server 2012 and Windows Server 2012 R2, but it is *not* a new network function. Planning, management, tracking, and auditing of IP addresses have been a thorn in every network administrator's side for many years. The only method of managing such facilities prior to Windows Server 2012 and Windows Server 2012 R2 was by the Dynamic Host Configuration Protocol (DHCP) and Domain Naming Service (DNS) management consoles, third-party databases or applications, spreadsheets, or in some cases even scraps of paper with details of every network node recorded. The advent of IPAM in Windows Server 2012 and Windows Server 2012 removes the necessity for all of these alternative methods.

IPAM provides a single point of administration for all DNS and IP management features within an Active Directory Forest. There are a number of key terms that need to be clearly understood prior to implementing IPAM. In addition, there are a number of requirements that need to be taken into consideration.

- ***IP address block:*** IP address blocks are the highest level conceptual entity in an IP address space. They are marked with a starting and ending IP address. For Public IP addresses, the address block is assigned by the Internet Registry (for smaller ranges, this is delegated by your Internet Service provider). An address block is used by network administrators to be the split into address ranges, which is the basis of DHCP scopes. An administrator can use IPAM to add, import, edit, and delete IP address blocks. IPAM automatically tracks the address ranges belonging to an address block. See Figure 13-1 for a hierarchical representation of the address block.
- ***IP address range:*** IP address ranges are the next hierarchical level of an IP address space, beneath the address block. Typically an address range is a subnet marked by a starting and ending address, using a subnet mask. An IP address range normally maps to a DHCP scope. IP address ranges can be added or imported by IPAM.
- ***IP addresses:*** IP addresses are the individual addresses that are contained in an IP address range. IPAM allows complete end-to-end management of both IPv4 and IPv6 IP addresses. IPAM automatically maps IP addresses to the correct range by using the start and end address of a range. IP addresses can be added manually or imported by IPAM from external sources.

Figure 13-1 shows the whole IP address space and how each component fits into the hierarchical model.

Figure 13-1

Displaying the IP address space

In order to successfully deploy IPAM, the following general requirements should be met:

- An IPAM server *must* be a domain member but *cannot* be a domain controller.
- The IPAM server should be a single purpose server. It is not recommended to install DHCP, DNS, or any other roles on the IPAM server.
- The IPAM server can manage only the IPv6 address space if IPv6 is enabled on that server.
- Always log on to the IPAM server with a domain account, *not* a local account.
- Ensure that the IPAM administrator is a member of the correct local IPAM security group on the IPAM server.
- To use IPAM to track and audit IP addresses, ensure that *log events on all domain controllers and NPS servers* is enabled.

Configuring an IPAM Server

IPAM requires several steps to successfully configure the server, discovery, and address space management. The planning stage is fairly simple, but the servers, services, and administrators must all be configured carefully to ensure the feature adds full value.

There are two main components within IPAM:

- **IPAM server:** Collects data from the managed DNS and DHCP servers within the discovery scope. The IPAM server also manages the Windows Internal Database. Remember that IPAM can use only the Windows Internal Database. The server also provides the Role-Based Access Control (RBAC) for the IPAM installation. All the IPAM security groups and roles are managed from the IPAM server.

- **IPAM client:** Provides the interface with which the IPAM administrator manages and configures the server. The client interfaces with the server and invokes the Windows PowerShell commands to carry out DHCP and DNS tasks as well as any remote management functions. The IPAM client is automatically installed on the IPAM server when the IPAM feature is installed. It is also possible to install the IPAM client on an alternative Windows Server 2012 or Windows Server 2012 R2 server without the IPAM server feature. Finally, it is also possible to manage IPAM using the IPAM client from a Windows 8 client with the Remote Server Administration Tools (RSAT) installed.

INSTALL IPAM ON A MEMBER SERVER

GET READY. Log on to the domain-joined computer where you want to install the IPAM feature, with administrative privileges. To install the IPAM feature, perform the following steps:

1. Open Server Manager, and click Manage > Add Roles and Features. The *Add Role Wizard* begins.
2. Click Next four times, until the *Select Features* dialog box appears.
3. Select the check box next to *IP Address Management (IPAM) Server*. Click Next. This loads the *Add Required Features* dialog box.
4. Click Add Features, click Next, and then click Install. Once the installation begins, click Close.

Once the installation is complete, the IPAM feature appears on the main screen of Server Manager.

Once the IPAM server has been installed, there are a number of steps required to configure it successfully. These are all shown on the main IPAM client screen.

The following IPAM tasks are required to configure the IPAM server installation.

Connect to IPAM Server

This step is automatically carried out when the client is running on an IPAM server. If the client is running from a remote server (not an IPAM server), the administrator needs to connect to the chosen IPAM server.

Provision the IPAM Server

IPAM provisioning is the process of allowing the IPAM server to configure and manage the necessary features and functions of the servers, services, and domain objects required for IPAM.

There are two methods of provisioning the IPAM server:

- Automatic Group Policy-based provisioning
- Manual provisioning

The default is Group Policy-based and once this is selected and provisioned, the only method for reversing that decision is to uninstall IPAM and then reinstall. The Group Policy-based provisioning method creates the Group Policy objects (GPOs) that allow the required access settings on all the IPAM managed servers. The GPOs created are:

- IPAM1_DHCP for DHCP servers
- IPAM1_DNS for DNS servers
- IPAM1_DC_NPS for domain controllers and NPS servers

In addition, the IPAM security groups are created, the IPAM database is created and role-based access is configured, and finally the access to the IPAM tasks and folders is configured.

Configuring IPAM Database Storage

With Windows Server 2012 R2, during the IPAM provisioning process, you can use Windows Internal Database (WID) or you can select Microsoft SQL Server so that you can use a dedicated SQL server. By using an external database, you have additional scalability, disaster recovery, and reporting.

During provisioning, the WID is selected by default and the database is stored in the C:\Windows\System32\IPAM\Database folder. However, if necessary, you can migrate the database from WID to SQL after IPAM has been provided by using the Move-IpamDatabase and Set-IpamDatabase Windows PowerShell cmdlets. Refer to Figure 13-2.

Figure 13-2

Configuring databases for IPAM

Configuring Server Discovery

Having installed and provisioned the IPAM server, the next step is to configure server discovery.

Configure Server Discovery

Server discovery is the process of defining which domains in the forest that contain servers will be managed by this IPAM server.

Start Server Discovery

IPAM discovery is the process of retrieving a list of all domain controllers, DNS servers, and DHCP servers from the active directory.

Select or add servers to manage and verify IPAM access

Once the IPAM discovery is complete, the IPAM administrator can select which servers, roles, and services will be managed from the list in server inventory.

Retrieve Data from Managed Servers

This final task launches various data collection tasks on the IPAM server to collect data from all the servers managed by this IPAM server.

Once the IPAM server tasks are complete, the IPAM server will create a schedule of tasks to repeat at various intervals.

Having completed the IPAM server tasks, the full server inventory will now appear (after a refresh) in the Server Manager IPAM console. The server inventory contains a list of managed servers and a panel containing the full relevant details for the selected server.

■ Creating and Managing IP Blocks and Ranges

THE BOTTOM LINE Once the installation and configuration is complete, the IPAM server needs to work with all the IP blocks and ranges.

The starting point for the configuration of IP address blocks and IP address ranges is the main IPAM screen, which is reached through Server Manager. Having reviewed the IP address space details previously in Figure 13-1, the first stage is to allocate IP address blocks for the server to track and manage.

CREATE AN IP ADDRESS BLOCK

GET READY. Log on to the IPAM server, with administrative privileges. To create IP address blocks, perform the following steps:

1. Open Server Manager, and click IPAM > IP Address Blocks, Tasks.
2. Click Add IP Address Block. The *Add or Edit IPv4 Address Block* dialog box opens.
3. Complete the dialog box fields with the required IP block data, and click OK.

The newly added IP address block is now listed in the top panel and the configuration details in the bottom panel of the IPAM IP address blocks section of the console.

After you create the IP address block, the next stage is to split the IP address block into IP address ranges. This procedure is also done through the IPAM console in Server Manager.

CREATE AN IP ADDRESS RANGE

GET READY. Log on to the IPAM server, with administrative privileges. To create an IP address range, perform the following steps:

1. Open Server Manager, and click IPAM > IP Address Range Groups, Tasks (refer to Figure 13-5).
2. Click Add IP Address Range. The *Add or Edit IPv4 Address Range* dialog box opens.
3. Complete the dialog box fields with the required Basic IP Range configuration data.
4. In this instance, there are additional custom configuration options to be made. This section allows the IPAM administrator to associate the IP address range with a number of selectable criteria (AD Site, Building, and so on). It is possible to select several user-entered values. Click Add and select the chosen options, entering the required user data, and then click OK.
5. Creating these attributes assists in the tracking and monitoring of IP address range utilization.
6. Click OK to finish the creation of the IP address range.

Having completed the IP configuration, the IPAM server will then maintain accurate records of utilization and allocations. In the situation where the IPAM server manages several IP address ranges, the custom configuration proves most useful to reduce the clutter in the console. Figure 13-3 shows the use of the custom attributes chosen previously to limit the number of IP address ranges as shown.

Figure 13-3

Displaying filtered IP address ranges

From the IP Address Range Groups console page, an IPAM administrator can carry out a number of actions on each range by right-clicking the IP Address Range Group, to open the context menu. The addition of these options significantly reduces the workload of an IPAM administrator. There is no requirement to remotely log on to a DHCP server and query the data directly.

The IP Address Inventory console allows the IPAM administrator to individually manage and edit any dynamic or static IP addresses monitored by the IPAM server. A number of DHCP and DNS management tasks can also be performed by right-clicking the IP address range to open the context menu. The console also provides detailed information on each address in the bottom panel.

In addition, the MONITOR AND MANAGE section of the console provides detailed DHCP Server and Scope management to ensure that all areas of the IP address space are covered.

Monitoring Utilization of IP Address Space

THE BOTTOM LINE

Having installed and configured the IPAM server, an IPAM administrator needs to monitor the utilization of IP addresses within his scope of control. IPAM has many monitoring tools available to make this task easier, preventing ranges from running out of available addresses or blocks running out of ranges.

The IPAM Server console provides a dedicated MONITOR AND MANAGE section. Within this section, there are four categories:

- DNS and DHCP Servers
- DHCP Scopes
- DNS Zone Monitoring
- Server Groups

The DHCP Scopes section provides a detailed breakdown of the level of utilization of all dynamic IP addresses. The utilization column is the first column of every console panel where IP addresses are listed.

To provide a more granular control of utilization, the IP ADDRESS SPACE section of the console provides a number of utilization tools.

The IP address blocks section allows the IPAM administrator to review block utilization by Public, Private, or all IP address blocks. IPAM summarizes all utilization statistics and trends at the address block level, based on the address ranges assigned to that block.

The IP Addresses section of the console enables complete end-to-end utilization management and displays any duplicate addresses as well as any expired or unexpectedly unallocated addresses.

IPAM allows the configuration of thresholds for the percentage of the IP address space that is utilized. IPAM then uses the preset thresholds to determine under and over utilization of IP address blocks, ranges, and range groups.

Migrating to IPAM

Most IP address space management is currently carried out using a mixture of spreadsheets, third-party applications, and printed materials. Having installed the IPAM feature and configured the provisioning and discovery, an IPAM administrator might choose to migrate all the IP address space data into the IPAM database.

Before an IPAM administrator can take advantage of the migration tools available, the feature must be correctly installed, provisioned, and configured for server discovery.

The IPAM client console options for importing IP address data from a Comma Separated Value (CSV) file include the following (refer to Figure 13-5):

- Import IP Address Block
- Import IP Address Ranges
- Import IP Addresses
- Import and Update IP Address Ranges

There is also an export option, which exports all IP address data to a user selected .CSV file. It is important to also consider that when backing up the IPAM server, the Windows Internal Database must be backed up to secure the IPAM data.

Delegating IPAM Administration

Network administration is a vast topic with many varied and differing roles required to carry it out successfully. Within IP address management, there are several sets of tasks that might require separate staff to carry them out. For this reason, IPAM relies on RBAC to provide the necessary delegate administrative features.

When the IPAM feature is installed, the provisioning process (if you selected automatic Group Policy-based provisioning) creates the RBAC roles to enable simple delegated administration of the whole IPAM infrastructure.

The roles are controlled by using the previously mentioned IPAM local security groups. These groups allow delegation of tasks to individuals whom you do not want to have full administrative access to your IPAM server and data. Simply place the necessary users or groups in the correct Local group on the IPAM server:

- **IPAM Users:** Users who are members of this group can view server discovery, IP address space, and server management information. Group members can also view IPAM and DHCP server operational events, but they cannot view IP address tracking information.
- **IPAM MSM Administrators:** Members of this group have IPAM Users privileges and can perform common IPAM multi-server management (MSM) tasks and server management tasks.
- **IPAM ASM Administrators:** Members of this group have IPAM Users privileges and can perform common IPAM address space management (ASM) tasks and IP address space tasks.
- **IPAM IP Audit Administrators:** Members of this group have IPAM Users privileges and can perform common IPAM management tasks and can view IP address tracking information.
- **IPAM Administrators:** Members of this group have the privileges to view all IPAM data and perform all IPAM tasks.

Managing IPAM Collections

An IPAM collection refers to the scheduled IPAM server tasks created at the installation of the IPAM feature. The collection of IP address space data, event log data, and DNS data is critical to a successful IPAM implementation.

Among all the Scheduled IPAM server tasks created at the installation of the IPAM feature, only a subset of these tasks are actual collection tasks (see Table 13-1).

Table 13-1

IPAM Collection Tasks

Task Name	Description	Default Frequency
AddressUtilization	Collects IP address space usage data from DHCP servers to display current and historical utilization.	2 hours
Audit	Collects DHCP and IPAM server operational events. Also collects events from domain controllers, NPS, and DHCP servers for IP address tracking.	1 day
ServerAvailability	Collects service status information from DHCP and DNS servers.	15 minutes
ServerConfiguration	Collects configuration information from DHCP and DNS servers for display in IP address space and server management functions.	6 hours
Service Monitoring	Collects DNS zone status events from DNS servers.	30 minutes

The collection tasks are first carried out as part of the initial post installation IPAM server tasks.

It is also possible to set off the server tasks at any point in time by selecting the *Retrieve data from the managed server* area of the quick start panel in the IPAM Overview console page or selecting *Retrieve all server data* from the tasks menu of the Server Inventory console page.

Having collected all the server data, it is possible to view the completed (or running tasks) by selecting the *More…* area of the Yellow information bar at the top of the IPAM Server Tasks panel. This option opens the Overview Tasks Details dialog box. This dialog box provides more detailed information than the main Overview console page.

■ Business Case Scenario

Scenario 13-1: Planning IPAM Deployment

You are an administrator of the Contoso Corporation. The Contoso Corporation has a forest root domain called contoso.com. There are subdomains in three trees: Eu.Contoso.com, US.contoso.com, and adatum.com.

The CTO has asked you to recommend an IPAM deployment option but wants each domain administrator to have full control of the infrastructure in his or her own domain.

What do you recommend?

14 LESSON

Configuring a Domain and Forest

■ Implementing Complex Active Directory Environments

THE BOTTOM LINE

A ***directory service*** stores, organizes, and provides access to information in a directory. Directory services are used for locating, managing, administering, and organizing common items and network resources, such as volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. One popular directory service used by many organizations is Microsoft's Active Directory.

Active Directory is a technology created by Microsoft that provides a variety of network services, including the following:

- Lightweight Directory Access Protocol (LDAP)
- Domain Name System (DNS) based naming and other network information
- Security mechanism for authentication that includes Kerberos-based and single sign-on authentication
- Security mechanism for authorization and auditing
- Central location for network administration and delegation of authority
- Policy-based management for user and computer accounts

Implementing Multi-Domain Active Directory Environments

With the number of objects that can be stored in an Active Directory domain, the use of organizational units to organize and manage those objects, the use of fine-grained Password Policies and Account Lockout Policies, and the ability to span multiple physical sites, many organizations need only one domain. However, sometimes legal or political reasons dictate that multiple domains must be used.

Active Directory is closely tied to DNS, which is used to locate objects and network resources. DNS is often used to represent an Internet presence and maybe used within an organization. When one company purchases or merges with another company, each company might need to keep its own identity and presence.

As large organizations tend to have large Active Directory databases, it might be beneficial to divide a large AD DS database into a more manageable size. In addition, due to replication of information between domain controllers, smaller domains reduce replication traffic, which can be beneficial over slower WAN links. However, this is only a benefit if there are a large number of accounts on the remote domain.

A single domain offers centralized management, where a set of administrators manage everything within the domain; although multiple domains can be centrally managed, multiple domains offer decentralized management, where different administrators manage

each domain. If an organization establishes a presence in a foreign country and there are political or legal reasons to have separate security domains, you might consider implementing separate domains.

Some companies define user domains and resource domains. A user domain, as it sounds, is used to manage users. Administrators of the user domain have full administrative control over the user accounts, and create, manage, and remove user accounts. Resource domains are sometimes managed by different management teams, which help secure resources.

Before you decide to use multiple domains and create child domains, you need to do some planning and preparation. Because DNS is so closely tied to Active Directory and Active Directory requires DNS to operate, you might need to define DNS domains for the new Active Directory domain. Because the domain will be within the same tree, you can delegate DNS for the child domain. It should be noted that an existing DNS service might be sufficient and does not necessarily need a separate DNS domain.

DELEGATE DNS FOR A CHILD DOMAIN

GET READY. To delegate DNS for a child domain, perform the following steps:

1. Log in to a domain controller such as RWDC01 as contoso\administrator.
2. Open Server Manager, open the Tools menu, and click DNS. The *DNS Manager* opens.
3. Expand the DNS server, expand Forward Lookup Zones, click Contoso.com, and then click New Delegation.
4. When the *New Delegation Wizard* starts, click Next.
5. To represent North America, type NA in the *Delegated domain* text box, and click Next.
6. On the *Name Servers* page, click Add.
7. In the *New Name Server Record* dialog box, type RWDC01.contoso.com in the Server fully qualified domain name (FQDN). Then click <Click here to add an IP address> (see Figure 14-1), and type 192.168.1.50. Click OK.

Figure 14-1

Delegating a new name server

8. When the wizard is complete, click Finish.

Creating a child domain is similar to installing a stand-alone domain controller. The primary difference is that you must link the child domain to the parent domain.

CREATE A CHILD DOMAIN

GET READY. To create a child domain on a stand-alone server that is not part of a domain, perform the following steps:

1. Log in to a domain controller such as RWDC01 as contoso\administrator.
2. Open Server Manager, open the Manage menu, and click Add Roles and Features.
3. When the *Add Roles and Features Wizard* starts, click Next.
4. On the *Select installation type* page, click Next.
5. On the *Select destination server* page, click Next.
6. On the *Select server roles* page, click to select Active Directory Domain Services. When the *Add Roles and Features Wizard* dialog box opens, click Add Features.
7. Back on the *Select server roles* page, click Next.
8. On the *Select features* page, click Next.
9. On the *Active Directory Domain Services* page, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When the installation is complete, click Promote this server to a domain controller link.
12. When the *Active Directory Domain Services Configuration Wizard* starts, click Add a new domain to an existing forest.
13. With the *Select domain type* as *Child Domain*, type contoso.com in the *Parent domain name* text box. In the *New domain name* text box, type NA.
14. Click the Change button. Type the user name of contoso\administrator and the password of Password01. Click OK.
15. Back on the *Deployment Configuration* page, click Next.
16. On the *Domain Controllers Options* page, type Pa$$w0rd in the *Password* and *Confirm password* text boxes. Click Next.
17. On the *DNS Options* page, click Change. Type the user name of contoso\administrator and the password of Pa$$w0rd. Click OK. Click Next.
18. On the *Additional Options* page, click Next.
19. On the *Paths* page, click Next.
20. On the *Review Options* page, click Next.
21. On the *Prerequisites Check* page, confirm that there are no issues, and then click Install.
22. When the installation is complete, click Close.

Implementing Multi-Forest Active Directory Environments

Some organizations need more complex environments that require the organization to have multiple forests. By having a multi-forest organization, each forest has its own configuration, schema, and global catalogs.

Separate Active Directory forests also offer isolated security. By having separate forests, each forest root domain has the Schema Admins and Enterprise Admins AD DS forest. Separate forests are often deployed by government defense contractors and other organizations that require security isolation.

If two or more independent organizations want to share resources, but each organization does not trust the domain administrators of the partner's organization or you need a segmenting of duties, you should use multiple forests with manually implemented trust relationships. Trusts are discussed in Lesson 15, "Configuring Trusts."

The ***Active Directory schema*** defines the objects and attributes of those objects. Because the schema is shared between domains, the domain admins of the various domains must agree on the schema changes. Therefore, if you require different schemas, you can use multiple forests.

Upgrading Existing Domains and Forests

THE BOTTOM LINE

As a general rule, as each version of Windows is introduced, the new version includes new features and functionality that was not available previously. Therefore, to get the most out of Windows servers, you should consider upgrading the domain controllers, domains, and forests to Windows Server 2012 R2.

Because Active Directory is a key component to many organizations, you must maintain Active Directory and be careful when upgrading to a newer version. Depending on your needs, the current state of Active Directory, and the hardware that Active Directory is running on, there are several options you can use to upgrade the Active Directory environment. These options include:

- ***In-place upgrade:*** If the domain controller is running Windows Server 2008 or Windows Server 2008 R2, you can upgrade each domain controller one-by-one to Windows Server 2012 R2. Because the Windows Server functional level will be Windows Server 2008 or Windows Server 2008 R2, some schema changes need to be done when using the Server Manager to install AD DS on the first Windows Server 2012 R2 domain controller.
- **Add servers running Windows Server 2012 R2 and promote to domain controllers:** As long as the functional level of the domain and forest is at least Windows Server 2008 mode, you will be able to install Windows Server 2012 R2 servers onto the domain. You can then install the AD DS and promote the server to a domain controller. Similar to an in-place upgrade, the schema is updated when you use the Server Manager to install AD DS on the first Windows Server 2012 domain controller.
- **Create a new AD DS Windows Server 2012 R2 domain and migrate the objects to the new domain or merge the domains together:** By adding new domains, you can perform a gradual upgrade to Windows Server 2012 R2, as you migrate resources to a domain that is running Windows Server 2012. By adding the extra domains, you will have different AD DS domains coexist and share resources until all objects are migrated or merged.

Of these, the "add servers running Windows Server 2012 R2 and promote to domain controllers" is the best option because you start with clean installation of Windows. The "in-place upgrade" option does not start as a clean installation of Windows" and the "create a new domain" option takes the most work to complete and might cause a little confusion when managing resources.

Understanding Functional Levels

To provide backward compatibility with older systems, Windows domains and forests can run at various levels of functionality. However, to get the most out of the domain controllers and utilize all of the available features, you need to upgrade the domain controllers to Windows Server 2012 R2 and raise the domain and forest functional level to Windows Server 2012 R2. However, as you move to the newer domain and forest functional levels, you might prevent older systems from operating in the upgraded environment.

Domain functional levels and ***forest functional levels*** allow administrators to enable domain- or forest-wide Active Directory features within your network environment, while maintaining compatibility with older operating systems. The functional level of the domain or forest depends on the version of the domain controllers in the domain or forest. After all of the domain controllers are upgraded within a domain or forest, the domain or forest functional level can be upgraded so that newer features can be made available.

RAISING DOMAIN FUNCTIONAL LEVELS

As of Windows Server 2012 R2, there are five available domain functional levels: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2. If you have multiple domains within a tree, you can upgrade the functional level of a domain without affecting the other domains. Windows Server 2012 or Windows Server 2012 R2 domain controllers do not support the Windows 2000 native mode functional level that was available with Windows Server 2008 R2 and earlier.

The Windows Server 2003 domain functional level supports domain controllers running Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2. It does not allow the presence of Windows 2000 domain controllers.

To raise the domain functional level, you must be a member of the Domain Admins group. In addition, the PDC Emulator must be available.

Before you can raise the domain functional level, you need to ensure that all domain controllers within that domain are running the required version of the Windows operating system. For example, to raise the domain functional level to Windows Server 2012, you must upgrade or retire any domain controllers with Windows Server 2008 R2 or earlier. It should also be noted that generally raising the domain functional level is a one-way process that cannot be reversed, short of performing an authoritative restore of Active Directory. The only exception to date is when you raise the domain functional level to Windows Server 2008 R2. If the forest functional level is Windows Server 2008 or lower, you have the option of rolling the domain functional level back to Windows Server 2008.

RAISE THE DOMAIN FUNCTIONAL LEVEL

GET READY. To raise the domain functional level, perform the following steps:

1. Log in to a domain controller such as RWDC01 as contoso\administrator.
2. Open Server Manager, and open Active Directory Users and Computers.
3. Right-click the Active Directory Domains and Trusts, and click Raise Domain Functional Level.
4. Select the desired domain functional level,and click Raise.
5. When it gives a warning saying that process may not be able to be reversed, click OK.
6. When the functional level has been raised successfully, click OK.
7. Close the Active Directory Users and Computers console.

RAISING FOREST FUNCTIONAL LEVELS

Forest functional levels are similar to domain forest functional levels, except that it affects all domains within the forest. Windows Server 2012 R2 domain controllers support the following forest functional levels: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.

When a forest is raised to a functional level, older domain controllers cannot be introduced into the domain. The forest functional level assumes that all domains are raised to the same level before the forest is raised. For example, to raise the forest functional level to Windows Server 2012 R2, you first have to raise the domain functional levels of all domains to Windows Server 2012 R2. Similar to the domain functional level, raising the forest functional level is generally an irreversible procedure.

To raise the forest functional level, you must be a member of the Enterprise Admins group. In addition, the Schema Master role must be available.

Before you can raise the forest functional level, you need to ensure that all domains are running the required version of the Windows operating system. For example, to raise the domain functional level to Windows Server 2012, all domains must be set to Windows Server 2012. Similar to domain functional levels, generally raising the domain functional level is a one-way process that cannot be reversed, short of performing an authoritative restore of Active Directory. The only exception to date is when you raise the forest functional level to Windows Server 2008 R2 and if the Active Directory Recycle Bin is not enabled, you have the option of rolling the forest functional level back to Windows Server 2008.

RAISE THE FOREST FUNCTIONAL LEVEL

GET READY. To raise the forest functional level, perform the following steps:

1. Log in to a domain controller such as RWDC01 as contoso\administrator.
2. Open Server Manager, and open Active Directory Domains and Trusts.
3. Right-click the Active Directory Domains and Trusts, and click Raise Forest Functional Level.
4. Select the desired forest functional level and click Raise.
5. When it gives a warning that when you raise a forest, you may not be able to reverse it, click OK.
6. When the forest has been raised successfully, click OK.
7. Close Active Directory Domains and Trusts.

Upgrading Windows Server 2008 and Windows Server 2008 R2 to Windows Server 2012 Domain Controllers

To upgrade from Windows Server 2008 or Windows Server 2008 R2 Active Directory Domain Services (AD DS), you can upgrade the operating system of the existing domain controllers to Windows Server 2012 or Windows Server 2012 R2 (assuming the hardware can support it), or introduce Windows Server 2012 or Windows Server 2012 R2 servers as domain controllers, and then decommission the older domain controllers.

If you have a server running an old operating system, and you want to move to the new operating system, you can choose to perform an upgrade or perform a clean install. An upgrade usually consists of starting the install program and letting the new files overwrite the old files. Although the upgrade tends to be simple, and quicker, the ***clean install*** allows you to start fresh with no old files or configuration on the machine. Of course, performing a clean

install of the operating system, installing any additional software, and configuring Windows and the software require more work. However, when you want the most reliable system, it is always best to perform a clean install.

For a domain that is running in Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 functional level, you can install Windows Server 2012 and add the computer to the domain. However, before you promote a server running Windows Server 2012 to a domain controller, you must upgrade the schema.

In previous versions of Windows, you would use the adprep.exe tool to upgrade the schema. However, while the Windows Server 2012 includes adprep32.exe has been deprecated. Instead, the Active Directory Domain Services Installation Wizard that is included in Server Manager incorporates the commands necessary to upgrade the AD DS forest schema.

PERFORM AN UPGRADE INSTALLATION

GET READY. To upgrade from Windows Server 2008 or Windows Server 2008 R2 to Windows Server 2012 or Windows Server 2012 R2, perform the following steps:

1. Log in to a domain controller such as RWDC01 as contoso\administrator.
2. Insert the Windows Server 2012 or Windows Server 2012 R2 installation disk into the DVD drive and start the Setup program. This displays the *Windows Setup* window.
3. Click Install Now. The *Windows Setup Wizard* opens, displaying the *Select the operating system you want to install* page.
4. Select the operating system edition and installation option you want to install and click Next. This displays the *License Terms* page.
5. Select the I accept the license terms check box and click Next. This displays the *Which type of installation do you want?* page.
6. Click the Upgrade: Install Windows and keep files, settings, and applications option. This displays the *Compatibility report (saved to your desktop)* page.
7. Note the compatibility information provided by the Setup program and click Next. This displays the *Upgrading Windows* page.

   After several minutes, during which the Setup program upgrades Windows Server 2008 or Windows Server 2008 R2 to Windows Server 2012 or Windows Server 2012 R2 and restarts the computer several times, the system finalizes the installation and the Windows sign-on screen appears.

Before you perform the upgrade, you should always check for hardware and software compatibility. After the installation is completed, you should then open the *Device Manager* and check for missing device drivers, run Windows updates, check for updates for non-Microsoft software, and check the Event Viewer for errors.

Configuring Multiple UPN Suffixes

THE BOTTOM LINE

Users can log on by using one of two ways: Domain username (domain_name\username) or the ***user principal names (UPNs)***, which uses an e-mail address format (such as username@domainname.ext). The global catalog resolves the UPN name to a username. Multiple UPN suffixes can be used to allow users to log on using an e-mail account name with different DNS namespace names.

To add multiple UPN suffixes, you use the Active Directory Domains and Trusts management console to manage the domain properties. After adding the additional UPN suffixes, users can log on with the alternative UPN suffixes. Of course, similar to when two users cannot use the same login name with a multi-domain environment, you must make sure that the UPNs are unique.

CONFIGURE MULTIPLE UPN SUFFIXES

GET READY. To configure multiple UPN suffixes, perform the following steps:

1. Log in to a domain controller such as RWDC01 as contoso\administrator.
2. Open Server Manager, and open Active Directory Domains and Trusts.
3. Right-click Active Directory Domains and Trusts, and then click Properties.
4. On the *UPN Suffixes* tab, type an alternative UPN suffix for the forest, and then click Add. Repeat the process until you add all desired UPN suffixes.
5. When done, click OK to close the *Properties* dialog box.

Business Case Scenarios

Scenario 14-1: Upgrading the Functional Level

You have a forest that includes five domains and two trees. It contains the following domains:

Contoso.com	3 Windows Server 2003 R2 domain controllers
Support.contoso.com	3 Windows Server 2003 R2 domain controllers and 1 Windows Server 2008 R2 domain controller
Sales.contoso.com	3 Windows Server 2008 domain controllers
Litware.com	2 Windows Server 2003 domain controller and 1 Windows 2000 Server domain controller
Partner.litware.com	2 Windows Server 2003 R2 domain controllers

What are the steps to promote the forest to the Windows Server 2012 R2 functional level?

Scenario 14-2: Working with UPN Suffixes

The Contoso Corporation is a holding company for 20 other companies. Each company has its own independent presence on the Internet and is functionally independent from the other companies. Although you have only one domain, you would like each company to function with its own domain name when logging using the UPN. What do you need to do?

15 LESSON

Configuring Trusts

Configuring Trusts

THE BOTTOM LINE

Trusts are relationships between one Windows domain and another Windows domain or non-Microsoft Kerboros v5 realm. Trusts are created to allow users in one domain the ability to authenticate and then access resources on another domain, forest, or realm.

Understanding Trusts

When you think of trusts, several different scenarios might come to mind. For example, think of a building manager who has several businesses renting the different office spaces in the building. Each business needs separate access to the office spaces. As part of the contract with the businesses, the building manager is required to have garbage removed and to have each office space vacuumed nightly. To meet the requirements of the renting businesses and the cleaners, the building manager needs to have keys made to allow access to the required areas. Each employee to each business needs to own a key to get in the front doors and to his respective offices and nowhere else. The cleaners need to have a master key to get into the front doors, all offices, maintenance closets, and every other room that has a trash receptacle. As you can tell, there are several different types of trust relationships among the building manager, employees, and the cleaning company.

Apply the previous example to domain and forest trusts. Think of the building manager as the Enterprise Administrator, think of each business as its own domain within the forest, and think of each employee as a user account. All have access to the building (forest), but when it comes to specific resources, each is limited by the security permissions required in each domain, essentially an internal forest trust as shown in Figure 15-1.

Now think of the cleaning company; its employees (user accounts) need access to everything in the forest, but they are from an entirely different company. Consider them an external forest. The building manager goes through a bid or interview process to find a trustworthy company to clean the building. Once the building owner finds the right cleaning business, he must "trust" it and provide it and its employees with the required access. This type of trust in a Windows Server environment is a ***one-way forest trust***. The business owner is the trusting root domain, and the cleaning company is the trusted root domain in another forest. The action of the business owner physically passing the keys to the cleaning company indicates the outbound direction of the trust; their receipt and acceptance of the keys is the incoming action.

Figure 15-1

Understanding trusts

Creating External Trusts

THE BOTTOM LINE

An ***external trust*** is a one-way or two-way nontransitive trust between domains that are not in the same forest, and that are not already included in a forest trust. External trusts connect two domains in separate forests to allow users in the trusted domain the capability to authenticate and/or access resources in the trusting domain. Because external trusts are nontransitive, any existing trusts already in place with the trusting domain cannot be traversed by members of the external trust's trusted domain users.

To accommodate external trusts, the trusting domain generates and stores, in AD DS, Foreign Security Principles for each security principle (Users, Computers, and Groups) of the trusted domain. This allows users of the trusted domain to become members of domain local groups in AD DS and to be added to Access Control Lists (ACL) of resources in the trusting domain. It is highly recommended to *not* modify the automatically generated Foreign Security Principles located in the trusting domain.

External trusts are also recommended for granting users access to resources in a single domain in an external forest that is not already part of a forest trust as illustrated in Figure 15-2. To create an external trust, you must be a member of the Domain Admins group, Enterprise Admins group, or have been delegated the authority with the appropriate permissions to create the trust. To create a two-way trust, you need the appropriate permissions or work with the other Domain Administrator to create trusts in both domains.

Figure 15-2

Understanding external trusts

To create an external trust, use the Active Directory Domains and Trusts tool.

CREATE A ONE-WAY EXTERNAL TRUST USING ACTIVE DIRECTORY DOMAINS AND TRUSTS

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. You must also ensure DNS has been configured to resolve the new trust. To create a one-way, external trust from ADATUM.LOCAL to CONTOSO.LOCAL, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut and, from the context menu, select Run as Administrator. If it is required, log in with a user account that is a member of the Domain Admins, Enterprise Admins or an equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain that will be the trusting side of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, and then click the New Trust button. The *New Trust Wizard* opens. Click Next.
4. Type in the Fully Qualified Domain Name (FQDN) of the domain that will be added to the trust, and then click Next.
5. Choose the External trust option if it is not already selected, and then click Next.

6. Select the direction One-way: outgoing option and, then click Next.
7. Select the Both this domain and the selected domain option, and then click the Next button.
8. Enter the username and password of a user with Domain Admin, Enterprise Admin, or equivalent rights in the specified domain, and then click Next.
9. Choose the Domain-wide authentication option, and click Next.
10. The *Trust Selections Complete* prompt appears. Click Next to create the trust.
11. On success, this displays the *Trust Creation Complete* prompt. Click Next.
12. To confirm the trust, select the Yes, confirm the outgoing trust tab, and then click Next.
13. Verify that the trust was successfully created, and then click Finish. Close the *SID Filtering information* box when prompted.
14. You now see the trusted domain listed in the list of outgoing trusts. Click Finish.

Creating Forest Trusts

THE BOTTOM LINE A forest trust is a one-way or two-way transitive trust between two forest root domains.

Forest trusts are implemented when users of an internal forest need to authenticate to and/or gain access to all resources of an external forest as illustrated in Figure 15-3. When creating a forest trust, every domain within a forest has a two-way trust with one another from the forest root domain down; therefore, a forest trust is transitive to all domains within the trusting forest.

Figure 15-3

Understanding one-way forest trusts

Consider creating forest trusts in the following scenarios:

- Integrating two forests during an acquisition or merger
- Collaborating two businesses closely with one another
- Combining all resources and users of a single company with multiple forests
- Accessing an application provided by a service provider in a forest with another user forest

To create a forest trust, both domains of the trust must be the forest root domain and have a Forest Functional Level of Windows Server 2003 or higher. The DNS infrastructure must be able to accommodate DNS requests between forests. You must be a member of the Domain Admins group, Enterprise Admins group, or have been delegated the authority with the appropriate permissions to create the trust. To create a two-way trust, you need an account in the external domain with the appropriate permissions or work closely with the other Domain Administrator or Enterprise Administrator to complete the two-way trust.

To create a forest trust, use either the Active Directory Domains and Trusts tool or the `netdom` command.

CREATE A ONE-WAY FOREST TRUST USING ACTIVE DIRECTORY DOMAINS AND TRUSTS

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. You must also ensure DNS has been configured to resolve the new trust. To create a one-way forest trust from ADATUM.LOCAL to CONTOSO.LOCAL, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut and, from the context menu, select Run as Administrator. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain that will be the trusting side of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, and then click the New Trust button. The *New Trust Wizard* opens. Click Next.
4. Type in the Fully Qualified Domain Name (FQDN) of the domain that will be added to the trust and click Next.
5. Choose the Forest trust option if not already selected, and click Next.
6. Select the direction One-way: outgoing option, and click Next.
7. Select the Both this domain and the selected domain option, and click the Next button.
8. Enter in the username and password of a user with Domain Admin, Enterprise Admin, or equivalent rights in the specified domain, and click Next.
9. Choose the Forest-wide authentication option, and click Next.
10. The *Trust Selections Complete* prompt appears. Click Next to create the trust.
11. On success, this displays the *Trust Creation Complete* prompt. Click Next.
12. To confirm the trust, select Yes, confirm the outgoing trust tab, and click Next.
13. Verify that the trust was successfully created, and click Finish. Close the *SID Filtering information* box if prompted.
14. You now see the trusted forest listed in the list of outgoing trusts. Click Finish.

Creating Shortcut Trusts

THE BOTTOM LINE

A shortcut trust is a one-way or two-way transitive trust between domains that are in the same forest. Shortcut trusts are primarily used to improve performance when authenticating to and accessing resources in an internal forest.

Shortcut trusts shorten the authentication trust path between two domains. If you have several domains and/or child domains in a forest, the authentication to the requested domain in the forest will have to travel up the authentication path to the root domain, and then to the domain the user is authenticated to. In some instances, the time for the Kerberos ticket to traverse the authentication path might be unacceptable or cause problems if there are any domain controller outages along the path. This can be resolved by implementing a shortcut trust between two domains in an internal forest. This allows the Kerberos ticket to travel, point-to-point, and allows authentication directly to the destination domain as illustrated in Figure 15-4.

Figure 15-4

Understanding two-way shortcut trusts

Shortcut trusts can be one-way or two-way trusts, however, keep in mind, if only one, one-way trust is created, the authentication path will be optimized only for authentication to the trusting domain. If users of each domain are authenticating to one another's domain, create a two-way shortcut trust.

You will not be able to create a shortcut trust between two domains in separate forests.

To create a shortcut trust, you must be a member of the Domain Admins group, Enterprise Admins group, or have been delegated the authority with the appropriate permissions to create the trust. To create a two-way trust, you need the appropriate permissions or work with the Domain Administrator or Enterprise Administrator in the other domain to create trusts in both domains.

To create a shortcut trust, use the Active Directory Domains and Trusts tool.

CREATE A SHORTCUT TRUST USING ACTIVE DIRECTORY DOMAINS AND TRUSTS

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To create a two-way shortcut trust between TREYRESEARCH.LOCAL and US.ADATUM.LOCAL, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut and, from the context menu, select Run as Administrator. If required, log in with a user account

that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.

2. Right-click the domain that will be one side of the trust, and then select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, and then click the New Trust button. The *New Trust Wizard* opens. Click Next.
4. Type the Fully Qualified Domain Name (FQDN) of the domain that will be added to the trust, and then click Next.
5. Select the direction Two-way option, and click Next.
6. Select the Both this domain and the selected domain option, and then click the Next button.
7. Enter the username and password of a user with Domain Admin, Enterprise Admin, or equivalent rights in the specified domain, and then click Next.
8. The *Trust Selections Complete* prompt appears. Click Next to create the trust.
9. After the trust successfully creates, this displays the *Trust Creation Complete* prompt. Click Next.
10. To confirm the outgoing trust, select Yes, confirm the outgoing trust option, and then click Next.
11. To confirm the incoming trust, select Yes, confirm the incoming trust option, and then click Next.
12. Verify that the trust was successfully created, and then click Finish.
13. You now see the trusted domain listed in the list of outgoing trusts. Click Finish.

Creating Realm Trusts

THE BOTTOM LINE A realm trust is a one-way or two-way, transitive or nontransitive trust between an AD DS domain and a non-Microsoft Kerberos v5 realm.

Realm trusts are used to allow users to authenticate and access resources in a non-Windows Kerberos v5 realm, or to allow users in a non-Windows Kerberos v5 realm access to resources in an AD DS domain (see Figure 15-5). Because not all authentication domains and realms are Microsoft, this added benefit allows the non-Microsoft solutions interoperability with one another.

Figure 15-5

Understanding two-way realm trusts

Consider using realm trusts in the following scenarios:

- Users in an AD DS domain need to access resources or log in to clients in a UNIX or MIT realm.
- Users in a UNIX or MIT realm need to access resources in an AD DS domain.

To create a realm trust, you must be a member of the Domain Admins group, Enterprise Admins group, or have been delegated the authority with the appropriate permissions to create the trust. To create a two-way trust, you need the appropriate permissions or work with the Domain Administrator or Enterprise Administrator in the non-Windows Kerberos v5 realm to create trusts in both environments.

To create a realm trust, use the Active Directory Domains and Trusts tool.

CREATE A REALM TRUST USING ACTIVE DIRECTORY DOMAINS AND TRUSTS

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To create a one-way realm trust from ADATUM.LOCAL to CONTOSOREALM.COM, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut and, from the context menu, select Run as Administrator. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain that will be the trusting side of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, and then click the New Trust button. The *New Trust Wizard* starts. Click Next.
4. Type in the Fully Qualified Domain Name (FQDN) of the domain that will be added to the trust and click Next.
5. Choose the Realm trust option if not already selected, and click Next.
6. In the *Transitivity of Trust* window, select the transitivity Nontransitive option. Click Next.
7. Select the direction One-way: outgoing option, and click Next.
8. Select a strong *Trust password* to share with the Realm Administrator, and enter and confirm the password. Click Next.
9. The *Trust Selections Complete* prompt appears. Click Next to create the trust.
10. Verify that the trust was successfully created. Remember that you have created only one side of the trust. Contact the Realm Administrator with the secure trust password to finish the trust, and click Finish.

MODIFY TRANSITIVITY OF REALM TRUSTS USING ACTIVE DIRECTORY DOMAINS AND TRUSTS

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To modify the transitivity of the trust from ADATUM.LOCAL to CONTOSOREALM.COM, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut and, from the context menu, select Run as Administrator. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain that will be the trusting side of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, highlight the realm trust you want to modify, and then click the Properties button.
4. At the bottom of the trust's *Properties* window, select the type of transitivity required for the trust. Click OK.
5. Once modified, click OK and close all displayed windows.

Configuring Trust Authentication

THE BOTTOM LINE Trust authentication defines how explicit the authentication and access to the trusting domain will be.

There are three scopes of trust authentication: selective authentication, domain-wide authentication, and forest-wide authentication. There are instances in which all users are not needed to log in to the trusting domain or forest or only specified users need to authenticate and access resources in the trusting domain. Trust authentication is configured on external and forest trusts.

Configuring Selective Authentication

Selective authentication allows explicit authentication and access to resources in an external trust or forest trust.

In many cases, when you create an external trust or a forest trust, you will not want all users of the trusted domain to authenticate and access all resources in the trusting domain. By enabling selective authentication, you can prevent all users from having access, and then explicitly allow a security group or stand-alone user access to the resources they need access to. The downside of implementing selective authentication is the administrative overhead involved to configure and maintain user access to resources. Each member server or computer account in the trusting domain that holds a required resource needs to be configured to allow authentication to the users in the trusted domain.

Users of the trusted domain are unable to access resources in the trusting domain until they are explicitly configured on the computer object's Discretionary Access Control List (DACL) in the Active Directory Users and Computers tool by checking the *Allowed to Authenticate* check box. By granting them access on the resource DACL, they will access as illustrated in Figure 15-6. It is best practice to configure a security group and add users to the group that need to access the resource.

Figure 15-6

Configuring selective authentication

Selective authentication is configurable only on external trusts and forest trusts.

ENABLE SELECTIVE AUTHENTICATION

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins

or delegated equivalent security groups. To create a one-way external trust from ADATUM.LOCAL to CONTOSO.LOCAL, perform the following steps:

1. Click Start and click the Active Directory Domains and Trusts shortcut. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain that is part of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, highlight the domain or forest trust you want to modify, and then click the Properties button.
4. Select the Authentication tab and choose Selective Authentication. Click OK. Close all displayed windows when complete.

Configuring Domain-Wide Authentication

In an external trust, ***domain-wide authentication*** allows unrestricted user access by users in the trusted domain to the resources in the trusting domain.

After an external trust is created, all users in the trusted domain will be able to authenticate and access the resources in the trusting domain.

Used in scenarios in which all users must be able to log in to workstations and resources in the trusting domain, domain-wide authentication automatically allows access. Enable or disable domain-wide authentication based on your enterprise requirements:

- Enable domain-wide authentication when all users in the trusted domain need to authenticate against the trusting domain.
- Disable domain-wide authentication when only a select few or a group of users in the trusted domain need to authenticate and access resources in the trusting domain.

Domain-wide authentication is configurable only in an external trust.

Configuring Forest-Wide Authentication

Forest-wide authentication allows unrestricted user authentication and access by users in the trusted forest to the resources in a trusting forest.

After forest trust creation, all users in the trusted forest will be able to authenticate and access the resources in the trusting forest. In a multi-domain forest, all users within each domain in the forest are able to authenticate and access resources in the trusting domain.

Used in scenarios where all users must be able to log in to workstations and resources in the trusting forest, forest-wide authentication automatically allows access to the users. Enable or disable forest-wide authentication based on your enterprise requirements:

- Enable forest-wide authentication when all users in the trusted forest need to authenticate against the trusting forest.
- Disable forest-wide authentication when only a select few or a group of users in the trusted forest need to authenticate and access resources in the trusting forest.

Forest-wide authentication is configurable only in a forest trust.

DISABLE DOMAIN-WIDE OR FOREST-WIDE AUTHENTICATION

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To create a one-way forest trust from ADATUM.LOCAL to CONTOSO.LOCAL, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut, and from the context menu, select Run as Administrator. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain or forest that is part of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, highlight the domain or forest trust you want to modify, and then click the Properties button.
4. Select the Authentication tab and choose Selective Authentication. Click OK. Close all displayed windows when complete.

Configuring SID Filtering

THE BOTTOM LINE

Enabled by default, ***SID filtering*** removes injected SIDs and sIDhistory to allow only the Principle Security Identifier (SID) to be seen by the trusting domain.

SID filtering protects trusting domains from malicious users. Malicious users might attempt to inject SIDs of an elevated user or group in the trusting domain to the sIDHistory of a user in the trusted domain.

When SID filtering is disabled, the malicious user can successfully inject the sIDHistory and gain privileged administrative access to resources in the trusting domain. It is best practice to keep SID filtering enabled unless absolutely necessary.

SID filtering can be disabled in the following scenarios:

- User accounts have been involved in a domain migration. If a domain migration has been done, a user will be given a new principle SID in relation to the domain they have been migrated to while maintaining the old SID in the sIDHistory attribute. If the administrator migrated the previous SIDs, the sIDHistory attribute will be populated with the old SID. The previous SID might have been kept to retain access to network resources in the old domain. This can cause problems because if the old SID is filtered off within a trust, the user will lose access to resources still pointing to the old SID.
- There is complete personal trust between all Domain Admins and Enterprise Admins within both trusts.

DISABLE SID FILTERING FOR AN EXTERNAL TRUST

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To disable SID filtering on ADATUM.LOCAL with its external trust to CONTOSO.LOCAL, perform the following steps:

1. Click Start, right-click the Windows PowerShell shortcut, and from the context menu, select Run as Administrator. If required, log in with a user account that is a member

of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.

2. Run the `netdom` command where *adatum.local* is the Trusting_Domain_Name and *contoso.local* is the Trusted_Domain_Name. Notice external trusts SID filtering uses the "QUARANTINE" switch.

```
netdom trust abldatum.local /Domain:contoso.local /
quarantine:No /userD:[DomainAdminUser] /
passwordD:[password | *]
```

DISABLE SID FILTERING FOR A FOREST TRUST

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To disable the SID filtering on ADATUM.LOCAL with its forest trust to CONTOSO.LOCAL, perform the following steps:

1. Click Start, right-click the Windows PowerShell shortcut, from the context menu, select Run as Administrator. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Run the `netdom` command where *adatum.local* is the Trusting_Domain_Name and *contoso.local* is the Trusted_Domain_Name. Notice forest trust SID filtering uses the "ENABLESIDHISTORY" switch.

```
netdom trust adatum.local /Domain:contoso.local /
enablesidhistory:No /userD:[DomainAdminUser] /
passwordD:[password | *]
```

Configuring Name Suffix Routing

THE BOTTOM LINE Name suffix routing manages how authentication requests are passed to each AD DS forest in a forest trust.

When a forest trust is created, all unique suffixes are routed across the trust by default. This allows users in each forest the ability to authenticate to resources in the trusting forest through the means of a unique name suffix.

Unique name suffixes must be unique to the forest and include the following suffixes:

- User principle name (UPN)
- Service principle name (SPN)
- Domain Name System (DNS) name
- Forest or domain tree name that is not a child to the tree

In a forest trust, it is common and recommended that users authenticate by using a forest unique identifier, such as an e-mail address. Because e-mail addresses are truly unique, this solution allows for a smoother authentication process between two forests.

Name suffixes can be modified or excluded from being routed across a forest trust. By excluding an already routed name suffix, future authentication requests by those unique name suffixes will be disallowed.

By default, after a forest trust is created, any new name suffixes added to the trusted forest are disabled. To enable new name suffixes that have been added after the forest trust creation, enable the name suffix by using the Active Directory Domains and Trusts tool.

CONFIGURE NAME SUFFIX ROUTING

GET READY. Log on to the domain controller in your domain in which you will create the trust. You must log in as a user that is a member of the Domain Admins, Enterprise Admins, or delegated equivalent security groups. To modify name suffix routing for names in the CONTOSO.LOCAL trusted domain, perform the following steps:

1. Click Start, right-click the Active Directory Domains and Trusts shortcut and, from the context menu, select Run as Administrator. If required, log in with a user account that is a member of the Domain Admins, Enterprise Admins, or equivalent security group. This displays the *Active Directory Domains and Trusts* tool.
2. Right-click the domain that is part of the trust and select Properties. This displays the domain name *Properties* window.
3. Click the Trusts tab, highlight the forest trust you want to modify, and then click the Properties button.
4. Select the Name Suffix Routing tab and review the name suffixes listed for the trusted forest.
5. Highlight the name suffix you want to modify and choose Disable or Enable to modify the routing of the name suffix.
6. If you want to exclude names not included in the list, click the Edit button. In the *Edit name suffix* window, click Add. Type the name suffix in the *Add Excluded Name Suffix* window, and click OK to add the selection. Notice that you can also change the routing status of a name suffix and its children. Click OK to save.
7. Click OK on each displayed window to save changes. Close all displayed windows when completed.

Business Case Scenarios

Scenario 15-1: Planning for Trusts

You are the Enterprise Administrator for a high-end graphics company, contosographics.com. The company recently announced that it will purchase another quality graphics company, adatumgraphics.com. You are tasked to plan for and to integrate both forests with one another. As part of the plan, you need to take into consideration the following needs:

- Users will not be allowed to log into workstations in the other forest.
- The sales teams will need to access all files in the following shares: filesrv.contosographics.local\Sales and dfssrv01.adatumgraphics.local\MoneyMaking.
- The graphics teams needs to access all files in the following shares: contgsrv1.contosographics.local\Working_Pubs, contgsrv2.contosographics.local\Completed_Pubs, dfsgrfx01.adatumgraphics.local\InProgress and dfsgrfx02.adatumgraphics.local\Finals.
- The company managers need to access all shares accessible by the Sales and Graphics teams and nothing else.

What will you recommend as the best solution to meet the needs during the acquisition? What other solutions you can think of that might meet the requirements?

Scenario 15-2: Resolving a Bring Your Own Device Dilemma

Your company consists of ten separate forests spread out across the country and have no existing trusts in place. Your team is investigating implementing a remote desktop infrastructure for all employee workstations. As part of the plan, in some cities the workstations will be replaced with thin clients, and in others, employees will be required to bring their own device. All server infrastructure will be housed at the company headquarters datacenter. All users in all cities need to be able to log in to the virtual machines served from the datacenter with their company e-mail address. What problems do you see with the current setup? What should be included in your plan to meet the company's authentication requirements and future growth needs?

16 LESSON

Configuring Sites

Configuring Sites and Subnets

THE BOTTOM LINE

Sites and subnets define the physical design of an Active Directory Domain Services (AD DS) domain. Sites allow clients, authentication, and applications to access domain controllers and services within a physical location before needing to cross a Wide Area Network (WAN) link. Sites also utilize the high speed networks of the local network to quickly replicate data between domain controllers within the site.

With AD DS sites, each site represents a physical location. When a client attempts to authenticate or look for resources within the forest, it will send its request to the closest domain controller. The domain controller utilizes the client's IP address and subnet, for the optimal way to allow authentication. Using AD DS, the domain controller examines the client IP address and subnet, and compares it against the defined sites and subnets to determine its location. If a client's network address and subnet belong in the same site as the domain controllers, it will authenticate the client to domain controllers within the site storing the client site information in the client's registry. If the client belongs to another site, it will store the site information in the client's registry and direct it to ask a domain controller in the remote site for authentication.

If there are no sites defined or if they are defined improperly, the authentication or service request might get sent to another physical site. By crossing over the WAN to find resources and to authenticate against domain controllers in a separate site, increased latency and decreased response time to the client are highly likely across slow connections.

Configuring Sites

It is important to configure sites and subnets within your environment to allow for efficient use of domain resources. A misconfigured site or subnet can lead to slow logon times, latent access of file shares across the WAN, and latent access to business resources.

Sites are representative of the physical AD DS domain topology and contain domain controllers, clients, and services. At forest creation, the default site created is called *Default-First-Site-Name* and contains all domain controllers added to the domain until new sites and subnets are created.

Sites group together domain controllers at the same physical location to allow efficient replication between one another on high speed internal networks before sending any directory changes to remote locations or branch offices.

Sites and subnets allow clients to authenticate to domain controllers in the same site, locally access resources such as Distributed File System (DFS), and to access to site-aware applications such as Microsoft Exchange by contacting the resources within the site before traversing the WAN to find the next closest domain controller or resource.

All domain controllers within a site replicate with one another in a process called ***Intrasite replication***, which is the replication of compressed data that occurs across site links between domain controllers located in different sites.

Intersite replication, through the use of Bridgehead servers, replicates directory partitions from one site's bridgehead server to another site's bridgehead server. Each bridgehead server then replicates the changes internal to its replica domain controllers through Intrasite replication.

Sites are not limited for use with only AD DS. Sites can also be configured for use in Active Directory Lightweight Directory Services (AD LDS) instances.

In a large environment, with multiple branch offices containing users and domain computers, placing a domain controller at the branch office can prevent problems if a WAN link fails. Because sites and subnets affect all domain controller replication and client connectivity, you must have Domain Administrator rights in the forest root domain or in a multi-domain environment, Enterprise Administrator rights in the forest, to perform any forest-affecting changes within the AD DS.

ADD A SITE

GET READY. Log on to a domain controller as a user who is a member of one of the following groups, forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To create a site, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. Right-click the Sites container found within the *Active Directory Sites and Services* tool and select New Site... This displays the *New Object – Site* window.
3. Type in the name of the new site.
4. Select the corresponding site link object from the list.
5. Click OK.
6. Confirm that the new site is now listed in the *Active Directory Sites and Services* tree.
7. Close the *Active Directory Sites and Services* tool.

Configuring Subnets

Subnets are created to group and assign computers within the same network subnet to a site. Subnets can be assigned only to one site and can be IPv4 or IPv6 subnets. At logon, domain controllers assign clients to sites based on their network address and subnet.

When designing an AD DS site topology, make sure all IP ranges used by clients and servers are added to subnets list and assigned to a site for optimized service access and domain controller referencing.

Once assigned to a site, clients and services become "site-aware" to other clients, services, and servers within the same subnet and site. Site-aware clients look for and utilize resources within the same site before looking to other sites for references.

When using private IP address ranges, ensure that they are created and assigned to the correct site. In multi-domain forests, ensure that the Enterprise Administrators, or the Domain Administrators, across the separate domains communicate the use of private IP addresses and subnets, to avoid conflicts. Because subnets can be assigned only to one site, the use of private IP address ranges in multiple domains might become an issue during client logon and service requests are initiated if duplicate private subnets are used in more than one domain.

When clients are unable to assign themselves to a site, the domain controller that authenticates the client at logon logs a NO_CLIENT_SITE entry in `%SystemRoot%\debug\ netlogon.log` and `%SystemRoot%\debug\netlogon.bak`, indicating which IP and hostname cannot find a client site to be a part of. To prevent this from happening, create the subnet of the clients being logged and assign to the correct site.

ADD A SUBNET

GET READY. Log on to a domain controller as a user who is a member of one of the following groups, forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To create a subnet, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. If needed, expand the Sites container.
3. Right-click the Subnets container and select New Subnet... This displays the *New Object – Subnet* window.
4. Using network prefix notation, type in the address prefix within the *Prefix::* text box (for example: 192.168.100.0/24).
5. Select the corresponding site object from the list as displayed in Figure 16-1, and click OK.

Figure 16-1

Creating a new subnet object

6. Confirm that the new subnet is now listed within the *Subnets* container found in the *Active Directory Sites and Services* tree.
7. Close the *Active Directory Sites and Services* tool.

Creating and Configuring Site Links

Site links define the logical replication link between sites to perform Intersite replication, allowing for faster and optimized replication between sites based on configured costs and frequencies. Site links manage the logical flow of replication between physical sites.

Created by default, the DEFAULTIPSITELINK site link object is created at forest creation. When new domains and domain controllers are added to the forest, if new sites links are not manually created, they will all become members of the DEFAULTIPSITELINK site. In large enterprise environments, spanning several physical locations, replication traffic is at the mercy of the WAN links between physical locations. This situation can cause replication issues when there is a mix of reliable and unreliable network paths between sites. Physical infrastructure between sites might differ and have different requirements of when to utilize bandwidth.

To resolve the problem of costly bandwidth and timing restrictions of physical connections, you can implement site links. By creating site links, you can tell AD DS who to replicate with, where to replicate, when to replicate, what path to attempt replication on first, and how often to replicate. This allows the optimization of AD DS replication traffic between sites by using the optimal, least expensive, available route. To modify site links, you must be a member of the Domain Admins group.

Newly created sites should follow a standard naming scheme representing the sites involved within the link or by using another type of descriptor for ease of troubleshooting and recognition throughout the forest. New sites are created using the Active Directory Sites and Subnets tool by expanding *Inter-Site Transports*, right-clicking the *Transport* type, and selecting *New Site Link…*.

SITE LINK BRIDGES

Site link bridging allows transitive linking between all sites in the forest. By default, Bridge All Site Links is enabled, permitting site link bridging between all sites in the forest.

In scenarios in which a Hub-and-Spoke Topology are preferred and a transitive link between two or more sites, but not all, is required, implement a site link bridge to allow transitivity between the required sites.

A ***Hub-and-Spoke Topology*** is created by an Enterprise Administrator disabling the Bridge All Site Links option, and then creating site link bridges between a central "hub" site and each of its remote "spoke" sites (see Figure 16-2). This forces all replication to between the hub-and-spoke bridge site members. Remote sites in a Hub-and-Spoke Topology are not configured to replicate with each other unless a site link bridge is configured. Configuring a Hub-and-Spoke Topology forces all replication to take place through the hub site before replicating back to branch offices. A disadvantage of the Hub-and-Spoke Topology is the inability to directly replicate directory partitions between branch offices. All replication must cross the WAN to replicate with the hub site and then traverse through a WAN connection again to reach the second branch office. This increases the time it takes for the second branch office to receive directory changes.

Figure 16-2

Understanding Hub-and-Spoke Topology

Site link bridges are used when the Bridge All Site Links option is disabled to allow transitive linking between sites not directly connected (see Figure 16-3).

Figure 16-3

Understanding site link bridge integration

CREATE A SITE LINK AND SITE LINK BRIDGE

GET READY. Log on to a domain controller as a user who is a member of one of the following groups: forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To create a site link or site link bridge, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. If needed, expand the Sites container.
3. If needed, expand the Inter-Sites Transports container.
4. Right-click the IP container and select New Site Link... This displays the *New Object—Site Link* window. To create a new site link bridge, select New Site Link... This displays the *New Object—Site Link Bridge* window.
5. Provide the name for the new *Site Link* or *Site Link Bridge*, within the text box.
6. Add at least two sites to the link, by selecting the sites from the *Sites not in this link:* selection box, and clicking the Add button.

7. Click OK.
8. Confirm that the new site link is now listed within the *Sites* > *Inter-Site Transports* > *IP* container found in the *Active Directory Sites and Services* tree.
9. Close the *Active Directory Sites and Services* tool.

DISABLE BRIDGE ALL SITE LINKS

GET READY. Log on to a domain controller as a user who is a member of one of the following groups: forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To disable the Bridge All Site Links option, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. If needed, expand the Sites container listed within the *Active Directory Sites and Services* tool.
3. If needed, expand the Inter-Sites Transports container.
4. Right-click the IP container, and select Properties.
5. Uncheck the Bridge all site links check box.
6. Click OK.
7. Configure each spoke site to connect to the hub site if a Hub-and-Spoke Topology was intended.
8. When completed, close the Active Directory Sites and Services tool.

SITE LINK COSTS

By default, site link costs are configured with a cost value of 100. Site link costs can be configured to allow AD DS to replicate over one link before replicating over another one. Replication always replicates over the lowest cost link between sites.

As an example, think of a hub spoke configuration between four sites. With the hub site as the primary datacenter for the domain and each branch office as a spoke to the hub, each branch office connects to the primary datacenter on a high-speed WAN. With the Bridge All Site Links option off, all replication is replicated to the hub site, and then down to the other spokes, not branch office to branch office. Now, imagine that you have a slow and costly satellite connection between two of the branch offices. Though it is less efficient and expensive to use the satellite link, you plan to use the satellite link as a backup path in the event that the link between the branch office and the primary datacenter fails.

You can configure a new site link between the branch offices to utilize the satellite link as a backup link if the optimal site link between the sites is down. To do so, you create a new site link between the branch offices and assign a higher cost to those links.

When replicating between sites, the total cost of the replication path to the destination is added and assessed. If the total cost of the replication is cheaper by going over one route than over another, the lowest total cost route will perform the replication.

MODIFY SITE LINK COSTS

GET READY. Log on to a domain controller as a user who is a member of one of the following groups: forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To modify site link costs, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.

2. If needed, expand the Sites container.
3. If needed, expand the Inter-Sites Transports container.
4. Select the IP container. Notice the site links listing in the window.
5. From the list of site links, right-click the site link you want to modify and select Properties. This displays the *LinkName Properties* window.
6. Modify the Cost: value to reflect the requirements of the enterprise.
7. Click OK to save the changes.
8. Confirm that the new site link cost is reflected within the site link list.

REPLICATION INTERVAL

The ***replication interval*** defines how often replication across the site link occurs. By default, replication on site links are configured to occur every 180 minutes and can be modified within the site link properties. Replication between sites might need to occur more frequently if there are constant changes to AD DS that need to be seen in branch offices immediately. The replication interval can be configured to allow replication every 15 minutes across site links.

MODIFY THE REPLICATION INTERVAL

GET READY. Log on to a domain controller as a user who is a member of one of the following groups: forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To modify the replication interval, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. If needed, expand the Sites container.
3. If needed, expand the Inter-Sites Transports container.
4. Select the IP container. Notice the site links listing in the window.
5. From the list of site links, right-click the site link you want to modify and select Properties. This displays the *LinkName Properties* window.
6. Modify the Replicate every: value, to reflect the requirements of the enterprise.
7. Click OK to save the changes.
8. Confirm that the new site link replication interval value is reflected within the site link list.
9. Close the *Active Directory Sites and Services* tool.

REPLICATION SCHEDULE

The ***replication schedule*** defines when the replication is allowed to occur. By default, replication is scheduled to occur 24 hours a day, 7 days a week, and can be modified within the site link properties. This ensures replication occurs constantly. In the previous example of using a satellite link for a backup path, imagine that satellite link is three times more costly to replicate traffic across that link during its peak hours, 7AM–6PM, Monday thru Friday. You can configure the site link properties to replicate only across the satellite network between 6PM–7AM Monday thru Friday and all hours of the day Saturday and Sunday.

MODIFY THE REPLICATION SCHEDULE

GET READY. Log on to a domain controller as a user who is a member of one of the following groups: forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To modify the replication schedule, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. If needed, expand the Sites container.
3. If needed, expand the Inter-Sites Transports container.
4. Select the IP container. Notice the site links listing in the window.
5. From the list of site links, right-click the site link you want to modify and select Properties. This displays the *LinkName Properties* window.
6. Click the Change Schedule... button.
7. Using your mouse, click and hold the left mouse button dragging the cursor over the range of time you want to modify, releasing the mouse button after selected.
8. Choose Replication Not Available or Replication Available to remove or add the time range to the replication schedule.
9. Click OK to save the changes.
10. Click OK to close the displayed window.

Managing Site Coverage

Not all environments require a domain controller at each site. In certain scenarios, you might allow sites to be automatically covered by a domain controller in an adjacent site.

AUTOMATIC SITE COVERAGE

Domain controllers in sites can take over for missing domain controllers in remote sites. If a site does not have a domain controller to authenticate clients against, depending on cost, domain controllers in the closest site will automatically register an SRV record in the client site to automatically cover the site for the missing domain controller. This allows clients to be able to contact the closest domain controller to access the resources needed.

The clients in the site that are automatically covered are still traversing the WAN to connect to the domain controller for authentication and resource access.

DISABLE AUTOMATIC SITE COVERAGE

Unfortunately, Windows Server 2003 domain controllers perform automatic site coverage in sites with Read-only Domain Controllers (RODCs) because they are unable to recognize that an RODC might be currently covering a site. If the closest site to an RODC contains only Windows Server 2003 domain controllers, there are a few options that are recommended.

- Download the RODC compatibility pack for the Windows Server 2003 domain controllers.
- Upgrade the domain controllers in the next closest site to at least Windows Server 2008.
- Modify the site costs to a site running only Windows Server 2008 domain controllers.
- Disable automatic site coverage on the Windows Server 2003 domain controllers, through the registry or Group Policy.

DISABLE AUTOMATIC SITE COVERAGE ON WINDOWS SERVER 2003

WARNING Always use caution when making changes in the registry and back up the registry before changes are made. Always fully understand the steps you perform before the steps are acted upon.

GET READY. Log on to a Windows Server 2003 domain controller as a user that is a member of the forest root domain Domain Admins or Enterprise Admins group of the Windows Server 2003 domain controller that will be modified. To disable automatic site coverage on a Windows Server 2003 domain controller, perform the following steps.

1. From the Windows Server 2003 domain controller, click Start, select Run, type in REGEDIT, and click OK.
2. Navigate to HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters.
3. Right-click the Parameters key, hover over New, and select DWORD Value.
4. Name the new entry AutoSiteCoverage and press Enter.
5. Double-click AutoSiteCoverage to *Edit the DWORD Value*.
6. To disable AutoSiteCoverage, modify the *Value data* to 0. To enable AutoSiteCoverage, modify the *Value data* to 1.
7. Close the *Registry Editor* window when complete.

Managing Registration of SRV Records

Domain controller SRV records are a critical part of domain controller and client communications. All domain controllers register an SRV record for their clients to find them.

After a member server is promoted to become a domain controller, it registers itself in DNS for advertisement so clients know how to find it. As you learned previously, clients ask the DNS for a list of all domain controllers and a list of domain controllers within its site for efficient authentication to occur. In DNS, the domain controller registers SRV records for the client to find. During this process, if AD DS recognizes that there are no domain controllers in another site, it will allow a domain controller to register its SRV records in the site, performing Automatic Site Coverage. During SRV registration, the _kerberos and _ldap SRV records are created and advertised at the following locations in the domain's zone: _msdcs/dc/_Sites/Sitename/_tcp and _msdcs/dc/_tcp.

NETLOGON SERVICE

The NETLOGON service running on a domain controller is the service that requests and issues that the registration request of the SRV records to DNS. In versions previous to Windows Server 2008, you were required to run *netdiag/fix* to re-register SRV records on a domain controller. On servers running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the SRV records and _msdcs zone records can be reregistered by stopping then starting the NETLOGON service on the domain controller. A reboot will also perform a reregistration of SRV records, but will cause unneeded downtime.

NETLOGON.DNS

When a domain controller registers its SRV records in DNS, it creates a copy of those records and stores them locally in the NETLOGON.DNS file. The NETLOGON.DNS file located within the `%systemroot%\System32\config\` can be viewed in Notepad.exe. The NETLOGON.DNS provides critical information when troubleshooting SRV record registration on a domain controller. If removed or renamed, the NETLOGON.DNS will be restored with existing records for the DNS server at the next reboot or next NETLOGON service stop and start command on the domain controller.

Moving Domain Controllers between Sites

Moving a domain controller to a different site is a simple task once your environment is ready for the change to occur.

During domain controller promotion, you are prompted to assign the domain controller to a site. If you do not choose the site for the domain controller to be added to during promotion, it will assign itself to a site based on the IP address it has at the time of promotion. If it is one of the first domain controllers added to a forest, the domain controllers will be placed into the Default-First-Site-Name site until the site, subnet, and site link topology are in place. Once the site topology is in place, the domain controllers can be moved to the appropriate sites and replicate properly with one another. The Default-First-Site-Name site can be renamed to match the naming standard for its current location or it can be removed if it is not part of the new topology.

Depending on the roles installed on a domain controller that will be moved to a different site, you need to do some planning and prepare to make some network adapter, DNS server, and environment changes.

PREPARING THE DOMAIN CONTROLLER, DNS, AND ENVIRONMENT

Before moving the domain controller to a new site, review the following steps:

1. Assign the new IP, subnet, gateway, preferred DNS, alternate DNS, and WINS (if still in use) addresses to the domain controller. After completing this task, verify that all host (A), host (AAAA), and name server (NS) records have updated automatically in DNS.
2. If the server is or will be a DNS server, modify the client and server environment to match the upcoming change.
3. Update any DNS delegations the domain controller is a part of by updating, from the parent domain, the Name Servers tab of the delegated zone.
4. If the server is configured to be a forwarder for any other DNS server, modify the Forwarders tab on the DNS server that is forwarding the queries to the domain controller's new IP address.
5. Verify sites and subnets are configured correctly for the new site. The new site needs to contain the IP range and subnet of the domain controller's new IP address.
6. If the domain controller had previously been manually configured to be a preferred bridgehead server, remove the manual configuration from the domain controller and any others before moving it to the new site. It is best practice to allow AD DS to dynamically assign bridgehead servers. If you choose to not follow best practice, ensure a bridgehead server has been assigned or still exists in each site.
7. Move the domain controller to the new site.
8. Verify that the domain controller SRV records have been registered to reflect the new site.

MOVE A DOMAIN CONTROLLER TO A NEW SITE

GET READY. Log on to a domain controller as a user who is a member of one of the following groups: forest root domain Domain Admins, Enterprise Admins, or delegated equivalent security group. To move a domain controller to a new site, perform the following steps:

1. Click Start, and click the Active Directory Sites and Services shortcut. This displays the *Active Directory Sites and Services* tool.
2. If needed, expand the Sites container.

3. Expand the site name where the server is located.
4. Expand Servers.
5. Right-click the server object that will be moved to the new site.
6. Select Move....
7. Choose the site name that will contain the server.
8. Click OK.
9. Expand the site that the server has just been moved to and confirm that the server has moved.
10. Expand the server object, and verify that the *NTDS Settings* object exists.
11. Close the *Active Directory Sites and Services* tool.

Business Case Scenarios

Scenario 16-1: Configuring Replication between New Sites

You are the Enterprise Administrator for a new worldwide company headquartered in South Dakota. You currently have one site link, DEFAULTIPSITELINK, in AD DS. Over the past month, three new offices have opened up: one in Montana, one in New Zealand, and the last in Spain. Each new site has three domain controllers. Replication between sites is not happening efficiently and when your support teams attempt to connect to Active Directory Users and Computers, they are rarely connecting to their local domain controller. What steps must you take to resolve the support team's issues?

Scenario 16-2: Planning for Private IP Addressing

You are the Enterprise Administrator for a large forest with 20 domains. A Network administrator for one of the domains has recently contacted you with a list of private IP addresses he would like added to the site. When you connect to AD DS, you notice those IPs already exist and are tied to an entirely separate site and you cannot add that range to the requested site. What must be done to approach this situation?

17 LESSON

Managing Active Directory and SYSVOL Replication

Managing Active Directory Replication

THE BOTTOM LINE

Active Directory replication is a critical piece of every Active Directory Domain Services (AD DS) environment. By replicating all naming contexts or directory partitions of AD DS, all domain controllers throughout the enterprise keep one another up-to-date with all changes, ranging from schema updates to modifying items as simple group membership. Having accurate and up-to-date directory partitions allows enterprise operations to run smoothly.

AD DS replication occurs between two or more domain controllers, a source domain controller, and a replica domain controller. The replication process does the following:

- Replicates new changes/updates
- Replicates updates of directory objects
- Ensures all directory updates are transferred to a replica partner
- Keeps all directory partitions up to date
- Keeps all domain controllers synchronized
- Replicates contents of the SYSVOL folder

Through the replication process, the domain controllers keep each other informed about changes happening with objects and partitions connected to the domain controller. Put simply, a change is made on a domain controller and is automatically replicated to a replica domain controller.

Replication occurs between domain controllers within a site, intrasite replication, or between domain controllers in separate sites, intersite replication. Each process ensures correct information is relayed to replica domain controllers as fast and as efficiently as possible.

Controlling Active Directory Replication

As an administrator of an enterprise, there will be instances where replication needs to happen at your discretion (for example, when troubleshooting connectivity between domain controllers or forcing replication of partitions and/or objects between multiple domain controllers before normal replication occurs).

Through the use of REPADMIN and the Active Directory Sites and Services tool, you can control when replication happens, and whether you need it to happen within a site or across the enterprise.

USING THE REPADMIN COMMAND TO CONTROL ACTIVE DIRECTORY REPLICATION

From a command prompt window on a domain controller, you can control replication between domain controllers by using REPADMIN.exe. Before running REPADMIN.EXE across a multisite or multidomain environment, verify you have the proper access to each subdomain, domain tree, and replication partners that will participate in the replication process. Failure to have the required privileges prevents you from forcing replication across the enterprise.

USING THE ACTIVE DIRECTORY SITES AND SERVICES TOOL TO CONTROL ACTIVE DIRECTORY REPLICATION

By using the AD DS tool as a domain administrator or enterprise administrator, you are able to force replication between two domain controllers. Simply expand the site containing the domain controllers, expand the domain controller, select *NTDS Settings*, and right-click on the domain controller you with to replicate to and select *Replicate Now*.

You can also use the AD DS tool to check the replication topology between domain controllers in a site. This can be done by expanding the Site and Domain Controller objects, right-clicking on *NTDS Settings,* hovering over *All Tasks,* and selecting *Check Replication Topology*. This performs the same check that happens when issuing the REPADMIN /KCC command from command prompt.

MANAGE ACTIVE DIRECTORY REPLICATION USING REPADMIN

GET READY. To force replication of all directory partitions, push the synchronization throughout the enterprise, and return domain controller names as Distinguished Names using one REPADMIN command, perform the following steps:

1. From the lower left corner of the Windows Server 2012 R2 taskbar, right-click Start and select Command Prompt. The *Administrator: Command Prompt* window appears.
2. From the *Administrator: Command Prompt* window, enter the `REPADMIN /SyncAll /APed` command.
3. View the results and search for errors. If errors exist, take action to resolve the errors.
4. Continue to run `REPADMIN /SyncAll /APed` until no errors exist.
5. Close the *Administrator: Command Prompt* window.

Configuring Read-Only Domain Controllers

Read-only domain controllers (RODCs) are used in environments where there is a need for a domain controller in a branch office that does not have a secured physical environment. They are also used where there is a risk of theft, or even rarely, where there is an application that requires installation on a domain controller that users must log in to at the terminal or with terminal services.

When planning for a new branch office or remote site, take into consideration the use of an RODC as a form of security if a secure datacenter is not available. Although placing an RODC in a site that contains writable Windows Server 2008 domain controllers provides limited security benefits, it can be used for those business applications requiring access to a domain controller and prevents changes from being made to the overall directory. RODCs should be used only for branch office security considerations, unless there are absolute requirements within an environment.

CONFIGURING REPLICATION TO A READ-ONLY DOMAIN CONTROLLER

As the name "read-only domain controller" implies, its involvement with AD DS is truly read-only. ***Unidirectional replication*** means replication occurs in only one direction, from a writeable domain controller to the read-only domain controller. Read-only domain controllers can only pull the domain partition from a writable Windows Server 2008 or higher domain controller; however, the application and global catalog partitions can be pulled from a domain controller running Windows Server 2003 or higher. Other replica domain controllers within the domain or site are unable to use an RODC as a source domain controller.

In order for an RODC to act as a replica server, there must be a writeable domain controller within the same domain as the RODC. In addition, the writable domain controller in the next closest site must be running Windows Server 2008 or higher. If the next closest site contains only a Windows Server 2003 server, the RODC will traverse site link bridges to reach the closest, writable, Windows Server 2008 domain controller. If the Bridge All Site Links option is disabled and the hub site contains only Windows Server 2003 domain controllers, a Site Link Bridge must be created to allow the RODC to connect to a writable Windows Server 2008 domain controller.

This need to connect to a writable Windows Server 2008 domain controller is required because the Password Replication Policy (PRP) applied to the RODC can be configured and enforced only from a writable Windows Server 2008 domain controller.

RODCs replicate AD DS partitions and Distributed File System Replication (DFSR) of the SYSVOL folder unidirectional. Other DFSR shares, not part of the AD DS process, located on the RODC replicate bidirectional with its configured replication partners.

Implementing ***Filtered Attribute Sets*** allows administrators the ability to mark attributes as "Confidential" when being replicated to RODCs. Attributes marked as confidential and that are part of the Filtered Attribute Set will not be replicated to an RODC. This provides additional security if there are attributes configured in the schema that contain information that can cause a security breach if a domain controller is stolen or compromised (for example, passwords, Social Security numbers, and Encryption Keys).

If there are plans to implement a Filtered Attribute Set, you must raise the Forest Functional Level to at least Windows Server 2008. Although configuring the Filtered Attribute Set does not require a Forest Functional Level of Windows Server 2008, it is highly recommended, because malicious users can take advantage of attribute replication from Windows Server 2003 domain controllers. Windows Server 2003 domain controllers permit requested changes to be replicated, whether configured as confidential or not.

To configure the Filtered Attribute Set, the configuration of the attribute must be done on a Windows Server 2008, Windows Server 2012, or Windows Server 2012 R2 domain controller that holds the Schema Master FSMO role. The Filtered Attribute Set and Confidential options are configured by modifying the attribute that you intend to not be replicated. From ADSI Edit, connect to the schema, and within the properties of the confidential attribute, modify its *searchFlags* attribute. To turn on the Read-Only Filtered Attribute Set, configure the 10th bit to be 0x200, and then turn on the Confidential bit by configuring the 7th bit to 0x080. Or simply add 640 to the existing decimal configuration of the attributes searchFlags attribute.

CONFIGURE FILTERED ATTRIBUTE SETS

GET READY. To configure Filtered Attribute Sets, perform the following steps:

1. Click Start and open ADSI Edit.
2. At the top of *ADSI Edit* window, click Action and select Connect to... The *Connection Settings* window opens.
3. From the *Select a well-known Naming Context:* selection, select Schema. From the *Select or type a domain or server:* selection, choose the domain controller running the Schema Master role, and click OK.
4. From the *ADSI Edit* window, expand Schema, and select the CN=SCHEMA, CN=Configuration,DC=YourDomain,DC=YourDomainSuffix container.
5. From the list of attributes, find and double-click on CN=Employee-ID. The *CN=Employee-ID Properties* window appears.
6. Scroll down, find, and double-click on searchFlags. The *Integer Attribute Editor* window appears.
7. Record its current value, add 640 to the value, enter the sum of the values in the *Value* text box, and click OK.
8. The new searchFlags value from the *CN=Employee-ID Properties* window should now read and/or contain the following value *0x280 = (CONFIDENTIAL|RODC_FILTERED)* as shown in Figure 17-1. The Employee-ID value is no longer replicated to the RODC.

Figure 17-1

Modifying the Confidential RODC filtered attribute

9. Click Cancel to discard your changes or click OK to save your changes. Close the *CN=Employee-ID Properties* window.
10. Close the *ADSI Edit* window.

CONFIGURING PASSWORD REPLICATION POLICY FOR RODCS

To provide authentication of users and computers at a branch office that utilizes an RODC, the RODC must know and store the password of that user or computer. Otherwise, users and computers will traverse the WAN to authenticate to the next closest writable domain controller causing unneeded latency and WAN usage during the logon process. Because RODCs run the risk of theft or compromise at remote locations, not all users within a domain will need their credentials stored at the remote location. The same goes for privileged users, including domain administrators and enterprise administrators. If an RODC is stolen and compromised, all user accounts that have authenticated against the RODC, and have had their passwords cached, will need their passwords changed because their account has been compromised and the business is at risk. This is why user accounts, such as domain administrators and enterprise administrators, should never be cached and remotely access through terminal services or authenticate against an RODC at the site. To give a user or group elevated permissions to the RODC, configure the user or group under the Managed By tab of the RODCs computer account.

As a safeguard, to prevent unwanted users from logging into or authenticating against an RODC, all users except for those that are members of the Allowed RODC Password Replication Group will be allowed to authenticate to the RODC. The Allowed RODC Password Replication Group, by default, allows members to authenticate to the RODC. Keep in mind, the user or group that you configured under the Managed By tab are not, by default, allowed to log on or authenticate against the RODC unless they are members of the Allowed RODC Password Replication Group. As an additional option, to prevent users from authenticating against the RODC, add the users or user group to the Denied RODC Password Replication Group.

By modifying the ***Password Replication Policy (PRP)*** of the RODC within the Active Directory Users and Computers tool, you can *allow* or *deny* passwords to be cached for users.

When adding users to the Allowed RODC Password Replication Group, do not forget that computers have passwords as well. You must also add the users' computers that will be at the remote site to the Allowed RODC Password Replication Group. This eliminates authentication problems if the WAN link fails and computers attempt to authenticate. This concept of the PRP allows credentials to be cached on the RODC.

Password Prepopulation is the ability for a domain controller to store user credentials before a user logs into the RODC. Password Prepopulation allows user credentials to be pushed to the RODC before those users attempt log on to the RODC. Benefits of Password Prepopulation include the following:

- Initial logons are faster, since the authentication process won't have to traverse the WAN to the closest, writable, Windows 2008 or later, domain controller.
- The ability to prepare an RODC before shipment to the remote site if no WAN link is available when the RODC is brought online.

In order for Password Prepopulation to cache passwords, the users and computers must have their accounts configured to have their passwords replicated, or have been added to the Allowed RODC Password Replication Group.

READ-ONLY DOMAIN CONTROLLER SECURITY

In the event of an RODC theft or compromise, the user passwords need to be changed immediately at the hub site. To meet this immediate need, the fastest way to force all users, who have authenticated or who have their credentials cached on that RODC, simply delete the RODC object from the Active Directory Users and Computers tool. When you initiate

the deletion of the RODC, you are prompted and given the option to reset all users passwords, reset all computer passwords, and export a list of compromised accounts.

Upon deletion, all passwords that have been cached will be reset to a random password. Users that had their user account passwords cached need to reset their password or contact the helpdesk to reset their passwords. All computers that have had their passwords reset will need to be rejoined to the domain.

CONFIGURE PASSWORD REPLICATION POLICIES ON AN RODC

GET READY. To create a staged RODC computer account and configure generic user and computer account credentials for password replication, perform the following steps. Once completed, you remove the staged read-only domain computer account and force all users with passwords replicated to be reset.

1. Click Start, and click Active Directory Users and Computers to open the *Active Directory Users and Computers* tool.
2. From the *Computers* container, precreate a generic computer account.
3. From the *Users* container, precreate a Generic User account.
4. Right-click on the Domain Controllers OU and select Pre-create Read-only Domain Controller Account. The *Active Directory Domain Services Installation Wizard* opens. Click Next.
5. On the *Network Credentials* window, authenticate with a domain administrator user account, and click Next.
6. On the *Specify the Computer Name* window, enter the computer name for the Staged RODC, and click Next.
7. On the *Select a Site* window, select a site for the new domain controller, and click Next.
8. On the *Additional Domain Controller Options* window, verify that DNS Server and Global catalog are selected, and click Next.
9. On the *Delegation of RODC Installation and Administration* window, click Next. You will not select a user or group in this exercise.
10. On the *Summary* window, review the selections and click Next.
11. On the *Completing the Active Directory Domain Services Installation Wizard* window, click Finish.
12. From the *Active Directory Users and Computers* tool, select the Domain Controllers OU.
13. Within the *Domain Controllers* OU, double-click on the RODCServerName you just created. The *RODCServerName Properties* window appears.
14. From the *RODCServerName Properties* window, select the Password Replication Policy tab. Notice the Allowed and Denied users, computers, and groups listed.
15. From the list, double-click Allowed RODC Password Replication Group. The *Allowed RODC Password Replication Group Properties* window appears.
16. Click on the Members tab. Within the *Members* tab, click Add. The *Select Users, Contacts Computers, Service Accounts* window appears.
17. Click Object Types…. In the *Object Types* window, check the Computers check box and click OK. You are returned to the *Select Users, Contacts Computers, Service Accounts* window.
18. Enter the object names of the precreated computer and user accounts you created in Steps 2 and 3. Click Check Names verifying the names resolve correctly, and click OK.
19. Verify that the user and computer are listed in the *Members* tab, and click OK.

20. From the *RODCServerName properties* window, click Advanced. The *Advanced Password Replication Policy for RODCServerName* window appears.
21. From the *Advanced Password Replication Policy for RODCServerName* window, click the Prepopulate Passwords... button. The *Select Users and Computers* window appears.
22. Enter the object names of the precreated computer and user accounts you created in Steps 2 and 3. Click Check Names verifying the names resolve correctly, and click OK. The *Prepopulate Passwords* window appears. Verify that you want to send the current account passwords to the RODC, and click Yes.
23. Because you cannot prepopulate account credentials on a Pre-staged RODC, you receive an error indicating you are unable to reach the RODC. In an environment with a live RODC, it succeeds and the accounts are listed within the *Policy Usage* tab of the *Advanced Password Replication Policy for RODCServerName* window. Click OK to close the error. This returns you to the *Advanced Password Replication Policy for RODCServerName* window. Click Close, to close the open window.
24. At the *RODCServerName Properties* window, click OK.
25. Within the *Domain Controllers* OU, right-click on the precreated RODC RODCServerName, and select Delete. You are prompted to verify you want to delete the Computer account. Click Yes, and the *Deleting Domain Controller* window appears.
26. Review the options available when deleting the RODC, and provide a path and file name in the Location: text box. Click Delete. The *Delete Domain Controller* window appears warning you that you are about to reset all user account passwords that have been cached and all metadata for the domain controller will be removed. Click OK. If the RODC is a global catalog, you will be asked again if you are sure you want to delete it. Click Yes.
27. The pre-staged RODC has been removed, and any user and computer account passwords that have been cached on the domain controller have been reset to random values.
28. Once complete, close the *Active Directory Users and Computers* tool.

Monitoring Replication

Monitoring replication allows you to troubleshoot and narrow down problems between domain controllers when replication is not working properly. Monitoring replication in your enterprise allows you to ensure all domains within the enterprise are receiving updates to all directory partitions, keeping users and directory data fully accessible.

MONITORING REPLICATION WITH REPADMIN

By using REPADMIN.EXE, you can monitor your environment for failures and take action to put a resolution in place. Use the following commands to monitor replication:

- **`REPADMIN.EXE /ReplSummary`:** This command also can be run as `REPADMIN /ReplSum`. It examines all inbound and outbound replication between domain controllers and returns a replication summary of the forest or specified domain controllers. After contacting and inventorying the domain controllers, it will then populate with a summary of failures and deltas (new changes) returned during its examination.
- **`REPADMIN.EXE /ShowRepl`:** Categorized by directory partitions, this command returns the replication status of all inbound connections from source domain controllers to the domain controller it is run from.
- **`REPADMIN.EXE /ShowRepl /RepsTo`:** Displays a summary of all outbound replication connections to replica domain controllers using the domain controller the command is run from as the source domain controller.

- **`REPADMIN.EXE /Queue:`** Displays the current inbound connections that are queued for replication. To view the active inbound replication queue of a domain controller from that domain controller, run `REPADMIN /Queue DCName`.
- **`REPADMIN.EXE /FailCache:`** Displays link and connection failure attempts found by the KCC.

MONITORING REPLICATION WITH ACTIVE DIRECTORY REPLICATION STATUS TOOL (ADREPLSTATUS)

Released by Microsoft in 2012, the Active Directory Replication Status Tool (ADREPLSTATUS) allows for much simpler and straightforward monitoring and troubleshooting, taking the results returned and placing them into an easy-to-use application. Using existing tools and commands such as REPADMIN.EXE, the Active Directory Replication Status Tool (ADREPLSTATUS) identifies, prioritizes, and assists in resolving replication errors on specified domain controllers, a domain, or the entire forest. The Active Directory Replication Status Tool auto-discovers domain controllers, gathers replication summaries, returns the results in a filterable, sortable list, and links directly to TechNet, providing direct access and faster turnaround time to resolve replication errors.

Compatible with operating systems including Server 2003/XP and later, you can download the latest version of the Active Directory Replication Status Tool (ADREPLSTATUS) from the Microsoft Download Center.

Before installation, ensure you have installed the required versions of .NET Framework the Active Directory Replication Status Tool (ADREPLSTATUS) might require (.NET Framework 3.5.1 and .NET Framework 4.0).

MONITOR ACTIVE DIRECTORY REPLICATION USING THE ACTIVE DIRECTORY REPLICATION STATUS TOOL (ADREPLSTATUS)

GET READY. To use the Active Directory Replication Status Tool, perform the following steps:

1. If not already installed, download and install the .NET Framework versions required for your operating system.
2. Download and install the Active Directory Replication Status Tool from the *Microsoft Download Center*.
3. On the Desktop of the client the tool is installed on, double-click AD Replication Status Tool.
4. Examine the contents of the *Home* tab and the *Configuration/Scope Settings*.
5. Select Forest from the *Configuration/Scope Settings,* and click Refresh Replication Status.
6. Once completed, if not already displayed, click the Replication Status Viewer tab and review the results.
7. After you review the *Replication Status Viewer* tab, select the Replication Error Guide tab and examine the *Error Code, Message,* and *TechNet Article Link* columns.
8. If errors are shown, click the Error Code listed in the *Replication Error Guide*.
9. Follow the direction provided by the displayed TechNet Article, and make the required changes.
10. After changes are made, run Refresh Replication Status from the *AD Replication Status Tool*.

11. Continue troubleshooting and resolving errors until there are no longer errors reported.
12. Close the *AD Replication Status Tool* when completed.

Upgrading SYSVOL Replication to Distributed File System Replication (DFSR)

Many environments started off as an Active Directory environment running Windows Server 2003 or earlier, prior to the addition of Windows Server 2008, Windows Server 2012, and Windows Server 2012 R2. The replication process of recently upgraded domain's SYSVOL folders might still be configured to use the File Replication Services (FRS). The SYSVOL folder on each domain controller contains a copy of logon scripts and Group Policies, and it is a repository for public access files used by domain controllers.

If you recently upgraded your domain servers to Windows Server 2012 R2, it will be beneficial to migrate your SYSVOL folder replication from FRS to DFSR to take advantage of multimaster replication, scheduling, easier administration, and all other benefits of Distributed File System Replication concepts.

With Windows Server 2012 R2, upgrading to DFSR provides more reliable and easier to support replication solutions. It also provides improved integration with environments that contain RODCs.

UNDERSTANDING THE FRS TO DFSR MIGRATION PROCESS

To upgrade from FRS to DFSR, the Domain Functional Level must be Windows Server 2008 or higher. This means that all domain controllers in the domain must be at least Windows Server 2008 or higher. If there are existing Windows Server 2003 domain controllers in the environment, they will need to be upgraded or removed in accordance with best practices to allow the Domain Functional Level to be raised. So plan and prepare accordingly before the migration.

GLOBAL STATES

There are four Global States of an FRS to DFSR upgrade. Each one allows all domain controllers to balance and prepare for the next state.

- **Start (State 0):** Live AD DS SYSVOL replication between domain controllers is performed using FRS. DFSR is not being performed. FRS replication occurs with the SYSVOL folder.
- **Prepared (State 1):** Live AD DS SYSVOL replication between domain controllers is performed using FRS. A separate behind-the-scenes SYSVOL replication using DFSR is performed on the domain controllers in parallel with the live replication. FRS replication occurs with the SYSVOL folder. DSFR occurs with the SYSVOL_DFSR folder.
- **Redirected (State 2):** Live AD DS SYSVOL replication between domain controllers is performed using DFSR. A separate behind-the-scenes SYSVOL replication using FRS is performed on the domain controllers in parallel with the live replication. DFSR occurs with the SYSVOL_DFSR folder. FRS replication occurs with the SYSVOL folder.
- **Eliminated (State 3):** All Live AD DS SYSVOL replication between domain controllers is performed using DFSR. FRS SYSVOL replication is removed, including the SYSVOL folder and its contents, if it was not open during the elimination operation. DFSR occurs with the SYSVOL_DFSR folder.

WARNING

You must understand the migration states and what replication types, FRS or DFSR, are replicating at each state of the migration. Thoroughly test and verify that each state is operating as designed throughout the migration process. Having a full understanding of the process and what steps are being performed reduces the risk of errors and your ability to rollback. You must also perform the action on each state in order. Do not attempt to skip any states. Doing so might leave your environment in a failed state. Practice and test the migration in a lab environment before performing the full migration in a production environment.

PREPARING THE DOMAIN FOR MIGRATION

Before migrating FRS to DFSR, you must plan and understand the process from beginning to end. Follow the steps below to prepare for the migration.

1. Before beginning your migration, download and understand the *SYSVOL Replication Migration Guide: FRS to DFS Replication Guide* from the Microsoft Download Center.
2. Upgrade and/or remove, by using best practices, all domain controllers running Windows Server 2003. Your domain must have only domain controllers running Windows Server 2008, Windows Server 2012, and/or Windows Server 2012 R2.
3. Ensure all domain controllers are online and accessible with one another.
4. Raise the Domain Functional Level to Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
5. Verify that the replication is working as designed. Download the *Ultrasound Monitoring and Troubleshooting Tool for File Replication Services* from the Microsoft Download Center to verify the health of the current FRS environment.
6. Take any action to resolve replication problems reported by Ultrasound that might exist. If replication problems did exist and have since been resolved, allow replication to fully complete, ensuring domain controllers have the same data within their SYSVOL folders.
7. Back up the SYSVOL folder.
8. Verify on the PDC emulator that the DFSR service is running and Start Type is set to *Automatic*.
9. If the SYSVOL folder is open on any domain controller, close the window. Failure to do so locks the SYSVOL folder as in use, and it will not be deleted during the Eliminated state.
10. Run the migration process from the domain controller that is operating the PDC emulator FSMO role.

Once the migration process is complete and all domain controllers are upgraded and are using DFSR, you can use the `DFSRDIAG` command from an elevated command prompt to troubleshoot and diagnose problems.

UPGRADE SYSVOL REPLICATION TO DFSR

GET READY. To migrate SYSVOL from FSR to DFSR, perform the following steps:

1. Download, review, and fully understand the *SYSVOL Replication Migration Guide: FRS to DFS Replication Guide*.
2. Verify that your domain meets all prerequisites and replication is working. If open on any domain controllers, close all windows displaying *SYSVOL* or *NETLOGON*.
3. Log on to the domain controller that holds the PDC emulator role.

4. From the lower left corner of the *Windows Server 2012 R2* taskbar, right-click the Start menu and select Command Prompt. The *Administrator: Command Prompt* window appears.
5. Migrate all domain controllers to the Prepared state by issuing the following command:

   ```
   dfsrmig /SetGlobalState 1
   ```

6. Verify that all domain controllers have migrated successfully to the Global state (Prepared), by issuing the following command:

   ```
   dfsrmig /GetMigrationState
   ```

7. Once all domain controllers are in the Prepared state, migrate all domain controllers to the Redirected state by issuing the following command:

   ```
   dfsrmig /SetGlobalState 2
   ```

8. Verify all domain controllers have migrated successfully to the Global state (Redirected), by issuing the following command:

   ```
   dfsrmig /GetMigrationState
   ```

9. Verify replication is working properly by running the following command:

   ```
   REPADMIN /ReplSum
   ```

10. Back up the system state of all domain controllers.
11. Once you have verified all domain controllers are in the Redirected state and replication is working between all domain controllers, migrate all domain controllers to the Eliminated state by issuing the following command. This is *not* reversible and might take some time to complete:

    ```
    dfsrmig /SetGlobalState 3
    ```

12. Verify all domain controllers have migrated successfully to the Global state (Eliminated), by issuing the following command:

    ```
    dfsrmig /GetMigrationState
    ```

13. Verify the SYSVOL folder no longer exists.
14. Verify the current DFSR Global state is Eliminated and has succeeded, by issuing the following command:

    ```
    dfsrmig /GetGlobalState
    ```

15. Verify that the SYSVOL and NETLOGON shares continue to exist on all domain controllers and point to their corresponding folder located within *C:\Windows\SYSVOL_DFSR\sysvol* by logging into each domain controller and running the following command from *Command Prompt:*

    ```
    net share
    ```

16. Navigate to the *C:\Windows* directory and verify that the *SYSVOL* directory no longer exists.
17. If you are no longer using FRS on your domain controllers, it might be uninstalled.
18. When the installation is complete, click Close.

Business Case Scenarios

Scenario 17-1: Handling a Stolen Remote Site

You are the enterprise administrator for a multidomain, multisite forest. A remote site that held 30 desktops and 2 RODCs has been a victim of theft. All computers and servers have been stolen from the site. You have been notified within hours of the theft and are asked to reset all user account passwords, reset all computer accounts, and provide a list of all user accounts that have had their passwords potentially compromised. What steps must you take to perform the requested actions and to generate a report?

Scenario 17-2: Upgrading SYSVOL to DFSR

You are a domain administrator for a single forest, single domain. Your enterprise administrator has tasked you with planning and preparing the domain for an upgrade to DFSR for SYSVOL replication. Your environment contains two Windows Server 2003 domain controllers and two Windows Server 2012 R2 domain controllers. What steps must you take to prepare the domain for the upgrade?

18 LESSON

Implementing Active Directory Federation Services

Understanding Active Directory Federation Services

THE BOTTOM LINE

Active Directory Federation Services (AD FS) role allows administrators to configure ***Single Sign-On (SSO)*** for web-based applications across a single organization or multiple organizations without requiring users to remember multiple usernames and passwords. This enables you to configure Internet-facing business-to-business (B2B) applications between organizations. For example, a user from contoso.com can use contoso.com credentials to access a web-based application that is hosted by adatum.com.

Traditionally, if users from one organization/domain need to access a website provided by another organization/domain, you can do it one of two ways:

- For the web application, depending on the web application, create web or domain accounts for the user and have the user log in with the second account. Unfortunately, this does not give a single sign-on solution.
- Create a virtual private network (VPN) between the two organizations and establish a trust relationship between the two Active Directory domains. Although this gives a single sign-on solution, it is difficult to set up and maintain.

AD FS-enabled applications are claims based, which allows a much more scalable authentication model for Internet-facing applications. Therefore, AD FS is an identity access solution that allows any browser-based clients to access a website with a single login to one or more protected Internet-facing applications, even when the user accounts and applications are on different networks and exist within different organizations via a federated trust relationship.

An AD FS configuration consists of two types of organizations:

- ***Resource organizations:*** Organizations that own the resources or data that are accessible from the AD FS-enabled application, similar to a trusting domain in a traditional Windows trust relationship.
- ***Account organizations:*** Organizations that contain the user accounts that access the resources controlled by resource organizations.

Federation can be used within a single organization. Therefore, the single organization is the resource organization and the account organization.

Of course, to establish an identity federation partnership, both partners agree to create a ***federated trust relationship***. Each partner defines what resources are accessible to the other organization, and how access to the resources is enabled. User identities and their associated credentials are stored, owned, and managed by the organization where the user is located.

Claims based access control uses a trusted identity provider to provide authentication. The trusted identity provider issues a token to the user, which is then presented to the application or service as proof of identity. In other words, with claims-based authentication, users can authenticate to the Active

Directory that is located within their organization, and be granted a claim based on that authentication. The claim is then presented to an application that is running in a different organization.

The organization that accepts the claim and has the application the user is trying to access will require key information in the claim (for example, an e-mail address or User Principal Name (UPN) to identify the user, and group membership to specify the access allowed within the application by the user).

To keep the claims secure, all communications occur over HTTPS. Of course, both organizations need to agree on the format for exchanging claims. To simplify this process, a set of specifications identified as web services have been identified, which can be used when implementing AD FS.

Web services are based on Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), and Universal Discovery Description and Integration (UDDI). It also uses Security Assertion Markup Language (SAML), which is an XML-based standard for exchanging claims between an identity provider and a service or application provider. The communication between federation servers is based around an XML document that stores the X.509 certificate for token-signing, and the SAML 1.1 or 2.0 token.

In the simplest scenario, an organization may deploy a federation server to be used with its own web applications. If the web application is running on Windows and is part of the same domain as the users who are accessing the web application, you can bypass the federation server and grant access directly to the Active Directory users. However, in more complicated scenarios, an organization might require AD FS.

When a single organization uses AD FS, you need only one federation server (not including what might be needed for high-availability). If the network with the federation server is completely isolated, you need a second server to act as a federation proxy server.

■ Implementing AD FS

THE BOTTOM LINE

Before you implement AD FS, you need to plan your implementation. You should also create a test environment so that you can foresee the potential problems.

First, you should make sure that the client and servers can communicate with the necessary computers, which includes:

- The client must be able to communicate with the web application, the resource federation server (or federation server proxy), and the account federation server (or federation proxy) using HTTPS.
- If you are using federation server proxy, you must be able to communicate with the federation servers in the same organization using HTTPS.
- The internal clients must be able to communicate with the organization's federation servers.
- The client federation server must be able to communicate with the client domain controllers for authentication.

The domain controllers must be running a minimum of Windows Server 2003 with SP1. The federation servers must be joined to the AD DS domain.

AD FS requires DNS names for internal federation servers to which they connect, and the web application that they are trying to use. If the user is an external user, he or she also needs to resolve the name of the internal federation server through the proxy server.

When installing the AD FS server role, you then configure the server as either a federation server or federation server proxy. After installing the federation server role, you can configure the server as a claims provider, a relying party, or both. The claims provider provides the users signed tokens that contain claims, whereas the relying party receives the security tokens from a

trusted claims provider. The relying party accepts and validates the claim, and then issues new security tokens that the web server can use to provide appropriate access to the application.

Installing AD FS

Installing the Active Directory Federation Services role and creating the federation server is a simple process using Server Manager. To configure the federation server, you will need a SSL certificate.

With Windows Server 2012, the Active Directory Federation Services role includes the Federation Service, AD FS 1.1 Web Agents, and Federation Service Proxy. With Windows Server 2012 R2, AD FS only includes the Federation Service. If you need a reverse proxy, you will instead install the Remote Access role, specifically the Web Application Proxy role service.

INSTALL THE ACTIVE DIRECTORY FEDERATION SERVICES

GET READY. To install the Active Directory Federation Services, perform the following steps:

1. On *Server01*, click the Server Manager button on the task bar to open the *Server Manager*.
2. At the top of *Server Manager*, click Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Select Active Directory Federation Services and click Next.
6. On the *Select features* page, click Next.
7. On the *Active Directory Federation Services (AD FS)* page, click Next.
8. On the *Confirm installation selections* page, click Install.
9. When the installation is complete, leave the installation screen open for the next exercise.

Creating a Standalone Federation Server

You can configure Active Directory Federation Services as either a standalone server or as part of a server farm. You would use a standalone server when you want to evaluate AD FS or you want to use it for a small production environment. If you need high availability or load-balancing, you will create an AD FS farm.

Before you create the standalone federation server, you will need to have a managed service account, which will be used to run the federation services. You will also need an SSL digital certificate. If you need to import the digital certificate, you will import the certificate from a .pfx file, which will include the public and private key.

CREATE A STANDALONE FEDERATION SERVER

GET READY. To create a standalone federation server, perform the following steps:

1. On *Server01*, using the Server Manager, click Configure the federation service on this server.
2. In the *Active Directory Federation Services Configuration Wizard*, on the *Welcome page*, the Create the first federation server in a federation server farm is already selected. Click Next.
3. On the *Connect* to *AD DS* page, click Next.
4. On the *Specify Service Properties* page, select the certificate for the federation server. If a certificate is not available, you will need to import a certificate from a .pfx file using the Import button.

5. In the *Federation Service Name* box, type the name of the Federation Service (such as Contoso Corporation). Click Next.
6. On the *Specify Service* Account page, select the Use an existing domain user account or group Managed Service Account option and then click Select. In the *Select User or Service Account* dialog box, in the *Enter the object name to select* text box, type the name of a service account (such as *adfs*) and then click OK.
7. Back on the *Specify Service Account* page, in the *Account Password* text box, type in the password for the *adfs* service account and then click Next.
8. On the Specify Configuration Database page, Create a database on this server using *Windows Internal Database is already* selected. Click Next.
9. On the *Review* Options page, click Next.
10. On the *Pre-requisite Checks* page, click Configure.

After the federation server is created, you will manage the Federation Service by using the AF FS console (as shown in Figure 18-1) or by using Windows PowerShell. In both methods, you

Figure 18-1

Accessing the AD FS console

can manage certificates within AD FS and you can create and manage Claims Provider Trusts, Relying Party Trusts, Attribute Stores, and Authentication Policies.

Implementing Claims-Based Authentication

To implement claims-based authentication in a lab environment, you would use three servers. The RWDC01 acts as the domain controller. Server01 is the federation server, and Server02 is the application that will use the claims.

To install and configure AD FS for a single organization, you need to perform the following steps:

1. Install the AD FS server role.
2. Create and configure a server authentication certificate in IIS.
3. Create a standalone federation server.
4. Install and configure Windows Identity Foundation (WIF) and a sample application.
5. Create and configure the WIF application pool.
6. Configure the WIF sample application to trust incoming claims.
7. Configure AD FS to send claims to the application.
8. Configure the claim rule for the sample application.
9. Test access to the application.

Normally as a server administrator, you only deploy the application; you do not create the application. So for the test environment, you install the Windows Identity Foundation SDK 4.0, which can be found on the Microsoft website. To install the Windows Identity Foundation SDK 4.0, you need to install .NET Framework 3.5 and the Windows Identity Foundation 3.5, which is not included with Windows Server 2012 or Windows Server 2012 R2.

INSTALL THE WINDOWS IDENTITY FOUNDATION SDK 4.0

GET READY. To install the Windows Identity Foundation SDK 4.0, perform the following steps:

1. On *Server02*, click the Server Manager button on the task bar to open the *Server Manager*.
2. At the top of *Server Manager*, click Manage and click Add Roles and Features. The *Add Roles and Feature Wizard* opens.
3. On the *Before you begin* page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. On the *Select server roles* page, click Next.
6. On the *Select features* page, expand .Net Framework 3.5 Features, and click to select the .NET Framework 3.5 (includes .NET 2.0 and 3.0).
7. Click to select the Windows Identity Foundation 3.5. Click Next.
8. On the *Confirm installation selections* page, click Install.
9. When the installation is complete, click Close.
10. To install the *Windows Identity Foundation SDK*, double-click the WindowsIdentityFoundation-SDK-4.0.msi.
11. When the *Windows Identity Foundation SDK 4.0 Setup Wizard* starts, click Next.
12. On the *End-User License Agreement* page, click to select the I accept the terms in the License Agreement option. Click Next.

13. On the *Destination Folder* page, click Next.
14. On the *Ready to install Windows Identity Foundation SDK 40* page, click Install.
15. When the installation is complete, click Finish.
16. Close the Welcome to the Microsoft Windows Identity Foundation window.

The Windows Identity Foundation SDK 4.0 includes a sample WIF application. After you install the sample WIF application, you need to configure the application. Lastly, you need to create an application pool for the application.

CREATE AND CONFIGURE A SAMPLE WIF APPLICATION

GET READY. To create and configure a Sample WIF application, perform the following steps:

1. Using *Server Manager*, open the Tools menu, and click Internet Information Services (IIS) Manager.
2. When the *Internet Information Services (IIS) Manager* console opens, click Create Self-Signed Certificate.
3. On the *Specify Friendly Name* page, in the *Specify a friendly name for the certificate* text box, type Server02.contoso.com. Click OK.
4. In the left pane, expand Sites and click the Default Web Site.
5. Under Actions, click Bindings.
6. When the *Site Bindings* page opens, click Add.
7. When the *Add Site Binding* dialog box opens, change the *Type* to https. Then under *SSL certificate*, select the server02, contoso.com, and click OK.
8. Click Close to close the *Site Bindings* dialog box.
9. On the task bar, click the folder to open Windows Explorer and navigate to the `C:\Program Files (x86)\Windows Identity Foundation SDK\v4.0\Samples\Quick Start\Using Managed STS` folder.
10. Double-click setup.bat. When the application has been created, click OK.
11. Close the command prompt window and the Windows Explorer window.
12. Click the Start menu button, click the down arrow to show all programs, and click Windows Identity Foundation Federation Utility.
13. When the *Federation Utility Wizard* opens, in the *Application configuration location* text box, type the following:

    `C:\Program Files (x86)\Windows Identity Foundation SDK\v4.0\Samples\Quick Start\Using Managed STS\ClaimsAwareWebAppwithManagedSTS\web.config`
14. In *Application URI*, type `https://server02.contoso.com/ClaimsAwareWebAppWithManagedSTS` to indicate the path to the sample application that will trust the incoming claims from the federation server. Click Next to continue.
15. On the *Security Token Service* page, select Use an existing STS, type `https://server01.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml` for the *STS WS-Federation metadata document location* text box, and then click Next to continue.
16. When you get a warning because you are using a self-signed certificate, click Yes.
17. On the *STS signing certificate chain validation error*, with Disabled certificate chain validation already selected, click Next.
18. On the *Security token encryption* page, select No encryption, and then click Next.
19. On the *Offered claims* page, review the claims that will be offered by the federation server, and then click Next.

20. On the *Summary* page, click Finish.
21. When you have successfully configured the application, click OK.
22. Using the *Server Manager*, open the Tools menu, and click Internet Information Services (IIS) Manager.
23. When the *Internet Information Services (IIS) Manager* console opens, click Application Pools.
24. In the *Actions* pane, click Add Application Pool.
25. When the *Add Application Pool* dialog box opens, in the *Name* text box, type WIFSamples and click OK.
26. Click WIFSamples, and click Advanced Settings.
27. In the *Advanced Settings* dialog box, expand Process Model.
28. Change the *Load User Profile* setting from False to True.
29. Click OK to close the *Advanced Settings* dialog box.
30. In the left pane, expand Sites, expand Default Web Site, and click ClaimsAwareWebAppWithManagedSTS.
31. In the *Actions* pane, click Basic Settings.
32. When the *Edit Application* dialog box opens, click Select.
33. When the *Select Application Pool* dialog box opens, change the *Application pool* to WIFSamples and click OK.
34. Click OK to close the *Edit Application* dialog box.

In a test environment, it is common to use self-signed digital certificates. When you use self-signed certificates, you get warnings when accessing websites using self-signed certificates. To avoid the errors, and to allow the application using WIF to function properly, you need to add the websites digital certificate into the local computer Trusted Root Certification Authorities store.

ADD SELF-SIGNED CERTIFICATES TO TRUSTED ROOT CERTIFICATION AUTHORITY STORE

GET READY. To add self-signed certificates to Trusted Root Certification Authority store, perform the following steps:

1. Open Internet Explorer and visit the `https://server02.contoso.com/ClaimsAwareWebAppWithManagedSTS/` website.
2. If it asks you to log in, log in as Administrator with the Password of Pa$$word.
3. At the top of the IE window, click Certificate error, and click View certificates.
4. When the *Certificate* dialog box opens, on the *General* tab, click Install Certificate.
5. When the *Welcome to the Certificate Import Wizard* starts, click Local Machine, and click Next.
6. On the *Certificate Store* dialog box, click Place all certificates in the following store, and click Browse.
7. When the *Select Certificate Store* dialog box opens, click Trusted Root Certification Authorities, and click OK.
8. Back on the *Certificate Store* page, click Next.
9. When the wizard is complete, click Finish.
10. When the import is successful, click OK.

Implementing Relying Party Trusts

A relying party trust identifies the relying party so that the federation server knows which applications can use AD FS. It also defines the claim rules, from the claims provider. The relying party is defined on the federation server.

In a single organization that uses AD FS, the relying party trust defines how the AD FS server interfaces with the applications. When you configure the relying party trust, you specify the URL of the internal application, and configure settings such as whether the application supports SAML 2.0 or whether it requires AD FS 1.0 tokens, the SSL certificate and URL used by the web server, and the issuance authorization rules for the application. If you are configuring a Business-to-Business Federation, you need to create additional relying party trusts for each federated organization.

When configuring a relying party trust, you have three options:

- **Import data about the relying party through the federation metadata:** If the AD FS federation server or federation proxy server is accessible through the network from your AD FS federation server, you can enter the host name or URL for the partner federation server. The AD FS connects to the AD FS federation server to download the federation metadata, which includes all the information that is required to configure the relying party trust. The trust also downloads the SSL certificate that the partner federation server uses.
- **Import data about the relying party from a file:** If the partner federation server is not directly accessible from the federation server, you can export the configuration information to a file, which you can then upload. The configuration file includes the configuration information for the partner organization and the SSL certificate that the partner federation server uses.
- **Manually configure the claims provider trust:** Allows you to manually configure all of the settings for the claims to provide trust.

IMPLEMENT RELYING PARTY TRUSTS

GET READY. To implement relying party trusts, perform the following steps:

1. In the *AD FS Management* console, click AD FS, expand Trust Relationships, and click Relying Party Trusts.
2. Right-click Relying Party Trusts, and click Add Relying Party Trust.
3. When the *Add Relying Party Trust Wizard* opens, click Start.
4. On the *Select Data Source* page, click Import data about the relying party published online or on a local network, type `https://server02.contoso.com/ClaimsAwareWebAppWithManagedSTS/`, and then click Next.
5. On the *Specify Display Name* page, in the *Display name* text box, type WIF Sample App, and then click Next.
6. On the *Configure Multi-factor Authentication Now?* page, *I do not want to configure multi-factor authentication settings for this relying party trust at this time* option is already selected. Click Next.
7. On the *Choose Issuance Authorization Rules* page, click Permit all users to access this Relying Party, and then click Next.
8. On the *Ready to Add Trust* page, review the relying party trust settings, and then click Next to save the configuration.
9. On the *Finish* page, click Close to exit the wizard.

Configuring Authentication Policies

Starting in Windows Server 2012, you can use authentication policies with AD FS to give you more control on who can use an AD FS application or service.

In Windows Server 2012 R2, AD FS can be accessed with authentication policies and multi-factor authentication (including using user, device, location, and authentication data). The ***authentication policy*** specifies the type of authentication globally for applications and services that are secured by AD FS or for a particular application per relying party trust.

CONFIGURE A GLOBAL AUTHENTICATION POLICY

GET READY. To configure a global authentication policy, perform the following steps:

1. Using *Server Manager*, click Tools > AD FS Management.
2. In the *AD FS* console, click Authentication Policies.
3. In the *Primary Authentication* section, click Edit. You can also right-click Authentication Policies and choose Edit Global Primary Authentication or, under the *Actions* pane, select Edit Global Primary Authentication.
4. In the *Edit Global Authentication Policy* dialog box, on the *Primary* tab, you can configure the following settings:
   - Authentication methods to be used for primary authentication including *Forms Authentication* and *Certificate Authentication* for *Extranet*, and *Forms Authentication*, *Certificate Authentication*, and *Windows Authentication* for *Intranet*.
   - Enable Device authentication via the *Enable device authentication* check box.
5. To close the *Edit Global Authentication Policy* dialog box, click OK.

CONFIGURE PRIMARY AUTHENTICATION PER RELYING PARTY TRUST

GET READY. To configure primary authentication per relying party trust, perform the following steps:

1. Using *Server Manager*, click Tools > AD FS Management.
2. In the *AD FS* console, click Authentication Policies\Per Relying Party Trust (as shown in Figure 18-2), and then click the relying party trust for which you want to configure authentication policies.

Figure 18-2

Accessing the Authentication Policies node

3. Either right-click the relying party trust for which you want to configure authentication policies and choose Edit Custom Primary Authentication or, under the *Actions* pane, select Edit Custom Primary Authentication.
4. In the Edit Authentication Policy dialog box, you can select or deselect the Users are required to provide credentials each time at sign in check box.
5. Click OK to close the *Edit Authentication Policy* dialog box.

Configuring Multi-Factor Authentication

With Windows Server 2012 R2, AD FS access control is enhanced with ***multi-factor authentication (MFA)***, including user, group, device, location, and authentication data. Windows Server 2012 R2 includes new claim types, such as client application, device operating system type, device operating system version, public key, thumbprint, inside corporate network, and password expiration time.

Using multifactor access control with AD FS in Windows Server 2012 R2 has the following benefits:

- Allows for flexible authorization policies that allow you to permit or deny access based on user, device, network location, and authentication state.
- Allows creating issuance authorization rules for relying party applications.
- Provides a rich UI experience for the common multifactor access control scenarios.
- Provides rich claims language and Windows PowerShell support for advanced multifactor access control scenarios.
- Allows you to use custom 'Access Denied' messages.

CONFIGURE GLOBAL MULTI-FACTOR AUTHENTICATION

GET READY. To configure global multi-factor authentication, perform the following steps:

1. Using *Server Manager*, click Tools > AD FS Management.
2. In the *AD FS* console, click the Authentication Policies node.
3. In the *Multi-factor Authentication* section (as shown in Figure 18-3), click Edit. You can also right-click Authentication Policies and choose Edit Global Multi-factor Authentication or, under the *Actions* pane, select Edit Global Multi-factor Authentication.

Figure 18-3

Accessing the Multi-factor Authentication settings

4. In the *Edit Global Authentication Policy* dialog box, under the *Multi-factor* tab, you can configure the following settings as part of the global multi-factor authentication policy:
   - If Multi-factor Authentication is required for the specified user and groups.
   - If MFA is required for unregistered or registered devices.
   - If MFA is required for Extranet or Intranet.
   - Which additional authentication method can be used with MFA, such as Certificate Authentication.
5. Click OK to close the *Edit Global Authentication Policy* dialog box.

Configuring Workplace Join

As users are using multiple computers and devices to access email and other business related applications and services, and as users use their personal devices—particularly if the organization uses a Bring Your Own Device (BYOD) policy)—you need to let users with non-company devices access the company resources while maintaining security. With ***Workplace Join*** technology, users can join their devices to the organization network without joining the device to the Active Directory domain. You can then manage access based on a wide range of attributes.

When the user joins the devices using Workplace Join technology, the device becomes a known device. To use Workplace Join, you must have Windows Server 2012 R2 with the AD FS role service installed. In addition, the client must be using the Windows 8.1 client operating system or iOS-based devices (such as an iPad).

An AD FS service, ***Device Registration Service (DRS)*** provisions a device object in AD DS and issues a certificate for the Workplace-Joined device. The certificate will be used to represent device identity when access organization resources. When accessing resources on the organization, the SSO will allow the user to be prompted for their domain credentials only once during the lifetime of the SSO session. However, an administrator can enforce a password prompt or reauthentication of some resources.

Before you add the device, you will need to configure the Device Registration Service for Windows Server 2012 R2. To configure the Device Registration Service, execute the following Windows PowerShell commands:

```
Initialize-ADDeviceRegistration
Enable-AdfsDeviceRegistration
```

You will then open the AD FS Management console, navigate to Authentication Policies, click Edit Global Primary Authentication, and then click to select the Enable Device Authentication. Click OK. Lastly, the client must trust the issuer of the SSL certificate that is used for the federation server and must be able to validate certificate revocation information for the certificate.

JOIN THE DEVICE

GET READY. To join the device, perform the following steps:

1. Log on to the client Windows device with a Microsoft account.
2. On the *Start* screen, open the Charms bar and then select the Settings charm. Select Change PC Settings.
3. On the *PC Settings* page, select Network and then click Workplace.
4. In the *Enter your UserID to get workplace access or turn on device management* dialog box, type the user name (such as JSmith@contoso.com) and then click Join.
5. When prompted for credentials, type the username and the associated password. Click OK. You should now see the message: This device has joined your workplace network.

Business Case Scenarios

Scenario 18-1: Creating a Federation Partnership

You are an administrator for the Contoso Corporation. You are partnering with Litware.com, which will order products from the Contoso Corporation. Therefore, you need to deploy an application that the users of Litware can access over the Internet. What should you do?

Scenario 18-2: Managing BYOD Devices

Your company has just implemented a BYOD policy where users can user their own smartphones and tablets at work. Therefore, these devices will need to be able to access a variety of AD FS application and services as well as other internal resources. What must you do to allow those devices to connect to your organization securely?

Installing and Configuring Active Directory Certificate Services (AD CS)

LESSON 19

Understanding the Active Directory Certificate Services

THE BOTTOM LINE

Active Directory Certificate Services (AD CS) is a server role that allows you to issue and manage digital certificates as part of a public key infrastructure. ***Public key infrastructure (PKI)*** is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates. PKI consists of certification authorities (CAs) and registration authorities that verify and authenticate the validity of each entity that is involved in an electronic transaction through the use of public key cryptography. Within the PKI, the ***certificate authority (CA)*** binds a public key with respective user identities and issues digital certificates containing the public key.

Installing an Enterprise Certificate Authority

The CA is a Windows Server 2012 or Windows Server 2012 R2 server role that verifies the identity of the certificate requestors; issues certificates to requesting users, computers, and services; and manages certificate revocation.

Depending on your needs, you can install AD CS on multiple Windows servers to create an infrastructure of CAs. The first CA is known as the *root CA*, which establishes the PKI in the network and provides the highest point in the whole structure.

Each of the components that make up the PKI are deployed as role services of the AD CS server role. Each role service is responsible for a specific portion of the certificate infrastructure, while working together to form a complete solution.

Role services of the AD CS role include:

- **CA:** The component that issues certificates to users, computers, and services and manages certificate validity.
- ***CA Web Enrollment:*** The component that provides a method to issue and renew certificates for users, computers, and devices that are not joined to the domain, are not connected directly to the network, or are for users of non-Windows operating systems.
- ***Online Responder:*** The component that configures and manages Online Certificate Status Protocol (OCSP), which is used to validate and revoke certificates.

- ***Network Device Enrollment Service:*** The component that can be used to assign certificates to routers, switches, and other network devices.
- ***Certificate Enrollment Web Service:*** The component that allows computers to connect to a CA using a web browser to request, renew, and install issued certificates; retrieve CRLs; download a root certificate; and enroll over the Internet or across forests.
- ***Certificate Authority Policy Web Service:*** The component that is enables users to obtain certificate enrollment policy information.

When you install a CA, you have the following choices:

- Standalone CA or Enterprise CA
- Root CA or Subordinate CA

The ***standalone CA*** works without Active Directory and does not need Active Directory, however, the server can be a member of a domain. Users can request certificates using a manual procedure or web enrollment, where they have to identify information and specify the certificate they need. By default, all certificate requests submitted to standalone CAs are held in a pending queue until a CA administrator approves them. However, you can configure standalone CAs to issue certificates automatically upon request, but this is less secure and is usually not recommended.

An ***enterprise CA*** requires Active Directory and is typically used to issue certificates to users, computers, devices, and servers for an organization. Users can request certificates using manual enrollment, web enrollment, auto-enrollment, or an enrollment agent. Because information for a user or computer can be retrieved from Active Directory, templates can be used to generate certificates with the appropriate attributes for the specified certificate type.

The top of the certificate hierarchy is the ***root CA***. Because everything branches from the root, it is trusted by all clients within an organization. Although smaller organizations have only one CA, larger organizations have a root CA with multiple subordinate CAs. Although the enterprise CA can issue certificates to end users, it is usually used to issue certificates to subordinate CAs.

Although there is only one root CA, there can be one or more ***subordinate CA***. The number of subordinate CAs needed are determined by geographical location and number of clients.

To install the Active Directory Certificate Services Server role, you need to be logged in as an enterprise administrator.

INSTALL THE ACTIVE DIRECTORY CERTIFICATE SERVICES SERVER ROLE

GET READY. To install and configure the Active Directory Certificate Services Server Role, perform the following steps:

1. In the *Server Manager* console, click Add roles and features.
2. When the *Add Roles and Features Wizard* opens, click Next.
3. On the *Select installation type* page, click Next.
4. On the *Select destination server* page, click Next.
5. On the *Select server roles* page, select Active Directory Certificate Services. When the *Add Roles and Features Wizard* window appears, click Add Features, and then click Next.
6. On the *Select features* page, click Next.
7. On the *Active Directory Certificate Services* page, click Next.

8. On the *Select role services* page, ensure that Certification Authority is selected, and then click Next.
9. On the *Confirm installation selections* page, click Install.
10. On the *Installation progress* page, after installation is successful, click Configure Active Directory Certificate Services on the destination server.
11. On the *Credentials* page, click Next.
12. On the *Select role services to configure* page, click Certification Authority and click Next.
13. On the *Setup Type* page, select Enterprise CA or Standalone CA, and then click Next.
14. On the *CA Type* page, ensure that Root CA is selected, and then click Next.
15. On the *Private Key* page, ensure that Create a new private key is selected, and then click Next.
16. On the *Cryptography for CA* page, keep the default selections for Cryptographic Service Provider (CSP) and Hash Algorithm. For better security, change the *Key length* to 4096, and then click Next.
17. On the *CA Name* page (see Figure 19-1), click Next.

Figure 19-1

Specifying the name of the CA

18. On the *Validity Period* page, the default is 5 years. Click Next.
19. The *CA Database* page displays where the certificate database will be stored. Click Next.
20. On the *Confirmation* page, click Configure.
21. On the *Results* page, click Close.

INSTALL SUBORDINATE CERTIFICATE SERVICES SERVER ROLE

GET READY. To install and configure the Active Directory Certificate Services Server Role, perform the following steps:

1. In the *Server Manager* console, click Add roles and features.
2. When the *Add Roles and Features Wizard* opens, click Next.
3. On the *Select installation type* page, click Next.
4. On the *Select destination server* page, click Next.
5. On the *Select server roles* page, select Active Directory Certificate Services. When the *Add Roles and Features Wizard* window appears, click Add Features, and then click Next.
6. On the *Select features* page, click Next.
7. On the *Active Directory Certificate Services* page, click Next.
8. On the *Select role services* page, ensure that Certification Authority is selected, and then click Next.
9. On the *Confirm installation selections* page, click Install.
10. On the *Installation progress* page, after installation is successful, click Configure Active Directory Certificate Services on the destination server.
11. On the *Credentials* page, click Next.
12. On the *Select role services to configure* page, click Certification Authority and click Next.
13. On the *Setup Type* page, select Enterprise CA or Standalone CA, and then click Next.
14. On the *CA Type* page, ensure that Subordinate CA is selected, and then click Next.
15. On the *Private Key* page, ensure that Create a new private key is selected, and then click Next.
16. On the *Cryptography for CA* page, keep the default selections for Cryptographic Service Provider (CSP) and Hash Algorithm. For better security, change the *Key length* to 4096, and then click Next.
17. On the *CA Name* page, click Next.
18. On the *Certificate Request* page, select Send a certificate request to a parent CA. Then with the CA name, click Select, click the CA that you installed in the previous exercise, and click OK page. Click Next.
19. The *CA Database* page displays where the certificate database will be stored. Click Next.
20. On the *Confirmation* page, click Configure.
21. On the *Results* page, click Close.

Configuring AIA and CRL Distribution Points

After a CA is installed, you must configure the ***Authority Information Access (AIA) extension*** and ***CRL distribution point (CDP) extension*** before the CA issues any certificates. They are necessary to validate the certificates. The AIA extension specifies where to find up-to-date certificates for the CA. The CDP extension specifies where to find up-to-date CRLs that are signed by the CA. These extensions apply to all certificates that are issued by that CA.

The AIA extension specifies the locations from which users can obtain the certificate for this CA. Certificate Chaining is a process that builds one or more certificate paths, which trace to the self-signed or root certificate, and helps determine whether a digital certificate can be trusted or not.

When someone loses their house key, it a good idea to change the locks on the door in case someone has stolen the house key and will use it later to illegally enter the house. Similarly with certificates, a CA could improperly issue a certificate or a private key might have been compromised. You want to revoke the certificate so that the keys will no longer be valid and used in the future. In addition, after a set period of time, certificates expire.

Certificate Revocation List (CRL) is a digitally signed list issued by a CA that contains a list of certificates issued by the CA that have been revoked. The list includes all individual revoked certificates including the serial number of the certificate, the date that the certificate was revoked, and the revocation reason.

The application uses a CDP to check the CRL for a revoked certificate. The CDP is a certificate extension that indicates where the certificate revocation list for a CA can be retrieved.

The AIA and CDP extensions can be published to Active Directory, web servers including FTP servers, and file servers. For computers that are not members of Active Directory, you should place the CA certificate and CRL on web servers by using the HTTP protocol.

CONFIGURE CERTIFIED REVOCATION LIST (CRL) DISTRIBUTION

GET READY. To configure Certified Revocation List (CRL) Distribution, perform the following steps:

1. Using *Server Manager*, open the Tools menu and click Certification Authority.
2. When the *Certification Authority* console opens, right-click Revoked Certificates, and then click Properties.
3. In the *Revoked Certificates Properties* window, set the *CRL publication interval* to 1 Day and the Delta CRL *Publication interval* to 1 hour, and then click OK.
4. Right-click the CA, and click Properties.
5. Click the Extensions tab. Figure 19-2 shows the default CRL distribution points.

Figure 19-2

Specifying the CRL distribution points

6. To add additional CRL points, click Add.
7. In the *Add Location* dialog box, you can type the location in the *Location* text box. As shown by the example, you can insert variables by choosing the variable and clicking the Insert button.
8. Click OK to close the *Add Location* dialog box.
9. Click OK to close the *Properties* dialog box.
10. Close *Certification Authority* console.

Because CRLs can become large, depending on the number of certificates issued and revoked by a CA, you can also publish smaller, interim CRLs called *delta CRLs*. ***Delta CRLs*** contain only the certificates revoked since the last regular CRL was published. This allows clients to retrieve the smaller delta CRL and more quickly build a complete list of revoked certificates. The use of delta CRLs also allows revocation data to be published more frequently because the size of the delta CRL usually does not require as much time to transfer as a full CRL.

A ***certification practice statement (CPS)*** is a policy that is defined by the issuing organization's responsibilities when issuing the certificates including identifying the organization issuing the certificates, what the certificates will be used for the process used when assigning the certificates, how the certificates are revoked, and how the certificates are protected. The CPS should be available publically to internal and external users.

Installing and Configuring Online Responder

An Online Responder is a trusted server that runs the Online Responder service and Online Responder Web proxy to receive and respond to individual client requests for information about the status of a certificate. It implements the ***Online Certificate Status Protocol (OSCP)*** protocol, which allows a recipient of a certificate to submit a certificate status request to a responder by using the Hypertext Transfer Protocol (HTTP).

Different from certificate revocation lists, which are distributed periodically and contain information about all certificates that have been revoked or suspended, an Online Responder receives and responds only to individual requests from clients for information about the status of a certificate. As a result, Online Responders can process certificate status requests more efficiently than can CRLs.

You can install an Online Responder on Windows Server 2008 Enterprise, Windows Server 2008 R2 Enterprise, Windows Server 2012, or Windows Server 2012 R2. You should install Online Responders after the CAs, but before issuing any client certificates. It is recommended to install the Online Responder on a different computer than a CA. If you need scalability and high availability, you can use Network Load Balancing (NLB).

The following operating systems can use an Online Responder for validation of certificate status:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1

For the clients to use the Online Responder, you must configure the CAs to include the URL of the Online Responder in the AIA extension of issued certificates. The OCSP client uses this URL to validate the certificate status. You must also issue the OCSP Response Signing certificate template, so that the Online Responder can also enroll that certificate.

When you configure a CA to support the Online Responder service, IIS will be installed on the computer when you install the Online Responder role. You will then have to configure an OCSP Response Signing certificate template on the CA and auto-enrollment must be used to issue the OCSP Response Signing certificate to the computer. Lastly, you need to include the URL for the Online Responder in the AIA extension of certificates issued by the CA.

INSTALL THE ONLINE RESPONDER ROLE

GET READY. To install the Online Responder Role, perform the following steps:

1. Using *Server Manager*, open the Manage menu and click Add roles and features.
2. When the *Add Roles and Feature Wizard* opens, click Next.
3. On *the Select installation type* page, click Next.
4. On the *Select destination* page, click Next.

5. On the *Select server roles* page, expand Active Directory Certificate Services (Installed), and then select Online Responder. When it asks to add features, click Add Features. Click Next.
6. On the *Select Features* page, click Next.
7. On the *Confirm installation selections* page, click Install.
8. When the message displays that the installation succeeded, click Configure Active Directory Certificate Services on the destination server.
9. When the *AD CS Configuration Wizard* opens, click Next.
10. On the *Role Services* page, click to select Online Responder, and then click Next.
11. Click Configure.
12. Click Close two times.
13. Using *Server Manager*, open the Certification Authority console.
14. In the *Certification Authority* console, right-click the CA, and then click Properties.
15. When the *Properties* dialog box opens, click Authority Information Access (AIA), and then click Add.
16. When the *Add Location* dialog box opens, type http://<servername>/ocsp (if the server is called *rwdc01*, you would type http://rwdc01/ocsp), and then click OK.
17. Click to select the Include in the AIA extension of issued certificates check box.
18. Click to select the Include in the online certificate status protocol (OCSP) extension check box, and then click OK.
19. When it asks you to restart AD CS, click Yes.
20. In the *certsrv* console, expand CA, right-click the Certificate Templates folder, and then click Manage.
21. In the *Certificate Templates* console, double-click the OCSP Response Signing template.
22. In the *OCSP Response Signing Properties* dialog box, click the Security tab. Under *Permissions for Authenticated Users*, select the Allow check box for Autoenroll, and then click OK.
23. Close the Certificate Templates console.
24. In the *Certification Authority* console, right-click the Certificate Templates folder, point to New, and then click Certificate Template to Issue.
25. In the *Enable Certificate Templates* dialog box, select the OCSP Response Signing template, and then click OK.
26. Using *Server Manager*, click Tools, and then click Online Responder Management.
27. When the *ocsp* console opens (see Figure 19-3), right-click Revocation Configuration, and then click Add Revocation Configuration.

Figure 19-3

Viewing the Online Responder Configuration console

28. When the *Add Revocation Configuration Wizard* starts, click Next.
29. On the *Name the Revocation Configuration* page, in the *Name* text box, type Contoso CA Online Responder, and then click Next.
30. On the *Select CA Certificate Location* page, *Select a certificate for an Existing enterprise CA option* is already selected. Click Next.
31. On the *Choose CA Certificate* page, click Browse, click the certificate for the CA, and click OK. Then click Next.
32. On the *Select Signing Certificate* page, verify that Automatically select a signing certificate and Auto-Enroll for an OCSP signing certificate are both selected, and then click Next.
33. On the *Revocation Provider* page, click Finish.
34. Close the ocsp console.

Implementing Administrative Role Separation

Because certificates and CAs are important security tools used for a company, you need to consider using separation of duties to maintain the security of PKI infrastructure. You can use role-based administration to organize CA administrators into separate, predefined CA roles, each with his or her own set of tasks.

All CA roles are assigned and modified by members of local Administrators, Enterprise Admins, or Domain Admins. On enterprise CAs, local administrators, enterprise administrators, and domain administrators are CA administrators by default. If a standalone CA is installed on a server that is joined to an Active Directory domain, domain administrators are also CA administrators.

The ***CA administrator*** configures and maintains the CA. CA administrators have the ability to assign all other CA roles and renew the CA certificate. To make a user a CA Administrator,

you just open the *Certificate Authority* console, click *Properties*, click the *Security* tab, and grant the *Allow Manage CA Permission*. The Allow Manage CA permission allows the CA administrator to perform the following:

- Configure policy and exit modules.
- Start and stop the AD Certificate Services service.
- Configure AD CS roles and CA extensions.
- Define key recovery agents.
- Configure certificate manager restrictions.
- Delete one or more records in the CA database.
- Modify Certificate Revocation List (CRL) publication schedules.
- Read records and configuration information in the CA database.

The ***certificate manager*** issues and manages certificates, and approves certificate enrollment and revocation requests. To make a user a Certificate Manager, you just have to grant the Allow Issue and Manage Certificates, which grants the following:

- Perform bulk deletions in the CA database.
- Issue, approve, deny, revoke, reactivate, and renew certificates.
- Recover archived keys.
- Read records and configuration information in the CA database.

The ***backup operator*** backs up and restores files and directories. Backup Operators, which are assigned using Active Directory Users and Computers or Computer Management, can perform the following:

- Back up and restore the system state, including CA information.
- Start and stop the AD CS service.
- Possess the system backup user right.
- Read records and configuration information in the CA database.

By default, the local administrator holds the system backup user rights.

Auditors manage and read security logs on a computer running the AD CS role. Because they have the system audit user right, they can perform the following:

- Configure audit parameters.
- Read audit logs.
- Possess the system audit user right.
- Read records and configuration information in the CA database.

By default, the local administrator holds the system audit user rights. In addition to audit events, the computer must also be configured for auditing of object access using a group policy.

Configuring CA Backup and Recovery

By now, you should understand the importance of backups. If you lose your CA, you could lose your entire PKI infrastructure, which will stop users from logging on using a VPN tunnel, or accessing encrypted e-mails and files. Therefore, you need to know how to back up and restore the CA so that you can quickly bring the CA up after a disaster.

You can back up the entire server by backing up all files and the system state using Windows Server Backup. However, you can back up a CA without having to back up the entire server on which the CA is installed. You just need to back up the private and public key for the CA and the certificate database (including the certificate database logs). To perform a backup or restore, you must be a CA administrator or a member of the Backup Operators group, or equivalent.

BACK UP A CA USING THE CERTIFICATION AUTHORITY SNAP-IN

GET READY. To back up a CA using the Certification Authority snap-in, perform the following steps:

1. Using *Server Manager*, open the Certification Authority console.
2. In the console tree, right-click the name of the CA, click All Tasks, and click Back up CA.
3. When the *Certification Authority Backup Wizard* starts, click Next.
4. On the *Items to Back Up* page, click to select Private key and CA certificate and Certificate database and certificate database log options.
5. In the *Back up to this location* text box, type in the path to a folder. Click Next.
6. On the *Select a Password* page, type a password in the *Password* and *Confirm password* text boxes to help secure the private key. Click Next.
7. When the wizard is complete, click Finish.

In addition to the CA, you should also back up the Internet Information Services (IIS) metabase. If a damaged or missing IIS metabase is not restored, IIS will fail to start and result in Certificate Services web pages failing to load. You can use the IIS snap-in to back up the IIS metabase, or you can back up the system state. An alternative method is to recreate the IIS metabase and then use the certutil.exe -vroot command at a command line to reconfigure the IIS server to support the CA web pages.

Business Case Scenarios

Scenario 19-1: Securing a Two-Tier PKI

You want to deploy multiple CA servers to form a PKI consisting of several CA servers that will deploy certificates to the users and computers. How would you configure the servers to form the PKI and what steps would you use to secure the PKI?

Scenario 19-2: Backing Up a CA

You have just installed an Enterprise CA. What are the three ways that you can back up the CA so that it can be restored if the server fails in the future?

20 LESSON

Managing Certificates

Managing Digital Certificates

THE BOTTOM LINE

A ***digital certificate*** is similar to an electronic identification card used to certify the online identify of individuals, organizations, and computers. It contains a person's or an organization's name, a serial number, an expiration date, a copy of the certificate holder's public key (used for encrypting messages and creating digital signatures), and the digital signature of the Certification Authority (CA) that assigned the certificate so that recipients can verify that the certificate is real.

The most common digital certificate is the ***X.509 version 3***. The X.509 version 3 standard specifies the format for the public key certificate, certificate revocation lists, attribute certificates, and a certificate path validation algorithm.

There are only so many root CA certificates that are assigned to commercial third-party organizations. Therefore, when you acquire a digital certificate from a third-party organization, you might need to use a certificate chain to obtain the root CA certificate so that it can be trusted. In addition, you might need to install an intermediate digital certificate that links the assigned digital certificate to a trusted root CA certificate. The ***certificate chain***, also known as the certification path, is a list of certificates used to authenticate an entity. It begins with the certificate of the entity and ends with the root CA certificate.

The third tab of a certificate is the certification path, as shown in Figure 20-1. The path starts with the Subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

Figure 20-1

Viewing a certification path

On a local computer running Windows, the certificates are stored in a certificate store. Using the Certificates MMC snap-in, you can display the certificate store for a user, a computer, or a service according to the purpose for which the certificates were issued or by using their logical storage categories.

Windows can also publish certificates to Active Directory. Publishing a certificate in Active Directory enables all users or computers with adequate permissions to retrieve the certificate as needed.

Digital certificates can be imported and exported via electronic files. After you import a certificate, you should use the Certificates MMC to verify that the certificate is stored in the correct location.

Managing Certificate Templates

Certificate templates are used to simplify the task of administering a CA by allowing an administrator to identify, modify, and issue certificates that have been preconfigured for selected tasks. The Certificate Templates snap-in enables you to view and modify the properties for each certificate template, and copy and modify certificate templates.

Certificate templates are an integral part of the enterprise CA. They are used to establish a set of rules and format for certificate enrollment that are applied to incoming certificate requests. Certificate templates also give instructions to the client to create and submit a valid certificate request.

Certificates based on a certificate template can be issued only by an enterprise CA. The templates are stored in Active Directory Domain Services (AD DS) for use by every CA in the forest. This allows the CA to always have access to the current standard template and ensures consistent application of the certificate policy across the forest.

When accessing the Certificate Templates console, there are several preconfigured certificate templates that act as a starting point to use certificate templates. However, most organizations will need to customize the built-in templates by copying the current templates and creating new certificates based on the copied certificate. Some of these templates (as seen in Figure 20-2) include:

- **Basic EFS (Template Version 1):** Used by Encrypting File System (EFS) to encrypt data.
- **Computer Template Version 1:** Allows a computer to authenticate itself to the network.
- **EFS Recovery Agent (Template Version 1):** Allows the subject to decrypt files that were previously encrypted with EFS.
- **IPSEC (Template Version 1):** Used by IPsec to digitally sign, encrypt, and decrypt network communication when the subject name is supplied to the request.
- **Smartcard Logon (Template Version 1):** Allows the holder to authenticate using a smart card.
- **User (Template Version 1):** Used by users for email, EFS, and client authentication.
- **Web Server (Template Version 1):** Proves the identity of a Web server.

Figure 20-2

Viewing the Certificate Template console

Some certificates have a single purpose, whereas others have multiple purposes. A single-purpose certificate serves a single purpose, such as allowing users to log on with a smart card. Organizations utilize single-purpose certificates in cases where the certificate configuration differs from other certificates that are being deployed. A multi-purpose certificate serves more than one purpose (often unrelated) at the same time. Some templates (such as the User template) serve multiple purposes by default, but organizations often modify templates to serve additional purposes, so that users and computers have to enroll only once for a certificate.

Active Directory Certificate Services (AD CS) provides four schema versions of certificate templates:

- **Version 1 certificate templates:** Support general certificate needs and provide compatibility with clients and issuing CAs running Windows 2000 operating systems or later. Version 1 templates are installed by default during CA setup and cannot be deleted. The only property that can be modified on a version 1 template is the set of assigned permissions that control access to the template.
- **Version 2 certificate templates:** Introduced in Windows Server 2003. These certificates can be configured by an administrator to control the way certificates are requested, issued, and used. Version 2 templates provide support for certificate autoenrollment.
- **Version 3 certificate templates:** Introduced with Windows Server 2008. They support Suite B cryptographic algorithms. Suite B was created by the U.S. National Security Agency to specify cryptographic algorithms that must be used by U.S. government agencies to secure confidential information.
- **Version 4 certificate templates:** Introduced with Windows Server 2012, version 4 certificate templates allow administrators to separate what features are supported by which operating system version by adding a Compatibility tab to the certificate template Properties tab. Version 4 certificate templates also support both Cryptographic Service Providers (CSPs) and Key Storage Providers (KSPs). They can also be configured to require renewal with a same key.

Assuming that you use the corresponding version of Windows, you can upgrade the certificate template to a higher version.

When you access the properties of a certificate template, you have the following tabs:

- **General:** Specifies the template display name and template name. It allows you to modify the validity period and the renewal period and if the certificate is published in Active Directory.
- **Compatibility:** Used to specify the earliest operating system that can use a certificate.
- **Request Handling:** Specifies the purpose of the digital certificates and gives some control on the certificates that are made with this template.
- **Superseded Templates:** Specifies which certificate template that the current template will replace.
- **Extensions:** Specifies the application policies, basic constraints, issuance policies, and key usage.
- **Security:** Specifies you can access and use a certificate template.
- **Server:** Allows an administrator not to store certificates, requests, or revocation information in the CA database.
- **Cryptography:** Specifies the minimum key size and which providers can be used.
- **Subject Name:** Specifies what Subject name is used in the certificate.
- **Issuance Requirements:** Specifies if a certificate has to be approved, the number of authorized signatures, and what is required for reenrollment.

To configure certificate template permissions, you need to define the Discretionary Access Control List (DACL) for each certificate template in the Security tab (see Figure 20-3). The permissions that are assigned to a certificate template define which users or groups can read, modify, enroll, or autoenroll for that certificate template.

Figure 20-3

Modifying permissions for a certificate template

Similar to assigning NTFS or share permissions, it is best to assign the certificate template permissions to a global or universal group. It is also a best practice to keep the Read permission allocated to the Authenticated Users group to view the certificate templates in Active Directory and it allows a CA that runs under the System context of a computer account to view the certificate templates when assigning certificates.

CREATE A NEW USER CERTIFICATE TEMPLATE

GET READY. To create a new User Certificate Template, perform the following steps:

1. Using Server Manager, open the *Certification Authority* console.
2. Expand certificate authority, right-click Certificate Templates, and then select Manage.
3. When the *Certificate Templates* console opens, right-click the User template, and then click Duplicate Template.
4. Click the General tab.
5. Modify the Validity period for the certificate.
6. In the *Template display name* field, type Corporate User Certificate.
7. Click the Subject Name tab.
8. Clear the Include e-mail name in the subject name and the E-mail name check boxes.
9. Click the Extension tab.

10. Click Application Policies, and then click Edit.
11. When the *Edit Application Policies Extension* dialog box opens, click Add.
12. When the *Add Application Policy* dialog box opens, click Smart Card Logon, and then click OK two times.
13. Click the Superseded Templates tab.
14. Click Add. Click the User template, and then click OK.
15. Click OK to close the *Properties of New Template* dialog box.
16. Close the *Certification Template* console and *Certification Authority* console.

By default, only a handful of digital certificates are available to users and computers. To make other certificate templates available so that users or computers can request a certificate, you use the CA. You can then use the Certificates console to request a certificate.

CONFIGURE THE TEMPLATE SO IT CAN BE ISSUED

GET READY. To configure the template so it can be issued, perform the following steps:

1. Using Server Manager, open Certification Authority.
2. Right-click Certificate Templates, click New, and then click Certificate Template to Issue.
3. In the *Enable Certificate Templates* window, select the template that you want to make available, and click OK.
4. Close *Certification Authority*.

Implementing and Managing Certificate Deployment, Validation, and Revocation

In Windows 8/8.1 and, Windows Server 2012, and Windows Server 2012 R2 you can use multiple methods to enroll user and computer certificates. If you have hundreds, or even thousands, of users, you should use autoenrollment so that you can automatically deploy certificates to those users or computers.

The available methods for a user or computer to enroll for a certificate include:

- Manual enrollment
- CA Web enrollment
- Enrollment on behalf (enrollment agent)
- Autoenrollment

USING MANUAL ENROLLMENT

When you use ***manual enrollment***, you create a private key and certificate request is generated on a device such as a web service or a computer. The request is sent to the CA to generate the certificate. The certificate is sent back to the device for installation. You typically use manual enrollment when the device does not support autoenrollment, you do not want to wait for autoenrollment to be applied, or the certificate is not available through autoenrollment.

REQUEST A CERTIFICATE USING MANUAL ENROLLMENT

GET READY. To request a certificate using manual enrollment, perform the following steps:

1. Click the Start menu, type mmc.exe, and press the Enter key.
2. When the console opens, click File > Add/Remove snap-in.
3. When the *Add or Remove Snap-ins* dialog box opens, double-click Certificates.
4. On the *Certificates snap-in* dialog box, click My user account. Click Finish.
5. Expand the Certificates-Current User, expand Personal, and click Certificates.
6. Right-click the Certificates folder, click All Tasks, and click Request NewCertificate.
7. When the *Certificate Enrollment wizard* starts, click Next.
8. On the *Certificate Enrollment Policy* page, *Active Directory Enrollment Policy* is already selected. Click Next.
9. Click to select Corporate User Certificate and then click Enroll.
10. After the certificate has been installed, click Finish.

USING CA WEB ENROLLMENT

The ***CA Web enrollment*** uses a website on a CA to obtain certificates. The website uses Internet Information Server (IIS), and the AD CS web enrollment role has been installed and configured. The URL to make a request is `https://<servername>/certsrv`. Similar to the manual enrollment, CA Web enrollment is used on devices that do not support autoenrollment, or you do not want to wait for autoenrollment to be applied.

REQUEST A CERTIFICATE USING WEB ENROLLMENT

GET READY. To request a certificate using web enrollment, perform the following steps:

1. Open Internet Explorer and open the following URL:

   `https://<servername>/certsrv`

   For example, if the CA is RWDC01, you would open `http://rwdc01/certsrv`.
2. Click Request a certificate.
3. On the *Request a Certificate* page, click Advanced certificate request.
4. On the *Advanced Certificate Request*, click Create and submit a request to this CA. If you are asked to allow a web site to perform digital certificate operation on your behalf, click Yes.
5. On the *Advanced Certificate Request* page, specify the certificate template that you want to use. Click Submit. If you are asked to allow a web site to perform digital certificate operation on your behalf, click Yes.
6. On the *Certificate issued* page, click Install this certificate.
7. When the certificate has been installed, close *Internet Explorer*.

ENROLLING USING ENROLLMENT AGENTS

When you use ***enrollment on behalf (enrollment agent)***, the CA administrator creates an enrollment agent account for the user. The user with enrollment agent rights can then enroll for certificates on behalf of other users such as when the administrator needs to preload logon certificates of new employees' smart cards. The ***restricted enrollment agent*** allows you to limit the permissions for users (usually administrators and help desk personnel) who are designated as enrollment agents, and to enroll for smart card certificates on behalf of other users.

ENABLE ENROLLMENT AGENTS

GET READY. To enable enrollment agents, perform the following steps:

1. Be sure you are logged in as an administrator. Using Server Manager, open Certification Authority.
2. When the *certsrv* console opens, expand the CA, right-click Certificate Templates, and then click Manage.
3. When the *Certificate Templates* console opens, double-click Enrollment Agent.
4. Click the Security tab, and then click Add.
5. In the *Select Users, Computers, Service Accounts, or Groups* window, type the user that you want to add (such as John Smith), click Check Names, and then click OK.
6. On the *Security* tab, click the user you just added, select Allow for Read and Enroll permissions, and then click OK.
7. Close the *Certificate Templates* Console.
8. In the *certsrv* console, right-click Certificate Templates, point to New, and then click Certificate Template to Issue.
9. In the list of templates, click Enrollment Agent, and then click OK.
10. Switch to Server01, and log on as Contoso\JSmith with the password Password01.
11. Open a command prompt window and at a command prompt, type mmc.exe, and then press Enter.
12. In *Console1*, click File, and then click Add/Remove Snap-in.
13. Click Certificates, and then click Add.
14. With My user account selected, click Finish.
15. Click OK to close *Add or Remove Snap-ins*.
16. Expand Certificates – Current User, right-click Personal, click Certificates, right-click Certificates, point to All Tasks, and then click Request New Certificate.
17. When the *Certificate Enrollment Wizard* starts, click Next.
18. On the Select *Certificate Enrollment Policy* page, click Next.
19. On the *Request Certificates* page, select Enrollment Agent, and then click Enroll.
20. When the certificate is installed, click Finish.
21. Go back to the CA server.
22. In the *Certification Authority* console, right-click the CA, and then click Properties.
23. Click the Enrollment Agents tab.
24. Click Restrict enrollment agents.
25. When a warning states that restrictions on delegated enrollment agents can be enforced only on Windows Server 2008 CAs or later, click OK.
26. In the *Enrollment agents* section, click Add.
27. In the *Select User, Computer or Group* field, type JSmith, click Check Names, and then click OK.
28. Click Everyone, and then click Remove.
29. In the *certificate templates* section, click Add.
30. In the list of templates, click Corporate User Certificate, and then click OK.
31. In the *Certificate Templates* section, click <All>, and then click Remove.

32. In the *Permission* section, click Add.
33. In the *Select User, Computer or Group* field, type the name of the group that you want to restrict enrollment agents, click Check Names, and then click OK.
34. In the *Permission* section, click Everyone, and then click Remove.
35. Click OK to close the *Properties* dialog box.

USING AUTOENROLLMENT

Most certificates will be assigned through ***autoenrollment***, which are deployed using group policies, specifically the *Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Services Client – Auto-Enrollment* and *User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Services Client – Auto-Enrollment*. However, autoenrollment can be applied only to enterprise CA (not standalone CA), and you have to deploy schema template version 2 or higher. In addition, the user needs Read, Enroll, and Autoenroll permissions for the certificate to deployed. Certificates installed with Autoenroll are shown later in the lesson.

Managing Certificate Renewal

Every certificate has a validity period and a finite life. At the end of the validity period, the certificate is no longer considered acceptable, and the certificate will have to be renewed. Of course, it is always best to renew the certificate before the certificate actually expires.

You can renew certificates in much the same way as you request certificates. For example, you can use the Certificates console to renew a certificate or you can configure the GPO that assigned the certificate to automatically renew the certificate.

When you renew the certificate, you can renew with different keys or with the same keys. You can use the same key if the key is long enough and the key has not been in use too long where it could be cracked using trial and error.

RENEW A CERTIFICATE USING THE CERTIFICATES CONSOLE

GET READY. To renew a certificate using the Certificates console, perform the following steps:

1. Click the Start menu, type mmc.exe, and press the Enter key.
2. When the console opens, click File > Add/Remove snap-in.
3. When the *Add or Remove Snap-ins* dialog box opens, double-click Certificates.
4. On the Certificates snap-in dialog box, click My user account. Click Finish.
5. Expand the Certificates-Current User, expand Personal, and click Certificates.
6. If you want to use the new key, click All Tasks, and click Renew Certificate with new Key. If you want to use the same key, click All Tasks, Advanced Operations, and click Renew This Certificate with the Same key.
7. When the *Certificate Enrollment wizard* opens, click Next.
8. On the *Request Certificates* page, click Enroll.
9. When the certificate is installed, click Finish.

Managing Certificate Enrollment and Renewal Using Group Policies

As mentioned previously, you can use a group policy object (GPO) to perform autoenrollment of certificates and the renewal of certificates. Remember that autoenrollment can be used only to enterprise CA, and when you have been deploying schema template version 2 or higher. In addition, the user needs Enroll and Autoenroll permissions for the certificate to be deployed.

You can use the Default Domain Policy to install certificates for users and computers. However, for more control, you can use a new GPO. For example, with a different GPO, you can assign to specific OUs and use filtering.

INSTALL A USER CERTIFICATE USING AUTOENROLL

GET READY. To install a user certificate using autoenroll, perform the following steps:

1. Using Server Manager, open Group Policy Management.
2. Expand Forest: Contoso.com, expand Domains, expand Contoso.com, right-click Default Domain Policy, and then click Edit.
3. When the *Group Policy Management Editor* opens, expand User Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then click to highlight Public Key Policies.
4. In the right pane, double-click Certificate Services Client – Auto-Enrollment.
5. In the *Configuration Model* drop-down list box, click Enabled, as shown in Figure 20-4.

TAKE NOTE*

If you want to install a computer certificate, you will navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\.

Figure 20-4

Configuring the Auto-Enrollment Policy

6. Click to select the Renew expired certificates, update pending certificates, and remove revoked certificates option.
7. Click to select the Update certificates that use certificate templates option.
8. Click OK to close the *Properties* dialog box.
9. In the right pane, double-click the Certificate Services Client – Certificate Enrollment Policy object.
10. On the *Enrollment Policy* tab, set the *Configuration Model* to Enabled, and ensure that the certificate enrollment policy list displays the *Active Directory Enrollment Policy*.
11. Click OK to close the dialog box.
12. Close the *Group Policy Management Editor* and *Group Policy Management* console.

By default, group policy is applied when you restart computers, or at logon for users. In addition, group policies are refreshed every 90 minutes for domain members. If a certificate requires user interaction to complete the request, a pop-up window appears approximately 60 seconds after the user logs on. However, most certificates are installed without the user knowing enrollment is taking place. If you don't want to wait for the certificate to be applied, you can execute the `gpupdate /force` to refresh group policies.

Configuring and Managing Key Archival and Recovery

Because certificates often provide keys to the kingdom, you do not want to lose the keys. Therefore, you need to provide key archival and recovery when needed. To recover lost keys, you use a key archival and recovery agent. You can also use automatic or manual key archival and key recovery methods to ensure that you can gain access to data in the event that your keys are lost. It should also be emphasized that when restoring a key, the process does not provide data recovery. The restored key provides the ability to read a restored file but you need to use another mechanism to actually back up the encrypted data, such as Windows Server Backup.

The CSP encrypts a private key and stores the encrypted private key on the local profile and registry. If you lose a key, if the user profile gets deleted or corrupted, the operating system is reinstalled, the hard drive is rebuilt, the disk becomes corrupted, or the computer is stolen, you will also lose the encrypted private key.

To recover private keys, you need to archive (or back them up). Then you you use a ***Key Recovery Agent (KRA)***, which is a designated user who is able to retrieve the original certificate, private key, and public key that was used to encrypt the data, from the CA database. Similar to setting up an EFS recovery agent, you can apply a key archival in a version 2 certificate template, which then makes the CA store the subject's private key in the CA database as certificates are requested. Then during the key recovery process, the KRA retrieves the encrypted file that contains the certificate and private key from the CA database, and returns the certificate and private key to the user.

When you have a configured CA to issue a KRA certificate, any user with Read and Enroll permission on the KRA certificate template can enroll and become a KRA. As a result, Domain Admins and Enterprise Admins receive permission by default. Of course, you should assign the KRA certificate to trusted users only. The KRA's recovery key is securely stored and the keys are in a separate physical secure location.

To perform key archival, you must perform the following:

1. Configure the KRA certificate template.
2. Configure Certificate Managers.
3. Enable KRA.
4. Configure user templates.

CONFIGURE THE KRA CERTIFICATE TEMPLATE

GET READY. To configure the KRA certificate template, perform the following steps:

1. Using the Server Manager, open Certification Authority.
2. In the Certification Authority console, expand the CA node, right-click the Certificates Templates folder, and then click Manage.
3. In the Details pane, right-click the Key Recovery Agent certificate, and then click Properties.
4. In the *Key Recovery Agent Properties* dialog box, click the Issuance Requirements tab.
5. Clear the CA certificate manager approval check box.
6. Close the *Certificate Templates* console.
7. In the *Certification Authority* console, right-click Certificate Templates, click New, and then click Certificate Template to Issue.
8. In the *Enable Certificate Templates* dialog box, select the Key Recovery Agent template, and then click OK.

CONFIGURE CERTIFICATE MANAGERS

GET READY. To configure the certificate managers, perform the following steps:

1. Click the Start menu, type mmc.exe, and press the Enter key.
2. When the console opens, click File > Add/Remove Snap-in.
3. In the *Add or Remove Snap-ins* dialog box, click Certificates, and then click Add.
4. In the *Certificates snap-in* dialog box, click My user account, click Finish, and then click OK.
5. Expand the Certificates - Current User node, right-click Personal, click All Tasks, and then click Request New Certificate.
6. When the *Certificate Enrollment Wizard* opens, click Next.
7. On the *Select Certificate Enrollment Policy* page, click Next.
8. On the *Request Certificates* page, select the Key Recovery Agent check box. Click Enroll, and then click Finish.
9. Close the console.

ENABLE KRA

GET READY. To enable KRA, perform the following steps:

1. If the Certification Authority console is not open, open Certification Authority.
2. Right-click the CA, and click Properties.
3. In the CA *Properties* dialog box, click the Recovery Agents tab, and then select Archive the key.
4. Under *Key recovery agent certificates*, click Add.

5. In the *Key Recovery Agent Selection* dialog box, click the certificate that is for *Key Recovery Agent purpose* (as verified by using the *Click here to view certificate properties* option). It will most likely be last on the list. Then click OK two times.
6. When prompted to restart the CA, click Yes.

CONFIGURE THE USER TEMPLATES

GET READY. To configure the user template, perform the following steps:

1. If the *Certification Authority* console is not open, using the Server Manager, open Certification Authority.
2. Right-click the Certificates Templates folder, and then click Manage.
3. In the *Certificate Templates* console, right-click the User certificate, and then click Duplicate Template.
4. In the *Properties of New Template* dialog box, on the General tab, in the *Template display name* box, type Archive User.
5. On the Request Handling tab, select the Archive subject's encryption private key check box. When it says that there are no certification authorities currently issuing certificates based on this template, click OK.
6. Click the Subject Name tab, clear the E-mail name and Include e-mail name in subject name check boxes, and then click OK.
7. Close the Certificate Templates console.
8. In the *Certification Authority* console, right-click the Certificates Templates folder, click New, and then click Certificate Template to Issue.
9. When the *Enable Certificate Templates* dialog box opens, click the Archive User template, and then click OK.
10. Close the *Certification Authority* console.

When you need to recover a certificate key, you will then perform the following:

1. Find the certificate and its serial number.
2. Retrieve the PKCS #7 BLOB from the database.
3. Retrieve the BLOB file and convert the file to a PKCS #12 (.pfx).
4. Import the certificate where needed.

RECOVER A CERTIFICATE

GET READY. To recover a certificate, perform the following steps:

1. On a server, such as Server01, login as a user account such as JSmith.
2. Click the Start menu, type mmc.exe, and press the Enter key.
3. In the *Console1* console, click File, and then click Add/Remove Snap-in.
4. When the *Add or Remove Snap-ins* dialog box opens, click Certificates, and then click Add. Click OK.
5. Expand the Certificates - Current User node, right-click Personal, click All Tasks, and then click Request New Certificate.
6. When the *Certificate Enrollment Wizard* opens, click Next.
7. Click Next.

8. On the *Request Certificate* page, click to select the Archive User check box, click Enroll, and then click Finish.
9. In the *Personal\Certificates* folder, delete the new certificate that you just added that is based on the Archive User certificate template.
10. Go to the CA server and open the *Certification Authority* console.
11. Expand the CA and click Issued Certificates.
12. In the details pane, double-click a certificate with the name and with the *Certificate Template name of Archive User*.
13. In the *Certificate* dialog box, click the Details tab.
14. Highlight the serial number, right-click the highlighted serial number, and copy the serial number to the Clipboard by pressing Ctrl+C.
15. Open Windows PowerShell console from task bar.
16. In the Windows PowerShell console window that appears, type the following command (where <serial number> is the serial number that you copied), and then press Enter:

    ```
    certutil -getkey <serial number> c:\outputblob
    ```

    If you paste the serial number from Notepad, remove spaces between numbers.
17. To convert the outputblob file into a pfx file, execute the following command:

    ```
    Certutil -recoverkey c:\outputblob c:\ jsmith.pfx
    ```
18. When prompted for a password, type Password01 in the *password*, and *confirm the password* text boxes.
19. Close the *Windows PowerShell* window.

The pfx file is the certificate file that contains the public and private keys. It can be copied to whatever computer the user is using and the certificate can be imported for the user.

■ Business Case Scenarios

Scenario 20-1: Deploying Digital Certificates

You are an administrator for the Contoso Corporation. You want to implement a VPN that requires all users who want to connect to the corporation using a VPN client to have the IPsec digital certificate. Therefore, you want to deploy the digital certificate to all users in your corporation. What do you need to do to make this happen?

Scenario 20-2: Recovering a Digital Certificate

You are an administrator for the Contoso Corporation. Because the certificates are an essential part of the security infrastructure, you need to ensure that all certificates can be recovered if a system needs to be replaced or if a certificate becomes lost. What do you need to do?

21 LESSON

Installing and Configuring Active Directory Rights Management Services

Understanding Active Directory Rights Management

THE BOTTOM LINE

Active Directory Rights Management Services (AD RMS) is technology used to provide an extra level of security to documents such as email and Microsoft Office documents by using encryption to limit who can access a document or web page and what can be done with a document or web page. For example, you can limit if a document or web page can be printed, copied, edited, forwarded, or deleted. RMS helps contain confidential information so that it stays within the organization and helps limit who can access the data.

Basic security mechanisms included with Windows are rights and permissions. ***Rights*** specify what a user or group can do on a system. For example, backup operators can back up files even if the user or group does not have permissions to the file or folder. Rights also define who can shut down or reboot a computer, who can logon to a computer, and so on. Rights are defined using Group Policy Objects (GPOs).

Permissions specify what a user or group can do with an object. For example, NTFS permissions are used to specify who can access and read a file, who can modify a file, who can delete a file, and who can manage the file.

However while rights and permissions are powerful tools, they do have their limitations. For example, anyone who can access and read a file protected with NTFS can copy the file to a USB drive or other storage device, email the file, or print the file, allowing a user to easily steal or copy confidential information.

AD RMS is an information protection technology is used to minimize unauthorized transmission of data or data leakage, specifically with Microsoft products and operating systems including Microsoft Exchange, Microsoft SharePoint, and the Microsoft Office suite.

Understanding the Rights Management Processes

After the AD RMS server is installed and configured and the clients are configured to use the AD RMS server, when accessing secure documents, the decryption of a document occurs transparently. In addition, when using applications that are aware of AD RMS, it is quite easy to secure a document or email.

The AD RMS infrastructure has the following components:

- ***AD RMS Server:*** A Windows server that is a member of an Active Directory Domain Services (AD DS) domain. When you install AD RMS servers, the location of the server is published to AD DS to a location known as the service connection point. Because RMS can be an important component when securing documents, AD RMS might deploy AD RMS with high availability using clustering.
- ***AD RMS client:*** Computers with the AD RMS client. Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 operating systems have the client built-in. The client for Windows XP, Windows Server 2003, and Windows Server 2003 R2 can be downloaded and installed. Computers that are members of the domain query AD DS for the service connection point to determine the location of AD RMS services.
- ***AD RMS Enabled Applications:*** An application that allows users to create and consume AD RMS-protected content. Examples of AD RMS clients include Microsoft Word, Microsoft Excel, and Microsoft Outlook.
- ***AD RMS root certification cluster:*** The first AD RMS server that you deploy in a forest. It manages all licensing and certification traffic for the domain in which it is installed. The configuration information is installed in a Microsoft SQL database. AD RMS root certification clusters are typically found in large branch offices to distribute licenses that are used in content consumption and publishing.
- ***Licensing-only cluster:*** An optional component that is not part of the root cluster. However, it relies on the root cluster for certification and other services. It provides both publishing licenses and use licenses to users. It is typically used when supporting unique right management requirements of a department or when supporting rights management of external business partners.

For AD RMS to operate, it uses various certificates and licenses to encrypt and limit access to the files or emails.

The following shows how a document is protected and accessed using AD RMS:

1. When an author configures rights protection for information the first time, he or she receives a client licensor certificate from the AD RMS server.
2. When the author defines a collection of usage rights and usage of the file, the application encrypts the file with a symmetric key.
3. This symmetric key is encrypted to the public key of the AD RMS server that is used by the author.
4. When a recipient opens the file using an AD RMS application or browser, if the recipient does not have an account certificate on the current host, one will be issued to the user.
5. When the user has the account certificate, the application or browser transmits a request to the author's AD RMS server for a Use License.
6. The AD RMS server determines whether the recipient is authorized. If the recipient is authorized, the AD RMS server issues a Use License.

7. The AD RMS server decrypts the symmetric key that was encrypted in step 3, using its private key.
8. The AD RMS server re-encrypts the symmetric key using the recipient's public key and adds the encrypted session key to the Use License.

If an application or browser does not support AD RMS, the user will not be able to open RMS-protected content.

Installing a Licensing or Certificate AD RMS Server

An AD RMS deployment consists of one or more servers known as a cluster. Additional servers can be added for scalability if you use a dedicated SQL server. When you deploy AD RMS in a single forest, you will have a single AD RMS cluster. If you have multiple forests, each forest will have its own AD RMS root cluster. Only one root cluster can exist in an AD DS forest.

Although you can use the Windows Internal Database for a test environment, you should use a dedicated SQL server, particularly if you need to have more than one server. You should not deploy AD RMS on a domain controller. If you do, the service account that AD RMS uses must be a member of the Domain Admins group.

CREATE AD RMS SERVICE ACCOUNTS AND GROUP AND CREATE A DNS CNAME FOR AD RMS

GET READY. To create an AD RMS service account and group and to create a DNS CNAME for an AD RMS server, perform the following steps:

1. On a domain controller, using Server Manager, click Tools > Active Directory Administrative Center.
2. On the *Active Directory Administrative Center*, right-click Contoso (local), click New, and then click Organizational Unit.
3. When the *Create Organizational Unit* dialog box opens, type Service Accounts in the *Name* text box, and click OK.
4. Right-click the Service Accounts OU, click New, and then click User.
5. When the *Create User* dialog box opens, enter the following:

   First name: ADRMS_SVC

   User UPN logon: ADRMS_SVC

   Password: Password01

   Password options: Other password options

   Password never expires: Enabled

   User cannot change password: Enabled
6. Click OK to close the *Create User* dialog box.
7. Right-click Users organization unit, click New, and then click Group.
8. When the *Create Group* dialog box opens, type the following:

   Group name: RMS Users

   E-mail: RMSUsers@Contoso.com
9. Click Members.
10. Click Add. Type John Smith and click OK.
11. Click OK to close the *Create Group* dialog box.

12. Close Active Directory Administrative Center.
13. Using Server Manager, click Tools > DNS.
14. In *DNS Manager*, expand the DNS server Forward Lookup Zones and click contoso.com.
15. Right-click the contoso.com domain and click New Alias (CNAME).
16. In the *New Resource Record* dialog box, enter the following:

    Alias name: ADRMS

    Fully qualified domain name (FQDN) for target host: server02.contoso.com
17. Click OK to close the *New Resource Record* dialog box.
18. Close *DNS Manager*.

INSTALL AD RMS

GET READY. To install AD RMS, perform the following steps:

1. On Server02, using Server Manager, click Manage, and then click Add Roles and Features.
2. When the *Add Roles and Features Wizard* opens, click Next.
3. On the *Select installation type* page, click Next.
4. On the *Select destination server* page, click Next.
5. Click to select Active Directory Rights Management Services. When you are asked to add features, click Add Features.
6. Back at the *Select server roles* page, click Next.
7. At the *Select features* page, click Next.
8. On the *Active Directory Rights Management Services* page, click Next.
9. When the *Role Services* page appears, if Active Directory Rights Management Server is already selected, click Next.
10. On the *Confirm installation selections* page, click Install.
11. When the installation is complete, click Close.
12. Using Server Manager, click the AD RMS node.
13. At the top of the *Servers* section, next to *Configuration required for Active Directory Rights Management Services at SERVER02* (as shown in Figure 21-1), click More.

Figure 21-1

Viewing the AD RMS node in Server Manager

14. When the *All Servers Task Details* dialog box page opens, click Perform additional configuration.
15. When the *AD RMS Configuration wizard* starts, click Next.
16. On the *AD RMS Cluster* page, if Create a new AD RMS root cluster is already selected, click Next.
17. On the *Configuration Database Server* page, click Use Windows Internal Database on this server. Click Next.
18. On the *Server Account* page, click Specify.
19. In the *Windows Security* dialog box, enter the following details, click OK, and then click Next:
    - **Username:** ADRMS_SVC
    - **Password:** Pa$$w0rd
20. On the *Cryptographic Mode* page, click Cryptographic Mode 2, and then click Next.
21. On the *Cluster Key Storage* page, click Use AD RMS centrally managed key storage, and then click Next.
22. On the *Cluster Key Password* page, enter the password Password01 in the *Password* and *Confirm Password* dialog box, and then click Next.

23. On the *Cluster Web Site* page, verify that Default Web Site is selected, and then click Next.
24. On the *Cluster Address* page, provide the following information, and then click Next:
    - **Connection Type:** Use an unencrypted connection (http://)
    - **Fully Qualified Domain Name:** adrms.contoso.com
    - **Port:** 80
25. On the *Licensor Certificate* page, type Contoso AD RMS, and then click Next.
26. On the *SCP Registration* page, click Register the SCP now, and then click Next.
27. On the *Confirmation* page, click Install.
28. When the installation is successful, click Close.
29. To manage AD RMS, you must sign out of Windows. Therefore, click Start > Administrator, and then click Sign Out.

The primary tool to manage AD RMS is using the Active Directory Rights Management Services console (see Figure 21-2). When you open the console, you can see the cluster name, the intranet and extranet cluster URLs, and the location of the databases.

Figure 21-2

Looking at the Active Directory Rights Management Services console

When AD RMS is deployed, the following administration groups are created:

- **AD RMS Enterprise Administrators:** Have access to all features in the AD RMS console. During installation of AD RMS, the installing user account is automatically added to this group.
- **AD RMS Template Administrators:** Can only access rights policy template administration features in the AD RMS console.
- **AD RMS Auditors:** Access the reports feature in the AD RMS console.
- **AD RMS Service Group:** Act as the AD RMS service account. During the installation of AD RMS, the user account designated as the service account is automatically added to this group.

To change the AD RMS service account or the cluster key password, you need to be a member of the AD RMS Enterprise Administrators group, and a member of the local administrators group on the server.

Managing AD RMS Service Connection Point

The Active Directory Rights Management Services (AD RMS) ***service connection point (SCP)*** is an object in Active Directory that holds the web address of the AD RMS certification cluster. It was defined during the installation of AD RMS. AD RMS-enabled applications use the SCP to find the AD RMS service.

Only one SCP for AD RMS can exist in your Active Directory forest. An SCP can be viewed using ADSI Edit or LDP. To view the SCP, connect to the configuration container in ADSI Edit and navigate the following nodes:

```
CN=Configuration [server name], CN=Services,
CN=RightsManagementServices, CN=SCP
```

The Certification links show in the Cluster Details of the Active Directory Rights Management Services console.

If you need to remove a previous SCP so that you can install a new AD RMS, you can remove an SCP by using the ADScpRegister.exe tool included in the RMS Administration Toolkit, which can be downloaded using the Microsoft Download Center's website. You can also use ASDI Edit.

To register the SCP, you must be a member of the local AD RMS Enterprise Administrators group and the Active Directory Domain Services (AD DS) Enterprise Admins group.

CHANGE THE SCP

GET READY. To change the SCP, perform the following steps:

1. Using the Server Manager, click Tools > Active Directory Rights Management Services.
2. When the *Active Directory Rights Management Services* console opens, right-click the server, and then click Properties.
3. When the *Properties* dialog box open, click the SCP tab.
4. On the *SCP* tab (see Figure 21-3), click to select the Change SCP option.

Figure 21-3

Changing SCP

5. Click to select the Set SCP to current certification cluster, and type the new URL.
6. Click OK to close the *Properties* dialog box.

AD DS clients automatically get the SCP from Active Directory. If you have a client computer that is not part of the Active Directory forest, you must use registry keys to point to the AD RMS cluster. These registry keys are created in:

```
HKEY_Local_Machine\Software\Microsoft\MSDRM\ServiceLocation\Activation
```

The Activation key is a string, which would have the value of:

```
http(s)://<your_cluster>/wmcs/certification
```

Managing RMS Templates

Rights policy templates, also known as RMS templates, are used to enforce the rights that a user or group has on rights-protected content. They allow you to standardize the implementing AD RMS policies across the organization. One template may be used on documents to grant view-only rights, which block the ability to edit, save, or print. If used with Microsoft Exchange Server, you can configure the template to block the ability to forward or reply to a message.

Rights policy templates are created using the Active Directory Rights Management Services console. The templates are stored in the AD RMS database, but can also be stored in XML format. When a document is protected, the document author can choose to protect content by applying the existing template. When protected content is accessed, the AD RMS-aware application checks with AD RMS to verify that it has the most recent version of the template.

AD RMS templates support the following rights:

- **Full Control:** Gives a user full control over an AD RMS–protected document including the ability to give other people access to the document.
- **View:** Gives a user the ability to view an AD RMS–protected document.
- **Edit:** Allows a user to modify an AD RMS–protected document.
- **Save:** Allows a user to use the Save function with an AD RMS–protected document.
- **Export (Save as):** Allows a user to use the Save As function with an AD RMS–protected document.
- **Print:** Allows an AD RMS–protected document to be printed.
- **Forward:** Used with Exchange Server, allows the recipient of an AD RMS–protected message to forward that message.
- **Reply:** Used with Exchange Server, allows the recipient of an AD RMS–protected message to reply to that message.
- **Reply All:** Used with Exchange Server, allows the recipient of an AD RMS–protected message to use the Reply All function to reply to that message.
- **Extract:** Allows the user to copy data from the file. If this right is not granted, the user cannot copy data from the file.
- **Allow Macros:** Allow the user to utilize macros.
- **View Rights:** Allow the user to view assigned rights.
- **Edit Rights:** Allow the user to modify the assigned rights.

Different from NTFS permissions, AD RMS rights can only be granted and cannot be explicitly denied. If a user has not been assigned rights to the document or email, users will automatically be denied to the document or email.

AD RMS templates can also be used to configure documents with the following properties:

- **Content expiration:** Determines when the content expires. The options are Never, Expires on a particular date, or Expires after a set number of days.
- **Use license expiration:** Determines the time interval in which the use license expires. When the use license expires, a new one needs to be acquired.
- **Enable users to view protected content using a browser add-on:** Allows content to be viewed using a browser add-on, which allows a user to not have an AD RMS–aware application to access a document.
- **Require a new use license each time content is consumed:** This option also disables client-side caching, which means that the document cannot be accessed when the computer is offline.
- **Revocation policies:** Allows the use of a revocation list so that you can revoke rights to consume content after the rights have been granted. By default, the revocation list is checked once every 24 hours.

CREATE A DISTRIBUTED RIGHTS POLICY TEMPLATE

GET READY. To create a distributed rights policy template, perform the following steps:

1. Using the Server Manager, open the Active Directory Rights Management Services console.
2. Expand the cluster, and click Rights Policy Templates.
3. In the *Actions* pane, click Create Distributed Rights Policy Template.
4. When the *Create Distributed Rights Policy Template Wizard* starts, click Add.

5. On the *Add New Template Identification Information* page, enter the following information, and then click Add:
   - **Language:** English (United States)
   - **Name:** Read-only template
   - **Description:** Read only access. No copy or print
6. Click Next.
7. On the *Add User Rights* page, click Add.
8. On the Add User or Group dialog box, enter managers@contoso.com, and then click OK.
9. When *managers@contoso.com* is selected, under the *Rights* section, click the View right. The Grant owner (author) full control right with no expiration is selected. Click Next.
10. On the *Specify Expiration Policy* page, choose the following settings and then click Next:
    - Content Expiration: Expires after the following duration (days): 7
    - Use license expiration: Expires after the following duration (days): 7
11. On the *Specify Extended Policy* page, click Require a new use license every time content is consumed (disable client-side caching), and then click Next.
12. On the *Specify Revocation Policy* page, click Finish.

After an AD RMS policy template is applied to a document, when the template is updated, the protected documents using the template are also modified. Template changes occur when the EUL is acquired. If EULs are configured not to expire and the user who is accessing the document already has a license, then the user may not receive the updated template.

It is recommended that you do not delete templates. If you do delete a template, any document that uses the template will become inaccessible to everyone except the members of the super users group. Instead, it is recommended to archive templates.

You can view the rights associated with a template by selecting the template in the Active Directory Rights Management Services console, and then in the Actions menu, clicking *View Rights Summary*.

In some instances, you may have a need for users to access RMS-protected content when the user is offline and not have access to the RMS server. You can configure computers to acquire and store published rights policy templates automatically, so that they are available offline. To enable this feature, computers must run the following Windows operating systems:

- Windows Vista SP1 or newer
- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Next, you need to configure a local copy of the available rights policy templates. To accomplish this, you need to perform the following:

1. In Task Scheduler, enable the AD RMS Rights Policy Template Management (Automated) Scheduled Task.

2. Edit the following registry key:

   `HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM to %LocalAppData%\Microsoft\DRM\Templates`
3. Create a shared folder to store the templates.
4. Open the Active Directory Rights Management Services console, right-click the *Rights Policy Templates* node, and then click *Properties* to specify the location of the shared folder to which the templates will be published.

As the scheduled task executes, the AD RMS client polls the AD RMS cluster for new templates and updates the existing templates.

Configuring Exclusion Policies

Exclusion policies allow you to specify which user accounts, client software, and applications are automatically denied access to AD RMS. They also allow you to specify a minimum version of the AD RMS client software.

The User Exclusion policy allows you to configure AD RMS so that specific user accounts cannot obtain Use Licenses. User Exclusion is disabled by default. After you enable User Exclusion, you can specify the RACs based on the user's email address (Active Directory Domain Services accounts) or public key strings (for external users).

WARNING The Application Exclusion can be circumvented by renaming the executable file.

Application Exclusion allows you to block specific applications, such as Office PowerPoint, from creating or consuming AD RMS–protected content. Application Exclusion is disabled by default. After enabling application exclusion information, you can add an exclusion, where you specify the name of the executable file and the minimum and maximum version of the executable.

The Lockbox Exclusion allows you to exclude older AD RMS clients. Lockbox version exclusion is disabled by default. After you have enabled Lockbox version exclusion, you must specify the minimum lockbox version that can be used with the AD RMS cluster.

ENABLE AND CONFIGURE APPLICATION EXCLUSION

GET READY. To enable and configure application exclusion, perform the following steps:

1. Using the Server Manager, open the Active Directory Rights Management Services console.
2. Expand the cluster, and click Exclusion Policies node.
3. Click Manage application exclusion list.
4. In the *Actions* pane, click Enable Application Exclusion.
5. In the *Actions* pane, click Exclude Application.
6. In the *Exclude Application* dialog box, enter the following information, and then click Finish:
   - Application File name: Powerpnt.exe
   - Minimum version: 14.0.0.0
   - Maximum version: 16.0.0.0
7. To close the Exclude Application dialog box, click Finish.

Backing Up and Restoring AD RMS

As with any recovery from a disaster, the best method of recovery for AD RMS is to have a back up of the AD RMS environment from which you can restore. If the RMS server and any remote database servers are a virtual machine, you can back up VMs using Windows Backup with Hyper-V. If not, you will have to back up all related machines using Windows Backup, including the system state and all databases.

In a worst-case scenario, if you have recreate the entire AD RMS system from scratch, you will need to back up the following three databases from the database server:

- **Configuration database:** Stores, shares, and retrieves all configuration data and other data that the service needs to manage account certification, licensing, and publishing services for a whole cluster.
- **Directory services database:** Contains information about users, identifiers (such as e-mail addresses), security ID (SID), group membership, and alternate identifiers.
- **Logging database:** The historical data about client activity and license acquisition.

To back up these databases, you can use Windows Backup (as explained in the 70-411 course) or you can use SQL Server Management Studio. If you lose the SQL server, you will just have to restore or rebuild the computer with the same name, install or restore the SQL server software, and then restore the AD RMS databases.

If you have to recreate a new AD RMS cluster, you will need to first delete the existing Service Connection Point from Active Directory using the Active Directory Sites and Services, specifically the Services\RightsManagementServices\SCP node. You will then install a new database server or provision a database server that will host the new AD RMS database. You can then install the new AD RMS cluster with the same AD RMS URL that points to the new AD RMS database. If necessary, you will finish by restoring the SQL databases from backup.

The AD RMS protected content will not typically be found on the AD RMS server. For all intents and purposes, you should regularly back up those folders that contain AD RMS protected content for any other account that can open and read the files. If the content is missing, you can restore the files from backup. In some situations, you might need to use a super user to back up protected individual files or emails within Microsoft SharePoint or Exchange.

■ Business Case Scenarios

Scenario 21-1: Protecting Confidential Information

You are the administrator for the Contoso Corporation. The Contoso Corporation has some design documents that must not fall into the hands of competitors. You want to ensure that the documents cannot be forwarded to anyone outside of the company. What should you do?

Scenario 21-2: Recovering AD RMS

You are the administrator for the Contoso Corporation. Your AD RMS server crashed. You have a back up of the databases, but you do not have a back up of the AD RMS server. What should you do to restore everything back to the way it was?

Microsoft® Official Academic Course

Installing and Configuring Windows Server® 2012 R2 Exam 70-410

Craig Zacker

WILEY

Credits

VP & PUBLISHER	Don Fowley
EXECUTIVE EDITOR	John Kane
DIRECTOR OF SALES	Mitchell Beaton
EXECUTIVE MARKETING MANAGER	Chris Ruel
MICROSOFT PRODUCT MANAGER	Keith Loeber of Microsoft Learning
TECHNICAL EDITORS	Jeff T. Parker
	Kenneth Hess
	Brian Svidergol
EDITORIAL PROGRAM ASSISTANT	Allison Winkle
ASSISTANT MARKETING MANAGER	Debbie Martin
SENIOR PRODUCTION MANAGER	Janis Soo
CREATIVE DIRECTOR	Harry Nolan
COVER DESIGNER	Tom Nery
SENIOR PRODUCT DESIGNER	Thomas Kulesa
CONTENT EDITOR	Wendy Ashenberg
PRODUCTION EDITOR	Joyce Poh

This book was set in Garamond by Aptara, Inc. and printed and bound by Bind-Rite Robbinsville. The covers were printed by Bind-Rite Robbinsville.

Copyright © 2014 by John Wiley & Sons, Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc. 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, (201) 748-6011, fax (201) 748-6008. To order books or for customer service, please call 1-800-CALL WILEY (225-5945).

Microsoft, Active Directory, AppLocker, Bing, BitLocker, DreamSpark, Hyper-V, Internet Explorer, SQL Server, Visual Studio, Win32, Windows Azure, Windows, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

The 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, John Wiley & Sons, Inc., Microsoft Corporation, nor their resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

ISBN 978-1-118-88231-3

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

www.wiley.com/college/microsoft *or*
call the MOAC Toll-Free Number: 1+(888) 764-7001 (U.S. & Canada only)

Preface

Welcome to the Microsoft Official Academic Course (MOAC) program for becoming a Microsoft Certified Solutions Associate for Windows Server 2012 R2. MOAC represents the collaboration between Microsoft Learning and John Wiley & Sons, Inc. Microsoft and Wiley teamed up to produce a series of textbooks that deliver compelling and innovative teaching solutions to instructors and superior learning experiences for students. Infused and informed by in-depth knowledge from the creators of Windows Server 2012 R2, and crafted by a publisher known worldwide for the pedagogical quality of its products, these textbooks maximize skills transfer in minimum time. Students are challenged to reach their potential by using their new technical skills as highly productive members of the workforce.

Because this knowledgebase comes directly from Microsoft, the architect of Windows Server 2012 R2 and creator of the Microsoft Certified Solutions Associate exams, you are sure to receive the topical coverage that is most relevant to students' personal and professional success. Microsoft's direct participation not only assures you that MOAC textbook content is accurate and current, it also means that students will receive the best instruction possible to enable their success on certification exams and in the workplace.

■ The Microsoft Official Academic Course Program

The Microsoft Official Academic Course series is a complete program for instructors and institutions to prepare and deliver great courses on Microsoft software technologies. With MOAC, we recognize that because of the rapid pace of change in the technology and curriculum developed by Microsoft, there is an ongoing set of needs beyond classroom instruction tools for an instructor to be ready to teach the course. The MOAC program endeavors to provide solutions for all these needs in a systematic manner in order to ensure a successful and rewarding course experience for both instructor and student, including technical and curriculum training for instructor readiness with new software releases; the software itself for student use at home for building hands-on skills, assessment, and validation of skill development; and a great set of tools for delivering instruction in the classroom and lab. All are important to the smooth delivery of an interesting course on Microsoft software, and all are provided with the MOAC program.

Conventions and Features Used in This Book

This book uses particular fonts, symbols, and heading conventions to highlight important information or to call your attention to special steps.

Convention	Meaning
THE BOTTOM LINE	This feature provides a brief summary of the material to be covered in the section that follows.
WARNING	*Warning* points out instances when error or misuse could cause damage to the computer or network.
A ***shared printer*** can be used by many individuals on a network.	Key terms appear in bold italic.
`cd\windows\system32`	Commands that are to be typed are shown in a special font.
Click Install Now.	Any button on the screen you are supposed to click on or select will appear in blue.

Instructor Support Program

The Microsoft Official Academic Course programs are accompanied by a rich array of resources that incorporate the extensive textbook visuals to form a pedagogically cohesive package.

- The **Instructor's Guide** contains chapter summaries and lecture notes.
- The **Test Bank** contains hundreds of questions organized by lesson in multiple-choice, best answer, build list, and essay formats. A complete answer key is provided.
- **Lecture Presentation Slides.** A complete set of PowerPoint presentations is available to enhance classroom presentations. Tailored to the text's topical coverage, these presentations are designed to convey key Windows Server 2012 R2 concepts addressed in the text.
- **MOAC Labs Online.** MOAC Labs Online is a cloud-based environment that enables students to conduct exercises using real Microsoft products. These are not simulations but instead are live virtual machines in which faculty and students can perform activities as they would on a local machine. MOAC Labs Online relieves the need for lab setup, configuration, and most troubleshooting tasks. This represents an opportunity to lower costs, eliminate the hassle of lab setup, and support and improve student access and portability. Contact your Wiley rep about including MOAC Labs Online with your course offering.

About the Author

Craig Zacker is an instructor, writer, editor, and networker whose computing experience began in the days of teletypes and paper tape. After making the move from minicomputers to PCs, he worked as a network administrator and PC support technician while operating a freelance desktop publishing business. After earning a Master's Degree in English and American Literature from New York University, Craig worked extensively on the integration of Microsoft Windows operating systems into existing internetworks, supported fleets of Windows workstations, and was employed as a technical writer, content provider, and webmaster for the online services group of a large software company. Since devoting himself to writing and editing full-time, Craig has authored or contributed to dozens of books on operating systems, networking topics, and PC hardware. He has also published articles with top industry publications, developed online training courses for the various firms, and authored the following Microsoft Official Academic Course (MOAC), Academic Learning Series (ALS), and Self-Paced Training Kit titles:

MOAC: Installing and Configuring Windows Server 2012 (Exam 70-410)

MOAC: Windows Server 2008, Enterprise Administrator (Exam 70-647)

MOAC: Windows 7 Configuration (Exam 70-680)

MOAC: Windows Server Administrator (Exam 70-646)

MOAC: Configuring Windows Server 2008 Application Services (Exam 70-643)

MOAC: Configuring Microsoft Windows Vista (Exam 70-620)

MOAC: Implementing & Administering Security in a Windows Server 2003 Network (Exam 70-299)

MOAC: Managing & Maintaining a Microsoft Windows Server 2003 Environment (Exam 70-290)

ALS: Network+ Certification, Second, Third, and Fourth Editions

ALS: Planning & Maintaining a Windows Server 2003 Network Infrastructure (Exam 70-293)

ALS: Microsoft Windows 2000 Network Infrastructure Administration, Second Edition (2002)

MCSE Self-Paced Training Kit (Exam 70-293): Planning & Maintaining a Microsoft Windows Server 2003 Network Infrastructure (2003)

MCSA/MCSE Self-Paced Training Kit: Microsoft Windows 2000 Network Infrastructure Administration, Exam 70-216, Second Edition (2002)

MCSA Training Kit: Managing a Windows 2000 Network Environment (2002)

Network+ Certification Training Kit, First and Second Editions (2001)

Network+ Certification Readiness Review (2001)

Brief Contents

1 Installing Servers 1
2 Configuring Servers 18
3 Configuring Local Storage 32
4 Configuring File and Share Access 47
5 Configuring Print and Document Services 63
6 Configuring Servers for Remote Management 78
7 Creating and Configuring Virtual Machine Settings 88
8 Creating and Configuring Virtual Machine Storage 100
9 Creating and Configuring Virtual Networks 111
10 Configuring IPv4 and IPv6 Addressing 121
11 Deploying and Configuring the Dynamic Host Configuration Protocol (DHCP) Service 134
12 Deploying and Configuring the DNS Service 144
13 Installing Domain Controllers 159
14 Creating and Managing Active Directory Users and Computers 175
15 Creating and Managing Active Directory Groups and Organizational Units 185
16 Creating Group Policy Objects 197
17 Configuring Security Policies 207
18 Configuring Application Restriction Policies 223
19 Configuring Windows Firewall 232

Contents

Lesson 1: Installing Servers 1

Selecting a Windows Server 2012 R2 Edition 1
- Supporting Server Roles 2

Installing Windows Server 2012 R2 4
- System Requirements 4
- Performing a Clean Installation 5

Choosing Installation Options 7
- Using Server Core 8
- Using Features on Demand 10

Upgrading Servers 11
- Upgrade Paths 11
- Preparing to Upgrade 11
- Performing an Upgrade Installation 12

Migrating Roles 13
- Installing Windows Server Migration Tools 14
- Using Migration Guides 16

Business Case Scenarios 17

Lesson 2: Configuring Servers 18

Completing Post-Installation Tasks 18
- Using Command-Line Tools 18
- Converting Between GUI and Server Core 19
- Configuring NIC Teaming 20

Using Server Manager 24
- Adding Roles and Features 24
- Deploying Roles to VHDs 27
- Configuring Services 28

Delegating Server Administration 30

Using Windows PowerShell Desired State Configuration 30

Business Case Scenarios 31

Lesson 3: Configuring Local Storage 32

Planning Server Storage 32
- Determining the Number of Servers Needed 32
- Estimating Storage Requirements 33
- Using Storage Spaces 34

Understanding Windows Disk Settings 35
- Selecting a Partition Style 35
- Understanding Disk Types 36

Working with Disks 37
- Creating and Mounting VHDs 38
- Creating a Storage Pool 40
- Creating a Simple Volume 42
- Extending and Shrinking Volumes and Disks 44

Business Case Scenario 46

Lesson 4: Configuring File and Share Access 47

Creating Folder Shares 47

Assigning Permissions 50
- Understanding the Windows Permission Architecture 51
- Understanding Basic and Advanced Permissions 52
- Setting Share Permissions 53
- Understanding NTFS Authorization 55
- Assigning Basic NTFS Permissions 56

Configuring Volume Shadow Copies 58

Configuring NTFS Quotas 60

Configuring Work Folders 61

Business Case Scenarios 62

Lesson 5: Configuring Print and Document Services 63

Deploying a Print Server 63
Understanding the Windows Print Architecture 63
Sharing a Printer 64
Managing Printer Drivers 65
Using Remote Access Easy Print 66
Configuring Printer Security 67
Managing Printers 69
Using the Print and Document Services Role 72
Using the Print Management Console 74
Business Case Scenarios 77

Lesson 6: Configuring Servers for Remote Management 78

Using Server Manager for Remote Management 78
Adding Servers 79
Managing Non-Domain Joined Servers 81
Managing Windows Server 2012 R2 Servers 81
Managing Down-Level Servers 84
Working with Remote Servers 86
Business Case Scenarios 87

Lesson 7: Creating and Configuring Virtual Machine Settings 88

Virtualizing Servers 88
Virtualization Architectures 88
Installing Hyper-V 90
Using Hyper-V Manager 90
Creating a Virtual Machine 91
Creating Generation 1 and Generation 2 VMs 92
Configuring Guest Integration Services 92
Using Enhanced Session mode 94
Allocating Memory 95
Configuring Resource Metering 97
Using Remote FX 98
Business Case Scenarios 99

Lesson 8: Creating and Configuring Virtual Machine Storage 100

Working with Virtual Disks 100
Understanding Virtual Disk Formats 101
Creating Virtual Disks 102
Configuring Pass-Through Disks 104
Modifying Virtual Disks 105
Creating Checkpoints 106
Configuring Storage Quality of Service 107
Connecting to a SAN 107
Using Fibre Channel 109
Connecting Virtual Machines to a SAN 109
Business Case Scenarios 110

Lesson 9: Creating and Configuring Virtual Networks 111

Using Virtual Networking 111
Creating Virtual Switches 111
Creating Virtual Network Adapters 114
Configuring NIC Teaming in a Virtual Network Environment 118
Creating Virtual Network Configurations 119
Business Case Scenarios 120

Lesson 10: Configuring IPv4 and IPv6 Addressing 121

Understanding IPv4 Addressing 121
IPv4 Classful Addressing 121
Classless Inter-Domain Routing 122
IPv4 Subnetting 123
Supernetting 124
Assigning IPv4 Addresses 124
Understanding IPv6 Addressing 127
Introducing IPv6 127
IPv6 Address Types 127
Assigning IPv6 Addresses 128
Planning an IP Transition 129
Tunneling 130
Business Case Scenarios 133

Lesson 11: Deploying and Configuring the Dynamic Host Configuration Protocol (DHCP) Service 134

Understanding DHCP 134
Deploying a DHCP Server 135
Creating a Scope 136
Configuring DHCP Options 138
Creating a Reservation 139
Using PXE 139
Deploying a DHCP Relay Agent 140
Business Case Scenarios 143

Lesson 12: Deploying and Configuring the DNS Service 144

Understanding the DNS Architecture 144
Creating a DNS Standard 144
DNS Naming 145
Understanding the DNS Domain Hierarchy 146
Understanding DNS Communications 147
Comprehending DNS Server Caching 147
Using DNS Forwarders 149
Designing a DNS Deployment 149
Resolving Internet Names 150
Hosting Internet Domains 150
Creating Internet Domains 151
Deploying a DNS Server 151
Creating Zones 152
Creating Resource Records 154
Configuring DNS Server Settings 157
Business Case Scenarios 158

Lesson 13: Installing Domain Controllers 159

Introducing Active Directory 159
Understanding Active Directory Architecture 159
Deploying Active Directory Domain Services 162
Installing the Active Directory Domain Services Role 162
Creating a New Forest 163
Adding a Domain Controller to an Existing Domain 165
Installing AD DS on Server Core 168
Using Install from Media (IFM) 169
Upgrading Active Directory Domain Services 170
Deploying Active Directory IaaS on Windows Azure 171
Removing a Domain Controller 171
Configuring the Global Catalog 172
Troubleshooting DNS SRV Registration Failure 173
Business Case Scenarios 174

Lesson 14: Creating and Managing Active Directory Users and Computers 175

Creating User Objects 175
Creating Single Users 176
Creating User Templates 178
Creating Multiple Users 179
Creating Computer Objects 181
Managing Active Directory Objects 182
Joining Computers to a Domain 182
Managing Disabled Accounts 183
Business Case Scenarios 184

Lesson 15: Creating and Managing Active Directory Groups and Organizational Units 185

Working with Organizational Units 185
Creating OUs 185
Using OUs to Delegate Active Directory Management Tasks 187
Working with Groups 189
Working with Default Groups 190
Nesting Groups 190
Creating Groups 191
Managing Group Memberships 193
Converting Groups 194
Business Case Scenarios 195

Lesson 16: Creating Group Policy Objects 197

Introducing Group Policy 197
Understanding Group Policy Objects 198
Configuring a Central Store 199
Using the Group Policy Management Console 199
Creating and Linking Nonlocal GPOs 200
Using Security Filtering 201
Managing Starter GPOs 202
Configuring Group Policy Settings 203
Creating Multiple Local GPOs 203
Business Case Scenarios 205

Lesson 17: Configuring Security Policies 207

Configuring Security Policies Using Group Policy 207
Defining Local Policies 209
Using Security Templates 214
Configuring Local Users and Groups 216
Using the User Accounts Control Panel 217
Using the Local Users and Groups Snap-In 218
Configuring User Account Control 220
Configuring User Account Control Settings 221
Business Case Scenarios 222

Lesson 18: Configuring Application Restricted Policies 223

Installing Software with Group Policy 223
Configuring Software Restriction Policies 224
Enforcing Restrictions 224
Configuring Software Restriction Properties 225
Using AppLocker 227
Understanding Rule Types 227
Creating Rules Automatically 229
Creating Rules Manually 230
Business Case Scenarios 230

Lesson 19: Configuring Windows Firewall 232

Building a Firewall 232
Understanding Windows Firewall Settings 232
Using the Windows Firewall Control Panel 233
Allowing Applications 234
Using the Windows Firewall with Advanced Security Console 236
Configuring Profile Settings 236
Creating Rules 237
Importing and Exporting Rules 239
Creating Rules Using Group Policy 240
Creating Connection Security Rules 241
Business Case Scenarios 241

www.wiley.com/college/microsoft *or*
call the MOAC Toll-Free Number: 1+(888) 764-7001 (U.S. & Canada only)

Installing Servers

LESSON 1

Selecting a Windows Server 2012 R2 Edition

THE BOTTOM LINE Microsoft releases all its operating systems in multiple editions, which provides consumers with various price points and feature sets.

When planning a server deployment, you should choose the operating system edition based on multiple factors, including the following:

- The roles you intend the servers to perform
- The virtualization strategy you intent to implement
- The licensing strategy you plan to use

Compared with Windows Server 2008, Microsoft has simplified the process of selecting a Windows Server 2012 R2 edition by reducing the available products. As with Windows Server 2008 R2, Windows Server 2012 R2 requires a 64-bit processor architecture. All 32-bit versions have been eliminated, and there is no build supporting Itanium processors. This leaves Windows Server 2012 R2 with the following core editions:

- **Windows Server 2012 R2 Datacenter:** This edition is designed for large and powerful servers with up to 64 processors and fault-tolerance features such as hot add processor support. As a result, this edition is available only through the Microsoft volume-licensing program and from original equipment manufacturers (OEMs), bundled with a server.
- **Windows Server 2012 R2 Standard:** This edition includes the full set of Windows Server 2012 features, varying from the Datacenter edition only by the number of virtual machine instances permitted by the license.
- **Windows Server 2012 R2 Essentials:** This edition includes nearly all the features in the Standard and Datacenter editions, except for Server Core, Hyper-V, and Active Directory Federation Services. This edition is limited to one physical or virtual server instance and a maximum of 25 users.
- **Windows Server 2012 R2 Foundation:** This reduced version of the operating system is designed for small businesses that require only basic server features such as file and print services and application support. This edition includes no virtualization rights and is limited to 15 users.

These various editions are priced commensurate with their capabilities. Obviously, your goal is to purchase the most inexpensive edition that provides all your needs. The following sections examine the primary differences between the Windows Server 2012 R2 editions.

Supporting Server Roles

Windows Server 2012 R2 includes predefined combinations of services called ***roles*** that implement common server functions.

Computers running the Windows Server 2012 R2 operating system can perform a wide variety of tasks, using both the software included with the product and third-party applications. The activities Windows Server 2012 R2 performs for network clients are known as roles. After you install the Windows Server 2012 R2 operating system, you can use Server Manager or ***Windows PowerShell*** to assign one or more roles to that computer.

The roles included with Windows Server 2012 R2 fall into three basic categories:

- **Directory services** store, organize, and supply information about a network and its resources.
- **Infrastructure services** provide support services for network clients.
- **Application services** provide communications services, operating environments, or programming interfaces for specific applications.

Table 1-1 lists the roles that Microsoft supplies with Windows Server 2012 R2.

Table 1-1

Windows Server 2012 R2 Server Roles

Directory Services	Infrastructure Services	Application Services
Active Directory Certificate Services implements certification authorities (CAs) and other services that facilitate the creation and management of the public key certificates used by the identity and access control elements of the Windows Server 2012 R2 security infrastructure.	**DHCP (Dynamic Host Configuration Protocol) Server** provides network clients with dynamically assigned IP addresses and other TCP/IP configuration settings, such as subnet masks, default gateway addresses, and Domain Name System (DNS) server addresses.	**Application Server** provides an integrated environment for deploying and running server-based business applications designed within (or expressly for) the organization, such as those requiring the services provided by Internet Information Services (IIS), Microsoft .NET Framework 2.0 and 3.0, COM+, ASP .NET, Message Queuing, or Windows Communication Foundation (WCF).
Active Directory Domain Services (AD DS) configure the server to function as an Active Directory domain controller, which stores and manages a distributed database of network resources and application-specific information.	**DNS Server** provides name-to-address and address-to-name resolution services for AD DS and Internet clients. The Windows Server 2012 R2 DNS server implementation also supports dynamic DNS and DHCP integration.	**Fax Server** enables you to manage fax devices and clients to send and receive faxes over the network.
Active Directory Federation Services create a single sign-on environment by implementing trust relationships that enable users on one network to access applications on other networks without providing a secondary set of logon credentials.	**Hyper-V** provides a hypervisor-based environment in which administrators can create virtual machines, each of which provides an isolated instance of the operating system environment.	**File and Storage Services** install tools and services that enhance Windows Server 2012 R2's basic ability to provide network clients with access to files stored on server drives, including Distributed File System (DFS), DFS Replication, Storage Manager for Storage Area Networks (SANs), fast file searching, and file services for UNIX clients.

(continued)

Table 1-1

(continued)

Directory Services	Infrastructure Services	Application Services
Active Directory Lightweight Directory Services (AD LDS) implement a Lightweight Directory Access Protocol (LDAP) directory service that provides support for directory-enabled applications without incurring the extensive overhead of AD DS.	**Network Policy and Access Services (NPAS)** implement services such as Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which enforce security policies for network users.	**Print and Document Services** provides clients with access to printers attached to the server or to the network, as well as centralized network printer and print server management, and printer deployment using Group Policy. Document services enable you to route images from network-attached scanners to users.
Active Directory Rights Management Services (AD RMS) make up a client/server system that uses certificates and licensing to implement persistent usage policies, which can control access to information, no matter where a user moves it.	**Remote Access** provides remote users with access to network resources by using DirectAccess and VPNs, as well as LAN and NAT routing services.	**Remote Desktop Services** enable clients on the network or on the Internet to access server-based applications remotely or the entire Windows desktop by using server resources.
	Volume Activation Services automate the management of Microsoft host keys and Key Management System (KMS) hosts.	**Web Server (IIS)** installs Internet Information Services (IIS) 7.5, which enables the organization to publish websites and web-based applications for use by intranet, extranet, and/or Internet clients.
	Windows Deployment Services (WDS) enable you to install Windows operating systems remotely on computers throughout the enterprise.	
	Windows Server Essentials Experience enables Standard and Datacenter servers to run Essentials services, such as Remote Web Access.	
	Windows Server Update Services (WSUS) automate the process of disseminating operating-system updates to Windows computers throughout the enterprise.	

Some Windows Server 2012 R2 editions include all these roles, whereas others include only some of them. Selecting the appropriate edition of Windows Server has always been a matter of anticipating the roles that the computer must perform. At one time, this was a relatively simple process. You planned your server deployments by deciding which ones would be domain controllers, which ones would be web servers, and so forth. After you made these decisions, you were done, because server roles were largely static.

With the increased focus on virtualization in Windows Server 2012 R2, however, more administrators must consider not only what roles servers must perform at the time of the deployment, but also what roles they will perform in the future.

By using virtualized servers, you can modify your network's server strategy at will to accommodate changing workloads and business requirements, or to adapt to unforeseen circumstances. Therefore, the process of anticipating the roles servers will perform must account for the potential expansion of your business, as well as possible emergency needs.

■ Installing Windows Server 2012 R2

THE BOTTOM LINE

A clean installation is the simplest way to deploy Windows Server 2012 R2 on a bare metal computer—that is, a computer with no operating system installed—or a computer with a partition that you are willing to reformat (losing all the data on the partition in the process).

If a computer is brand new and has no operating system installed on it, it cannot start until you supply a boot disk, such as a Windows Server 2012 R2 installation disk. During installation, you select the disk partition on which you want to install the operating system, and the Setup program copies the operating system files there.

System Requirements

Choosing the correct hardware for a server requires an understanding of the tasks it will perform.

As of this writing, the minimum system requirements for all editions of Windows Server 2012 R2 are as follows:

- 1.4 GHz 64-bit processor
- 512 MB RAM
- 32 GB disk space
- DVD or USB flash drive
- Super VGA (1024x768) or higher resolution monitor

Having 32 GB of available disk space should be considered an absolute minimum. The system partition needs extra space if you install the system over a network or your computer has more than 16 GB of RAM installed. The additional disk space is required for paging, hibernation, and dump files. In practice, you are unlikely to come across a computer with 32 GB RAM and only 32 GB disk space. If you do, free more disk space or invest in additional storage hardware.

Not until you have decided how you will deploy your applications and what roles an application server will perform should you begin selecting the hardware that goes into the computer. Suppose that your organization decides to deploy an application suite such as Microsoft Office on all company workstations. If you decide to install the applications on each individual workstation, each computer must have sufficient memory and processor speed to run them efficiently. The application servers on the network then has to perform only relatively simple roles, such as file and print services, which do not require enormous amounts of server resources.

By contrast, if you decide to deploy the applications using Remote Desktop Services, you can use workstations with a minimal hardware configuration, because the servers take most of the burden. In this case, you need a more powerful application server in terms of processor and memory, or perhaps even several servers sharing the client load.

Server roles can also dictate requirements for specific subsystems within the server computers, as in the following examples:

- Servers hosting complex applications might require more memory and faster processors.
- File servers can benefit from disk arrays and hard drives with higher speeds and larger caches, or even a high performance drive interface, such as SCSI (Small Computer System Interface, pronounced "scuzzy").
- Web servers receiving large amounts of traffic might need higher-end network adapters or multiple adapters to connect to different subnets.
- Streaming media servers require sufficient hardware in all subsystems, because any performance bottleneck in the server can interrupt the client's media experience.

Enterprises with extensive server requirements might want to consider specialized server hardware, such as a storage area network, network attached storage, or a server cluster.

As part of Microsoft's increased emphasis on virtualization and cloud computing in its server products, the company has increased the maximum hardware configurations significantly for Windows Server 2012 R2. Table 1-2 lists these maximums.

Table 1-2

Maximum Hardware Configurations in Windows Server Versions

	Windows Server 2012 R2	Windows Server 2008 R2
Logical Processors	640	256
RAM	4 terabytes	2 terabytes
Failover cluster nodes	64	16

Performing a Clean Installation

A clean installation can be the basis for a new server, or the initial phase of a server migration.

To perform a clean installation of Windows Server 2012 R2, use the following procedure.

PERFORM A CLEAN INSTALLATION

GET READY. Prepare the computer for the Windows Server 2012 R2 installation by making sure that all its external peripheral devices are connected and powered on.

1. Turn on the computer and insert the Windows Server 2012 R2 installation disk into the DVD drive.
2. Press any key to boot from the DVD (if necessary). A progress indicator screen appears as Windows is loading files.

MORE INFORMATION

The device that a PC uses to boot is specified in its system (or BIOS) settings. In some cases, you might have to modify these settings to enable the computer to boot from the Windows Server 2012 R2 DVD. If you are not familiar with the operation of a particular computer, watch the screen carefully as the system starts and look for an instruction specifying what key to press to access the system settings.

The computer loads the Windows graphical interface and the Windows Setup page appears, as shown in Figure 1-1.

Figure 1-1

The Windows Setup page

3. By using the drop-down lists provided, select the appropriate language to install, time and currency format, and keyboard or input method, and then click Next. Another Windows Setup page appears.
4. Click Install Now. The Windows Setup Wizard appears, displaying the *Select the operating system you want to install* page.
5. Select the operating system edition and installation option you want to install and click Next. The *License Terms* page appears.
6. Select the I accept the license terms check box and click Next. The *Which type of installation do you want?* page, appears.
7. Because you are performing a clean installation and not an upgrade, click the Custom: Install Windows Only (advanced) option. The *Where do you want to install Windows?* page appears.
8. From the list provided, select the partition on which you want to install Windows Server 2012 R2, or select an area of unallocated disk space where the Setup program can create a new partition. Then click Next. The *Installing Windows* page appears.

9. After several minutes, during which the Setup program installs Windows Server 2012 R2, the computer restarts and the *Settings* page appears, as shown in Figure 1-2.

Figure 1-2

The Settings page

10. In the Password and Reenter Password text boxes, type the password to be associated with the Administrator account and press *Enter*. The system finalizes the installation and the Windows sign-on screen appears.

Choosing Installation Options

THE BOTTOM LINE

Many enterprise networks today use servers dedicated to a particular role. When a server is performing a single role, does it really make sense to have so many other processes running on the server that contribute little to that role?

Many IT administrators today are so accustomed to graphical user interfaces (GUIs) that they are unaware that there was ever any other way to operate a computer. When the first version of Windows NT Server appeared in 1993, many complained about wasting server resources on graphical displays and other elements that they deemed unnecessary. Up until that time, server displays were usually minimal, character-based, monochrome affairs. In fact, many servers had no display hardware at all, relying instead on text-based remote administration tools, such as Telnet.

Using Server Core

Windows Server 2012 R2 includes an installation option that addresses those old complaints about wasting server resources on graphical displays.

When you select the Windows ***Server Core*** installation option, you get a stripped-down version of the operating system. There is no Taskbar, no desktop Explorer shell, no Microsoft Management Console, and virtually no graphical applications. All you see when you start the computer is a single window with a command prompt.

The advantages of running servers using Server Core are several:

- **Hardware resource conservation:** Server Core eliminates some of the most memory- and processor-intensive elements of the Windows Server 2012 R2 operating system, thus devoting more of the system hardware to running essential services.
- **Reduced disk space:** Server Core requires less disk space for the installed operating system elements, as well as less swap space, which maximizes the utilization of the server's storage resources.
- **Reduced patch frequency:** Windows Server 2012 R2's graphical elements are among the most frequently patched features, so running Server Core reduces the number of patches that you must apply. Fewer patches also mean fewer server restarts and less downtime.
- **Reduced attack surface:** The less software there is running on the computer, the fewer entrances are available for attackers to exploit. Server Core reduces the potential openings presented by the operating system, increasing its overall security.

When Microsoft first introduced the Server Core installation option in Windows Server 2008, the idea was intriguing, but few administrators took advantage of it. The main reason for this was that most server administrators were not sufficiently conversant with the command-line interface to manage a Windows server without a GUI.

In Windows Server 2008 and Windows Server 2008 R2, the decision to install the operating system via the Server Core option was irrevocable. After you installed the operating system using Server Core, in no way could you get the GUI back except to perform a complete reinstallation. That has all changed in Windows Server 2012 and Windows Server 2012 R2. You can now switch a server from the Server Core option to the Server with a GUI option, and back again, at will, using Windows PowerShell commands.

This ability means that you can install Windows Server 2012 R2 using the Server with a GUI option, if you want to, configure the server using the familiar graphical tools, and then switch the server to Server Core, to take advantage of the benefits listed earlier.

SERVER CORE DEFAULTS

In Windows Server 2012 R2, Microsoft is attempting to fundamentally modify the way administrators work with their servers. Server Core is now the default installation option because in the new way of managing servers, you should rarely, if ever, have to work at the server console, either physically or remotely.

Windows Server has long been capable of remote administration, but this capability has been a piecemeal affair. Some Microsoft Management Console (MMC) snap-ins enabled administrators to connect to remote servers, and Windows PowerShell 2.0 provided some remote capabilities from the command line, but Windows Server 2012 R2, includes comprehensive remote administration tools that virtually eliminate the need to work at the server console.

The Server Manager application in Windows Server 2012 R2 enables you to add servers from all over the enterprise and create server groups to facilitate the configuration of multiple systems simultaneously. The new Windows PowerShell 4.0 environment increases the number of available commands—known as ***cmdlets***—from 230 to well over 2,000.

With tools like these, it is possible for you to install your servers using the Server Core option, execute a few commands to join each server to an AD DS domain, and then never touch the server console again. You can perform all subsequent administration tasks, including deployment of roles and features, by using Server Manager and Windows PowerShell from a remote workstation.

SERVER CORE CAPABILITIES

In addition to omitting most of the graphical interface, a Server Core installation omits some of the server roles found in a Server with a GUI installation. However, the Server Core option in Windows Server 2012 R2 includes 12 of the 19 roles, plus support for SQL Server 2012, as opposed to only 10 roles in Windows Server 2008 R2 and 9 in Windows Server 2008.

Table 1-3 lists the roles and features that are available and not available in a Windows Server 2012 R2 Server Core installation.

Table 1-3

Windows Server 2012 R2 Server Core Roles

Roles Available in Server Core Installation	Roles Not Available in Server Core Installation
Active Directory Certificate Services	Active Directory Federation Services
Active Directory Domain Services	Application Server
Active Directory Lightweight Directory Services	Fax Server
Active Directory Rights Management Services	Network Policy and Access Services
DHCP Server	Remote Desktop Services: • Remote Desktop Gateway • Remote Desktop Session Host • Remote Desktop Web Access
DNS Server	Volume Activation Services
File and Storage Services	Windows Deployment Services
Hyper-V	
Print and Document Services	
Remote Desktop Services: • Remote Desktop Connection Broker • Remote Desktop Licensing • Remote Desktop Virtualization Host	
Remote Access	
Web Server (IIS)	
Windows Server Update Services	

Using Features on Demand

During a Windows Server 2012 R2 installation, the Setup program copies the files for all operating system components from the installation medium to a directory called ***WinSxS,*** the side-by-side component store. This enables you to activate any features included with Windows Server 2012 R2 without having to supply an installation medium.

The drawback of this arrangement is that the WinSxS directory occupies a significant amount of disk space, much of which is, in many cases, devoted to data that will never be used.

With the increasing use of virtual machines to distribute server roles, enterprise networks often have more copies of the server operating system than ever before, and therefore more wasted disk space. Also, the advanced storage technologies often used by today's server infrastructures, such as storage area networks (SANs) and solid state drives (SSDs), are making that disk space more expensive.

Features on Demand, introduced in to Windows Server 2012, is a third state for operating system features that enables administrators to conserve disk space by removing specific features not only from operation, but also from the WinSxS directory.

This state is intended for features that you do not intend to install on a particular server. If, for example, you want to disable the Server Graphical Shell feature in Windows Server 2012 R2 to prevent Internet Explorer, Windows Explorer, and the desktop shell from running, and you want to remove the files that provide those features from the disk completely, you can do so with Features on Demand. By removing all the disk files for all your unused features on all your virtual machines, the accumulated savings in disk space can be substantial.

Features on Demand provide a third installation state for each feature in Windows Server 2012 R2. In versions of the operating system prior to Windows Server 2012, you could only enable or disable features. Windows Server 2012 R2 provides the following three states:

- Enabled
- Disabled
- Disabled with payload removed

To implement this third state, you must use the Windows PowerShell `Uninstall-WindowsFeature` cmdlet, which now supports a new `-Remove` flag. Thus, the Windows PowerShell command to disable the Server Graphical Shell and remove its source files from the WinSxS directory would be as follows:

```
Uninstall-WindowsFeature Server-Gui-Shell -Remove
```

Deleting the source files for a feature from the WinSxS folder does not make them irretrievably gone. If you try to enable that feature again, the system downloads it from Windows Update or, alternatively, retrieves it from an image file you specify using the `-Source` flag with the `Install-WindowsFeature` cmdlet. This enables you to retrieve the required files from a removable disk or from an image file on the local network. You can also use Group Policy to specify a list of installation sources.

TAKE NOTE*

This ability to retrieve source files for a feature from another location is the actual functionality to which the name Features on Demand is referring. Microsoft often uses this capability to reduce the size of updates downloaded from the Internet. After the user installs the update, the program downloads the additional files required and completes the installation.

Upgrading Servers

THE BOTTOM LINE

An in-place upgrade is the most complicated form of Windows Server 2012 R2 installation. It is also the lengthiest and the most likely to cause problems during its execution. Whenever possible, Microsoft recommends that administrators perform a clean installation, or migrate required applications and settings instead.

During an in-place upgrade, the Setup program creates a new Windows folder and installs the Windows Server 2012 R2 operating system files into it. This is only half of the process, however. The program must then migrate the applications, files, and settings from the old OS. This calls for a variety of procedures, such as importing the user profiles, copying all pertinent settings from the old registry to the new one, locating applications and data files, and updating device drivers with new versions.

While in-place upgrades often proceed smoothly, the complexity of the upgrade process and the large number of variables involved means that many things can potentially go wrong. To minimize the risks involved, you must to take the upgrade process seriously, prepare the system beforehand, and have the ability to troubleshoot any problems that might arise. The following sections discuss these subjects in detail.

Upgrade Paths

Upgrade paths for Windows Server 2012 R2 are quite limited. In fact, they are easier to specify when you can perform an upgrade than when you cannot.

If you have a 64-bit computer running Windows Server 2008 or Windows Server 2008 R2, you can upgrade it to Windows Server 2012 R2 as long as you use the same (or a lower) operating system edition.

Windows Server 2012 R2 does not support the following:

- Upgrades from Windows Server versions prior to Windows Server 2008
- Upgrades from Windows workstation operating systems
- Cross-edition upgrades, such as Windows Server 2008 Standard Edition to Windows Server 2012 R2 Datacenter Edition
- Cross-platform upgrades, such as 32-bit Windows Server 2008 to 64-bit Windows Server 2012 R2
- Upgrades from any Itanium edition
- Cross-language upgrades, such as from Windows Server 2008, U.S. English, to Windows Server 2012 R2, French

In any of these cases, the Windows Setup program does not permit the upgrade to proceed.

Preparing to Upgrade

Before you begin an in-place upgrade to Windows Server 2012 R2, you should perform a number of preliminary procedures to ensure that the process goes smoothly and that server data is protected.

Consider the following before you perform any upgrade to Windows Server 2012 R2:

- **Check hardware compatibility.** Make sure that the server meets the minimum hardware requirements for Windows Server 2012 R2.
- **Check disk space.** Make sure that sufficient free disk space is on the partition where the old operating system is installed. During the upgrade procedure, sufficient disk space is needed to hold both operating systems simultaneously. After the upgrade is complete, you can remove the old files, freeing up some additional space.
- **Confirm that software is signed.** All kernel-mode software on the server, including device drivers, must be digitally signed, or the upgrade will not proceed. If you cannot locate a software update for any signed application or driver, you must uninstall the application or driver before you proceed with the installation.
- **Check application compatibility.** The Setup program displays a Compatibility Report page that can point out possible application compatibility problems. You can sometimes solve these problems by updating or upgrading the applications. Create an inventory of the software products installed on the server and check the manufacturers' websites for updates, availability of upgrades, and announcements regarding support for Windows Server 2012 R2. In an enterprise environment, you should test all applications for Windows Server 2012 R2 compatibility, no matter what the manufacturer says, before you perform any operating system upgrades.
- **Ensure computer functionality.** Make sure that Windows Server 2008 or Windows Server 2008 R2 is running properly on the computer before you begin the upgrade process. Check the Event Viewer console for warnings and errors. You must start an in-place upgrade from within the existing operating system, so you cannot count on Windows Server 2012 R2 to correct any problems that prevent the computer from starting or running the Setup program.
- **Perform a full backup.** Before you perform any upgrade procedure, you should back up the entire system, or at the very least the essential data files. Removable hard drives make this a simple process, even if the computer does not have a suitable backup device.
- **Purchase Windows Server 2012 R2.** Be sure to purchase the appropriate Windows Server 2012 R2 edition for the upgrade, and have the installation disk and product key handy.

Performing an Upgrade Installation

Windows Server 2012 R2 permits you to perform an upgrade installation only after you have met the prerequisites described in the previous section.

To perform a Windows Server 2012 R2 upgrade installation from Windows Server 2008 or Windows Server 2008 R2, use the following procedure.

PERFORM AN UPGRADE INSTALLATION

GET READY. Start the server and log on using an account with administrative privileges.

1. Insert the Windows Server 2012 R2 installation disk into the DVD drive and start the Setup program. The Windows Setup window appears.
2. Click Install Now. The *Get important updates for Windows Server* page appears.
3. Click No thanks. The Windows Setup Wizard appears, displaying the *Select the operating system you want to install* page.

4. Select the operating system edition and installation option you want to install and click Next. The *License Terms* page appears.
5. Select the I accept the license terms check box and click Next. *The Which type of installation do you want?* page appears.
6. Click the Upgrade: Install Windows and keep files, settings, and applications option. The *Compatibility report (saved to your desktop)* page appears, as shown in Figure 1-3.

Figure 1-3

The Compatibility Report page

7. Note the compatibility information provided by the Setup program and click Next. The *Upgrading Windows* page appears.

   After several minutes, during which the Setup program upgrades Windows Server 2008 or Windows Server 2008 R2 to Windows Server 2012 R2 and restarts the computer several times, the system finalizes the installation and the Windows sign-on screen appears.

During the upgrade process, when the system restarts, the boot menu provides an option to roll back to the previous operating system version. However, after the upgrade is complete, this option is no longer available; uninstalling Windows Server 2012 R2 and reverting to the old operating system version is not possible.

Migrating Roles

THE BOTTOM LINE

Migration is the preferred method of replacing an existing server with one running Windows Server 2012 R2. Unlike an in-place upgrade, a migration copies vital information from an existing server to a clean Windows Server 2012 R2 installation.

During a migration, virtually all the restrictions listed earlier concerning upgrades do not apply. By using the Windows Server Migration Tools and migration guides supplied with Windows Server 2012 R2, you can migrate data between servers under any of the following conditions:

- **Between versions:** You can migrate data from any Windows Server version since Windows Server 2003 SP2 to Windows Server 2012 R2. This includes migrations from one server running Windows Server 2012 R2 to another.
- **Between platforms:** You can migrate data from an x86- or x64-based server to an x64-based server running Windows Server 2012 R2.
- **Between editions:** You can migrate data between servers running different Windows Server editions.
- **Between physical and virtual instances:** You can migrate data from a physical server to a virtual one, or the reverse.
- **Between installation options:** You can migrate data from a server running Windows Server 2008 R2 to one running Windows Server 2012 R2, even when one server is using the Server Core installation option and the other uses the Server Core with a GUI option.

TAKE NOTE*

Windows Server 2012 R2 does not support migrations between different language versions of the operating system. You also cannot migrate data from Server Core installations of Windows Server 2008, because Server Code in that version does not include support for Microsoft .NET Framework.

Migration at the server level is different from any migrations you might have performed on workstation operating systems. Rather than perform a single migration procedure that copies all user data from the source to the destination computer at once, in a server migration you migrate roles or role services individually.

Windows Server 2012 R2 includes a collection of migration guides that provide individualized instructions for each role supported by Windows Server 2012 R2. Some roles require the use of the Windows Server Migration Tools; others do not.

Installing Windows Server Migration Tools

Windows Server Migration Tools is a Windows Server 2012 R2 feature that consists of Windows PowerShell cmdlets and help files that enable administrators to migrate certain roles between servers.

Before you can use the migration tools, however, you must install the Windows Server Migration Tools feature on the destination server running Windows Server 2012 R2, and then copy the appropriate version of the tools to the source server.

Windows Server Migration Tools is a standard feature that you install on Windows Server 2012 R2 using the Add Roles and Features Wizard in Server Manager, as shown in Figure 1-4, or the `Install-WindowsFeature` Windows PowerShell cmdlet.

Figure 1-4

The Select Features page of the Add Roles and Features Wizard

After you install the Windows Server Migration Tools feature on the destination server, you must create a distribution folder containing the tools for the source server. This distribution folder must contain the appropriate files for the platform and the operating system version of the source server.

To create the distribution folder on a server running Windows Server 2012 R2 with the Windows Server Migration Tools feature already installed, use the following procedure.

CREATE A WINDOWS SERVER MIGRATION TOOLS DISTRIBUTION FOLDER

GET READY. Start the destination server running Windows Server 2012 R2 and log on using an account with administrative privileges.

1. Open a Command Prompt window.
2. Switch to the directory containing the Windows Server Migration Tools files by typing the following command and pressing Enter:

   ```
   cd\windows\system32\ServerMigrationTools
   ```

3. Run the SmigDeploy.exe program with the appropriate command line switches for the platform and operating system version of the source server, using the following syntax:

   ```
   SmigDeploy.exe /package /architecture [x86|amd64] /os
   [WS08|WS08R2|WS03] /path <deployment_folder_path>
   ```

The SmigDeploy.exe program creates a new folder in the directory you specify for the *<deployment_folder_path>* variable, assigning it a name and location based on the command-line switches you specify. For example, if you enter the following command and press Enter, the program creates a folder called C:\SMT_ws08R2_amd64 containing the Server Migration Tools.

```
SmigDeploy.exe /package /architecture amd64 /os WS08R2 /path C:\
```

After you create the distribution folder, you must copy it to the source server by any standard means, and then register the Windows Server Migration Tools on the source server using the following procedure.

CREATE A WINDOWS SERVER MIGRATION TOOLS DISTRIBUTION FOLDER

GET READY. Start the source server and log on using an account with administrative privileges.

1. Open a Command Prompt window.
2. Switch to the folder containing the Windows Server Migration Tools that you previously copied to the server.
3. Run the SmigDeploy.exe program with no parameters on the command line, as follows:

   ```
   SmigDeploy.exe
   ```

When you execute SmigDeploy.exe, the program registers the Windows Server Migration Tools on the source server and opens a Windows PowerShell window in which you can use those tools.

To use the migration tools in a new Windows PowerShell session, you must open a Windows PowerShell window with elevated user rights and then add the appropriate snap-in, using the following syntax:

```
Add-PSSnapin Microsoft.Windows.ServerManager.Migration
```

Using Migration Guides

After you install the Windows Server Migration Tools on both the source and the destination servers, you can proceed to migrate data between the two.

By using the migration tools, you can migrate certain roles, features, shares, operating system settings, and other data from the source server to the destination server running Windows Server 2012 R2. Some roles require the use of the migration tools while others do not, having their own internal communication capabilities.

For example, the Print and Document Services role includes a Printer Migration Wizard (and a command-line tool called Printbrm.exe) that enables you to export printers on a source server to a file and import the file on the destination server. Roles that do not have capabilities like this rely on the Windows Server Migration Tools.

Migrating all the Windows Server roles does not involve any one procedure, whether the roles have their own migration tools or not. Instead, Microsoft provides detailed migration guides for individual roles, and sometimes for individual role services within a role.

Business Case Scenarios

Scenario 1-1: Preparing for an Upgrade to Windows Server 2012 R2

Walk through the steps an administrator needs to do to prepare for an upgrade to Windows Server 2012 R2.

Scenario 1-2: Switching to GUI Installation

A server is running the Server Core installation of Windows Server 2012 R2. What would you do if you desired the GUI installation?

2 LESSON

Configuring Servers

Completing Post-Installation Tasks

THE BOTTOM LINE

As part of the new emphasis on cloud-based services in Windows networking, Windows Server 2012 R2 contains various tools that have been overhauled to facilitate remote server management capabilities.

With the new Server Manager, for example, you can fully manage Windows servers without ever having to interact directly with the server console, either physically or remotely. However, immediately after the operating system installation, you might have to perform some tasks that require direct access to the server console. These tasks might include the following:

- Configuring the network connection
- Setting the time zone
- Renaming the computer
- Joining a domain
- Enabling Remote Desktop
- Configuring Windows Update settings
- Installing and configuring Windows PowerShell Desired State Configuration (DSC)

Using Command-Line Tools

If you selected the Server Core option when installing Windows Server 2012 R2, you can perform the same post-installation tasks from the command line.

At the very minimum, you need to rename the computer and join it to a domain. To perform these tasks, use the Netdom.exe command.

To rename a computer, run Netdom.exe with the following syntax:

```
netdom renamecomputer %ComputerName% /NewName: <NewComputerName>
```

To restart the computer as directed, use the following command:

```
shutdown /r
```

Then, to join the computer to a domain, use the following syntax:

```
netdom join %ComputerName% /domain:<DomainName>
/userd:<UserName> /passwordd:*
```

In this command, the asterisk (*) in the `/passwordd` parameter causes the program to prompt you for the password to the user account you specified.

These commands assume that a DHCP server has already configured the computer's TCP/IP client. If this is not the case, you must configure it manually before you can join a domain. To assign a static IP address to a computer using Server Core, you can use the Netsh.exe program or the New-NetIPAddress cmdlet provided by Windows PowerShell.

Converting Between GUI and Server Core

In Windows Server 2012 R2, you can convert a computer installed with the full GUI option to Server Core and add the full GUI to a Server Core computer.

This is a major improvement in the usefulness of Server Core over the version in Windows Server 2008 R2, in which you can change the interface only by reinstalling the entire operating system. With this capability, you can install servers with the full GUI, use the graphical tools to perform the initial setup, and then convert them to Server Core to conserve system resources. If later it becomes necessary, it is possible to reinstall the GUI components.

To convert a full GUI installation of Windows Server 2012 R2 to Server Core using Server Manager, use the following procedure.

CONVERT A GUI SERVER TO SERVER CORE

GET READY. Log on to the server running Windows Server 2012 R2 by using an account with administrative privileges. The Server Manager window appears.

1. From the Manage menu, select Remove Roles and Features. The Remove Roles and Features Wizard appears, displaying the *Before you begin* page.
2. Click Next. The *Select destination server* page appears.
3. Select the server you want to convert to Server Core and click Next. The *Remove Server Roles* page appears.
4. Click Next. The *Remove features* page appears.
5. Scroll down in the list and expand the User Interfaces and Infrastructure feature, as shown in Figure 2-1.

Figure 2-1

The *Remove features* page in Server Manager

6. Clear the check boxes for the following components:
   - Graphical Management Tools and Infrastructure
   - Server Graphical Shell
7. The *Remove features that require Graphical Management Tools and Infrastructure* dialog box appears, with a list of dependent features that must be uninstalled. Click Remove Features.
8. Click Next. The *Confirm removal selections* page appears.
9. Select the Restart the destination server automatically if required check box and click Remove. The *Removal progress* page appears as the wizard uninstalls the feature.
10. Click Close. When the removal is completed, the computer restarts.

To add the full GUI to a Server Core computer, you must use Windows PowerShell to install the same features you removed in the previous procedure.

Configuring NIC Teaming

A new feature in Windows Server 2012 and Windows Server 2012 R2, NIC teaming enables administrators to combine the bandwidth of multiple network interface adapters, providing increased performance and fault tolerance.

Virtualization enables you to separate vital network functions on different systems without having to purchase a separate physical computer for each one. However, one drawback of this practice is that a single server hosting multiple virtual machines is still a single point of failure for all of them. A single malfunctioning network adapter, a faulty switch, or even an unplugged cable can bring down a host server and all its VMs with it.

NIC teaming—also called bonding, balancing, and aggregation—is a technology that has been available for some time, but was always tied to specific hardware implementations. The NIC teaming capability in Windows Server 2012 R2 is hardware independent and enables you to combine multiple physical network adapters into a single interface. The results can include increased performance by combining the throughput of the adapters and protection from adapter failures by dynamically moving all traffic to the functioning NICs.

NIC teaming in Windows Server 2012 R2 supports two modes:

- **Switch Independent Mode:** All network adapters are connected to different switches, providing alternative routes through the network.
- **Switch Dependent Mode:** All network adapters are connected to the same switch, providing a single interface with the adapters' combined bandwidth.

In Switch Independent Mode, you can choose between two configurations. The active/active configuration leaves all network adapters functional, providing increased throughout. If one adapter fails, all traffic shunts to the remaining adapters. In the active/standby configuration, one adapter is left offline, to function as a failover in the event the active adapter fails. In active/active mode, an adapter failure causes a performance reduction; in active/standby mode, the performance remains the same before and after an adapter failure.

In Switch Dependent Mode, you can choose static teaming, a generic mode that balances traffic between the adapters in the team, or you can opt to use the Link Aggregation Control Protocol defined in IEEE 802.3ax, assuming that your equipment supports it.

In Windows Server 2012, there was one significant limitation in NIC teaming. If your traffic consisted of large TCP sequences, such as a Hyper-V live migration, the system avoided using multiple adapters for those sequences to minimize the number of lost and out-of-order TCP segments. You therefore did not realize any performance increase for large file transfers using TCP. In Windows Server 2012 R2, a new Dynamic Mode splits these large TCP sequences into smaller units and sitributes them among the NICs in a team. This is now the default load balancing mode in Windows Server 2012 R2.

You can create and manage NIC teams using Server Manager or Windows PowerShell. To create a NIC team using Server Manager, use the following procedure.

CREATE A NIC TEAM

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges. The Server Manager window appears.

1. In the navigation pane, click the Local Server icon. The Local Server homepage appears.
2. In the Properties tile, click the *NIC Teaming* hyperlink. The *NIC Teaming* window appears, as shown in Figure 2-2.

Figure 2-2

The *NIC Teaming* window in Server Manager

3. In the Teams tile, click the Tasks menu and select New Team. The *New team* page appears.
4. Click the Additional properties down arrow to expand the window.
5. In the Team Name text box, type the name you want to assign to the team.
6. In the Member adapters box, select the network adapters you want to add to the team.
7. In the Teaming Mode drop-down list, select one of the following options:
   - Static Teaming
   - Switch Independent
   - LACP
8. In the Load balancing mode drop-down list, select one of the following options:
   - Address Hash
   - Hyper-V Port
   - Dynamic
9. If you selected Switch Independent for the Teaming mode value, use the Standby adapter drop-down list to select one of adapters you added to the team to function as the offline standby.
10. Click OK. The new team appears in the Teams tile, as shown in Figure 2-3.

After you create a NIC team, you can use the NIC Teaming window to monitor the status of the team and the team interface you created. The team itself and the individual adapters all have status indicators that inform you if an adapter goes offline.

Figure 2-3

A new NIC team in the *NIC Teaming* window in Server Manager

If this does occur, the indicator for the faulty adapter immediately switches to disconnected, as shown in Figure 2-4, and depending on which teaming mode you chose, the status of the other adapter might change as well.

Figure 2-4

A NIC team with a failed adapter

Using Server Manager

THE BOTTOM LINE

The Server Manager tool in Windows Server 2012 R2 is a completely new application that is the first and most obvious evidence of a major paradigm shift in Windows Server administration.

In previous version of Windows Server, an administrator wanting to install a role using graphical controls had to work at the server console by either physically sitting at the keyboard or connecting to it using Remote Desktop Services (formerly Terminal Services). By contrast, the Windows Server 2012 R2 Server Manager can install roles and features to any server on the network, and even to multiple servers or groups of servers at once.

Adding Roles and Features

The Server Manager program in Windows Server 2012 R2 combines what used to be separate wizards for adding roles and features into one, the Add Roles and Features Wizard.

If you add multiple servers to the Server Manager interface, they are integrated into the Add Roles and Features Wizard, so you can deploy roles and features to any of your servers.

To install roles and features using Server Manager, use the following procedure.

INSTALL ROLES AND FEATURES USING SERVER MANAGER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges. The Server Manager window appears.

1. From the Manage menu, select Add Roles and Features. The Add Roles and Features Wizard appears, displaying the *Before you begin* page.
2. Click Next. The *Select Installation Type* page appears.
3. Leave the *Role-based or feature-based installation* radio button selected and click Next. The *Select destination server* page appears, as shown in Figure 2-5.

Figure 2-5

The *Select destination server* page in the Add Roles and Features Wizard

4. Select the server on which you want to install the roles and/or features. If the server pool contains a large number of servers, you can use the filter text box to display a subset of the pool based on a text string. After you select the server, click Next. The *Select Server Roles* page appears, as shown in Figure 2-6.

Figure 2-6

The *Select Server Roles* page in the Add Roles and Features Wizard

5. Select the role or roles you want to install on the selected server. If the roles you select have other roles or features as dependencies, an *Add features that are required* dialog box appears.
6. Click Add Features to accept the dependencies, and then click Next. The *Select features* page appears, as shown in Figure 2-7.

Figure 2-7

The *Select features* page in the Add Roles and Features Wizard

7. Select any features you want to install in the selected server and click Next. Dependencies also might appear for your feature selections.
8. The wizard displays pages specific to the roles and/or features you have chosen. Most roles have a *Select role services* page, on which you can select which elements of the role you want to install. Complete each of the role- or feature-specific pages and click Next. A *Confirm installation selections* page appears.
9. Select from the following optional functions, if desired:
   - **Restart the destination server automatically if desired** causes the server to restart automatically when the installation completes, if the selected roles and features require it.
   - **Export configuration settings** create an XML script documenting the procedures performed by the wizard, which you can use to install the same configuration on another server using Windows PowerShell.
   - **Specify an alternate source path** specifies the location of an image file containing the software needed to install the selected roles and features. Use this option when you have previously deleted teh source fiels from the system using Features on Demand.
10. Click Install. The *Installation progress* page appears. Depending on the roles and features installed, the wizard might display hyperlinks to the tools needed to perform required post-installation tasks. When the installation is completed, click Close to terminate the wizard.

After you install roles on your servers, the roles appear as icons Server Manager's the navigation pane. These icons actually represent ***role groups***. Each role group contains all instances of that role found on any of your added servers. You can therefore administer the role across all servers on which you have installed it.

Deploying Roles to VHDs

In addition to installing roles and features to servers on the network, Server Manager also enables administrators to install them to virtual machines currently in an offline state.

In an enterprise virtualization strategy, administrators frequently maintain virtual machines (VMs) in an offline state. For example, you might have an offline web server VM stored on a backup host server, in case the computer hosting your main web server VMs should fail. Server Manager enables you to select a virtual hard disk (VHD) file and install or remove roles and features without having to deploy the VM.

To install roles and/or features to an offline VHD file, use the following procedure.

INSTALL ROLES AND FEATURES TO AN OFFLINE VHD FILE

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges. The Server Manager window appears.

1. From the Manage menu, select Add Roles and Features. The Add Roles and Features Wizard appears, displaying the *Before you begin* page.
2. Click Next. The *Select Installation Type* page appears.
3. Leave the *Role-based or feature-based installation* radio button selected and click Next. The *Select Destination Server* page appears.
4. Select the Select a virtual hard disk radio button.
5. A Virtual Hard Disk text box appears at the bottom of the page. In this text box, type in or browse to the location of the VHD file you want to modify.
6. In the Server Pool box, select the server that the wizard should use to mount the VHD file, as shown in Figure 2-8, and click Next. The *Select Server Roles* page appears.

Figure 2-8

The *Select Destination Server* page in the Add Roles and Features Wizard

TAKE NOTE*

The wizard must mount the VHD file on the server you select, and look inside and determine which roles and features are already installed and which are available for installation. Mounting a VHD file makes it available only through the computer's file system; it is not the same as starting the virtual machine using the VHD.

7. Select the role or roles you want to install on the selected server, adding the required dependencies, if necessary, and click Next. The *Select features* page appears.
8. Select any features you want to install in the selected server and click Next. Dependencies also might appear for your feature selections.
9. The wizard then displays pages specific to the roles and/or features you have chosen, enabling you to select role services and configure other settings. Complete each of the role- or feature-specific pages and click Next. A *Confirmation* page appears.
10. Click Install. The *Installation progress* page appears.
11. When the installation is completed, click Close to dismount the VHD and terminate the wizard.

Configuring Services

Most Windows Server roles and many features include *services*, programs that run continuously in the background, typically waiting for a client process to send a request to them. Server Manager provides access to services running on servers all over the network.

When you first look at the Local Server homepage in Server Manager, one tile that you find there is the Services tile, as shown in Figure 2-9. This tile lists all the services installed on the server and specifies the operational status and their Start Types. When you right-click a service, the context menu provides controls that enable you to start, stop, restart, pause, and resume the service.

Figure 2-9

The Services tile in Server Manager

The Services tile in Server Manager is not unlike the traditional Services MMC snap-in found in previous versions of Windows Server. However, although you can start and stop a service in Server Manager, you cannot modify its Start Type, which specifies whether the service should start automatically with the operating system. For that, you must use the Services MMC snap-in.

Another difference of the Services tile in Windows Server 2012 R2 Server Manager is that it appears in many locations throughout Server Manager, displaying a list of services for a different context in each location. This is a good example of the organizational principle of the new Server Manager. The same tools, repeated in many places, provide a consistent management interface to different sets of components.

For example, when you select the All Servers icon in the navigational pane, you see first the Servers tile, as usual, containing all the servers you have added to the Server Manager console. When you select some or all servers and scroll down to the Services tile, you see the same display as before, except that it now contains all services for all the computers you selected. This enables you to monitor the services on all servers at once.

In the same way, when you select one of the role group icons, you can select from the servers running that role and the Services tile will contain only the services associated with that role for the servers you selected.

To manipulate other server configuration settings, you must use the Services MMC snap-in as mentioned earlier. However, you can launch that, and many other snap-ins, by using Server Manager.

After selecting a server from the Servers pane in any group homepage, click the Tools menu to display a list of the server-specific utilities and MMC snap-ins, including the Services snap-in, directed at the selected server.

Delegating Server Administration

THE BOTTOM LINE

As networks grow in size, so does the number of administrative tasks to perform regularly and the size of the IT staffs needed to perform them. Delegating administrative tasks to specific individuals is a natural part of enterprise server management, as is assigning those individuals the permissions they need—and only the permissions they need—to perform those tasks.

On smaller networks, with small IT staffs, it is common for task delegation to be informal, and for everyone in the IT department to have full access to the entire network. However, on larger networks, with larger IT staffs, this becomes increasingly impractical. For example, you might want the newly hired junior IT staffers to be able to create new user accounts, but you do not want them to be able to redesign your Active Directory tree or change the CEO's password.

Delegation, therefore, is the practice by which administrators grant other users a subset of the privileges that they themselves possess. As such, delegation is as much a matter of restricting permissions as it is of granting them. You want to provide individuals with the privileges they need, while protecting sensitive information and delicate infrastructure.

Using Windows PowerShell Desired State Configuration

THE BOTTOM LINE

Desired State Configuration (DSC) is the next phase in the development of Windows PowerShell, a process that began over a decade ago and first appeared as a Windows component in Windows PowerShell 1.0, released in 2006.

Windows Server 2012 R2 expanded the functionality of Windows PowerShell by using the command line infrastructure as an underlayment for all of the new graphical capabilities in the operating system. Windows PowerShell 3.0 added thousands of new cmdlets, making it possible to accomplish any task you might perform in Server Manager from the command line.

In Windows PowerShell 4.0, DSC provides a new scripting model that enables administrators to create modules called *configurations*, which consist of *nodes* representing computers and *resources* that define elements that administrators want to define as part of the configuration for a particular node. The scripts use the standard Microsoft Operations Framework (MOF) format.

For example, a relatively simple script to deploy a Web server might appear as follows:

```
Configuration CompanyWeb
{
   Node "ServerB"
   {
      WindowsFeature IIS
      {
          Ensure = "Present"
          Name = "Web-Server"
      }
      File CopyWebSite
      {
         Ensure = "Present"
         Type = "Directory"
         Recurse = $true
```

```
            SourcePath = $WebsitePath
            DestinationPath = "C:\inetpub\wwwroot"
            Requires = "[WindowsFeature]IIS"
        }
    }
}
```

In this script, the node block identifies the computer to be configured, and the WindowsFeature and File blocks are both built-in resources that you can use to define the configuration you want to deploy. The WindowsFeature block specifies that the configuration must install the Web-Server role, and the File block copies the content files for a Web site to the node from a location defined by the $WebsitePath variable. DSC includes many other built-in resources that you can use to define more complex configuration elements, such as system services, registry settings, environment variables, and user and group accounts. It is also possible for administrators to create their own custom resources.

Once you have created a configuration script, you can deploy it by executing the defined configuration name–in this case CompanyWeb–from a Windows PowerShell prompt, using the Start-DscConfiguration cmdlet.

In large enterprise deployments, administrators can create a centralized DSC server by installing the Windows PowerShell Desired State Configuration Service, a Windows PowerShell feature that uses the Internet Information Services Web server to deploy configuration logic and data to nodes all over the network. After storing DSC configuration scripts on the server, administrators can configure nodes to check periodically for changes in their configurations, using the Test-DscConfiguration cmdlet, or configure the server to push new configurations to nodes as needed.

Business Case Scenarios

Scenario 2-1: Installing Roles with a Batch File

Mark Lee is an IT technician whose supervisor has assigned the task of configuring 20 new servers, which Mark is to ship to the company's branch offices around the country. He must configure each server to function as a file server with support for DFS and UNIX clients, a print server with support for Internet and UNIX printing, a fax server, and a secured, intranet Web/FTP server for domain users. Write a Windows PowerShell script that Mark can use to install all of the required software elements on a server.

Scenario 2-2: Deploying Roles to VHDs

You maintain several virtual machines (VMs) in an offline state. How do you proceed to add a particular role to one of those VMs?

3 LESSON

Configuring Local Storage

Planning Server Storage

THE BOTTOM LINE

A Windows server can conceivably perform its tasks using the same type of storage as a workstation—that is, one or more standard hard disks connected to a standard drive interface such as Serial ATA (SATA). However, a server's I/O burdens vary quite differently from those of a workstation, and file requests from dozens or hundreds of users can easily overwhelm a standard storage subsystem. Also, standard hard disks offer no fault tolerance and their scalability is limited.

A variety of storage technologies are better suited for server use. The process of designing a storage solution for a server depends on several factors, including the following:

- The amount of storage the server needs
- The number of users that will be accessing the server at the same time
- The sensitivity of the data to be stored on the server
- The importance of the data to the organization

Determining the Number of Servers Needed

When is one big file server preferable to several smaller ones?

One of the most frequently asked questions when planning a server deployment is whether using one big server or several smaller ones is better. In the past, you might have considered the advantages and disadvantages of using one server to perform several roles versus distributing the roles among several smaller servers. Today, however, the emphasis is on virtualization, which means that although you might have many virtual machines running different roles, they could all be running on a single large physical server.

If you are considering large physical servers or your organization's storage requirements are extremely large, you must also consider the inherent storage limitations of Windows Server 2012 R2, as listed in Table 3-1.

Table 3-1

Windows Server 2012 R2 Storage Limitations

Attribute	Limit Based on the On-Disk Format
Maximum size of a single file	2^{64}-1 bytes
Maximum size of a single volume	Format supports 2^{78} bytes with 16KB cluster size. Windows stack addressing allows 2^{64} bytes
Maximum number of files in a directory	2^{64}
Maximum number of directories in a volume	2^{64}
Maximum filename length	32K Unicode characters
Maximum path length	32K
Maximum size of any storage pool	4 petabytes
Maximum number of storage pools in a system	No limit
Maximum number of spaces in a storage pool	No limit

The number of sites your enterprise network encompasses and the technologies you use to provide network communication between those sites can also affect your plans. If, for example, your organization has branch offices scattered around the world and uses relatively expensive wide area networking (WAN) links to connect them, installing a server at each location would probably be more economical than to have all your users access a single server via WAN links.

Within each site, the number of servers you need can depend on how often your users work with the same resources and how much fault tolerance and high availability you want to build into the system. For example, if each department in your organization typically works with its own applications and documents and rarely needs access to those of other departments, deploying individual servers to each department might be preferable. If everyone in your organization works with the same set of resources, centralized servers might be a better choice.

Estimating Storage Requirements

The amount of storage space you need in a server depends on various factors, not just the initial requirements of your applications and users.

For an application server, start by allocating the amount of space needed for the application files themselves, plus any other space the application needs, as recommended by the developer. If users will store documents on the server, allocate a specific amount of space for each user the server will support. Then, factor in the potential growth of your organization and your network, both in terms of additional users and additional space required by each user, and of the application itself, in terms of data files and updates.

In addition to the space allocated to applications and individual users, you must also consider the storage requirements for the following server elements:

- **Operating system:** The size of the operating system installation depends on the roles and features you choose to install. A typical Windows Server 2012 R2 installation with the File Services role needs just over 10 GB, but the system requirements recommend 40 GB.
- **Paging file:** The traditional formula for the size of the paging file—pagefile.sys—on a computer running Windows is 1½ times the amount of memory installed on the computer. However, this formula has now come into question, due to the large amounts

of memory in some servers and the increasing use of Hyper-V. Virtual machines require physical, not virtual, memory, so you do not need to count the memory allotted to your VMs when calculating your paging file size.

- **Memory dump:** When Windows Server 2012 R2 experiences a serious malfunction, it offers to dump the contents of the system memory to a file, which technicians can use for diagnostic purposes. The maximum size for a memory dump file is the amount of memory installed in the computer plus 1 MB. However, blue screens are relatively rare on Windows servers these days, and unless you are troubleshooting a chronic problem with the aid of a technician who can make use of a memory dump, you probably do not need to reserve space for this purpose.
- **Log files:** Be sure to consider any applications that maintain their own logs, in addition to the operating system logs. You can configure the maximum log size for Windows event logs and for most application logs, and add those values to calculate the total log space required.
- **Shadow copies:** The Windows Server 2012 R2 shadow copies feature automatically retains copies of files on a server volume in multiple versions from specific points in time. Shadow copies can use up to 10% of a volume, by default. However, Microsoft recommends enlarging this value for volumes containing frequently modified files.
- **Fault tolerance:** Fault-tolerance technologies, such as disk mirroring and disk parity, can profoundly affect disk consumption. Mirroring disks cuts the effective storage size in half, and parity can reduce it by as much as one third.

Using Storage Spaces

Windows Server 2012 R2 includes a new disk virtualization technology called ***Storage Spaces***, which enables a server to concatenate storage space from individual physical disks and allocate that space to create virtual disks of any size supported by the hardware.

This type of virtualization is a feature often found in SAN and NAS technologies, which require a substantial investment in specialized hardware and administrative skill. Storage Space provides similar capabilities, using standard direct-attached disk drives or simple external JBOD arrays.

Storage Spaces uses unallocated disk space on server drives to create storage pools. A ***storage pool*** can span multiple drives invisibly, providing an accumulated storage resource that you can expand or reduce as needed by adding disks to or removing them from the pool. By using the space in the pool, you can create ***virtual disks*** of any size.

Once created, a virtual disk behaves much like a physical disk, except that the actual bits might be stored on any number of physical drives in the system. Virtual disks can also provide fault tolerance by using the physical disks in the storage pool to hold mirrored or parity data.

Virtual disks can also be thinly provisioned, meaning that while you specify a maximum size for the disk, it starts out small and grows as you add data to it. You can therefore create a virtual disk with a maximum size that is larger than that of your storage space.

For example, if you plan to allocate a maximum of 10 TB for your database files, you can create a thin 10 TB virtual disk, even if you only have a 2 TB storage pool. The application using the disk will function normally, gradually adding data until the storage pool is nearly consumed, at which point the system notifies you to add more space to the pool. You can then install more physical storage and add it to the pool, gradually expanding it until it can support the entire 10 TB required by the disk.

After creating a virtual disk, you can create volumes on it, just as you would on a physical disk. Server Manager provides the tools needed to create and manage storage pools and virtual disks, as well as the capability to create volumes and file system shares, with some limitations.

Understanding Windows Disk Settings

THE BOTTOM LINE When preparing a disk for use, Windows Server 2012 R2 servers often require different settings than workstations.

When you install Windows Server 2012 R2 on a computer, the setup program automatically performs all preparation tasks for the primary hard disk in the system. However, when you install additional hard disk drives on a server, or when you want to use different settings from the system defaults, you must perform the following tasks manually:

- **Select a partitioning style:** Windows Server 2012 R2 supports two hard disk partition styles: the master boot record (MBR) partition style and the GUID (globally unique identifier) partition table (GPT) partition style. You must choose one of these partition styles for a drive; you cannot use both.
- **Select a disk type:** Windows Server 2012 R2 supports two disk types: basic and dynamic. You cannot use both types on the same disk drive, but you can mix disk types in the same computer.

Selecting a Partition Style

The term ***partition style*** refers to the method Windows operating systems use to organize partitions on the disk.

Servers running Windows Server 2012 R2 computers can use either of the following hard disk partition styles:

- ***Master Boot Record (MBR):*** The MBR partition style has been around since before Windows and is still a common partition style for x86-based and x64-based computers.
- ***GUID Partition Table (GPT):*** GPT has existed since the late 1990s, but no x86 versions of Windows prior to Windows Server 2008 and Windows Vista supports it. Today, most operating systems support GPT, including Windows Server 2012 R2.

MBR uses a partition table to point to the locations of the partitions on the disk. The MBR disk partitioning style supports volumes up to 2 TB in size, and up to either four primary partitions or three primary partitions and one extended partition on a single drive.

GPT varies from MBR in that partitions, rather than hidden sectors, store data critical to platform operation. GPT-partitioned disks also use redundant primary and backup partition tables for improved integrity. Although GPT specifications permit an unlimited number of partitions, the Windows implementation restricts partitions to 128 per disk. The GPT disk partitioning style supports volumes up to 18 exabytes (1 exabyte = 1 billion gigabytes, or 2^{60} bytes).

Unless the computer's architecture provides support for an Extensible Firmware Interface (EFI)–based boot partition, it is not possible to boot from a GPT disk. If this is the case, the system drive must be an MBR disk, and you can use GPT only on separate non-bootable disks used for data storage.

Before Windows Server 2008 and Windows Vista, all x86-based Windows computers used only the MBR partition style. Computers based on the x64 platform could use either the MBR or GPT partition style, as long as the GPT disk was not the boot disk.

Now that hard drives larger than 2 TB are readily available, the selection of a partition style is more critical than ever. When you initialize a physical disk using the traditional Disk Management snap-in, MBR is the default partition style, as it always has been. You can also use the snap-in to convert a disk between MBR and GPT partition styles, although you can do so only on disks that do not have partitions or volumes created on them.

When you use Server Manager to initialize a disk in Windows Server 2012 R2, it uses the GPT partition style, whether the disk is physical or virtual. Server Manager has no controls supporting MBR, although it does display the partition style in the Disks tile.

Table 3-2 compares some of the characteristics of the MBR and GPT partition styles.

Table 3-2

MBR and GPT Partition Style Comparison

Master Boot Record (MBR)	GUID Partition Table (GPT)
Supports up to four primary partitions or three primary partitions and one extended partition, with unlimited logical drives on the extended partition	Supports up to 128 primary partitions
Supports volumes up to 2 terabytes	Supports volumes up to 18 exabytes
Hidden (unpartitioned) sectors store data critical to platform operation	Partitions store data critical to platform operation
Replication and cyclical redundancy checks (CRCs) are not features of MBR's partition table	Replication and CRC protection of the partition table provide increased reliability

Understanding Disk Types

Most personal computers use basic disks because they are easiest to manage. Advanced volume types require the use of dynamic disks.

A ***basic disk*** using the MBR partition style uses primary partitions, extended partitions, and logical drives to organize data. A primary partition appears to the operating system as though it is a physically separate disk and can host an operating system, in which case it is known as the active partition.

During the operating system installation, the setup program creates a system partition and a boot partition. The system partition contains hardware-related files that the computer uses to start. The boot partition contains the operating system files, which are stored in the Windows file folder. In most cases, these two partitions are one and the same, the active primary partition that Windows uses when starting. The active partition tells the computer which system partition and operating system to use to start Windows.

When you work with basic MBR disks in Windows Server 2012 R2, you can create three volumes that take the form of primary partitions. When you create the fourth volume, the system creates an extended partition, with a logical drive on it, of the size you specified. If the disk still has free space left, the system allocates it to the extended partition (see Figure 3-1), which you can use to create additional logical drives.

Figure 3-1

Primary and extended partitions on a basic disk using MBR

When you select the GPT partition style, the disk still appears as a basic disk, but you can create up to 128 volumes, each of which appears as a primary partition, as shown in Figure 3-2. GPT disks have no extended partitions or logical drives.

Figure 3-2

Primary partitions on a basic disk using GPT

The alternative to using a basic disk is to convert it to a ***dynamic disk***. Converting a basic disk to a dynamic disk creates a single partition that occupies the entire disk. You can then create an unlimited number of volumes out of the space in that partition. Dynamic disks support several different types of volumes, as described in the next section.

Working with Disks

THE BOTTOM LINE

Windows Server 2012 R2 includes tools that enable you to manage disks graphically or from the command prompt.

All Windows Server 2012 R2 installations include the File and Storage Services role, which causes Server Manager to display a submenu when you click the icon in the navigational pane (see Figure 3-3). This submenu provides access to homepages that enable you to manage volumes, disks, storage pools, shares, and iSCSI devices.

Figure 3-3

The File and Storage Services submenu in Server Manager

Server Manager is the only graphical tool that can manage storage pools and create virtual disks. It can also perform some—but not all—of the standard disk and volume management operations on physical disks. As with the other Server Manager homepages, the File and Storage Services pages also enable you to perform tasks on any servers you have added to the interface.

Disk Management is a Microsoft Management Console (MMC) snap-in that is the traditional tool for performing disk-related tasks, such as the following:

- Initializing disks
- Selecting a partition style
- Converting basic disks to dynamic disks
- Creating partitions and volumes
- Extending, shrinking, and deleting volumes
- Formatting partitions and volumes
- Assigning and changing drive letters and paths

To access the Disk Management snap-in, you can open the Computer Management console and select Disk Management.

You can also manage disks and volumes from the command line by using the DiskPart.exe utility.

Creating and Mounting VHDs

Hyper-V relies on the ***Virtual Hard Disk (VHD)*** format to store virtual disk data in files that can easily be transferred from one computer to another.

The Disk Management snap-in in Windows Server 2012 R2 enables you to create VHD and VHDX files and mount them on the computer. As soon as the VHDs or VHDXes are mounted, you can treat them just like physical disks and use them to store data. Dismounting a VHD or VHDX packages the stored data in the file, so you can copy or move it as needed.

To create a VHD in Disk Management, use the following procedure.

CREATE A VHD

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges. The *Server Manager* window appears.

1. Click Tools > Computer Management.
2. In the Computer Management console, click Disk Management. The Disk Management snap-in appears.
3. From the Action menu, select Create VHD. The *Create and Attach Virtual Hard Disk* dialog box appears, as shown in Figure 3-4.

Figure 3-4

The *Create and Attach Virtual Hard Disk* dialog box

4. In the Location text box, specify the path and name for the file you want to create.
5. In the Virtual hard disk size text box, specify the maximum size of the disk you want to create.
6. Select one of the following virtual hard disk format options:
   - VHD: The original and more compatible format, which supports files up to 2,040 GB.
   - VHDX: A new version of the format that supports files up to 64 TB, but can be read only by computers running Windows Server 2012 R2, Windows Server 2012 and Windows 8.

7. Select one of the following virtual hard disk type options:
   - Fixed size allocates all disk space for the VHD file at once.
   - Dynamically expanding allocates disk space to the VHD or VHDX file as you add data to the virtual hard disk.
8. Click OK. The system creates the VHD or VHDX file and attaches it, so that it appears as a disk in the snap-in, as shown in Figure 3-5.

Figure 3-5

A newly created and attached VHD

After you create and attach the VHD or VHDX, it appears as an uninitialized disk in the Disk Management snap-in and in Server Manager. By using either tool, you can initialize the disk and create volumes on it, just as you would a physical disk. After storing data on the volumes, you can detach the VHD or VHDX and move it to another location or mount it on a Hyper-V virtual machine.

Creating a Storage Pool

After you install your physical disks, you can concatenate their space into a storage pool, from which you can create virtual disks of any size.

To create a storage pool via Server Manager, use the following procedure.

CREATE A STORAGE POOL

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges.

1. In the *Server Manager* window, click the File and Storage Services icon and, in the submenu that appears, click Storage Pools. The *Storage Pools* homepage appears, as shown in Figure 3-6.

Figure 3-6

The *Storage Pools* homepage

2. In the *Storage Pools* tile, select the primordial space on the server where you want to create the pool and then, from the Tasks menu, select New Storage Pool. The *New Storage Pool Wizard* appears, displaying the *Before you begin* page.
3. Click Next. The *Specify a storage pool name and subsystem* page appears.
4. In the Name text box, type the name you want to assign to the storage pool. Then, select the server on which you want to create the pool and click Next. The *Select physical disks for the storage pool* page appears.
5. Select the check boxes for the disks you want to add to the pool and click Next. The *Confirm selections* page appears.
6. Click Create. The wizard creates the new storage pool and the *View results* page appears.
7. Click Close. The wizard closes, and the *Storage Pools* homepage lists the new pool, as shown in Figure 3-7.

Figure 3-7

A new pool on the *Storage Pools* homepage

CLOSE the *Server Manager* window.

After you create a storage pool, you can modify its capacity by adding or removing physical disks. The *Tasks* menu in the *Physical Disks* tile on the *Storage Pools* homepage contains the following options:

- **Add Physical Disk** enables you to add a physical disk to the pool, as long as it is initialized and does not contain any volumes
- **Remove Disk** removes the space provided by a physical disk from the storage pool. This option appears only if all data already has been evicted from the disk.

WARNING When you use ***DiskPart.exe***, a command-line utility included with Windows Server 2012 R2, to manage basic disks, you can create four primary partitions, or three primary partitions and one extended partition. The DiskPart.exe utility contains a superset of the commands supported by the Disk Management snap-in. In other words, DiskPart can do everything Disk Management can do, and more. However, while the Disk Management Snap-in prevents you from unintentionally performing actions that might result in data loss, DiskPart has no safeties, and thus does not prohibit you from performing such actions. For this reason, Microsoft recommends that only advanced users use DiskPart and that they use it with due caution.

Creating a Simple Volume

Technically speaking, you create partitions on basic disks and volumes on dynamic disks. This is not just an arbitrary change in nomenclature. Converting a basic disk to a dynamic disk actually creates one big partition, occupying all space on the disk. The volumes you create on the dynamic disk are logical divisions within that single partition.

Windows versions prior to 2008 use the correct terminology in the Disk Management snap-in. The menus enable you to create partitions on basic disks and volumes on dynamic disks. Windows Server 2012 R2 uses the term *volume* for both disk types, and enables you to create any of the available volume types, whether the disk is basic or dynamic. If the volume type you select is not supported on a basic disk, the wizard converts it to a dynamic disk as part of the volume creation process.

Despite the menus that refer to basic partitions as volumes, the traditional rules for basic disks remain in effect. The New Simple Volume menu option on a basic disk creates up to three primary partitions. When you create a fourth volume, the wizard actually creates an extended partition and a logical drive of the size you specify. If any space remains on the disk, you can create additional logical drives in the extended partition.

To create a new simple volume on a basic or dynamic disk using the Disk Management snap-in, use the following procedure.

CREATE A NEW SIMPLE VOLUME

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges.

1. In the *Server Manager* window, click Tools > Computer Management.
2. In the *Computer Management* console, click Disk Management.
3. In the *Graphical View* of the *Disk Management* snap-in, right-click an unallocated disk area on which you want to create a volume. From the context menu, select New Simple Volume. The *New Simple Volume Wizard* appears.
4. Click Next to dismiss the *Welcome* page. The *Specify Volume Size* page appears.
5. Select the size for the new partition or volume, within the maximum and minimum limits stated on the page, using the Simple volume size in MB spin box, and then click Next. The *Assign Drive Letter or Path* page appears.
6. Configure one of the following options:
   - Assign the following drive letter: If you select this option, click the associated drop-down list for a list of available drive letters and select the letter you want to assign to the drive.
   - Mount in the following empty NTFS folder: If you select this option, either key the path to an existing NTFS folder or click Browse to search for or create a new folder. The folder you specify will list the entire contents of the new drive.

- Do not assign a drive letter or drive path: Select this option if you want to create the partition but are not yet ready to use it. When you do not assign a volume a drive letter or path, the drive is left unmounted and inaccessible. When you want to mount the drive for use, assign a drive letter or path to it.

7. Click Next. The *Format Partition* page appears, as shown in Figure 3-8.

Figure 3-8

The *Format Partition* page

8. Specify whether the wizard should format the volume and, if so, how. If you do not want to format the volume at this time, select the Do not format this volume option. If you do want to format the volume, select the Format this volume with the following settings option, and then configure the following associated options:
   - File system: Select the desired file system. The options available depend on the size of the volume, and can include ReFS, NTFS, exFAT, FAT32, or FAT.
   - Allocation unit size: Specify the file system's cluster size. The cluster size signifies the basic unit of bytes in which the system allocates disk space. The system calculates the default allocation unit size based on the size of the volume. You can override this value by clicking the associated drop-down list and then selecting one of the values. For example, if your client uses consistently small files, you may want to set the allocation unit size to a smaller cluster size.
   - Volume label: Specify a name for the partition or volume. The default name is New Volume, but you can change the name to anything you want.
   - Perform a quick format: When you select this option, Windows formats the disk without checking for errors. This is a faster method with which to format the drive, but Microsoft does not recommend it. When you check for errors, the system looks for and marks bad sectors on the disk so that your clients will not use those areas.
   - Enable file and folder compression: Selecting this option turns on folder compression for the disk. This option is available only for volumes being formatted with the NTFS file system.

9. Click Next. The Completing the New Simple Volume Wizard page appears.
10. Review the settings to confirm your options, and then click Finish. The wizard creates the volume according to your specifications.

CLOSE the console containing the Disk Management snap-in.

After you create a simple volume, you can use the Disk Management snap-in to modify its properties by extending or shrinking it, as described later in this lesson.

This procedure can create volumes on physical or virtual disks. You can also create simple volumes by using a similar wizard in Server Manager.

When you launch the New Volume Wizard in Server Manager, which you can do from the Volumes or Disks homepage, the options the wizard presents are virtually identical to those in the New Simple Volume Wizard in Disk Management.

The primary difference is that, like all Server Manager wizards, the New Volume Wizard includes a page that enables you to select the server and the disk on which you want to create volume, as shown in Figure 3-9. You can therefore use this wizard to create volumes on any disk, on any of your servers.

Figure 3-9

The *Select the server and disk* page in the New Volume Wizard in Server Manager

Extending and Shrinking Volumes and Disks

To extend or shrink a volume in the Disk Management snap-in, you simply right-click a volume and select *Extend Volume* or *Shrink Volume* from the context menu or from the *Action* menu.

The Disk Management snap-in extends existing volumes by expanding them into adjacent unallocated space on the same disk. When you extend a simple volume across multiple disks, the simple volume becomes a spanned volume. You cannot extend striped volumes.

In Server Manager, you can extend a simple volume using unallocated space on the same disk, but you cannot extend it to other disks to create a spanned volume.

To extend a volume on a basic disk, the system must meet the following requirements:

- A volume of a basic disk must be either unformatted or formatted with the NTFS file system.
- If you extend a volume that is actually a logical drive, the console first consumes the contiguous free space remaining in the extended partition. If you attempt to extend the logical drive beyond the confines of its extended partition, the extended partition expands to any unallocated space left on the disk.
- You can extend logical drives, boot volumes, or system volumes only into contiguous space, and only if the hard disk can be upgraded to a dynamic disk. The operating system enables you to extend other types of basic volumes into noncontiguous space but prompts you to convert the basic disk to a dynamic disk.

To extend a volume on a dynamic disk, the system must meet these requirements:

- When extending a simple volume, you can use only the available space on the same disk, if the volume is to remain simple.
- You can extend a simple volume across additional disks if it is not a system volume or a boot volume. However, after you expand a simple volume to another disk, it is no longer a simple volume; it becomes a spanned volume.
- You can extend a simple or spanned volume if it does not have a file system (a raw volume) or if you formatted it using the NTFS file system. (You cannot extend volumes using the FAT or FAT32 file systems.)
- You cannot extend mirrored or RAID-5 volumes, although you can add a mirror to an existing simple volume.

When shrinking volumes, the Disk Management snap-in frees up space at the end of the volume, relocating the existing volume's files, if necessary. The snap-in then converts that free space to new unallocated space on the disk. Server Manager cannot shrink volumes.

To shrink basic disk volumes and simple or spanned dynamic disk volumes, the system must meet the following requirements:

- The existing volume must not be full and must contain the specified amount of available free space for shrinking.
- The volume must not be a raw partition (one without a file system). Shrinking a raw partition that contains data might destroy the data.
- You can shrink a volume only if you formatted it using the NTFS file system. (You cannot shrink volumes using the FAT or FAT32 file systems.)
- You cannot shrink striped, mirrored, or RAID-5 volumes.
- You should always defragment a volume before you attempt to shrink it.

Physical disks, obviously, cannot be extended, but virtual disks can. In Server Manager, you can right-click a virtual disk and select *Extend Virtual Disk* from the context menu to display the Extend Virtual Disk dialog box.

If you elected to use thin provisioning when you created the virtual disk, you can even extend its size beyond the storage pool's current capacity. To actually store that much data on the disk, however, you must first expand the pool to provide enough space.

Business Case Scenario

Scenario 3-1: Planning Storage

On a new server running Windows Server 2012 R2, Morris created a storage pool that consists of two physical drives holding 1 TB each. Then he created three simple virtual disks out of the space in the storage pool. Using the Disk Management snap-in, Morris then created a RAID-5 volume out of the three virtual disks.

With this in mind, answer the following questions:

1. In what way is Morris's storage plan ineffectual at providing fault tolerance?
2. Why will adding a third disk to the storage pool fail to improve the fault tolerance of the storage plan?
3. How can Morris modify the storage plan to make it fault tolerant?

Configuring File and Share Access

LESSON 4

Creating Folder Shares

THE BOTTOM LINE Sharing folders makes them accessible to network users.

After you configure the disks on a file server, you must create shares for network users to be able to access those disks. You should have a sharing strategy in place by the time you are ready to actually create your shares. This strategy should consist of the following information:

- What folders you will share
- What names you will assign to the shares
- What permissions you will grant users to the shares
- What Offline Files settings you will use for the shares

If you are the Creator Owner of a folder, you can share it on a Windows Server 2012 R2 computer by right-clicking the folder in any File Explorer window, selecting *Share with, Specific People* from the context menu, and following the instructions in the *File Sharing* dialog box, as shown in Figure 4-1.

Figure 4-1

The *File Sharing* dialog box

This method of creating shares provides a simplified interface that contains only limited control over elements such as share permissions. You can specify only that the share users receive Read or Read/Write permissions to the share. If you are not the Creator Owner of the folder, you can access the *Sharing* tab of the folder's Properties sheet instead. Clicking the *Share* button launches the same dialog box, and clicking the *Advanced Sharing* button displays the Advanced Sharing dialog box. Clicking the Permissions button in the Advanced Sharing dialog box provides greater control over share permissions through the standard interface shown in "Setting Share Permissions," later in this lesson.

However, to take control of the shares on all your disks on all your servers and exercise granular control over their properties, use the *File and Storage Services* homepage in Server Manager.

Windows Server 2012 R2 supports two types of folder shares:

- *Server Message Blocks (SMB)* is the standard file-sharing protocol used by all versions of Windows.
- *Network File System (NFS)* is the standard file-sharing protocol used by most UNIX and Linux distributions.

When you install Windows Server 2012 R2, the setup program installs the Storage Services role service in the File and Storage Services role by default. When you create your first shared SMB folder, however, the system installs the File Server role service. To create NFS shares, you must manually install the Server for NFS role service.

To create a folder share using Server Manager, use the following procedure.

CREATE A FOLDER SHARE

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges. The Server Manager window appears.

1. Click the File and Storage Services icon and, in the submenu that appears, click Shares. The *Shares* homepage appears, as shown in Figure 4-2.

Figure 4-2

The Shares homepage

2. From the Tasks menu, select New Share. The *New Share Wizard* appears, displaying the *Select the profile for this share* page.
3. From the File share profile list, select one of the following options:
   - SMB Share–Quick provides basic SMB sharing with full share and NTFS permissions.
   - SMB Share–Advanced provides SMB sharing with full share and NTFS permissions and access to services provided by File Server Resource Manager.
   - SMB Share–Applications provides SMB sharing with settings suitable for Hyper-V and other applications.
   - NFS Share–Quick provides basic NFS sharing with authentication and permissions.
   - NFS Share–Advanced provides NFS sharing with authentication and permissions, plus access to services provided by File Server Resource Manager.
4. Click Next. The *Select the server and path for this share* page appears.
5. Select the server on which you want to create the share, and then either select a volume on the server or specify a path to the folder you want to share. Then click Next. The *Specify share name* page appears.
6. In the Share name text box, specify the name you want to assign to the share and click Next. The *Configure share settings* page appears.
7. Select any or all of the following options:
   - Enable access-based enumeration prevents users from seeing files and folders they do not have permission to access.
   - Allow caching of share enables offline users to access the contents of the share.
   - Enable BranchCache on the file share enables BranchCache servers to cache files accessed from this share.
   - Encrypt data access causes the server to encrypt remote file access to this share.

TAKE NOTE*

Offline Files, also known as client-side caching, is a Windows feature that enables client systems to maintain local copies of files they access from server shares. When a client selects the *Always available offline* option for a server-based file, folder, or share, the client system copies the selected data to the local drive and updates it regularly, so that the client user can always access it, even if the server is offline. To enable clients to use the Offline Files feature, the share must have the *Allow caching of share* check box selected. Windows Server 2012, Windows Server 2012 R2, Windows 8, and Windows 8.1 also have a new Always Offline mode for the Offline Files feature that causes clients to always use the cached copy of server files, providing better performance. To implement this mode, you must set the *Configure slow-link mode* Group Policy setting on the client to a value of 1 millisecond.

8. Click Next. The *Specify permissions to control access* page appears, as shown in Figure 4-3.

Figure 4-3

The *Specify permissions to control access* page of the New Share Wizard

9. Modify the default share and NTFS permissions as needed and click Next. The *Confirm selections* page appears.
10. Click Create. The *View results* page appears as the wizard creates the share.

CLOSE the *New Share Wizard.*

After you create a share with the wizard, the new share appears in the *Shares* tile of the *Shares* homepage in Server Manager.

You can now use the tile to manage a share by right-clicking it and opening its Properties sheet, or by clicking *Stop Sharing*. The Properties sheet for a share in Server Manager provides access to the exact same controls found on the *Specify permissions to control access* and *Configure share settings* pages in the New Share Wizard.

Assigning Permissions

THE BOTTOM LINE Protect your data by controlling who can access it.

Using Windows Server 2012 R2, you can control access to a file server to provide network users with the access they need, while protecting other files against possible intrusion and damage, whether deliberate or not. To implement this access control, Windows Server 2012 R2 uses permissions.

Permissions are privileges granted to specific system entities, such as users, groups, or computers, enabling them to perform a task or access a resource. For example, you can grant a specific user permission to read a file while denying that same user the permissions needed to modify or delete the file.

Windows Server 2012 R2 has several sets of permissions that operate independently of each other. As a server administrator, you should be familiar with the operation of the following four permission systems:

- Share permissions control access to folders over a network. To access a file over a network, a user must have appropriate share permissions (and appropriate NTFS permissions, if the shared folder is on an NTFS volume).
- NTFS permissions control access to the files and folders stored on disk volumes formatted with the NTFS file system. To access a file, whether on the local system or over a network, a user must have the appropriate NTFS permissions.
- Registry permissions control access to specific parts of the Windows registry. An application that modifies registry settings or a user attempting to manually modify the registry must have the appropriate registry permissions.
- Active Directory permissions control access to specific parts of an AD DS hierarchy. Although file servers typically do not function as AD DS domain controllers, server administrators might use these permissions when servicing computers that are members of a domain.

All these permission systems operate independently of each other and sometimes combine to provide increased protection to a specific resource. For example, you might grant Ralph the NTFS permissions needed to access a spreadsheet stored on a file server volume. If Ralph sits down at the file server console and logs on as himself, he can access that spreadsheet. However, if Ralph is working at his own computer, he cannot access the spreadsheet until you create a share containing the file and grant Ralph the proper share permissions.

For network users to be able to access a shared folder on an NTFS drive, you must grant them both share permissions and NTFS permissions. As you saw earlier, you can grant these permissions as part of the share creation process, but you can also modify the permissions at any time afterward.

Understanding the Windows Permission Architecture

Permissions protect all files, folders, shares, registry keys, and AD DS objects.

To store the permissions, each element has an ***access control list (ACL)***. An ACL is a collection of individual permissions, in the form of ***access control entries (ACEs)***. Each ACE consists of a ***security principal*** (the name of the user, group, or computer granted the permissions) and the specific permissions assigned to that security principal. When you manage permissions in any of the Windows Server 2012 R2 permission systems, you are actually creating and modifying the ACEs in an ACL.

It is important to understand that, in all Windows operating systems, permissions are stored as part of the protected element, not the security principal granted access. For example, when you grant a user the NTFS permissions needed to access a file, the ACE you create is stored in the file's ACL; it is not part of the user account. You can move the file to a different location, and its permissions go with it.

To manage permissions in Windows Server 2012 R2, you use a tab in the protected element's Properties sheet, like the one shown in Figure 4-4, with the security principals listed at the top and the permissions associated with them at the bottom. Share permissions are typically found on a *Share Permissions* tab, and NTFS permissions are located on a *Security* tab. All Windows permission systems use the same basic interface, although the permissions themselves vary. Server Manager also provides access to NTFS and share permissions, using a slightly different interface.

Figure 4-4

The Security tab of a Properties sheet

Understanding Basic and Advanced Permissions

The permissions protecting a particular system element are not like the keys to a lock, which provide either full access or no access at all. Permissions are designed to be granular, enabling you to grant specific degrees of access to security principals.

For example, you can use NTFS permissions to control not only who has access to a spreadsheet, but also the degree of access. You might grant Ralph permission to read and modify the spreadsheet, but Alice can only read it, and Ed cannot see it at all.

To provide this granularity, each Windows permission system has an assortment of permissions that you can assign to a security principal in any combination. Depending on the permission system you are working with, you might have dozens of different permissions available for a single system element.

If this is all starting to sound extremely complex, don't worry. Windows provides preconfigured permission combinations suitable for most common access control chores. When you open the Properties sheet for a system element and look at its *Security* tab, the NTFS permissions you see are called ***basic permissions***. Basic permissions are actually combinations of ***advanced permissions***, which provide the most granular control over the element.

For example, the NTFS permission system has 14 advanced permissions that you can assign to a folder or file. However, it also has 6 basic permissions that are various combinations of the 14 advanced permissions. You can also assign both types of permissions in a single ACE, combining a basic permission with one or more advanced permissions, to create a customized combination. In most cases, however, you work only with basic permissions. Many administrators rarely, if ever, work directly with advanced permissions.

If you do find it necessary to work with advanced permissions directly, Windows makes it possible. After you click the *Advanced* button on the *Security* tab of any Properties sheet, you access the ACEs for the selected system element directly through an *Advanced Security Settings* dialog box (see Figure 4-5). System Manager provides access to the same dialog box through a share's Properties sheet.

Figure 4-5

The *Advanced Security Settings* dialog box

Setting Share Permissions

On Windows Server 2012 R2, shared folders have their own permission system, which is completely independent from the other Windows permission systems.

For network users to access shares on a file server, you must grant them the appropriate share permissions. By default, the Everyone special identity receives the Allow Read share permission to any new shares you create using File Explorer. In shares you create using Server Manager, the Everyone special identity receives the Allow Full Control share permission.

To modify the share permissions for an existing share via File Explorer, you open the Properties sheet for the shared folder, select the *Sharing* tab, and click *Advanced Sharing* and then *Permissions* to open the *Share Permissions* tab, as shown in Figure 4-6.

Figure 4-6

The Share Permissions tab for a shared folder

By using this interface, you can add security principals and allow or deny them the three share permissions listed in Table 4-1.

Table 4-1

Share Permissions and their functions

Share Permission	Allows or Denies Security Principals the Ability to:
Full Control	• Change file permissions • Take ownership of files • Perform all tasks allowed by the Change permission
Change	• Create folders • Add files to folders • Change data in files • Change file attributes • Delete folders and files • Perform all actions permitted by the Read permission
Read	• Display folder names, filenames, file data and attributes • Execute program files • Access other folders within the shared folder

To set share permissions via Server Manager while creating a share or modifying an existing one, use the following procedure.

SET SHARE PERMISSIONS

GET READY. Log on to Windows Server 2012 R2, using an account with domain administrative privileges.

1. In the *Server Manager* window, click the File and Storage Services icon. In the submenu, click Shares. The *Shares* homepage appears.
2. In the *Shares* tile, right-click a share and, from the context menu, select Properties. The Properties sheet for the share appears.
3. Click Permissions. The *Permissions* page appears.
4. Click Customize Permissions. The *Advanced Security Settings* dialog box for the share appears.
5. Click the Share tab to display the interface shown in Figure 4-7.

Figure 4-7

The Share tab of the Advanced Security Settings dialog box for a share in Server Manager

6. Click Add. A *Permission Entry* dialog box for the share appears.
7. Click the Select a principal link to display the *Select User, Computer, Service Account, or Group* dialog box.
8. Type the name of or search for the security principal to which you want to assign share permissions and click OK. The *Permission Entry* dialog box displays the security principal you specified.
9. Select the type of permissions you want to assign (Allow or Deny).
10. Select the check boxes for the permissions you want to assign and click OK. The *Advanced Security Settings* dialog box displays the new access control entry you just created.
11. Click OK to close the *Advanced Security Settings* dialog box.
12. Click OK to close the share's Properties sheet.

CLOSE the *Server Manager* window.

When assigning share permissions, you must be aware that they do not combine like NTFS permissions. If you grant Alice the Allow Read and Allow Change permissions to the shared C:\Documents\Alice folder and later deny her all three permissions to the shared C:\Documents folder, the Deny permissions prevent her from accessing any files through the C:\Documents share, including those in the C:\Documents\Alice folder. However, she can still access her files through the C:\Documents\Alice share because of the Allow permissions. In other words, the C:\Documents\Alice share does not inherit the Deny permissions from the C:\Documents share.

Understanding NTFS Authorization

Most Windows installations today use the NTFS and ReFS file systems, as opposed to FAT32. One main advantage of NTFS and ReFS is that they support permissions, which FAT32 does not.

As described earlier in this lesson, every file and folder on an NTFS or ReFS drive has an ACL that consists of ACEs, each of which contains a security principal and the permissions assigned to that principal.

In the NTFS permission system, which ReFS also supports, the security principals involved are users and groups, which Windows refers to using ***security identifiers (SIDs)***. When a user attempts to access an NTFS file or folder, the system reads the user's security access token, which contains the SIDs for the user's account and all groups to which the user belongs. The system then compares these SIDs to those stored in the file or folder's ACEs, to determine what access the user should have. This process is called ***authorization***.

Assigning Basic NTFS Permissions

Most file server administrators work with basic NTFS permissions almost exclusively because they do not need to work directly with advanced permissions for most common access-control tasks.

Table 4-2 lists the basic permissions that you can assign to NTFS files or folders, and the capabilities that they grant to their possessors.

Table 4-2

NTFS Basic Permissions

Standard Permission	When Applied to a Folder, Enables a Security Principal to:	When Applied to a File, Enables a Security Principal to:
Full Control	• Modify the folder permissions • Take ownership of the folder • Delete subfolders and files contained in the folder • Perform all actions associated with all the other NTFS file permissions	• Modify the file permissions • Take ownership of the file • Perform all actions associated with all the other NTFS folder permissions
Modify	• Delete the folder • Perform all actions associated with the Write and the Read & Execute permissions	• Modify the file • Delete the file • Perform all actions associated with the Write and the Read & Execute permissions
Read and Execute	• Navigate through restricted folders to reach other files and folders • Perform all actions associated with the Read and List Folder Contents permissions	• Perform all actions associated with the Read permission • Run applications
List Folder Contents	• View the names of the files and subfolders contained in the folder	• Not applicable
Read	• See the files and subfolders contained in the folder • View the folder's ownership, permissions, and attributes	• Read the file contents • View the file's ownership, permissions, and attributes
Write	• Create new files and subfolders inside the folder • Modify the folder attributes • View the folder's ownership and permissions	• Overwrite the file • Modify the file attributes • View the file's ownership and permissions

To assign basic NTFS permissions to a shared folder, the options are essentially the same as with share permissions. You can open the folder's Properties sheet in File Explorer and select the *Security* tab, or you can open a share's Properties sheet in Server Manager, as in the following procedure.

ASSIGN BASIC NTFS PERMISSIONS

GET READY. Log on to Windows Server 2012 R2, using an account with domain administrative privileges. The Server Manager window appears.

1. Click the File and Storage Services icon and, in the submenu that appears, click Shares. The *Shares* homepage appears.
2. In the *Shares* tile, right-click a share and, from the context menu, select Properties. The Properties sheet for the share appears.
3. Click Permissions. The *Permissions* page appears.
4. Click Customize Permissions. The *Advanced Security Settings* dialog box for the share appears, displaying the *Permissions* tab, as shown in Figure 4-8. This dialog box is as close as the Windows graphical interface can come to displaying the contents of an ACL. Each line in the *Permission Entries* list is essentially an ACE and includes the following information:
   - *Type* specifies whether the entry allows or denies the permission.
   - *Principal* specifies the name of the user, group, or device principal receiving the permission.
   - *Access* specifies the name of the permission assigned to the security principal. If the entry is used to assign multiple advanced permissions, the word *Special* appears in this field.
   - *Inherited From* specifies whether the permission is inherited and, if so, from where it is inherited.
   - *Applies To* specifies whether the permission is to be inherited by subordinate objects and, if so, by which ones.

Figure 4-8

The *Advanced Security Settings* dialog box for a share in Server Manager

5. Click Add. A *Permission Entry* dialog box for the share appears.
6. Click the Select a principal link to display the *Select User, Computer, Service Account, or Group* dialog box.
7. Type the name of or search for the security principal to which you want to assign share permissions and click OK. The *Permission Entry* dialog box displays the security principal you specified.
8. From the Type drop-down list, select the type of permissions you want to assign (Allow or Deny).
9. From the Applies to drop-down list, specify which subfolders and files should inherit the permissions you are assigning.
10. Select the check boxes for the basic permissions you want to assign and click OK. The *Advanced Security Settings* dialog box displays the new access control entry you just created.
11. Click OK to close the *Advanced Security Settings* dialog box.
12. Click OK to close the Properties sheet.

CLOSE the *Server Manager* window.

Configuring Volume Shadow Copies

THE BOTTOM LINE

Volume Shadow Copies is a Windows Server 2012 R2 feature that enables you to maintain previous versions of files on a server, so that if users accidentally delete or overwrite a file, they can access a copy. You can implement shadow copies only for an entire volume; you cannot select specific shares, folders, or files.

To configure a Windows Server 2012 R2 volume to create shadow copies, use the following procedure.

CONFIGURE SHADOW COPIES

GET READY. Log on to Windows Server 2012 R2, using an account with domain administrative privileges.

1. Click the File Explorer icon on the taskbar to display the *File Explorer* window.
2. In the Folders list, expand the Computer container, right-click a volume and, from the context menu, select Configure Shadow Copies. The *Shadow Copies* dialog box appears, as shown in Figure 4-9.

Figure 4-9

The Shadow Copies dialog box

3. In the Select a Volume box, choose the volume for which you want to enable shadow copies. By default, when you enable shadow copies for a volume, the system uses the following settings:
   - It stores the shadow copies on the selected volume.
   - It reserves a minimum of 300 MB of disk space for the shadow copies.
   - It creates shadow copies at 7:00 AM and 12:00 PM every weekday.
4. To modify the default parameters, click Settings. The *Settings* dialog box appears.
5. In the Storage Area box, specify the volume where you want to store the shadow copies. For a server operating with a high I/O load, such as a file server, Microsoft recommends that, for best performance, you create the Shadow Copies storage area on another volume, one that does not have Shadow Copies enabled. However, some third-party backup utilities require shadow copies to be stored on the same volume as the data.
6. Specify the Maximum Size for the storage area or choose the No Limit option. If the storage area fills up, the system begins deleting the oldest shadow copies, so if many large files are stored on the volume, increasing the size of the storage area can be beneficial. However, no matter how much space you allocate to the storage area, Windows Server 2012 R2 supports a maximum of 64 shadow copies for each volume, after which the system begins deleting the oldest copies.
7. Click Schedule. The *Schedule* dialog box appears. By using the controls provided, you can modify the existing shadow copies tasks, delete them, or create new ones, based on your users' needs. Scheduling shadow copies to occur too frequently can degrade server performance and cause copies to be aged out too quickly, whereas scheduling them to occur too infrequently can cause users to lose work because the most recent copy is too old.

8. Click OK twice to close the *Schedule* and *Settings* dialog boxes.
9. Click Enable. The system enables the Shadow Copies feature for the selected volume and creates the first copy in the designated storage area.

CLOSE File Explorer.

After you complete this procedure, users can restore previous versions of files on the selected volumes from the *Previous Versions* tab on any file or folder's Properties sheet.

Configuring NTFS Quotas

THE BOTTOM LINE

Managing disk space is a constant concern for server administrators. One way to prevent users from monopolizing large amount of storage is to implement quotas. Windows Server 2012 R2 supports two types of storage quotas. The more elaborate of the two is implemented as part of File Server Resource Manager. The second, simpler option is NTFS quotas.

NTFS quotas enable you to set a storage limit for users of a particular volume. Depending on how you configure the quota, users exceeding the limit can be denied disk space or just receive a warning. The space consumed by individuals users is measured by the size of the files they own or create.

NTFS quotas are relatively limited in that you can set only a single limit for all users of a volume. The feature is also limited in the actions it can take in response to a user exceeding the limit. The quotas in File Server Resource Manager, by contrast, are much more flexible in the nature of the limits you can set and the responses of the program, which can send e-mail notifications, execute commands, and generate reports, as well as log events.

To configure NTFS quotas for a volume, use the following procedure.

CONFIGURE NTFS QUOTAS

GET READY. Log on to Windows Server 2012 R2, using an account with domain administrative privileges.

1. Click the File Explorer icon in the taskbar. The *File Explorer* window appears.
2. In the Folders list, expand the Computer container, right-click a volume and, from the context menu, select Properties. The Properties sheet for the volume appears.
3. Click the Quota tab to display the interface shown in Figure 4-10.

Figure 4-10

The Quota tab of a volume's Properties sheet

4. Select the Enable quota management check box to activate the rest of the controls.
5. If you want to prevent users from consuming more than their quota of disk space, select the Deny disk space to users exceeding quota limit check box.
6. Select the Limit disk space to radio button and specify amounts for the quota limit and the warning level.
7. Select the Log event check boxes to control whether users exceeding the specified limits should trigger log entries.
8. Click OK to create the quota and close the Properties sheet.

CLOSE Windows Explorer.

Configuring Work Folders

THE BOTTOM LINE

Work Folders is a Windows Server 2012 R2 feature that enables administrators to provide their users with synchronized access to their files on multiple workstations and devices, while storing them on a network file server. The principle is roughly the same as Microsoft's OneDrive service, except that the files are stored on a private Windows server, instead of a cloud server on the Internet. This enables administrators to maintain control over the files, backing them up, classifying them, and/or encrypting them as needed.

To set up the Work Folders environment, you install the Work Folders role service under the File and Storage Services role on a server running Windows Server 2012 R2. This installs the File Server role service, if it is not installed already, and the IIS Hostable Web Core feature, which makes it possible for the server to respond to incoming HTTP requests from Work Folders clients on the network. You then create a new type of share called a sync share.

On the client side, you configure Work Folders in the Windows 8.1 Control Panel, specifying the email address of the user and the location of the Work Folders on the local disk. The system also creates a system folder called Work Folders, which appears in File Explorer and in file management dialogs. When the user saves files to the Work Folders on the client system, they are automatically synchronized with the user's folder on the Work Folders server.

Users can configure as many Work Folders clients as they need on different computers or other devices. After saving files to their Work Folders on their office workstations, for example, users can go home and find those files already synchronized to their home computers. In the same way, Work Folders can synchronize a user's files to a portable device at the office, and the user can work on them while offline during the commute home. Arriving home and connecting to the Internet, the device synchronizes the files back to the server , so that the user finds the latest versions on the office computer the next day.

Work Folders is not designed to be a collaborative tool; it is just a means synchronizing folders between multiple devices, while enabling administrators to retain control over them. It is possible to specify that Work Folders files remain encrypted during synchronization, and administrators can impose secuity policies that force the use of lock screens and mandatory data wipes for lost machines.

■ Business Case Scenarios

Scenario 4-1: Assigning Permissions

While you are working the help desk for a corporate network, a user named Leo calls to request access to the files for Trinity, a new classified project. The Trinity files are stored in a shared folder on a Windows Server 2012 R2 workgroup file server, which is locked in a secured underground data storage facility in New Mexico. After verifying that he has the appropriate security clearance for the project, you create a new group on the file server called TRINITY_USERS and add Leo's user account to that group. Then, you add the TRINITY_USER group to the access control list for the Trinity folder on the file server, and assign the group the following NTFS permissions:

- Allow Modify
- Allow Read & Execute
- Allow List Folder Contents
- Allow Read
- Allow Write

Sometime later, Leo calls you to tell you that he is able to access the Trinity folder and read the files stored there, but he has been unable to save changes back to the server. What is the most likely cause of the problem?

Scenario 4-2: Accessing Orphaned Files

Libby, a new hire in the IT department, approaches you, her supervisor, ashen-faced. A few minutes earlier, the president of the company called the help desk and asked Libby to give his new assistant the permissions needed to access his personal budget spreadsheet. As she was attempting to assign the permissions, she accidentally deleted the BUDGET_USERS group from the spreadsheet's access control list. Libby is terrified because that group was the only entry in the file's ACL. Now, no one can access the spreadsheet file, not even the president or the Administrator account. Is there any way to gain access to the file, and if so, how?

Configuring Print and Document Services

LESSON 5

Deploying a Print Server

THE BOTTOM LINE

Like the file-sharing functions discussed in previous lessons, print device sharing is one of the most basic applications for which local area networks were designed.

Installing, sharing, monitoring, and managing a single network print device is relatively simple, but when you are responsible for dozens or even hundreds of print devices on a large enterprise network, these tasks can be overwhelming.

Understanding the Windows Print Architecture

You need to understand the terms that Microsoft uses when referring to the various components of the network printing architecture.

Printing in Microsoft Windows typically involves these four components:

- A ***print device*** is the actual hardware that produces hard-copy documents on paper or other print media. Windows Server 2012 R2 supports both *local print devices* directly attached to computer ports and *network interface print devices* connected to the network, either directly or through another computer.
- In Windows, a ***printer*** is the software interface through which a computer communicates with a print device. Windows Server 2012 R2 supports numerous physical interfaces, including Universal Serial Bus (USB), IEEE 1394 (FireWire), parallel (LPT), serial (COM), Infrared Data Access (IrDA), Bluetooth ports, and network printing services such as lpr, Internet Printing Protocol (IPP), and standard TCP/IP ports.
- A ***print server*** is a computer (or standalone device) that receives print jobs from clients and sends them to print devices locally attached or connected to the network.
- A ***printer driver*** is a device driver that converts the print jobs generated by applications into an appropriate string of commands for a specific print device. Printer drivers are designed for specific print devices and provide applications with access to all a print device's features.

TAKE NOTE*

Printer and *print device* are the most commonly misused terms of the Windows printing vocabulary. Obviously, many sources use *printer* to refer to the printing hardware. However, in Windows, printer and print device are not equivalents. For example, you can add a printer to a Windows Server 2012 R2 computer without a physical print device being present. The computer can then host the printer, print server, and printer driver. These three components enable the computer to process the print jobs and store them in a print queue until the print device is available.

UNDERSTANDING WINDOWS PRINTING

These four components—print device, printer, print server, and printer driver—work together to process the print jobs produced by Windows applications and turn them into hard-copy documents, as shown in Figure 5-1.

Figure 5-1

The Windows print architecture

Before you can print documents in Windows, you must install at least one printer. To install a printer in Windows, you must do the following:

- Select the print device's specific manufacturer and model.
- Specify the port (or other interface) the computer will use to access the print device.
- Supply a printer driver specifically created for that print device.

When you print a document in an application, you select the destination printer for the print job.

The printer is associated with a printer driver that takes the commands generated by the application and converts them into a ***printer control language (PCL)***, a language understood by the printer. PCLs can be standardized, like the PostScript language, or they can be proprietary languages developed by the print device manufacturer.

The printer driver enables you to configure the print job to use the print device's various capabilities. These capabilities are typically incorporated into the printer's Properties sheet. For example, your word-processing application does not know if your print device is color, monochrome, or supports duplex printing; the printer driver provides support for print device features such as these.

After the printer processes a print job, it stores the job in a print queue, known as a ***spooler***. Depending on the arrangement of the printing components, the spooled jobs might be in a PCL format, ready to go to the print device, or in an interim format, in which case the printer driver must process the spooled jobs into the PCL format before sending them to the device. If other jobs are waiting to be printed, a new job might wait in the spooler for some time. When the server finally sends the job to the print device, the device reads the PCL commands and produces the hard-copy document.

Sharing a Printer

Using Windows Server 2012 R2 as a print server can be simple or complex, depending on how many clients the server has to support and how much printing they do.

For a home or small business network, in which a handful of users need occasional access to the printer, no special preparation is necessary. However, if the computer must support heavy printer use, you might need the following hardware upgrades:

- **Additional system memory:** Processing print jobs requires system memory, just like any other application. If you plan to run heavy print traffic through a Windows Server 2012 R2 server, in addition to other roles or applications, make sure that the computer has sufficient memory to support all its functions.
- **Additional disk space:** When a print device is busy, the print server spools additional incoming print jobs temporarily on a hard drive until the print device is free to receive them. Depending on the amount of print traffic and the types of print jobs, the print server might require a substantial amount of temporary storage for this purpose.
- **Make the computer a dedicated print server:** In addition to memory and disk space, using Windows Server 2012 R2 as a print server requires processor clock cycles, just like any other application. On a server handling heavy print traffic, other roles and applications are likely to experience substantial performance degradation. If you need a print server to handle heavy traffic, consider dedicating the computer to print server tasks only and deploying other roles and applications elsewhere.

On a Windows Server 2012 R2 computer, you can share a printer as you are installing it or at any time afterward. On older printers, initiate the installation process by launching the *Add Printer Wizard* from the *Devices and Printers* control panel. However, most of the print devices on the market today use either a USB connection to a computer or an Ethernet or wireless connection to a network.

In the case of a USB-connected printer, you plug the print device into a USB port on the computer and turn on the device to initiate the installation process. Manual intervention is only required when Windows Server 2012 R2 does not have a driver for the print device.

For network-attached print devices, an installation program supplied with the product locates the print device on the network, installs the correct drivers, creates a printer on the computer, and configures the printer with the proper IP address and other settings.

After you install the printer on the Windows Server 2012 R2 computer that functions as your print server, you can share it with your network clients.

Managing Printer Drivers

Printer driver components enable your computers to manage the capabilities of your print devices. When you install a printer on a server running Windows Server 2012 R2, you install a driver that other Windows computers also can use.

The printer drivers you install on Windows Server 2012 R2 are the same drivers that Windows workstations and other server versions use, with one stipulation. As a 64-bit platform, Windows Server 2012 R2 uses 64-bit device drivers, which are suitable for other computers running 64-bit versions of Windows. If you have 32-bit Windows systems on your network, however, you must install a 32-bit driver on the server for those systems to use.

The *Additional Drivers* dialog box, accessible from the *Sharing* tab of a printer's Properties sheet, enables you to install drivers for other processor platforms. However, you must install those drivers from a computer running on the alternative platform.

In other words, to install a 32-bit driver for a printer on a server running Windows Server 2012 R2, you must access the printer's Properties sheet from a computer running 32-bit version of Windows. You can do this by accessing the printer directly through the network using Windows Explorer, or by running the Print Management snap-in on the 32-bit system and using it to manage your Windows Server 2012 R2 print server.

Using Remote Access Easy Print

When a Remote Desktop Services client connects to a server, it runs applications using the server's processor(s) and memory. However, if that client wants to print a document from one of those applications, it wants the print job to go to the print device connected to the client computer.

Remote Desktop Easy Print is the component that enables Remote Desktop clients to print to their local print devices. Easy Print takes the form of a printer driver installed on the server, along with the Remote Desktop Session Host role service.

The Remote Desktop Easy Print driver appears in the Print Management snap-in automatically but it is not associated with a particular print device. Instead, the driver functions as a redirector, enabling the server to access the printers on the connected clients.

On Windows Server 2012 R2, Easy Print requires no configuration other than the allowance of Remote Desktop connections or the installation of the Remote Desktop Services role. However, as soon as it is operational, it provides the server administrator with additional access to the printers on the Remote Desktop clients.

When a Remote Desktop client connects to a server via the Remote Desktop Connection program or the RD Web Access site, the printers installed on the client system are redirected to the server and appear in the Print Management snap-in as redirected server printers, as shown in Figure 5-2.

Figure 5-2

Printers redirected by Easy Print on a Remote Desktop server

A client running an application on the server can therefore print to a local print device via the redirected printer. You can also open the Properties sheet for the redirected printer in the usual manner and manipulate its settings.

Configuring Printer Security

Like folder shares, clients must have the proper permissions to access a shared printer.

Printer permissions are much simpler than NTFS permissions; they dictate whether users are allowed to use the printer, manage documents submitted to the printer, or manage the properties of the printer itself. To assign permissions for a printer, use the following procedure.

ASSIGN PRINTER PERMISSIONS

GET READY. Log on to Windows Server 2012 R2 using a domain account with Administrator privileges.

1. Open the Control Panel and select Hardware> Devices and Printers. The *Devices and Printers* window appears.
2. Right-click one of the printer icons in the window and, from the context menu, select Printer Properties. The printer's Properties sheet appears.

   Click the Security tab, as shown in Figure 5-3. The top half of the display lists all the security principals now possessing permissions to the selected printer. The bottom half lists the permissions held by the selected security principal.

Figure 5-3

The Security tab of a printer's Properties sheet

3. Click Add. The *Select Users, Computers, Service Accounts, or Groups* dialog box appears.

TAKE NOTE*

This procedure assumes that the Windows Server 2012 R2 computer is a member of an Active Directory domain. When you assign printer permissions on a standalone server, you select local user and group accounts to be the security principals that receive the permissions.

4. In the Enter the object names to select text box, type a user or group name, and then click OK. The user or group appears in the *Group or user names* list of the printer's properties sheet.
5. Select the security principal you added, and then select or clear the check boxes in the bottom half of the properties sheet to Allow or Deny the user any of the basic permissions.
6. Click OK to close the Properties sheet.

CLOSE the control panel.

Like NTFS permissions, printer permissions come in two types: basic and advanced. Each of the three basic permissions consists of a combination of advanced permissions, as listed in Table 5-1.

Table 5-1

Basic Printer Permissions

Permission	Capabilities	Advanced Permissions	Default Assignments
Print	• Connect to a printer • Print documents • Pause, resume, restart, and cancel the user's own documents	• Print • Read Permissions	Assigned to the Everyone special identity
Manage this printer	• Cancel all documents • Share a printer • Change printer properties • Delete a printer • Change printer permissions	• Print • Manage Printers • Read Permissions • Change Permissions • Take Ownership	Assigned to the Administrators group
Manage documents	• Pause, resume, restart, and cancel all users' documents • Control job settings for all documents	• Manage Documents • Read Permissions • Change Permissions • Take Ownership	Assigned to the Creator Owner special identity

Managing Printers

Users with the Allow Manage This Printer permission can go beyond manipulating queued documents; they can reconfigure the printer itself. Managing a printer refers to altering the operational parameters that affect all users and controlling access to the printer.

Generally, most software-based tasks that fall under the category of managing a printer are those you perform once while setting up the printer for the first time. Day-to-day printer management is more likely to involve physical maintenance, such as clearing print jams, reloading paper, and changing toner or ink cartridges. However, the following sections examine some of the printer manager's typical configuration tasks.

SETTING PRINTER PRIORITIES

In some cases, administrators with the Manage This Printer permission might want to give certain users in your organization priority access to a print device so that when print traffic is heavy, their jobs are processed before those of other users. To do this, you must create multiple printers, associate them with the same print device, and then modify their priorities, as described in the following procedure.

SET A PRINTER'S PRIORITY

GET READY. Log on to Windows Server 2012 R2 using an account with the Manage This Printer permission.

1. Open the Control Panel and select Hardware> Devices and Printers. The *Devices and Printers* window appears.
2. Right-click one of the printer icons and then, from the context menu, select Printer Properties. The Properties sheet for the printer appears.
3. On the *Advanced* tab set the Priority spin box to a number representing the highest priority you want to set for the printer. Higher numbers represent higher priorities. The highest possible priority is 99.
4. On the *Security* tab, add the users or groups that you want to provide with high-priority access to the printer and assign the Allow Print permission to them.
5. Revoke the Allow Print permission from the Everyone special identity.
6. Click OK to close the Properties sheet.
7. Create an identical printer, using the same printer driver and pointing to the same print device. Leave the Priority setting to its default value of 1 and leave the default permissions in place.
8. Rename the printers, specifying the priority assigned to each one.

CLOSE the control panel.

Inform the privileged users that they should send their jobs to the high-priority printer. All jobs sent to that printer are processed before those sent to the other, lower-priority printer.

SCHEDULING PRINTER ACCESS

Sometimes, you might want to limit certain users' access to a printer to specific times of the day or night. For example, your organization might have a color laser printer that the company's graphic designers use during business hours, but you permit other employees to use it after 5:00 PM. To do this, you associate multiple printers with a single print device, much as you did to set different printer priorities.

After creating two printers, both pointing to the same print device, you configure their scheduling using the following procedure.

SCHEDULE PRINTER ACCESS

GET READY. Log on to Windows Server 2012 R2 using an account with the Manage Printer permission. When the logon process is completed, close the *Initial Configuration Tasks* window and any other windows that open.

1. Open the Control Panel and select Hardware> Devices and Printers. The *Devices and Printers* window appears.
2. Right-click one of the printer icons and then, from the context menu, select Printer Properties. The Properties sheet for the printer appears.
3. On the *Advanced* tab, select the Available from radio button and then, in the two spin boxes provided, select the range of hours you want the printer to be available.
4. On the Security tab, add the users or groups that you want to provide with access to the printer during the hours you selected and grant them the Allow Print permission.
5. Revoke the Allow Print permission from the Everyone special identity.
6. Click OK to close the Properties sheet.

CLOSE the control panel.

The two printers are now available only during the hours you have specified.

CREATING A PRINTER POOL

As mentioned earlier, a printer pool increases the production capability of a single printer by connecting it to multiple print devices. When you create a printer pool, the print server sends each incoming job to the first print device it finds that is not busy. This effectively distributes the jobs among the available print devices, as shown in Figure 5-4, providing users with more rapid service.

Figure 5-4

Printer pooling shares print jobs among multiple print devices

To configure a printer pool, use the following procedure.

CREATE A PRINTER POOL

GET READY. Log on to Windows Server 2012 R2 using an account with the Manage Printer permission. When the logon process is completed, close the Initial *Configuration Tasks* window and any other windows that open.

1. Open the Control Panel and select Hardware> Devices and Printers. The *Devices and Printers* window appears.
2. Right-click one of the printer icons and then, from the context menu, select Printer Properties. The Properties sheet for the printer appears.
3. On the Ports tab, select all ports to which the print devices are connected (see Figure 5-5).

Figure 5-5

The Ports tab of a printer's Properties sheet

4. Select the Enable printer pooling check box, and then click OK.

CLOSE the control panel.

To create a printer pool, you must have at least two identical print devices, or at least print devices that use the same printer driver. The print devices must be in the same location, because you cannot tell which print device will process a given document. You must also connect all print devices in the pool to the same print server. If the print server is a Windows Server 2012 R2 computer, you can connect the print devices to any viable ports.

■ Using the Print and Document Services Role

THE BOTTOM LINE

All printer sharing and management capabilities discussed in the previous sections are available on any Windows Server 2012 R2 computer in its default installation configuration. However, installing the Print and Document Services role on the computer provides additional tools that are particularly useful to administrators involved with network printing on an enterprise scale.

When you install the Print and Document Services role using Server Manager's Add Roles and Features Wizard, a *Select role services* page appears, enabling you to select from the options listed in Table 5-2.

Table 5-2

Role Service Selections for the Print Services Role

Role Service	System Services Installed	Description
Print Server	Print Spooler (Spooler)	• Installs the Print Management console for Microsoft Management Console (MMC), which enables administrators to deploy, monitor, and manage printers throughout the enterprise. • Is the only required role service when you add the Print Services role.
Distributed Scan Server	Distributed Scan Server (ScanServer)	• Enables the computer to receive documents from network-based scanners and forward them to the appropriate users.
Internet Printing	• World Wide Web Publishing Service (w3svc) • IIS Admin Service (iisadmin)	• Creates a website that enables users on the Internet to send print jobs to shared Windows printers.
LPD Service	TCP/IP Print Server (LPDSVC)	• Enables UNIX clients running the LPR (line printer remote) program to send their print jobs to Windows printers.

To install the Internet Printing role service, you must also install the Web Server (IIS) role with certain specific role services. The *Add Roles and Features Wizard* enforces these dependencies by displaying an *Add features that are required for Internet Printing?* message box when you select the Internet Printing role service. Clicking *Add Features* causes the wizard to select the exact role services within Web Server (IIS) role that the Internet Printing service needs.

As always, Windows Server 2012 R2 adds a new icon to the Server Manager navigation pane when you install a role. The Print Services homepage contains a filtered view of print-related event log entries, a status display for the role-related system services and role services, and performance counters, as shown in Figure 5-6.

Figure 5-6

The Print Services node in Server Manager

Using the Print Management Console

The Print Management snap-in for MMC, an administrative tool, consolidates the controls for the printing components throughout the enterprise into a single console. With this tool, you can access the print queues and Properties sheets for all network printers in the enterprise, deploy printers to client computers via Group Policy, and create custom views that simplify the process of detecting print devices that need attention due to errors or depleted consumables.

Windows Server 2012 installs the Print Management console when you add the Print and Document Services role to the computer. You can also install the console without the role by adding the Print and Document Services Tools feature, found under *Remote Server Administration Tools* > *Role Administration Tools* in Server Manager.

When you launch the Print Management console, the default display includes in the scope (left) pane the nodes listed in Table 5-3.

Table 5-3

Print Management Nodes

Node	Description
Custom Filters	Contains composite views of all printers hosted by the print servers listed in the console, regulated by customizable filters
Print Servers	Lists all print servers that you have added to the console, and all drivers, forms, ports, and printers for each print server
Deployed Printers	Lists all printers you have deployed with Group Policy through the console

The following sections demonstrate some administration tasks you can perform with the Print Management console.

ADDING PRINT SERVERS

By default, the Print Management console displays only the local machine in its list of print servers. Each print server has four nodes beneath it, listing the drivers, forms, ports, and printers associated with that server.

To manage other print servers and their printers, you must first add them to the console, using the following procedure.

ADD A PRINT SERVER

GET READY. Log on to Windows Server 2012 R2 using a domain account with Administrator privileges.

1. In the *Server Manager* window, click Tools > Print Management. The *Print Management* console appears.
2. Right-click the Print Servers node and, from the context menu, click Add/Remove Servers. The *Add/Remove Servers* dialog box appears.
3. In the *Specify Print Server* section, click Browse. The *Select Print Server* dialog box appears.
4. Select the print server you want to add to the console and click Select Server. The server you selected appears in the *Add servers* box in the *Add/Remove Servers* dialog box.
5. Click Add to List. The server you selected appears in the *Print Servers* list.
6. Click OK. The server appears under the *Print Servers* node.

CLOSE the Print Management console.

You can now manage the printers associated with the server you have added to the console.

VIEWING PRINTERS

One major problem for printing on large enterprise networks is keeping track of dozens or hundreds of print devices, all in frequent use, and all needing attention regularly. Whether the maintenance required is a major repair, replenishing ink or toner, or just filling the paper trays, print devices cannot get the attention they need until an administrator is aware of the problem.

The Print Management console provides many ways to view the printing components associated with the network's print servers. To create views, the console takes the complete list of printers and applies various filters to it, selecting which printers to display. Under the Custom Filters node are four default filters, as listed in Table 5-4.

Table 5-4
Default Filters

Filter	Description
All Printers	Contains a list of all the printers hosted by all the print servers added to the console
All Drivers	Contains a list of all printer drivers installed on all print servers added to the console
Printers Not Ready	Contains a list of all printers that are not reporting a Ready status
Printers With Jobs	Contains a list of all printers that currently have jobs waiting in the print queue

Views such as Printer Not Ready are a useful way for you to identify printers that need attention, without having to browse individual print servers or search through a long list of every printer on the network. In addition to these defaults, you can create your own custom filters.

MANAGING PRINTERS AND PRINT SERVERS

After you use filtered views to isolate the printers you want to examine, selecting a printer displays its status, the number of jobs currently in its print queue, and the name of the print server hosting it. If you right-click the filter in the scope pane and, from the context menu, select *Show Extended View*, an additional pane appears containing the contents of the selected printer's queue (see Figure 5-7). You can manipulate the queued jobs just as you would from the print queue window on the print server console.

Figure 5-7

The Print Management console's extended view

The Print Management console also enables you to access the configuration interface for any printer or print server listed in any of its displays. Right-clicking a printer or print server anywhere in the console interface, and selecting *Properties* from the context menu, displays the same Properties sheet that you would see on the print server computer itself. You can then configure printers and print servers without having to travel to the site of the print server or establish a Remote Desktop connection to the print server.

DEPLOYING PRINTERS WITH GROUP POLICY

Configuring a print client to access a shared printer is a simple matter of browsing the network or the AD DS tree and selecting the printer. However, when you have to configure hundreds or thousands of print clients, the task becomes more complicated. AD DS helps simplify the process of deploying printers to large numbers of clients.

Publishing printers in the AD DS database enables users and administrators to search for printers by name, location, or model (if you populate the *Location* and *Model* fields in the printer object). To create a printer object in the AD DS database, you can either select the *List in the directory* check box while sharing the printer, or right-click a printer in the *Print Management* console and, from the context menu, select *List in Directory*.

To use AD DS to deploy printers to clients, you must configure the appropriate policies in a Group Policy Object (GPO). You can link a GPO to any domain, site, or organizational unit (OU) in the AD DS tree. When you configure a GPO to deploy a printer, all users or computers in that domain, site, or OU receive the printer connection by default when they log on.

Business Case Scenarios

Scenario 5-1: Enhancing Print Performance

You are a desktop support technician for a law firm with a group of 10 legal secretaries who provide administrative support to the attorneys. The secretaries use a single, shared, high-speed laser printer connected to a dedicated Windows Server 2012 R2 print server. They regularly print multiple copies of large documents, and although the laser printer is fast, it runs constantly. Sometimes, the secretaries have to wait 20 minutes or more after submitting a print job for their documents to reach the top of the queue. The office manager has offered to purchase additional printers for the department. However, the secretaries are accustomed to simply clicking the Print button, and don't like the idea of having to examine multiple print queues to determine which one has the fewest jobs before submitting a document. What can you do to provide the department with a printing solution that will enable the secretaries to utilize additional printers most efficiently?

Scenario 5-2: Troubleshooting Printer Delays

One of your small business clients has a print device connected to a server running Windows Server 2012 R2. He has shared the printer so that the other network users can access it. Often, the other users print large documents that take a long time to print, but sometimes your client and other users have important documents that need to be printed before any long documents that are waiting in the printer queue. What would you suggest to this user?

6 LESSON

Configuring Servers for Remote Management

Using Server Manager for Remote Management

THE BOTTOM LINE

Windows Server 2012 R2 facilitates remote server management, so that you do not need to work at the server console. This capability conserves server resources that can be devoted to applications.

Since Windows Server 2003, Server Manager has been the primary server administration tool for Windows Server. The most obvious improvement to the Server Manager tool in Windows Server 2012 R2 is the capability to perform administrative tasks on remote servers, as well as on the local system.

After you log on to a GUI installation of Windows Server 2012 R2 with an administrative account, Server Manager loads automatically, displaying the Welcome tile.

The Server Manager interface contains a navigation pane on the left with icons representing various views of server resources. Selecting an icon displays a homepage in the right pane, which contains tiles with information about the resource. The Dashboard page, which appears by default, contains, in addition to the Welcome tile, thumbnails that summarize the other views available in Server Manager, as shown in Figure 6-1. The other views include Local Server, All Servers, and server groups and role groups.

Figure 6-1

Dashboard thumbnails in Server Manager

Adding Servers

The primary difference between the Windows Server 2012 R2 Server Manager and previous versions is the capability to add and manage multiple servers at once.

Although only the local server appears in Server Manager when you first run it, you can add other servers, enabling you to manage them together. The servers you add can be physical or virtual, and can run any version of Windows Server since Windows Server 2003. After you add servers to the interface, you can create groups containing collections of servers, such as the servers at a particular location or those performing a particular function. These groups appear in the navigation pane, enabling you to administer them as a single entity.

To add servers in Server Manager, use the following procedure.

ADD SERVERS IN SERVER MANAGER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges. The Server Manager window appears.

1. In the navigation pane, click the All Servers icon. The All Servers homepage appears, as shown in Figure 6-2.

Figure 6-2

The All Servers homepage in Server Manager

2. From the Manage menu, select Add Servers. The Add Servers dialog box appears.
3. Select one of the following tabs to specify how you want to locate servers to add:
   - **Active Directory** enables you to search for computers running specific operating systems in specific locations in the local Active Directory Domain Services (AD DS) domain.
   - **DNS** enables you to search for servers in your configured Domain Name System (DNS) server.
   - **Import** enables you to supply a text file containing the names or IP addresses of the servers you want to add.
4. Initiate a search or upload a text file to display a list of available servers.
5. Select the servers you want to add and click the right arrow button to add them to the Selected list.
6. Click OK. The servers you selected are added to the All Servers homepage.

CLOSE the Server Manger console.

After you add remote servers to the Server Manager interface, they appear on the All Servers homepage. You can access them in various ways, depending on the Windows version the remote server is running.

ADDING WORKGROUP SERVERS

The procedure in the previous section assumes that the computer running Server Manager and the managed servers are members of an AD DS domain. You can usually add workgroup servers to Server Manager, but the system's attempts to access the remote servers fail with a "Credentials not valid" error.

Why is that? AD DS systems authenticate by using the Kerberos protocol, but Windows workgroup computers use an alternative authentication protocol called NTLM (NT LAN Manager). Essentially, the remote server tries to log on to the workgroup server and fails.

For the authentication to succeed, you must add the name of the workgroup server to the TrustedHosts list on the computer running Server Manager, by using a Windows PowerShell command with the following syntax:

```
Set-Item wsman:\localhost\Client\TrustedHosts
<servername> -Concatenate -Force
```

Managing Non-Domain Joined Servers

When you add servers that are members of an Active Directory Domain Services (AD DS) domain to the Server Manager interface, Windows Server 2012 R2 uses the standard Kerberos authentication protocol and your current logged on user credentials when connecting to the remote systems. You can also add servers that are not joined to an AD DS domain, but obviously, the system cannot authenticate using an AD DS account.

To manage a non-domain joined server using Server Manager and a server named MGMT01, you must first complete the following tasks:

- Supply administrative credentials for the non-domain joined server.
- Add the non-domain joined server to the MGMT01's WS-Management TrustedHosts list on the computer running Server Manager.

To add non-domain joined servers to Server Manager, you must use the DNS or Import option in the Add Servers Wizard. After creating the server entries, you must right-click each one and select Manage As from the context menu. This displays a Windows Security dialog box, in which you can supply credentials for an account with administrative privileges on the remote server.

Domain membership automatically establishes a trust relationship among the computers in the domain. To manage computers that are not in the same domain, you must establish that trust yourself by adding the computers you want to manage to the TrustedHosts list on the computer running Server Manager.

The TrustedHosts list exists on a logical drive called WSMan:; the path to the list itself is WSMan:\localhost\Client\TrustedHosts. To add a computer to the list, you use the Set-Item cmdlet in Windows PowerShell. After opening a Windows PowerShell session with administrative privileges on the computer running Server Manager, use the following command to add the servers you want to manage to the list:

```
Set-Item WSMan:\localhost\Client\TrustedHosts –value
<servername> -force
```

Managing Windows Server 2012 R2 Servers

After you add servers running Windows Server 2012 R2 to Server Manager, you can immediately use the Add Roles and Features Wizard to install roles and features on any server you add.

You can also perform other administrative tasks, such as configure NIC teaming and restart the server, because Windows Remote Management (WinRM) is enabled by default on Windows Server 2012 R2. ***WinRM*** is a Windows feature that enables administrators to execute management commands and scripts on remote computers, using a communications protocol called WS-Management Protocol.

CONFIGURING WINRM

WinRM enables you to manage a computer from a remote location using tools based on Windows Management Instrumentation (WMI) and Windows PowerShell. If the default WinRM setting has been modified, or if you want to change it manually, you can do so through the Server Manager interface.

On the Local Server homepage, the Properties tile contains a Remote management indicator that specifies the server's current WinRM status. To change the WinRM state, click the Remote management hyperlink to open the Configure Remote Management dialog box. Clearing the *Enable remote management of this server from other computers* check box disables WinRM, and selecting the check box enables it.

CONFIGURING WINDOWS FIREWALL

However, if you attempt to launch Microsoft Management Console (MMC) snap-ins targeting a remote server (such as the Computer Management console), you will receive an error because of the default Windows Firewall settings on Windows Server 2012 R2. MMC uses the Distributed Component Object Model (DCOM) for remote management, rather than WinRM, and these settings are not enabled by default.

To address this problem, you must enable the following inbound Windows Firewall rules on the remote server you want to manage:

- COM+ Network Access (DCOM-In)
- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

To modify the firewall rules on the remote system, you can use one of the following methods:

- Open the Windows Firewall with Advanced Security MMC snap-in on the remote server (if it is a Full GUI installation).
- Run the `Netsh AdvFirewall` command from an administrative command prompt.
- Use the NetSecurity module in Windows PowerShell.
- Create a Group Policy object containing the appropriate settings and apply it to the remote server.

For remote management solutions, the Group Policy method provides distinct advantages. Not only does it enable you to configure the firewall on the remote system without accessing the server console directly, it also can configure the firewall on Server Core installations without working from the command line. Finally, and possibly most important for large networks, you can use Group Policy to configure the firewall on all servers you want to manage at once.

To configure Windows Firewall settings using Group Policy, use the following procedure. This procedure assumes that the server is a member of an AD DS domain and has the Group Policy Management feature installed.

CONFIGURE WINDOWS FIREWALL WITH GROUP POLICY

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges. The Server Manager window appears.

1. Open the Group Policy Management console and create a new Group Policy object (GPO), giving it a name such as "Server Firewall Configuration."
2. Open the GPO you created using the Group Policy Management Editor.
3. Browse to the Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules node, as shown in Figure 6-3.

Figure 6-3

The *Windows Firewall with Advanced Security Inbound Rules* node in a Group Policy object

4. Right-click Inbound Rules and, from the context menu, select New Rule. The New Inbound Rule Wizard appears, displaying the Rule Type page.
5. Select the Predefined option and, in the drop-down list, select COM+ Network Access and click Next. The Predefined Rules page appears.
6. Click Next. The Action page appears, as shown in Figure 6-4.

Figure 6-4

The Action page of the New Inbound Rule Wizard

7. Leave the Allow the connection option selected and click Finish. The rule appears in the Group Policy Management Editor console.
8. Open the New Inbound Rule Wizard again.
9. Select the Predefined option and, in the drop-down list, select Remote Event Log Management and click Next. The Predefined Rules page appears, displaying the three rules in the Remote Event Log Management group.
10. Leave the three rules selected and click Next. The page appears.
11. Leave the *Allow the connection* option selected and click Finish. The three rules appear in the Group Policy Management Editor console.
12. Close the Group Policy Management Editor.
13. In the Group Policy Management console, link the Server Firewall Configuration GPO you just created to your domain.

CLOSE the Group Policy Management console.

The settings in the GPO you created deploy to your remote servers the next time they recycle or restart, and you can use MMC snap-ins, such as Computer Management and Disk Management, on them.

Managing Down-Level Servers

The Windows Firewall rules to enable for remote servers running Windows Server 2012 R2 are also disabled by default on computers running earlier versions of Windows Server, so you need to enable them there as well.

Unlike Windows Server 2012 R2, however, earlier versions of the operating system also lack the WinRM support needed for them to be managed using the new Server Manager.

By default, after you add servers running Windows Server 2008 or Windows Server 2008 R2 to the Windows Server 2012 R2 Server Manager, they appear with a manageability status that reads "Online – Verify WinRM 3.0 service is installed, running, and required firewall ports are open."

To add WinRM support to servers running Windows Server 2008 or Windows Server 2008 R2, you must download and install the following updates:

- .NET Framework 4.0
- Windows Management Framework 3.0

These updates are available from the Microsoft Download Center at Microsoft's website.

After you install the updates, the system automatically starts the Windows Remote Management service, but you must complete the following tasks on the remote server:

- Enable the Windows Remote Management (HTTP-In) rules in Windows Firewall.
- Create a WinRM listener by running the `winrm quickconfig` command at a command prompt with administrative privileges, as shown in Figure 6-5.

Figure 6-5

Creating a WinRM listener

- Enable the COM+ Network Access and Remote Event Log Management rules in Windows Firewall, as described in the previous section.

After installing the previous updates, you still have limitations to the management tasks you can perform on down-level servers from a remote location. For example, you cannot use the Add Roles and Features Wizard in Server Manager to install roles and features on down-level servers. These servers do not appear in the server pool on the *Select destination server* page.

However, you can use Windows PowerShell to install roles and features on servers running Windows Server 2008 and Windows Server 2008 R2 remotely, as in the following procedure.

INSTALL A FEATURE ON A DOWN-LEVEL SERVER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges. The Server Manager window appears.

1. Open a Windows PowerShell session with administrative privileges.
2. Establish a Windows PowerShell session with the remote computer by using the following command:

   ```
   Enter-PSSession <remote server name> -credential
   <user name>
   ```

3. Type the password associated with the user name you specified and press Enter.
4. Display a list of the roles and features on the remote server by using the following command:

   ```
   Get-WindowsFeature
   ```

5. Using the short name of the role or service as it appears in the Get-WindowsFeature display, install the component using the following command:

   ```
   Add-WindowsFeature <feature name>
   ```

6. Close the session with the remote server by using the following command:

   ```
   Exit-PSSession
   ```

CLOSE the Windows PowerShell window.

Working with Remote Servers

THE BOTTOM LINE After you add remote servers to Server Manager, you can access them using various remote administration tools.

Server Manager provides three basic methods for addressing remote servers, as follows:

- **Contextual tasks:** When you right-click a server in a Servers tile, anywhere in Server Manager, you see a context menu that provides access to tools and commands pointed at the selected server, as shown in Figure 6-6. Some are commands that Server Manager executes on the remote server, such Restart Server and Windows PowerShell. Others launch tools on the local system and direct them at the remote server, such as Microsoft Management Console snap-ins and the Install Roles and Features Wizard. Still others modify Server Manager itself, by removing servers from the interface. Other contextual tasks sometimes appear in the Tasks menus for specific panes.

Figure 6-6

Contextual tasks in Server Manager

- **Non-contextual tasks:** The menu bar at the top of the Server Manager console provides access to internal tasks, such as launching the Add Server and Install Roles and Features Wizards, as well as the Server Manager Properties dialog box, in which you can specify the console's refresh interval.
- **Non-contextual tools:** The console's Tools menu provides access to external programs, such as MMC snap-ins and the Windows PowerShell interface, that are directed at the local system.

Business Case Scenarios

Scenario 6-1: Managing Servers

Ralph is responsible for the 24 servers running a particular application, which are scattered all over his company's enterprise network. Ralph wants to use Server Manager on his Windows 8 workstation to manage those servers and monitor the events that occur on them. To do this, he must enable the incoming COM+ Network Access and Remote Event Log Management rules in Windows Firewall on the servers.

Because he can't travel to the locations of all the servers, and many of the sites do not have trustworthy IT personnel, Ralph has decided to use Group Policy to configure Windows Firewall on all of the servers. The company's Active Directory Domain Services tree is organized geographically, which means that Ralph's servers are located in many different OUs, all under one domain.

How can Ralph use Group Policy to deploy the required Windows Firewall rule settings to his 24 servers, and only those servers?

Scenario 6-2: Installing Windows PowerShell Web Access

You need a method to remotely manage a few servers from any client within the enterprise. You want to avoid any method that requires additional client software except a web browser. What will you use? Give an outline of tasks.

7 LESSON

Creating and Configuring Virtual Machine Settings

Virtualizing Servers

THE BOTTOM LINE

The concept of virtualizing servers has, in the past several years, grown from a novel experiment to a convenient lab and testing tool, as well as to a legitimate deployment strategy for production servers. Windows Server 2012 R2 includes the ***Hyper-V*** role, which enables you to create virtual machines, each of which runs in its own isolated environment. ***Virtual machine (VMs)*** are self-contained units that you can easily move from one physical computer to another, greatly simplifying the process of deploying network applications and services.

Server virtualization in Windows Server 2012 R2 is based on a module called a ***hypervisor***. Sometimes called a ***virtual machine monitor (VMM)***, the hypervisor is responsible for abstracting the computer's physical hardware and creating multiple virtualized hardware environments, called virtual machines (VMs). Each VM has its own (virtual) hardware configuration and can run a separate copy of an operating system. Therefore, with sufficient physical hardware and the correct licensing, a single computer running Windows Server 2012 R2 with the Hyper-V role installed can support multiple VMs, which you can manage as though they were standalone computers.

Virtualization Architectures

Virtualization products can use several different architectures to share a computer's hardware resources among several virtual machines.

The earlier types of virtualization products, including Microsoft Windows Virtual PC and Microsoft Virtual Server, require a standard operating system installed on a computer. This becomes the "host" operating system. Then you install the virtualization product, which adds the hypervisor component. The hypervisor essentially runs as an application on the host operating system, as shown in Figure 7-1, and enables you to create as many virtual machines as the computer has hardware to support.

Figure 7-1

A hybrid VMM sharing hardware access with a host operating system

This arrangement, in which the hypervisor runs on top of a host operating system, is called a *Type II virtualization*. By using the Type II hypervisor, you create a virtual hardware environment for each virtual machine. You can specify how much memory to allocate to each VM, create virtual disk drives by using space on the computer's physical drives, and provide access to peripheral devices. You then install a "guest" operating system on each virtual machine as though you were deploying a new computer. The host operating system then shares access to the computer's processor with the hypervisor, with each taking the clock cycles it needs and passing control of the processor back to the other.

Type II virtualization can provide adequate virtual machine performance, particularly in classroom and laboratory environments, but it does not provide performance equivalent to separate physical computers. Therefore, it is not recommended for high-traffic servers in production environments.

The virtualization capability built into Windows Server 2012 R2, called Hyper-V, uses a different type of architecture. Hyper-V uses *Type I virtualization*, in which the hypervisor is an abstraction layer that interacts directly with the computer's physical hardware—that is, without an intervening host operating system. The term *hypervisor* is intended to represent the next level beyond the term *supervisor*, concerning responsibility for allocating a computer's processor clock cycles.

The hypervisor creates individual environments called *partitions*, each of which has its own operating system installed and accesses the computer's hardware via the hypervisor. Unlike Type II virtualization, no host operating system shares processor time with the hypervisor. Instead, the hypervisor designates the first partition it creates as the parent partition and all subsequent partitions as child partitions, as shown in Figure 7-2.

Figure 7-2

A Type 1 VMM, with the hypervisor providing all hardware access

The parent partition accesses the system hardware through the hypervisor, just as the child partitions do. The only difference is that the parent runs the virtualization stack, which creates and manages the child partitions. The parent partition is also responsible for the subsystems that directly affect the performance of the computer's physical hardware, such as Plug and Play, power management, and error handling. These subsystems run in the operating systems on the child partitions as well, but they address only virtual hardware, whereas the parent, or root, partition handles the real thing.

Installing Hyper-V

THE BOTTOM LINE As soon as you have the appropriate hardware and the required licenses, you can add the Hyper-V role to Windows Server 2012 R2 via Server Manager, just as you would any other role.

Adding the Hyper-V role installs the hypervisor software, and, in the case of a full GUI installation, the management tools. The primary tool for creating and managing virtual machines and their components on Hyper-V servers is the Hyper-V Manager console. Hyper-V Manager provides you with a list of all the virtual machines on Windows Server 2012 R2 systems and enables you to configure both the server environments and those of the individual VMs. Windows PowerShell also includes a set of Hyper-V cmdlets that enable you to exercise complete control over VMs using that interface.

Microsoft recommends that you do not install other roles with Hyper-V. Any other roles that you need the physical computer to perform are better off implemented within one of the virtual machines you create with Hyper-V. You also might want to consider installing Hyper-V on a computer using the Server Core installation option to minimize the overhead expended on the partition. As with other roles, installing Hyper-V on Server Core excludes the management tools, which you must install separately as a feature.

Before you can install the Hyper-V role on a server running Windows Server 2012 R2, you must have appropriate hardware, as follows:

- A *64-bit processor* that includes hardware-assisted virtualization. This type of virtualization is available in processors that include a virtualization option, such of Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) technology.
- A *system BIOS* that supports the virtualization hardware and on which the virtualization feature has been enabled.
- Hardware-enforced *Data Execution Prevention (DEP)*, which Intel describes as eXecuted Disable (XD) and AMD describes as No eXecute (NS). CPUs use this technology to segregate areas of memory for either storage of processor instructions or for storage of data. Specifically, you must enable Intel XD bit (execute disable bit) or AMD NX bit (no execute bit).

Using Hyper-V Manager

THE BOTTOM LINE After you install the Hyper-V role and restart the computer, you can begin to create virtual machines and deploy operating systems on them.

The primary graphical tool for creating and managing virtual machines is the Hyper-V Manager console, which you can access from the *Tools* menu in Server Manager.

As with most of the Windows Server 2012 R2 management tools, including Server Manager itself, you can use the Hyper-V Manager console to create and manage virtual machines on multiple servers, enabling administrators to exercise full control over their servers from a central location.

To run Hyper-V Manager on a server that does not have the Hyper-V role, you must install the Hyper-V Management Tools feature. You also can find these tools in the Remote Server Administration Tools package.

After you install and launch the Hyper-V Manager console, you can add servers to the display by right-clicking the *Hyper-V Manager* node in the left pane and selecting *Connect to Server* from the shortcut menu. In the *Select Computer* dialog box that appears, you can type or browse to the name of a Hyper-V server.

The Hyper-V Manager console lists all the virtual machines on the selected server, along with status information about each one (see Figure 7-3).

Figure 7-3

The Hyper-V Manager console

Creating a Virtual Machine

After installing Hyper-V and configuring Hyper-V Manager, you are ready to create virtual machines and install the operating system on each virtual machine that you create.

By using Hyper-V Manager, you can create new virtual machines and define the hardware resources that the system should allocate to them. In the settings for a particular virtual machine, depending on the physical hardware available in the computer and the limitations of the guest operating system, you can specify the number of processors and the amount of memory a virtual machine should use, install virtual network adapters, and create virtual disks using various technologies, including storage area networks (SANs).

By default, Hyper-V stores the files that make up virtual machines in the folders you specified on the *Default Stores* page during the role installation. Each virtual machine uses the following files:

- A virtual machine configuration (.vmc) file in XML format that contains the virtual machine configuration information, including all settings for the virtual machine
- One or more virtual hard disk (.vhd or .vhdx) files to store the guest operating system, applications, and data for the virtual machine

A virtual machine may also use a saved-state (.vsv) file, if the machine has been placed into a saved state.

Creating Generation 1 and Generation 2 VMs

In Windows Server 2012 R2, the Hyper-V implementation includes a new type of virtual machine, which it refers to as Generation 2. The VM type created by all previous versions is called Generation 1. When you create a new virtual machine in the Hyper-V manager, the New Virtual Machine Wizard includes a new page on which you specify whether you want to create a Generation 1 or Generation 2 VM. The New-VM cmdlet in Windows PowerShell also enables you to include a new –Generation parameter.

Generation 1 VMs are designed to emulate the hardware found in a typical computer, and to do this, they use drivers for specific devices, such as an AMI BIOS, an S3 graphics adapter, and an Intel chipset and network adapter. Generation 1 VMs that you create with Windows Server 2012 R2 Hyper-V are completely compatible with all previous Hyper-V versions.

Generation 2 VMs use synthetic drivers and software-based devices instead, and provide advantages that include the following:

- UEFI boot Instead of using the traditional BIOS, Generation 2 VMs support Secure Boot, using the Universal Extensible Firmware Interface (UEFI), which requires a system to boot from digitally signed drivers and enables them to boot from drives larger than 2 TB, with GUID partition tables.
- SCSI disks Generation 2 VMs omit the IDE disk controller used by Generation 1 VMs to boot the system and use a high-performance virtual SCSI controller for all disks, enabling the VMs to boot from VHDX files and support hot disk adds and removes.

The end result is a Generation 2 virtual machine that deploys much faster than its Generation 1 counterparts, and performs better as well. The limitations, however, are that Generation 2 VMs can only run the following guest operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows 8 64-bit
- Windows 8.1 64-bit

Configuring Guest Integration Services

In some cases, certain Hyper-V guest operating system features do not function properly using the OS's own device drivers. Hyper-V, therefore, includes a software package called ***guest integration services***, which you can install on your virtual machines for compatibility purposes.

Some functions provided by the guest integration services package are as follows:

- **Operating system shutdown** enables the Hyper-V Manager console to remotely shut down a guest operating system in a controlled manner, eliminating the need for you to log on and manually shut the system down.
- **Time synchronization** enables Hyper-V to synchronize the operating system clocks in parent and child partitions.
- **Data Exchange** enables the operating systems on parent and child partitions to exchange information, such as OS version information and fully qualified domain names.
- **Heartbeat** implements a service in which the parent partition sends regular heartbeat signals to the child partitions, which are expected to respond in kind. A failure of a child partition to respond indicates that the guest OS has frozen or malfunctioned.
- **Backup** allows backup of Windows virtual machines using Volume Shadow Copy Services.

The Windows Server 2012, Windows Server 2012 R2, and Windows 8, and Windows 8.1 operating systems have the latest guest integration services software built in, so you do not need to install the package on VMs running those operating systems as guests. Earlier versions of Windows, however, have previous versions of the guest integration services package that need to be upgraded, and some Windows versions do not include the package at all.

To upgraded the guest integration services on a Windows guest OS, use the following procedure.

INSTALL GUEST INTEGRATION SERVICES

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu of the *Server Manager* window, choose Hyper-V Manager. The *Hyper-V Manager* console appears.
2. In the left pane, select a Hyper-V server.
3. In the Actions pane, start the virtual machine on which you want to install the guest integration services and click Connect. A *Virtual Machine Connection* window appears.
4. From the Action menu of the Virtual Machine Connection window, choose Insert Integration Services Setup Disk. Hyper-V mounts an image of the guest integration services disk to a virtual disk drive and displays an *Autoplay* window.
5. Click Install Hyper-V Integration Services. A message box appears, asking you to upgrade the existing installation.
6. Click OK. The system installs the package and prompts you to restart the computer.
7. Click Yes to restart the computer.

After you install or upgrade the guest integration services, you can enable or disable each individual function by opening the *Settings* dialog box for the virtual machine and selecting the *Integration Services* page, as shown in Figure 7-4.

Now, you are ready to configure and manage the virtual machine as though you were working on a physical server. You can modify the network configuration, enable remote desktop, load the appropriate roles and features, and install applications.

Figure 7-4

Integration Services settings for a virtual machine

Using Enhanced Session mode

In previous versions of Hyper-V, when you open a Virtual Machine Connection window in the Hyper-V Manager console, you receive mouse and keyboard connectivity, plus a limited cut and paste functionality. To obtain any further access, such as audio or print functionality, you could establish a Remote Desktop Services connection to the VM, but this requires the computers to be connected to the same network, which is not always possible.

Starting in Windows Server 2012 R2, Hyper-V supports an enhanced session mode that enables the Virtual Machine Connection window to redirect any of the following local resources to VMs running Windows Server 2012 R2 or Windows 8.1:

- Display configuration
- Audio
- Printers
- Clipboard
- Smart cards
- USB devices
- Drives
- Supported Plug and Play devices

The enhanced session mode works by establishing a Remote Desktop Protocol connection between the host computer and the VM, but it does not require a standard network path

because it uses the VMBus instead. VMBus is a high-speed conduit between the various partitions running on a Hyper-V server.

Enhanced session mode is enabled by default in Windows 8.1, but in Windows Server 2012 R2, you must enable it on the Enhanced Session Mode Policy page of the Hyper-V Settings dialog box.

Allocating Memory

Dynamic memory enables Hyper-V to adjust the amount of RAM allocated to virtual machines, depending on their ongoing requirements.

Some computer components can be virtualized. You can take some disk space and create a virtual hard drive out of it, and you can take an image file and create a virtual DVD drive. You can also create virtual network interface adapters and other components, which appear like the real thing in a VM. System memory is different, however; it has no substitute, so all Hyper-V can do is take the physical memory installed in the computer and allocate it among the various virtual machines.

When you create a virtual machine with the *New Virtual Machine Wizard*, you specify how much memory the VM should use on the *Assign Memory* page. Obviously, the amount of memory available for use is based on the physical memory installed in the computer.

After you create the virtual machine, you can modify the amount of memory allocated to it by shutting down the VM, opening its *Settings* dialog box, and changing the *Startup RAM* setting on the *Memory* page, as shown in Figure 7-5. This enables you to experiment with various amounts of memory and dial in the optimum performance level for the system.

Figure 7-5

Memory settings for a virtual machine

USING DYNAMIC MEMORY

In the first versions of Hyper-V, shutting down the virtual machine was the only way to modify its memory allocation. In the Windows Server 2012 R2 version, however, you can use a feature called dynamic memory to reallocate memory automatically to the VM from a shared memory pool as its demands change. If a virtualized server starts to experience larger amounts of client traffic, for example, Hyper-V can increase the memory allocated to the system, and then reduce it when the traffic subsides.

To use dynamic memory, you must enable it by selecting the *Enable Dynamic Memory* check box on the VM's *Memory* page of the *Settings* dialog box, and then configure the following settings:

- **Startup RAM** specifies the amount of memory that you want to allocate to the VM when it starts. When you are using dynamic memory, this value can be the minimum amount of memory needed to boot the system.
- **Minimum RAM** specifies the smallest amount of memory the VM can use at any time. Operating systems can conceivably require more memory to start up than they do to run, so this value can be smaller than the *Startup RAM* value.
- **Maximum RAM** specifies the largest amount of memory that the VM can use at any time. The value can range from a low equal to the *Startup RAM* value to a high of 64 GB.
- **Memory buffer** contains a percentage that Hyper-V uses to calculate how much memory to allocate to the VM, compared to its actual utilization, as measured by performance counters. For example, with the *Memory buffer* value set to 20%, a VM with applications and operating system that consume 1 GB of memory receives a dynamic allocation of 1.2 GB.
- **Memory weight** contains a relative value that specifies the priority of this VM, compared to the other VMs on the same computer. When the physical memory in the computer is insufficient to allocate the full buffered amount specified for each VM, the VMs with the highest memory weight settings receive priority.

In addition to configuring the virtual machine settings, the guest operating system on the virtual machine must have the Windows Server 2012 R2 guest integration services to use dynamic memory.

The *Hyper-V* console also enables you to monitor the current memory allocation for each virtual machine. By selecting a VM and clicking the *Memory* tab on the bottom pane, you can see the system's current Assigned Memory and other statistics.

CONFIGURING SMART PAGING

Windows Server 2008 R2 Hyper-V introduced dynamic memory, but Windows Server 2012 and Windows Server 2012 R2 improve on the concept by adding the *Minimum RAM* setting. This enables Hyper-V to reduce the memory used by a virtual machine to a level lower than that needed to start the system, reclaiming that memory for other uses.

The problem with having minimum RAM values that are lower than the startup RAM values is that the supply of physical memory can become depleted with too many VMs running simultaneously at their minimum RAM values. If this occurs, a VM that has to restart might be unable to do so because not enough free memory is available to increase its memory allocation from its minimum RAM value to its startup RAM value.

To address this possibility, Hyper-V includes a feature called ***smart paging***. If a VM has to restart and not enough memory is available to allocate its startup RAM value, the system uses hard disk space to make up the difference and begins paging memory contents to disk.

Disk-access rates are far slower than memory-access rates, of course, so smart paging incurs a severe performance penalty, but the paging occurs only for as long as it takes to restart the VM and return it to its minimum RAM allocation.

Hyper-V uses smart paging only in highly specific conditions, such as when a VM must be restarted, no free memory is available, and the memory needed cannot be freed up by other means.

You can use the *Smart Paging File Location* page in a VM's *Settings* dialog box to specify a location for the paging file. Selecting the fastest possible hard drive is recommended.

Configuring Resource Metering

THE BOTTOM LINE Resource metering is a Windows PowerShell-based feature in Windows Server 2012 R2 Hyper-V that enables you to document virtual machine usage via a variety of criteria.

Organizations might want to track the use of virtual machines for various reasons. For large corporations, it might be a matter of internal accounting and controlling ongoing expenses, such as wide area network (WAN) bandwidth. For service providers, it might be necessary to bill customers based on the VM resources they use.

Resource metering uses Windows PowerShell cmdlets to track various performance metrics for individual VMs, including the following:

- CPU utilization
- Minimum/maximum/average memory utilization
- Disk space utilization
- Incoming/outgoing network traffic

Resource metering statistics remain consistent, even when you transfer VMs between host systems using live migration or move virtual hard disk files between VMs.

To use resource metering, you must first enable it for the specific VM that you want to monitor, using the *Enable-VMResourceMetering* cmdlet with the following syntax:

```
Enable-VMResourceMetering –VMName <name>
```

After you enable metering, you can display a statistical report at any time by using the *Measure-VM* cmdlet with the following syntax, as shown in Figure 7-6:

```
Measure-VM –VMName <name>
```

Figure 7-6

Displaying metering data with Windows PowerShell

In addition to metering resources for entire virtual machines, you can also create resource pools that help you monitor specific VM components, such as processors, memory, network adapters, or virtual hard disks. You create a resource pool using the *New-VMResourcePool* cmdlet and then enable metering for the pool using *Enable-VMResourceMetering*.

By using techniques such as pipelining, you can use the resource metering cmdlets to gather data on virtual machine performance and export it to applications or data files.

Using Remote FX

RemoteFX is a Windows Server feature that enables remote computers to connect Hyper-V guest VMs with an enhanced desktop experience, including the following:

- Graphics adapter virtualization With an appropriate graphics adapter installed in the server, client systems can offload some of the graphics processing tasks they would normally perform locally. By rendering graphics on a high-performance adapter installed on the host server and sending the resulting bitmaps to the client in a highly-compressed format, RemoteFX conserves resources on the client system, as well as network bandwidth.
- USB redirection Enables USB devices connected to client computers to be redirected to the host server, including printer, scanner, interface, storage, and audio devices.
- Intelligent encoding and decoding The RemoteFX server can encode data using the system's CPU, GPU, or dedicated hardware. In the same way, the client system can decode incoming data using its CPU, GPU, or a hardware decoder. The systems can select different codecs, depending on the data type.

RemoteFX relies on the Remote Desktop Protocol (RDP) for client/server communications, just like Remote Desktop Services, but uses these new features to provide capabilities such as multitouch support and media redirection.

Setting up the host side of RemoteFX consists of the following basic steps.

1. Install the Hyper-V role on the host server.
2. Install a RemoteFX-approved server graphics adapter and an appropriate Windows Display Driver Model (WDDM) driver on the host server.
3. Install the Remote Desktop Virtualization Host role feature for the Remote Desktop Services role and restart the server.
4. In Hyper-V Manager, open the Hyper-V Settings dialog box and, under Physical GPUs, select the graphics adapter you installed and select the Use this GPU with RemoteFX checkbox.

To set up the client side of RemoteFX, complete the following basic steps.

1. Install Windows 8 Enterprise or Windows 8.1 Enterprise on a virtual machine.
2. Enable Remote Desktop on the virtual machine.
3. Install Hyper-V Integration Services on the virtual machine.
4. In Hyper-V Manager, open the Settings dialog box for the VM and, under Add Hardware, select RemoteFX 3D Video Adapter and specify the screen resolution and number of monitors you plan to use.
5. Turn on the VM and log on using RDP.

Business Case Scenarios

Scenario 7-1: Isolating Server Applications

You have two network accounting applications, neither of which is processor hungry. Both of these applications must be kept totally isolated from each other and from all other applications. Both applications will access a centralized database server. What server configuration solution do you recommend?

Scenario 7-2: Configuring Virtual Machine Memory

Alice has a computer running Windows Server 2012 R2 with 8 GB of memory installed, which she has configured as a Hyper-V server. After creating eight VMs with the New Virtual Machine Wizard, each with a startup RAM value of 1,024 MB, Alice is having trouble getting all eight VMs to boot. What settings can she modify to resolve the problem without changing the startup RAM value?

8

LESSON

Creating and Configuring Virtual Machine Storage

Working with Virtual Disks

THE BOTTOM LINE

When you create a virtual machine (VM) in Windows Server 2012 R2 Hyper-V, you emulate all the standard components that you typically find in a physical computer. When you virtualize memory, as discussed in Lesson 7, "Creating and Configuring Virtual Machine Settings," you take a portion of the physical memory in the computer and dedicate it to a VM. The same is true with hard disk space. Hyper-V uses a specialized ***virtual hard disk (VHD)*** format to package part of the space on a physical disk and make it appear to the virtual machine as though it is physical hard disk drive.

When you create a new virtual machine in Hyper-V by using the New Virtual Machine Wizard, the wizard creates a virtual storage subsystem that consists of two IDE (Integrated Drive Electronics) controllers and one SCSI (Small Computer Systems Interface) controller, as shown in Figure 8-1. The IDE controllers host the virtual machine's system drive and its DVD drive. As with their physical equivalents, each IDE controller can host two devices, so you can create two additional virtual drives and add them to the system.

The SCSI controller, in the default Generation 1 VM configuration, is unpopulated, and you can create additional drives and add them to that controller to provide the VM with additional storage. In a Generation 2 VM, the system and DVD drives are connected to the default SCSI controller and there is no IDE alternative. In a VM of either generation, you can also create additional SCSI controllers and add drives to them. By creating multiple drives and controllers, Hyper-V makes it possible to construct virtual storage subsystems that emulate almost any physical storage solution you might devise.

Figure 8-1

The default VM drive controller configuration

Understanding Virtual Disk Formats

Windows Server 2012 R2 Hyper-V supports the original VHD disk image file and the new VHDX format.

The original VHD format was created by a company called *Connectix* for its Virtual PC product. Microsoft later acquired the product and used the VHD format for all its subsequent virtualization products, including Hyper-V. There are three types of VHD files, as follows:

- **Fixed hard disk image:** This image file is a specified size in which all the disk space required to create the image is allocated during its creation. Fixed disk images can be considered wasteful in terms of storage, because they can contain large amounts of empty space, but they are also efficient from a processing standpoint, because there is no overhead due to dynamic expansion.
- ***Dynamic hard disk* image:** This image file has a specified maximum size, which starts out small and expands as needed to accommodate the data the system writes to it.
- ***Differencing hard disk* image:** This child image file is associated with a specific parent image. The system writes all changes made to the data on the parent image file to the child image, to facilitate a rollback at a later time.

VHD images are limited to maximum size of 2 terabytes (TB) and are compatible with all versions of Hyper-V, as well as Microsoft's Type 2 hypervisor products, such as Virtual Server and Virtual PC. Windows Server 2012 introduced an updated version of the format, which uses a VHDX filename extension.

VHDX image files can be as large as 64 TB, and they also support 4 KB logical sector sizes, to provide compatibility with new 4 KB native drives. VHDX files can also use larger block sizes (up to 256 MB), which enable you to fine-tune the performance level of a virtual storage subsystem to accommodate specific applications and data file types. However, VHDX files are not backwards compatible and can be read only by Windows Server 2012 R2 Hyper-V servers. If migrating your virtual machines from Windows Server 2012 R2 to an older version of Hyper-V is a remote possibility, you should continue using the VHD file format.

Creating Virtual Disks

Windows Server 2012 R2 Hyper-V provides several ways to create virtual disk files. You can create them as part of a virtual machine, or create them later and add them to a VM.

The graphical interface in Hyper-V Manager provides access to most of the VHD parameters, but the new Windows PowerShell cmdlets included in Windows Server 2012 R2 provide the most granular control over the disk image format.

CREATING A VIRTUAL DISK WITH A VM

The New Virtual Machine Wizard includes a Connect Virtual Hard Disk page, with which you can add a single disk to your new VM. The options for this disk are limited and consist of the following:

- **Create a virtual hard disk** enables you to specify the name, location, and size of a new virtual hard disk, but you can create only a dynamically expanding disk using the VHDX format.
- **Use an existing virtual hard disk** enables you to specify the location of an existing VHD or VHDX disk, which the VM presumably uses as its system disk.
- **Attach a virtual hard disk later** prevents the wizard from adding virtual disks to the VM configuration. The assumption is that you will manually add a disk later, before you start the virtual machine.

The object of this wizard page is to create the disk on which you will install the VM's operating system, or select an existing disk on which an OS is already installed. The disk the wizard creates is always a dynamically expanding one connected to IDE Controller 0 on a Generation 1 VM or the SCSI Controller on a Generation 2 VM.

CREATING A NEW VIRTUAL DISK

You can create a virtual hard disk file at any time, without adding it to a virtual machine, by using the *New Virtual Hard Disk Wizard in Hyper-V Manager*.

To create a new virtual disk, use the following procedure.

CREATE A NEW VIRTUAL DISK

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Hyper-V Manager. The *Hyper-V Manager* console appears.
2. In the left pane, select a Hyper-V server.
3. From the Action menu, select New > Hard Disk. The *New Virtual Hard Disk Wizard* appears, displaying the *Before You Begin* page.
4. Click Next. The *Choose Disk Format* page appears.

5. Select one of the following disk format options and click Next. The *Choose Disk Type* page appears.
   - VHD creates an image no larger than 2 TB, using the highly compatible VHD format.
   - VHDX creates an image up to 64 TB in size, using the new VHDX format.
6. Select one of the following disk type options and click Next. The *Specify Name and Location* page appears.
   - Fixed size creates a disk of a specific size, allocating all the space at once.
   - Dynamically expanding creates a disk that grows to the maximum size you specify as you add data.
   - Differencing creates a child drive that contains changes made to a specified parent drive.
7. Specify a filename for the disk image in the Name text box and, if desired, specify a location for the file other than the server default. Then, click Next. The *Configure Disk* page appears.
8. Select and configure one of the following options and click Next. The *Completing the New Virtual Hard Disk Wizard* page appears.
   - Create a new blank virtual hard disk specifies the size (or the maximum size) of the disk image file to create.
   - Copy the contents of the specified physical disk enables you to select one of the physical hard disks in the computer and copy its contents to the new disk image.
   - Copy the contents of the specified virtual hard disk enables you to select an existing virtual disk file and copy its contents to the new disk image.
9. Click Finish.

The wizard creates the new image disk and saves it to the specified location.

CREATING DIFFERENCING DISKS

A differencing disk enables you to preserve an existing virtual disk image file in its original state, while mounting it in an OS and even modifying its contents. For example, when building a laboratory setup, you can create a baseline system by installing a clean copy of an OS on a new virtual disk and configure the environment to your needs. Then, you can create a new child-differencing disk, using your baseline image as the parent. All subsequent changes you make to the system are written to the differencing disk, whereas the parent remains untouched. You can experiment on the test system, knowing that you can revert back to your baseline configuration by creating a new differencing disk.

You can create multiple differencing disks that point to the same parent image, enabling you to populate a lab network with as many virtual machines as you need, without having to repeatedly install the OS and while saving on disk space.

To create a cloned version of a baseline installation with a differencing disk, use the following procedure.

1. **Install and configure the baseline virtual machine:** Create a new virtual machine with a new disk image file and install a guest OS on it. Configure the OS as needed and install any roles, features, applications, or services you need.
2. **Generalize the parent image:** Open an elevated command prompt on the baseline system and run the *Sysprep.exe* utility. Sysprep configures the system to assign itself a new, unique security ID (SID) the next time the computer starts. This enables you to create multiple cloned systems from a single disk image.
3. **Create a parent disk image:** After you generalize the baseline installation, you no longer need the original virtual machine. You can delete everything except the VHD or VHDX file

containing the disk image. This file becomes your parent image. Open the Properties sheet for the image file and set the read-only flag, to ensure that the baseline does not change.

4. **Create a differencing disk:** Using the *New Virtual Hard Disk Wizard* or the *New-VHD* cmdlet for Windows PowerShell, create a new differencing disk, pointing to the baseline image you created and prepared previously as the parent image.
5. **Create a cloned virtual machine:** Create a new virtual machine and, on the *Connect Virtual Hard Disk* page, attach the differencing disk you created to it, by using the *Use an existing virtual hard disk* option.

You can then create additional cloned VMs, with differencing disks that use the same parent. Each one can function independently, and the parent disk will remain unchanged.

When you create a differencing drive by using the *New Virtual Hard Disk Wizard*, selecting the *Differencing* option on the *Choose Disk Type* page causes the *Configure Disk* page to appear. In the *Location* text box, you must specify the name of the file to use as the parent image.

In the same way, if you create the differencing disk by using Windows PowerShell, you must run the New-VHD cmdlet with the `-Differencing` parameter and the `-ParentPath` parameter, specifying the location of the parent disk.

Configuring Pass-Through Disks

So far, this lesson focusses primarily on virtual hard disks—that is, areas of space on a physical disk drive allocated for use by virtual machines. However, it is also possible for VMs to access physical disks directly.

A ***pass-through disk*** is a type of virtual disk that points not to an area of space on a physical disk, but to a physical disk drive itself, installed on the host computer. When you add a hard drive to any of the controllers in a virtual machine, you can select a physical hard disk, as opposed to virtual one.

To add a physical hard disk to a virtual machine, however, the VM must have exclusive access to it. That is, you must first take the disk offline in the parent OS, by using the *Disk Management* snap-in, as shown in Figure 8-2, or the *Diskpart.exe* utility. After the disk is offline, it is available for selection in the *Physical hard disk* drop-down list.

Figure 8-2

An offline disk in the Disk Management snap-in

Modifying Virtual Disks

Windows Server 2012 R2 and Hyper-V provide several ways for you to manage and manipulate virtual hard disk images without mounting them in a virtual machine.

After you create a virtual hard disk, whether you attach it to a virtual machine or not, you can manage it by using the *Edit Virtual Hard Disk Wizard* in *Hyper-V Manager*. To edit an existing VHD or VHDX file, use the following procedure.

EDIT A VIRTUAL DISK

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Hyper-V Manager. The *Hyper-V Manager* console appears.
2. In the left pane, select a Hyper-V server.
3. In the Actions pane, select Edit Disk. The *Edit Virtual Hard Disk Wizard* appears, displaying the *Before You Begin* page.
4. Click Next. The *Locate Disk* page appears.
5. Type or browse to the name of the VHD or VHDX file you want to open and click Next. The *Choose Action* page appears.
6. Select one of the following functions and click Next. The *Completing the Edit Virtual Hard Disk Wizard* page appears.
   - Compact reduces the size of a dynamically expanding or differencing disk by deleting empty space, while leaving the disk's capacity unchanged.
   - Convert changes the type of format of a disk by copying the data to a new disk image file.
   - Expand increases the capacity of the disk by adding empty storage space to the image file.
   - Shrink reduces the capacity of the disk by deleting empty storage space from the file.
   - Merge combines the data on a differencing disk with the parent disk to form a single composite image file.
7. Complete any new pages presented by the wizard as a result of your selection and click Finish.

The options that appear on the wizard's Choose Action page depend on the current status of the image file you select. For example, the Merge option only appears if you choose a differencing disk, and the Shrink option does not appear unless there is free space in the file that the wizard can delete.

In addition to these disk editing functions provided by Hyper-V Manager, it is also possible to use the Disk Management snap-in to mount a VHD or VHDX file as a drive and access its contents, just as if it was a physical disk.

Creating Checkpoints

In Hyper-V, a ***checkpoint*** is a captured image of the state, data, and hardware configuration of a virtual machine at a particular moment in time.

Creating checkpoints is a convenient way for you to revert a virtual machine to a previous state at will. For example, if you create a checkpoint just before applying a system update, and the update is somehow problematic, you can apply the checkpoint and return the VM to the state it was in before you applied the update.

Creating a checkpoint is as simple as selecting a running virtual machine in Hyper-V Manager and selecting Checkpoint from the Actions pane. The system creates a checkpoint file, with an AVHD or AVHDX extension, in the same folder as the virtual hard disk file, and adds the checkpoint to Hyper-V Manager display, as shown in Figure 8-3.

Figure 8-3

A checkpoint in Hyper-V Manager

Checkpoints is a useful tool for you implementing a test environment in Hyper-V, but this tool is not recommended for heavy use in production environments. Apart from consuming disk space, the presence of checkpoints can reduce the overall performance of a virtual machine's disk subsystem.

Configuring Storage Quality of Service

Because it is common for there to be more than one virtual hard disk hosted by a single physical hard disk, it is possible for one virtual disk to monopolize the input/output capacity of a physical disk, causing the other virtual disks to slow down. To help prevent this, Hyper-V in Windows Server 2012 R2 enables you to control the Quality of Service (QoS) for a given virtual hard disk.

To use QoS in Windows Server 2012 R2, you must first install the Hyper-V role. QoS management in Hyper-V takes the form of controls that enables you to specify the minimum and maximum input/output operations per second (IOPS) for a disk. The system can generate notifications for administrators when a disk's IOPS falls below a specified minimum requirement. To configure storage QoS, you open the Settings dialog box for a VM, expand a hard drive component, and select Advanced Features to display the Advanced Features page.

After selecting the Enable Quality of Service Management checkbox, you can specify minimum and maximum IOPS values for the disk, to throttle its throughout in 8 KB increments.

■ Connecting to a SAN

THE BOTTOM LINE

At its most basic level, a ***storage area network (SAN)*** is a network dedicated to high-speed connections between servers and storage devices.

Rather than installing disk drives into servers, or connecting them by using an external SCSI bus, a SAN consists of one or more drive arrays equipped with network interface adapters, which you connect to your servers by using standard twisted pair or fiber optic network cables. A SAN-connected server, therefore, has a minimum of two network adapters, one for the standard LAN connection and one for the SAN, as shown in Figure 8-4.

Figure 8-4

A server connected to a SAN

The advantages of SANs are many. By connecting the storage devices to a network rather than to the servers themselves, you avoid the limitations imposed by the maximum number of devices you can connect directly to a computer. SANs also provide added flexibility in their communications capabilities. Because any device on a SAN can communicate with any other device on the same SAN, high-speed data transfers can occur in any of the following ways:

- **Server to storage:** Servers can access storage devices over the SAN just as if they were connected directly to the computer.
- **Server to server:** Servers can use the SAN to communicate directly with each other at high speeds, to avoid flooding the LAN with traffic.
- **Storage to storage:** Storage devices can communicate among themselves without server intervention, such as to perform backups from one medium to another or to mirror drives on different arrays.

Although a SAN is not a high availability technology, you can make it into one by connecting redundant servers to the same network, as shown in Figure 8-5, enabling them to access the same data storage devices. If one server fails, another can assume its roles by accessing the same data, which is called *server clustering*.

Figure 8-5

Multiple servers connected to a SAN

Because they use standard networking technologies, SANs can also greatly extend the distances between servers and storage devices. You can design a SAN that spans different rooms, different floors, or even different buildings, just as you would with a standard computer network.

Using Fibre Channel

Fibre Channel is a high-speed serial networking technology that was originally designed for use with supercomputers, but which is now associated primarily with storage area networking.

Fibre Channel is a versatile technology, supporting various network media, transmission speeds, topologies, and upper-level protocols. Its primary disadvantage is that it requires specialized hardware that can be extremely expensive.

Installing a Fibre Channel SAN means building a new network with its own special medium, switches, and network interface adapters. In addition to the hardware costs, which can easily be 10 times that of a traditional Ethernet network, you should consider installation and maintenance expenses. Fibre Channel is a rather esoteric technology, with relatively few experts in the field. To install and maintain a Fibre Channel SAN, an organization must either hire experienced staff or train existing personnel on the new technology.

Connecting Virtual Machines to a SAN

In the past, the specialized networking technologies used to build Fibre Channel SANs made it difficult to use them with virtualized servers. However, since the Windows Server 2012 implementation, Hyper-V has supported the creation of virtual Fibre channel adapters.

A Hyper-V Fibre Channel adapter is essentially a pass-through device that enables a virtual machine to access a physical Fibre Channel adapter installed in the computer, and through that, the external resources connected to the SAN. With this capability, applications running on virtual machines can access data files stored on SAN devices, and you can use VMs to create server clusters with shared storage subsystems.

To support virtual Fibre Channel connectivity, the physical Fibre Channel host bus adapter(s) in the host computer must have drivers that explicitly support virtual Fibre Channel. This support is relatively rare, but more manufacturers are expected to update their drivers to provide the necessary support. Your SAN must also be able to address its connected resources using logical unit numbers (LUNs).

Assuming you have the appropriate hardware and software installed on the host commuter, you implement the Fibre Channel capabilities in Hyper-V by first creating a virtual SAN. You do this by using the *Virtual SAN Manager*, accessible from *Hyper-V Manager*. When you create the virtual SAN, the World Wide Node Names (WWNNs) and World Wide Port Names (WWPNs) of your host bus adapter appear, as shown in Figure 8-6.

Figure 8-6

WWNNs and WWPNs in a virtual SAN

The next step is to add a Fibre Channel adapter to a virtual machine from the *Add Hardware* page in the *Settings* dialog box. Then, the virtual SAN you created previously is available in the *Fibre Channel Adapter* page. Hyper-V virtualizes the SAN and makes the WWNNs and WWPNs available to the VM.

■ Business Case Scenarios

Scenario 8-1: Creating Differencing Disks

To conduct multiple tests, you require several VMs with the same baseline installation. You decide to employ differencing disks to create your VMs. Walk through the steps.

Scenario 8-2: Modifying Virtual Disks

You need to modify an existing VHD file. How do you proceed?

Creating and Configuring Virtual Networks

LESSON 9

Using Virtual Networking

THE BOTTOM LINE

Networking is a critical part of creating a virtual machine (VM) infrastructure. Depending on your network plan, the virtual machines you create on a Windows Server 2012 R2 Hyper-V server can require communication with other virtual machines, with the computers on your physical network, and/or with the Internet.

When you build a network out of physical computers, you install a network interface adapter in each one and connect it to a hardware switch. The same principle is true in a Hyper-V environment, except that you use virtual components rather than physical ones. Each virtual machine you create has at least one virtual network adapter, and you can connect that adapter to a virtual switch. This enables you to connect the virtual machines on your Hyper-V server in various network configurations that either include or exclude the systems on your physical network.

Therefore, Hyper-V creates a pool of 256 MAC addresses during the installation. You can create multiple virtual switches on a Hyper-V server and multiple network adapters in each virtual machine. Multiple virtual switches and network adapters enable you to create a flexible networking environment, which is suitable for anything from a laboratory or classroom network to a production environment. In addition, Windows Server 2012 R2 can create extensions for virtual switches, so that software developers can enhance their capabilities.

Creating Virtual Switches

A ***virtual switch***, like its physical counterpart, is a device that functions at layer 2 of the Open Systems Interconnect (OSI) reference model. A switch has a series of ports, each of which is connected to a computer's network interface adapter. Any computer connected to the switch can transmit data to any other computer connected to the same switch.

Unlike physical switches, the virtual switches created by Hyper-V can have an unlimited number of ports, so you don't need to connect switches together or use uplinks and crossover circuits.

CREATING A NEW VIRTUAL SWITCH

Hyper-V in Windows Server 2012 R2 supports three types of switches, which you must create in the *Virtual Switch Manager* before you can connect virtual machines to them.

To create a new virtual switch, use the following procedure.

CREATE A NEW VIRTUAL SWITCH

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Hyper-V Manager. The *Hyper-V Manager* console appears.
2. In the left pane, select a Hyper-V server.
3. From the Actions pane, select Virtual Switch Manager. The *Virtual Switch Manager* dialog box for the Hyper-V server appears, as shown in Figure 9-1.

Figure 9-1

The Virtual Switch Manager dialog box

4. In the Create virtual switch box, select one of the following switch types and click Create Virtual Switch. The *Virtual Switch Properties* page appears.
   - External: The virtual switch is bound to networking protocol stack in the host operating system and connected to a physical network interface adapter

in the Hyper-V server. Virtual machines running on the server's parent and child partitions can access the physical network to which the physical adapter is connected.

- Internal: An ***internal network switch*** is bound to a separate instance of the networking protocol stack in the host operating system, independent from the physical network interface adapter and its connected network. Virtual machines running on the server's parent and child partitions can access the virtual network implemented by the virtual switch, and the host operating system on the parent partition can access the physical network through the physical network interface adapter, but the virtual machines on the child partitions cannot access the physical network through the physical adapter.
- Private: A ***private network switch*** exists only in the Hyper-V server and is accessible only to the virtual machines running on the child partitions. The host operating system on the parent partition can still access the physical network through the physical network interface adapter, but it cannot access the virtual network created by the virtual switch.

5. Configure the following options, if desired:
   - Allow management operating system to share this network adapter: Selected by default when you create an external virtual switch, clearing this check box excludes the host operating system from the physical network, while allowing access to the child virtual machines.
   - Enable single root I/O virtualization (SR-IOV): This option enables you to create an external virtual switch that is associated with a physical network adapter capable of supporting SR-IOV. This option is only available when creating a new virtual switch; you cannot modify an existing switch to use this option.
   - Enable virtual LAN identification for management operating system: If your host computer is connected to a physical switching infrastructure that uses virtual LANs (VLANs) to create separate subnets, you can select the check box and enter a VLAN identifier to associate the virtual switch with a particular VLAN on your physical network.
6. Click OK. The new virtual switch appears in the left pane, in the list of virtual switches.

You can proceed to create additional virtual switches as needed. You can create only one switch for each physical network adapter in the computer, but you can create multiple internal or private switches, to create as many virtual networks as you need.

CONFIGURING MAC ADDRESSES

Every network interface adapter has a Media Access Control (MAC) address (sometimes called a *hardware address*) that uniquely identifies the device on the network. On physical network adapters, the MAC is assigned by the manufacturer and permanently entered in the adapter's firmware. The MAC address is a 6-byte hexadecimal value—the first 3 bytes is an organizationally unique identifier (OUI) that specifies the manufacturer, and the last 3 bytes identifies the adapter itself.

The MAC address is essential to the operation of a LAN, so the virtual network adapters on a Hyper-V server require them. The server has at least one real MAC address, provided in its physical network adaptor, but Hyper-V cannot use that one address for all of the virtual adapters connecting virtual machines to the network.

To provide MAC addresses for the virtual adapters, Hyper-V creates a pool of addresses and assigns addresses from this pool to virtual machines as you create them. To view or modify the MAC address pool for the Hyper-V server, you open the *Virtual Switch Manager* and select *MAC Address Range* under *Global Network Settings*.

The first 3 bytes of MAC address range are always 00-15-5D, which is an OUI registered by Microsoft. The fourth and fifth bytes of the MAC address are the last 2 bytes of the IP address assigned to the server's physical network adapter, converted to hexadecimal notation. The sixth and last byte of the MAC address contains the range of values from 00 to FF, which provides 256 possible addresses.

The Hyper-V server assigns the MAC addresses to the network adapters in virtual machines as you create the adapters. The adapters retain their MAC addresses permanently, or until the adapter is removed from the virtual machine. The server reclaims any unused addresses and reuses them.

The default pool of 256 addresses is expected to be sufficient for most Hyper-V virtual machine configurations, but if it is not, you can modify the *Minimum* and *Maximum* values to enlarge the pool. To prevent address duplication, you should change the second to last byte only, by making it into a range of addresses like the last byte.

WARNING When you modify the MAC address pool, and you have other Hyper-V servers on your network, you must be careful not to create the opportunity for duplicate MAC addresses to occur, or networking problems can result.

For example, the range illustrated in the figure provides 256 addresses with the following values:

```
00-15-1D-02-12-00 to 00-15-1D-02-12-FF
```

modifying only the least significant digit, as in the following values, increases the pool from 256 to 4,096.

```
00-15-1D-02-10-00 to 00-15-1D-02-1F-FF
```

Creating Virtual Network Adapters

After you create virtual switches in Hyper-V Manager, you can connect virtual machines to them by creating and configuring virtual network adapters.

When you create a new virtual machine, the default configuration includes one virtual network adapter. The *New Virtual Machine Wizard* includes a *Configure Networking* page, as shown in Figure 9-2, on which you can select one of the virtual switches you created.

Figure 9-2

The *Configure Networking* page in the New Virtual Machine Wizard

If you create only the default external virtual switch when installing Hyper-V, then connecting a virtual machine to the switch joins the system to the physical network.

USING SYNTHETIC ADAPTORS AND EMULATED ADAPTERS

Selecting the *Network Adapter* option in the *Add Hardware* page creates what is known in Hyper-V terminology as a *synthetic network adapter*. Hyper-V supports two types of network and storage adapters: synthetic and emulated (sometimes called *legacy*).

A ***synthetic adapter*** is a virtual device that does not correspond to a real-world product. Synthetic devices in a virtual machine running on a child partition communicate with the parent partition using a high-speed conduit called the ***VMBus***.

The virtual switches you create in Hyper-V reside in the parent partition and are part of a component called the network ***Virtualization Service Provider (VSP)***. The synthetic network adapter in the child partition is a ***Virtualization Service Client (VSC)***. The VSP and the VSC are both connected to the VMBus, which provides interpartition communications, as shown in Figure 9-3. The VSP, in the parent partition, provides the VSC, in the child partition, with access to the physical hardware in the host computer, that is, the physical network interface adaptor.

Figure 9-3

Synthetic network adapters communicate using the VMBUS

Because they have access to the hardware through the VMBus, synthetic adapters provide a much higher level of performance than the alternative—an emulated adapter. Synthetic adapters are implemented as part of the guest integration services package that run on supported guest operating systems. The one main drawback of synthetic network adapters is that they are not operational until the operating system is loaded on the virtual machine.

An ***emulated adapter*** (sometimes called a ***legacy adapter***) is a standard network adapter driver that communicates with the parent partition by making calls directly to the hypervisor, which is external to the partitions, as shown in Figure 9-4. This communication method is substantially slower than the VMBus used by the synthetic network adapters, and is therefore less desirable.

Figure 9-4

Emulated network adapters communicate using the hypervisor

To install an emulated adapter, you use the same procedure described previously, except that you select *Legacy Network Adapter* in the *Add Hardware* list. Unlike synthetic adapters, emulated adapters load their drivers before the operating system, so you can boot the virtual machine using the Preboot eXecution Environment (PXE) and deploy an operating system over the network.

This is one of the only scenarios in which an emulated adapter is preferable to a synthetic adapter. The other is when you install an operating system on your virtual machines that does not have a guest integration services package available for it.

CONFIGURING HARDWARE ACCELERATION SETTINGS

Some physical network interface adapters have features that are designed to improve performance by offloading certain functions from the system processor to components built into the adapter itself. Hyper-V includes support for some of these features, as long as the hardware in the physical network adapter supports them properly.

When you expand a network adapter in the Settings dialog box of a VM, you gain access to the Hardware Acceleration page. On this page, you can configure the following hardware acceleration settings:

- Enable virtual machine queue: Virtual machine queue (VMQ) is a technique that stores incoming packets intended for virtual machines in separate queues on the physical network adapter and delivers them directly to the VMs, bypassing the processing normally performed by the virtual switch on the parent partition.
- Enable IPsec task offloading: This setting uses the components on the network adapter to perform some of the cryptographic functions required by IPsec. You can also specify maximum number of security associations you want the adapter to be able to calculate.
- Single-root I/O virtualization: This setting enables the virtual adapter to use the SR-IOV capabilities of the physical adapter.

CONFIGURING ADVANCED NETWORK ADAPTER FEATURES

The Advanced Features page provides additional options for supporting network adapter capabilities, as follows:

- Static MAC address: By default, virtual network adapters receive a dynamically assigned MAC address from the Hyper-V server. However, you can also opt to create a static MAC address, by using this option. The only requirement is that no other adapter, virtual or physical, on the same network uses the same address.
- Enable MAC address spoofing: When enabled, the port in the virtual switch to which the virtual network adapter is connected can send and receive packets that contain any MAC address. The virtual switch port can also learn of new MAC addresses and add them in its forwarding table.
- Enable DHCP guard: This option prevents the adapter from processing messages sent by rogue DHCP servers.
- Port mirroring mode: This option enables the adapter to forward all the packets it receives over the network to another virtual adapter for analysis using an application such as Network Monitor.
- NIC teaming: This option enables the adapter to add its bandwidth to other adapters in the same guest operating system in a NIC teaming arrangement.

Configuring NIC Teaming in a Virtual Network Environment

As explained in objective 1.2, "Configuring Servers," NIC teaming is a Windows feature that enables administrators to join multiple network adapters into a single virtual adapter, for performance enhancement or fault tolerance purposes. Hyper-V virtual machines can also take advantage of NIC teaming, but they are limited to teams of only two, as opposed to the host operating system, which can have teams of up to 64 NICs.

To use NIC teaming in Hyper-V, you must complete three basic tasks, as follows:

- Create the NIC team in the Windows Server 2012 R2 R2 host operating system.
- In Hyper-V Manager, create an external virtual switch using the NIC team.
- Configure the virtual network adapter in a VM to connect to the virtual switch representing the NIC team.

CREATING THE NIC TEAM

NIC teams must consist of physical network interface adapters, so before you can use a NIC team in a virtual machine, you must create it in the host operating system. After installing two NICs in the host computer, you can create a NIC team with Server Manager in the usual manner, using the settings shown in Figure 9-5. Creating the team installs the Microsoft Network Adapter Multiplexor Driver, which appears as one of the components of the network connection representing the team.

Figure 9-5

The NIC Teaming dialog box

CREATING THE TEAM VIRTUAL SWITCH

Once you have created the NIC team, you can open the Virtual Switch Manager and create a new virtual switch by selecting the External network option and choosing Microsoft Network Adapter Multiplexor Driver from the drop-down list.

CONFIGURING A NIC TEAM VIRTUAL NETWORK ADAPTER

To configure a virtual machine to use a NIC team, you must use the Settings dialog box to modify the properties for a virtual network adapter, configuring it to use the team switch you created in the previous section, as shown in Figure 9-6.

Figure 9-6

The Network Adapter settings for a NIC team adapter

Finally, you must open the Advanced Features page for the network adapter and select the Enable the network adapter to be part of a team in the guest operating system checkbox. At this point, the NIC team is operational for the virtual machine. You can unplug one of the network cables, and the system will maintain its connection to the network.

Creating Virtual Network Configurations

Hyper-V makes it possible to extend virtually any existing physical network configuration into its virtual space, or create a completely separated and isolated network within the Hyper-V environment.

The basic default configuration of a Hyper-V virtual machine connects its network adapter to an external virtual switch, thus attaching the guest operating system on the virtual machine to the outside network. The virtual machine can then take advantage of services running on the outside network and send traffic through routers to other networks, including the Internet.

This type of arrangement can enable you to consolidate many physical servers into virtual machines on a single Hyper-V server, by providing them all with access to the entire network. There is no distinction here between the physical network and the virtual one in the Hyper-V space.

CREATING AN ISOLATED NETWORK

For testing and evaluation purposes, or for classroom situations, you might create isolated network environments. By creating internal or private virtual switches, you can create a network that exists only within the Hyper-V space, with or without the parent partition included.

An isolated network such as this suffers from the weaknesses of its strengths. If you want to install the guest operating systems using Windows Deployment Services or configure the virtual machines using DHCP, you must install and configure these services on your private network. The guest operating systems also do not have access to the Internet, which prevents them from downloading operating system updates. Again, you must deploy appropriate substitutes on the private network.

To provide your systems with updates, install two network adapters on each of your virtual machines, by connecting one to a private switch and one to an external switch. This procedure enables the virtual machines to access the Internet and the private network.

Another method for creating an isolated network is to use virtual LANs (VLANs). This is particularly helpful if you have virtual machines on different Hyper-V servers that you want to add to the isolated network. By connecting the network adapters to an external switch and configuring them with the same VLAN identifier, you can create a network within a network, which isolates the VLAN from other computers. You can, for example, deploy a DHCP server on your VLAN without it interfering with the other DHCP servers in your production environment.

■ Business Case Scenarios

Scenario 9-1: Creating a New Virtual Switch

You need all VMs networked to each other, plus to the host operating system. Only the host operating system will be connected to the external network. What do you do?

Scenario 9-2: Configuring Advanced Network Adapter Features

You are concerned about your VMs receiving rogue DHCP servers. How can you prevent this from happening?

Configuring IPv4 and IPv6 Addressing

LESSON 10

Understanding IPv4 Addressing

THE BOTTOM LINE

Many enterprise administrators are so comfortable working with IPv4 addresses that they are hesitant to change. Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR) have been excellent stopgaps to the depletion of the 32-bit IP address space for years, and many would like to see them continue as such. However, the IPv6 transition, long a specter on the distant horizon, is now suddenly approaching at frightening speed, and it is time for administrators not familiar with the new technologies to catch up—or be left behind.

The IPv4 address space consists of 32-bit addresses, notated as four 8-bit decimal values from 0 to 255, separated by periods, as in the example 192.168.43.100. This is known as dotted decimal notation, and the individual 8-bit decimal values are called *octets* or *bytes*.

Each address consists of *network bits*, which identify a network, and *host bits*, which identify a particular device on that network. To differentiate the network bits from the host bits, each address must have a subnet mask.

A ***subnet mask*** is another 32-bit value consisting of binary 1 bits and 0 bits. When compared to an IP address, the bits corresponding to the 1's in the mask are the network bits, whereas the bits corresponding to the 0's are the host bits. Thus, if the 192.168.43.100 address mentioned earlier has a subnet mask of 255.255.255.0 (which in binary form is 11111111.11111111.11111111.00000000), the first three octets (192.168.43) identify the network and the last octet (100) identifies the host.

IPv4 Classful Addressing

Because the subnet mask associated with IP addresses can vary, so can the number of bits used to identify the network and the host.

The original Internet Protocol (IP) standard defines three classes of IP addresses, which provide support for networks of different sizes, as shown in Figure 10-1.

Figure 10-1

The three IPv4 address classes

Table 10-1 lists the number of networks and hosts supported by each address class.

Table 10-1

IPv4 Address Classes

IP Address Class	Class A	Class B	Class C
First bit values (binary)	0	10	110
First byte value (decimal)	0–127	128–191	192–223
Number of network identifier bits	8	16	24
Number of host identifier bits	24	16	8
Number of possible networks	126	16,384	2,097,152
Number of possible hosts	16,777,214	65,534	254

The *First bit values (binary)* row in Table 10-1 specifies the values that the first 1, 2, or 3 bits of an address in each class must have. Early TCP/IP implementations used these bit values instead of a subnet mask to determine the class of an address. The binary values of the first bits of each address class limit the possible decimal values for the first byte of the address. For example, because the first bit of Class A addresses must be 0, the possible binary values of the first byte in a Class A address range from 00000000 to 01111111, which in decimal form are values ranging from 1 to 127. Thus, when you see an IP address in which the first byte is a number from 1 to 127, you know that this is a Class A address.

Classless Inter-Domain Routing

When IP was developed, no one imagined that the 32-bit address space would ever be exhausted. In the early 1980s, no networks had 65,536 computers, never mind 16 million, and no one worried about the wastefulness of assigning IP addresses based on these classes.

Because of that wastefulness, classful addressing was gradually obsolesced by a series of subnetting methods, including variable-length subnet masking (VLSM) and eventually ***Classless Inter-Domain Routing (CIDR)***. CIDR is a subnetting method that enables you

to place the division between the network bits and the host bits anywhere in the address, not just between octets. This makes it possible to create networks of almost any size.

CIDR also introduces a new notation for network addresses. A standard dotted-decimal address representing the network is followed by a forward slash and a numeral specifying the size of the network-identifying prefix. For example, 192.168.43.0/24 represents a single Class C address that uses a 24-bit network identifier, leaving the other 8 bits for up to 254 host identifiers. Each of those hosts would receive an address from 192.168.43.1 to 192.168.43.254, using the subnet mask 255.255.255.0.

However, by using CIDR, you can subnet this address further by allocating some of the host bits to create subnets. To create subnets for four offices, for example, you can take two of the host identifier bits, changing the network address in CIDR notation to 192.168.43.0/26. Because the network identifier is now 26 bits, the subnet mask for all four networks is now 11111111.11111111.11111111.11000000 in binary form, or 255.255.255.192 in standard decimal form.

IPv4 Subnetting

In most cases, enterprise administrators use addresses in one of the private IP address ranges to create the subnets they need. If you are building a new enterprise network from scratch, you can choose any private address block and make things easy on yourself by subnetting along the octet boundaries.

For example, you can take the 10.0.0.0/8 private IP address range and use the entire second octet as a subnet ID. This enables you to create up to 256 subnets with as many as 65,536 hosts on each one. The subnet masks for all the addresses on the subnets will be 255.255.0.0, and the network addresses will proceed as follows:

- 10.0.0.0/16
- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16
- . . .
- 10.255.0.0/16

Of course, when you are working on an existing network, the subnetting process will likely be more difficult. You might, for example, be given a relatively small range of addresses and be asked to create a certain number of subnets out of them. To do this, use the following procedure.

CALCULATE IPV4 SUBNETS

1. Determine how many subnet identifier bits you need to create the required number of subnets.
2. Subtract the subnet bits you need from the host bits and add them to the network bits.
3. Calculate the subnet mask by adding the network and subnet bits in binary form and converting the binary value to decimal.
4. Take the least significant subnet bit and the host bits, in binary form, and convert them to a decimal value.
5. Increment the network identifier (including the subnet bits) by the decimal value you calculated to determine the network addresses of your new subnets.

By using the same example from earlier in this lesson, if you take the 192.168.43.0/24 address and allocate two extra bits for the subnet ID, you end up with a binary subnet mask value of 11111111.11111111.11111111.11000000 (255.255.255.192 in decimal form, as noted earlier).

The least significant subnet bit plus the host bits gives you a binary value of 1000000, which converts to a decimal value of 64. Therefore, if we know that the network address of your first subnet is 192.168.43.0, the second subnet must be 192.168.43.64, the third 192.168.43.128, and the fourth 192.168.43.192.

Supernetting

In addition to simplifying network notation, CIDR also makes possible a technique called *IP address aggregation* or *supernetting*, which can help reduce the size of Internet routing tables. A ***supernet*** combines contiguous networks that all contain a common CIDR prefix. When an organization possesses multiple contiguous networks that can be expressed as a supernet, listing those networks in a routing table using only one entry, instead of many, becomes possible.

For example, if an organization has the following five subnets, standard practice would be to create a separate routing table entry for each one:

- 172.16.43.0/24
- 172.16.44.0/24
- 172.16.45.0/24
- 172.16.46.0/24
- 172.16.47.0/24

To create a supernet encompassing all five of these networks, you must isolate the bits they have in common. When you convert the network addresses from decimal to binary, you get the following values:

- 172.16.43.0 **10101100.00010000.00101**011.00000000
- 172.16.44.0 **10101100.00010000.00101**100.00000000
- 172.16.45.0 **10101100.00010000.00101**101.00000000
- 172.16.46.0 **10101100.00010000.00101**110.00000000
- 172.16.47.0 **10101100.00010000.00101**111.00000000

In binary form, you can see that all five addresses have the same first 21 bits. Those 21 bits become the network identifier of the supernet address, as follows:

```
10101100.00010000.00101
```

After zeroing out the host bits to form the network address and converting the binary number back to decimal form, as follows, the resulting supernet address is 172.16.40.0/21.

```
10101100.00010000.00101000.00000000  172.16.40.0/21
```

This one network address can replace the original five in routing tables duplicated throughout the Internet. Obviously, this is just an example of a technique that you can use to combine dozens or even hundreds of subnets into single routing table entries.

Assigning IPv4 Addresses

In addition to understanding how IP addressing works, you must be familiar with the methods for deploying IP addresses to the computers on a network.

You have three alternatives for assigning IPv4 addresses:

- Manual configuration
- Dynamic Host Configuration Protocol (DHCP)
- Automatic Private IP Addressing (APIPA)

The following sections cover the advantages and disadvantages of these methods.

MANUAL IPV4 ADDRESS CONFIGURATION

Configuring a TCP/IP client manually is not terribly difficult, nor is it very time-consuming. Most operating systems provide a graphical interface that enables you to enter an IPv4 address, a subnet mask, and various other TCP/IP configuration parameters. To configure IP address settings in Windows Server 2012 R2, use the following procedure.

CONFIGURE IP ADDRESS SETTINGS

GET READY. Log on to Windows Server 2012 R2 using an account with Administrative privileges.

1. In the left pane of the *Server Manager* window, click the Local Server icon. The Properties tile for the server appears.
2. In the *Properties* tile, click the Ethernet hyperlink. The *Network Connections* window appears.
3. Right-click the Ethernet icon and, from the context menu, select Properties. The *Ethernet Properties* sheet appears.
4. Select the Internet Protocol Version 4 (TCP/IPv4) component and click Properties. The *Internet Protocol Version 4 (TCP/IPv4) Properties* sheet appears, as shown in Figure 10-2.

Figure 10-2

The *Internet Protocol Version 4 (TCP/IPv4) Properties* sheet

5. Select the Use the following IP address radio button and configure the following parameters with appropriate values:
   - IP address specifies the IP address on the local subnet that identifies the network interface in the computer.
   - Subnet mask specifies the mask associated with the local subnet.
   - Default gateway specifies the IP address of a router on the local subnet, which the system uses to access destinations on other networks.
6. Select the Use the following DNS server addresses radio button and configure the following parameter with appropriate values:
   - Preferred DNS server specifies the IP address of the DNS server that the system uses to resolve host names into IP addresses.
   - Alternate DNS server specifies the IP address of the DNS server that the system uses to resolve host names into IP addresses when the preferred DNS server is not available.
7. Click OK twice to close the *Internet Protocol Version 4 (TCP/IPv4)* and *Ethernet* Properties sheets.

CLOSE the *Network Connections* window.

You also can configure the IP address settings on a Windows system from the command line, using the Netsh.exe program. However, the big problem with manual configuration is that a task requiring two minutes for one workstation requires several hours for 100 workstations and several days for 1,000. Manually configuring all but the smallest networks is highly impractical, and not just for reasons of time. You also need to track the IPv4 addresses you assign and make sure each system has a unique address. This can end up being a logistical nightmare, which is why few network administrators choose this option.

DYNAMIC HOST CONFIGURATION PROTOCOL

The ***Dynamic Host Configuration Protocol (DHCP)*** is a client/server application as well as an Application-layer protocol that enables you to allocate IP addresses dynamically from a pool. Computers equipped with DHCP clients automatically contact a DHCP server when they start, and the server assigns them unique addresses and all the other configuration parameters the TCP/IP client requires.

The DHCP server leases addresses to clients, and after a predetermined interval, each client either renews its address or releases it back to the server for reallocation. DHCP not only automates the address assignment process, but it also keeps track of the addresses it assigns, preventing any address duplication on the network.

AUTOMATIC PRIVATE IP ADDRESSING (APIPA)

Automatic Private IP Addressing (APIPA) is the name assigned by Microsoft to a DHCP failover mechanism used by all current Microsoft Windows operating systems. On Windows computers, the DHCP client is enabled by default. If, after several attempts, a system fails to locate a DHCP server on the network, APIPA takes over and automatically assigns an address on the 169.254.0.0/16 network to the computer. The system then uses the Address Resolution Protocol (ARP) to ensure that no other computer on the local network is using the same address.

For a small network that consists of only a single LAN, APIPA is a simple and effective alternative to installing a DHCP server. However, for installations consisting of multiple LANs, with routers connecting them, you must take more positive control over the IP address assignment process. This usually means deploying one or more DHCP servers in some form.

Understanding IPv6 Addressing

THE BOTTOM LINE

As most administrators know, IPv6 is designed to increase the size of the IP address space, thus providing addresses for many more devices than IPv4. The 128-bit address size of IPv6 allows for 2^{128} possible addresses, an enormous number that works out to over 54 million addresses for each square meter of the Earth's surface.

In addition to providing more addresses, IPv6 also reduces the size of the routing tables in the routers scattered around the Internet. This is because the size of the addresses provides for more than the two levels of subnetting currently possible with IPv4.

Introducing IPv6

IPv6 addresses are different from IPv4 addresses in many ways other than length.

Instead of the four 8-bit decimal numbers separated by periods that IPv4 uses, IPv6 addresses use a notation called *colon-hexadecimal format*, which consists of eight 16-bit hexadecimal numbers, separated by colons, as follows:

```
XX:XX:XX:XX:XX:XX:XX:XX
```

Each X represents 8 bits (or 1 byte), which in hexadecimal notation is represented by two characters, as in the following example:

```
21cd:0053:0000:0000:e8bb:04f2:003c:c394
```

IPv6 Address Types

IPv6 has no broadcast transmissions, and therefore no broadcast addresses, unlike IPv4.

IPv6 supports three address types:

- **Unicast:** provides one-to-one transmission service to individual interfaces, including server farms sharing a single address. IPv6 supports several types of unicast addresses, including global, link-local, and unique local, terms that identify the scope of the address. Each type of unicast has a different ***format prefix (FP)***, a sequence of bits that identifies the type, just as an IPv4 address uses a sequence of bits to identify its class.
- **Multicast:** provides one-to-many transmission service to groups of interfaces identified by a single multicast address.
- **Anycast:** provides one-to-one-of-many transmission service to groups of interfaces, only the nearest of which (measured by the number of intermediate routers) receives the transmission.

Subnet IDs

The organization then has the 16-bit subnet ID with which to create an internal subnet hierarchy, if desired. Some possible subnetting options are as follows:

- **One-level subnet:** By setting all subnet ID bits to 0, all the computers in the organization are part of a single subnet. This option is suitable only for smaller organizations.

- **Two-level subnet:** By creating a series of 16-bit values, you can split the network into as many as 65,536 subnets. This is the functional equivalent of IPv4 subnetting, but with a much larger subnet address space.
- **Multi-level subnet:** By allocating specific numbers of subnet ID bits, you can create multiple levels of subnets, sub-subnets, and sub-sub-subnets, suitable for an enterprise of almost any size.

In one example, designed to support a large international enterprise, you could split the subnet ID as follows:

- **Country (4 bits):** Creates up to 16 subnets representing countries in which the organization has offices
- **State (6 bits):** Creates up to 64 sub-subnets within each country, representing states, provinces, or other geographical divisions
- **Office (2 bits):** Creates up to four sub-sub-subnets within each state or province, representing offices located in various cities
- **Department (4 bits):** Creates up to 16 sub-sub-sub-subnets within each office, representing the various departments or divisions.

To create a subnet ID for a particular office, you need to assign values for each field. To use the value 1 for the United States, the Country bits would be as follows:

```
0001------------
```

To create a subnet for an office in Alaska, you can use a value of 49 in the State field, which in binary form would appear as follows:

```
----110001------
```

For the second office in Alaska, use the value 2 for Office bits, as follows:

```
----------10----
```

For the Sales department in the office, use the value 9 for the Department bits, as follows:

```
------------1001
```

The resulting value for the subnet ID, in binary form, would therefore be as follows:

```
0001110001101001
```

In hexadecimal form, that would be 1c69.

Because the organization that owns the prefix wholly controls the subnet ID, enterprise administrators can adjust the number of levels in the hierarchy and the number of bits dedicated to each level as needed.

Assigning IPv6 Addresses

The processes by which you assign IPv6 addresses to network computers are similar to those in IPv4.

As with IPv4, a Windows computer can obtain an IPv6 address by three possible methods:

- **Manual allocation:** A user or administrator manually supplies an address and other information for each network interface.
- **Self-allocation:** The computer creates its own address using a process called stateless address autoconfiguration.
- **Dynamic allocation:** The computer solicits and receives an address from a Dynamic Host Configuration Protocol (DHCPv6) server on the network.

MANUAL IPV6 ADDRESS ALLOCATION

For the enterprise administrator, manual allocation of IPv6 addresses is even more impractical than in IPv4, because of the length of the addresses involved. However, it is possible, and the procedure for doing so in Windows Server 2012 R2 is the same as that for IPv4, except that you open the *Internet Protocol Version 6 (TCP/IPv6) Properties* sheet.

Because of the difficulties working with IPv6 addresses manually, the following two options are far more prevalent.

STATELESS IPV6 ADDRESS AUTOCONFIGURATION

When a Windows computer starts, it initiates the ***stateless address autoconfiguration*** process, during which it assigns each interface a link-local unicast address. This assignment always occurs, even when the interface is to receive a global unicast address later. The link-local address enables the system to communicate with the router on the link, which provides additional instructions.

DYNAMIC HOST CONFIGURATION PROTOCOL V6

If you deal with a multi-segment network, you need to use unique local or global addresses for internetwork communication, so you need either routers that advertise the appropriate network prefixes or DHCPv6 servers that can supply addresses with the correct prefixes.

The Remote Access role in Windows Server 2012 R2 supports IPv6 routing and advertising, and the DHCP Server role supports IPv6 address allocation.

■ Planning an IP Transition

THE BOTTOM LINE

Many enterprise administrators are so comfortable working with IPv4 addresses that they are hesitant to change. Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR) have been excellent stopgaps to the depletion of the 32-bit IP address space for years, and many would like to see them continue as such. However, the IPv6 transition, long a specter on the distant horizon, is now suddenly approaching at frightening speed, and it is time for administrators not familiar with the new technologies to catch up—or be left behind.

The networking industry, and particularly the Internet, has made huge investments in IPv4 technologies, and replacing them with IPv6 has had to be a gradual process. In fact, this gradual process was supposed to have begun in earnest in 1998. However, many people treat their IPv4 equipment like household appliances; unless they stop working, replacing them is not necessary. Unfortunately, the day in which that equipment stops working is approaching rapidly. So, while it might not yet be time to embrace IPv6 exclusively, you should have the transition in mind as you design your networks and make your purchasing decisions.

Enterprise administrators can do as they want within the enterprise itself. If all network devices in the organization support IPv6, they can begin to use IPv6 addresses at any time. However, the Internet is still firmly based on IPv4 and will continue to be so for several years. There, an IPv4-to-IPv6 transition must be a gradual project that includes some period of support for both IP versions.

Now and for the immediate future, you must work under the assumption that the rest of the world is using IPv4, and that you must implement a mechanism for transmitting your IPv6 traffic over an IPv4 connection. Eventually, the situation will be reversed. Most of the world will be running IPv6, and the remaining IPv4 technologies will have to transmit their older traffic over new links.

Tunneling

Right now, many network services are IPv4 only, and comparatively few require IPv6. Those IPv6 services are coming, however.

The DirectAccess remote networking feature in Windows Server 2012 R2 and Windows 8.1 is an example of an IPv6-only technology, and much of its complexity is due to the need to establish IPv6 connections over the IPv4 Internet.

Tunneling is the primary method for transmitting IPv6 traffic over an IPv4 network. ***Tunneling***, in this case, is the process by which a system encapsulates an IPv6 datagram within an IPv4 packet, as shown in Figure 10-3. The system then transmits the IPv4 packet to its destination, with none of the intermediate systems aware of the packet's contents.

Figure 10-3

IPv6 traffic encapsulated inside an IPv4 datagram

Tunneling can work in various configurations, depending on the network infrastructure, including router-to-router, host-to-host, router-to-host, and host-to-router. However, the most common configuration is router-to-router, as in the case of an IPv4-only connection between an IPv6 branch office and an IPv6 home office, as shown in Figure 10-4.

Figure 10-4

Two IPv6 networks connected by an IPv4 tunnel

The two routers support both IPv4 and IPv6, and the local networks at each site use IPv6. However, the link connecting the two sites is IPv4 only. By creating a tunnel between the routers in the two offices, using their IPv4 interfaces, they can exchange IPv6 traffic as needed. Computers at either site can send IPv6 traffic to the other site, and the routers are responsible for encapsulating the IPv6 data in IPv4 packets for the trip through the tunnel.

Windows supports several different tunneling methods, both manual and automatic, as described in the following sections.

CONFIGURING TUNNELS MANUALLY

You can manually create semi-permanent tunnels that carry IPv6 traffic through an IPv4-only network. When a computer running Windows Server 2012 R2 or Windows 8.1 is functioning as one end of the tunnel, you can use the following command:

```
netsh interface ipv6 add v6v4tunnel "interface" localaddress remoteaddress
```

In this command, *interface* is a friendly name you want to assign to the tunnel you are creating; *localaddress* and *remoteaddress* are the IPv4 addresses forming the two ends of the tunnel. An example of an actual command would be as follows:

```
netsh interface ipv6 add v6v4tunnel "tunnel"
206.73.118.19 157.54.206.43
```

CONFIGURING TUNNELS AUTOMATICALLY

A number of mechanisms automatically create tunnels over IPv4 connections. These are technologies designed to be temporary solutions during the transition from IPv4 to IPv6. All of them include a mechanism for expressing an IPv4 address in the IPv6 format. The following sections describe IPv4-to-IPv6 transition technologies that Windows supports.

6to4

The ***6to4*** mechanism essentially incorporates the IPv4 connections in a network into the IPv6 infrastructure by defining a method for expressing IPv4 addresses in IPv6 format and encapsulating IPv6 traffic into IPv4 packets.

To enable IPv4 links to function as part of the IPv6 infrastructure, 6to4 translates public IPv4 addresses into IPv6 using the following format:

- **FP:** The 3-bit format prefix is 001 in binary, the standard global unicast value.
- **TLA:** A 13-bit TLA value for a 6to4 address is always 0002 in hexadecimal.
- **V4ADDR:** A 32-bit V4ADDR value contains the IPv4 dotted decimal address, split into four separate octets and converted into hexadecimal form.
- **SLA ID:** Organizations can use a 16-bit SLA ID (or subnet ID) field to create an internal hierarchy of sites or subnets.
- **Interface ID:** This 64-bit field identifies a specific interface on the network.

For example, to convert the IPv4 address 157.54.176.7 into a 6to4 IPv6 address, you begin with 2002 for the FP and TLA fields, and then convert the four decimal values from the IPv4 address into hexadecimal, as follows:

- 157 = 9d
- 54 = 36
- 176 = b0
- 7 = 07

Therefore, you end up with the following IPv6 address:

`2002:9d36:b007:`*subnetID*`:`*interfaceID*

The subnet and interface identifiers use the same values as any other IPv6 link on the network. The encapsulation method is the same as that for a manually created tunnel, with a standard IPv4 header and containing the IPv6 data as the payload. A 6to4 router examines incoming packets and, if it detects the 2002 value in the first block, knows to transmit the packet over the IPv4 interface, using the 32 bits following the 2002 block as the IPv4 address.

ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an automatic tunneling protocol used by the Windows workstation operating systems that emulates an IPv6 link using an IPv4 network.

ISATAP also converts IPv4 addresses into an IPv6 Link-layer address format, but it uses a different method than 6to4. An ISATAP address uses the following format:

- The first 64 bits consist of the standard link-local network identifier, the value fe80 following by 48 bits of 0s.

- The first 16-bit block of the interface identifier consists of all 0s, except for the seventh bit, which is set to 1 when the IPv4 address is globally unique, and the eighth bit, which is set to 1 when the IPv4 address identifies a multicast group. In most cases, this block consists of all 0s.
- The second 16-bit block of the interface ID consists of the value 5efe, which represents the concatenated OUI for ISATAP (5e) and the standardized value fe.
- The final 32 bits of the interface identifier consist of the IPv4 address in hexadecimal form.

Therefore, the IPv4 address 157.54.176.7 would have the following as its ISATAP address:

```
fe80:0000:0000:0000:0000:5efe:9d36:b007
```

In compressed form, the address appears as follows:

```
fe80::5efe:9d36:b007
```

ISATAP does not support multicasting, so it cannot locate routers in the usual manner, using the Neighbor Discovery protocol. Instead, the system compiles a potential routers list (PRL) using DNS queries and sends Router Discovery messages to them regularly, using Internet Control Message Protocol version 6 (ICMPv6).

Teredo

To use 6to4 tunneling, both endpoints of the tunnel must have registered IPv4 addresses. However, on many networks, the system that would function as the endpoint is located behind a NAT router, and therefore has an unregistered address. In such a case, the only registered address available is assigned to the NAT router itself, and unless the router supports 6to4 (which many do not), establishing the tunnel is impossible.

Teredo is a mechanism that addresses this shortcoming by enabling devices behind non-IPv6 NAT routers to function as tunnel endpoints. To do this, Teredo encapsulates IPv6 packets within Transport-layer User Datagram Protocol (UDP) datagrams, rather than Network-layer IPv4 datagrams, as 6to4 does.

For a Teredo client to function as a tunnel endpoint, it must have access to a Teredo server, with which it exchanges Router Solicitation and Router Advertisement messages to determine whether the client is located behind a NAT router.

Teredo clients have the most complicated form of IPv6 address yet, which uses the following format:

- **Prefix:** A 32-bit field that identifies the system as a Teredo client. Windows clients use the prefix value 2001:0000, or 2001::/32.
- **Server IPv4:** A 32-bit field containing the IPv4 address of the Teredo server the client uses.
- **Flags:** A 16-bit field, the first bit of which is the Cone flag, set to 1 when the NAT device providing access to the Internet is a cone NAT, which stores the mappings between internal and external addresses and port numbers. The second bit is reserved for future use. The seventh and eighth bits are the Universal/Local and Individual/Group flags, which are both set to 0. The Teredo standard calls for the remaining 12 bits to be set to 0, but Windows assigns a random number to these bits to prevent attackers from attempting to discover the Teredo address.
- **Port:** A 16-bit field that specifies the external UDP port that the client uses for all Teredo traffic, in obscured form. The obscuration of the port number (and the following IPv4 address) helps prevent the NAT router from translating the port as it normally would as part of its packet processing. To obscure the port, the system runs an exclusive OR (XOR) with the value ffff.
- **Client IPv4:** A 32-bit field that specifies the external IPv4 address that the client uses for all Teredo traffic, in obscured form. As with the Port field, the obscuration is the result of converting the IPv4 address to hexadecimal and running an XOR with the value ffffffff.

If, for example, the IPv4 address and port of the Teredo client are both 192.168.31.243:32000, the Teredo server uses the address 157.54.176.7, and the client is behind a cone NAT router, the Teredo address, in standard format, would consist of the elements listed in Table 10-2.

Table 10-2

Standard Teredo Address Format

Element	Description
2001:0000	Standard Teredo prefix
9d36:b007	Server IPv4 address (157.54.176.7) converted to hexadecimal
8000	Flags field with first bit set to 1 and all others 0
82ff	Client UDP port number (32000), converted to hexadecimal (7d00) and XORed with ffff
3f57:e00c	Client IPv4 address (192.168.31.243), converted to hexadecimal (C0a8:1ff3) and XORed with ffffffff

Thus, the final Teredo address is as follows:

```
2001:0000:9d36:b007:8000:82ff:3f57:e00c
```

To initiate communications, a Teredo client exchanges null packets called *bubbles* with the desired destination, using the Teredo servers at each end as intermediaries. The function of the bubble messages is to create mappings for both computers in each other's NAT routers.

Business Case Scenarios

Scenario 10-1: Calculating IPv4 Subnets

The enterprise administrator has assigned Arthur the network address 172.16.85.0/25 for the branch office network that he is constructing. Arthur calculates that this gives him 126 (2^7) IP addresses, which is enough for his network, but he has determined that he needs six subnets with at least 10 hosts on each one. How can Arthur subnet the address he has been given to satisfy his needs? What IP addresses and subnet masks will the computers on his branch office network use?

Scenario 10-2: Calculating IPv6 Interface IDs

Ed has three servers running Windows Server 2012 R2, for which he has to configure IPv6 global unicast addresses manually. The MAC addresses for the network interfaces in the three machines are as follows:

- 60-EB-69- 93-5E-E5
- 00-15-5D-02-12-05
- D4-AE-52-BF-C3-2D

What are the EUI-64 interface IDs that Ed will use for these three MAC addresses?

11 LESSON

Deploying and Configuring the Dynamic Host Configuration Protocol (DHCP) Service

Understanding DHCP

THE BOTTOM LINE

The ***Dynamic Host Configuration Protocol (DHCP)*** service automatically configures the Internet Protocol (IP) address and other TCP/IP settings on network computers by assigning addresses from a pool (called a *scope*) and reclaiming them when they are no longer in use.

Aside from being a time-consuming chore, manually configuring TCP/IP clients can result in typographical errors that cause addressing conflicts, which interrupt network communications. DHCP prevents these errors and provides many other advantages, including automatic assignment of new addresses when computers are moved from one subnet to another, and automatic reclamation of addresses that are no longer in use.

DHCP consists of three components:

- A *DHCP server application* responds to client requests for TCP/IP configuration settings.
- A *DHCP client* issues requests to servers and applies the TCP/IP configuration settings it receives to the local computer
- A *DHCP communications protocol* defines the formats and sequences of the messages exchanged by DHCP clients and servers

All Microsoft Windows operating systems include DHCP client capabilities, and all the server operating systems (including Windows Server 2012 R2) include Microsoft DHCP Server. Microsoft's DHCP implementation is based on public domain standards published by the Internet Engineering Task Force (IETF) as RFC 2131, "Dynamic Host Configuration Protocol," and RFC 2132, "DHCP Options and BOOTP Vendor Extensions," and is interoperable with other DHCP implementations.

The DHCP standards define three different IP address allocation methods:

- ***Dynamic allocation:*** The DHCP server assigns an IP address to a client computer from a scope for a specified length of time. DHCP servers using dynamic allocation only lease addresses to clients. Each client must periodically renew the lease to continue using the address. If the client allows the lease to expire, the address is returned to the scope for reassignment to another client.

- ***Automatic allocation:*** The DHCP server permanently assigns an IP address to a client computer from a scope. After the DHCP server assigns the address to the client, the only way to change it is to reconfigure the computer manually. Automatic allocation is suitable for networks where you do not often move computers to different subnets. It reduces network traffic by eliminating the periodic lease renewal messages needed for dynamic allocation. In the Windows Server 2012 R2 DHCP server, automatic allocation is essentially dynamic allocation with an indefinite lease.
- ***Manual allocation:*** The DHCP server permanently assigns a specific IP address to a specific computer on the network. In the Windows Server 2012 R2 DHCP server, manually allocated addresses are called *reservations*. You use manually allocated addresses for computers that must have the same IP address at all times, such as Internet web servers that have specific IP addresses associated with their host names in the DNS namespace. Although you can just as easily configure such computers manually, DHCP reservations prevent the accidental duplication of permanently assigned IP addresses.

In addition to IP addresses, DHCP also can provide clients with values for the other parameters needed to configure a TCP/IP client, including a subnet mask, default gateway, and DNS server addresses. The object is to eliminate the need for any manual TCP/IP configuration on a client system. For example, the Microsoft DHCP server includes more than 50 configuration parameters, which it can deliver along with the IP address, even though Windows clients can use only a subset of those parameters.

The RFC 2132 document, "DHCP Options and BOOTP Vendor Extensions," defines an extensive list of parameters that compliant servers should support, and most major DHCP server packages adhere closely to this list. Many of these parameters are designed for use by specific system configurations and are submitted by vendors for inclusion in the standard document.

Deploying a DHCP Server

THE BOTTOM LINE DHCP servers operate independently, so you must install the service and configure scopes on every computer that will function as a DHCP server.

The DHCP Server service is packaged as a role in Windows Server 2012 R2, which you can install by using the *Add Roles and Features Wizard*, accessible from the Server Manager console. To install the DHCP Server service on a Windows Server 2012 R2 computer with Server Manager, use the following procedure.

DEPLOY A DHCP SERVER

GET READY. Log on to Windows Server 2012 R2 using an account with Administrative privileges.

1. In the *Server Manager* window, click Manage and then click Add Roles and Features. The *Add Roles and Features Wizard* appears, displaying the *Before you begin* page.
2. Click Next. The *Select Installation Type* page appears.
3. Leave the *Role-based or feature-based installation* radio button selected and click Next. The *Select Destination Server* page appears.
4. Select the server on which you want to install the roles and/or features and click Next. The *Select Server Roles* page appears.

5. Select the DHCP Server check box. An *Add features that are required for DHCP Server* dialog box appears.
6. Click Add Features, and then click Next. The *Select features* page appears.
7. Click Next. The *DHCP Server* page appears.
8. Click Next. The *Confirm installation selections* page appears.
9. Click Install. The *Installation progress* page appears as the wizard installs the role.
10. Click Close. The wizard closes.

CLOSE Server Manager.

When you install the DHCP Server role on a computer that is a member of an AD DS domain, the DHCP Server is automatically authorized to allocate IP addresses to clients that are also members of the same domain. If the server is not a domain member when you install the role, and you join it to a domain later, you must manually authorize the DHCP server in the domain. To do this, right-click the server node in the DHCP console and, from the context menu, select *Authorize*.

After installing the DHCP Server role, you must configure the service by creating a scope before it can serve clients.

Creating a Scope

A *scope* is a range of IP addresses on a particular subnet that a DHCP server has selected for allocation.

In Windows Server versions prior to 2012, you can create a scope as you install the DHCP Server role. However, in Windows Server 2012 and Windows Server 2012 R2, the procedures are separate. To create a scope using the DHCP snap-in for Microsoft Management Console (MMC), use the following procedure.

CREATE A DHCP SCOPE

GET READY. Log on to Windows Server 2012 R2, using an account with Administrative privileges.

1. In the *Server Manager* window, click Tools and then click DHCP. The *DHCP* console appears.
2. Expand the server and IPv4 nodes.
3. Right-click the IPv4 node and, from the context menu, select New Scope. The *New Scope Wizard* appears, displaying the *Welcome* page.
4. Click Next. The *Scope Name* page appears.
5. Type a name for the scope into the Name text box and click Next. The *IP Address Range* page appears, as shown in Figure 11-1.

Figure 11-1

The *IP Address Range* page in the New Scope Wizard

6. In the Start IP address text box, type the first in the range of addresses you want to assign. In the End IP address text box, type the last address in the range.
7. In the Subnet Mask text box, type the mask value for the subnet on which the scope will operate and click Next. The *Add Exclusions and Delay* page appears.
8. In the Start IP address and End IP address text boxes, specify a range of addresses you want to exclude from the scope. You can also specify a delay interval between the server's receipt of DHCPDISCOVER messages and its transmission of DHCPOFFER messages. Then click Next. The *Lease Duration* page appears.
9. Specify the length of the leases for the addresses in the scope and click Next. The *Configure DHCP Options* page appears.
10. Select Yes, I want to configure these options now and click Next. The *Router (Default Gateway)* page appears.
11. In the IP address text box, specify the address of a router on the subnet served by the scope and click Add. Then click Next. The *Domain Name and DNS Servers* page appears, as shown in Figure 11-2.

Figure 11-2

The *Domain Name and DNS Servers* page in the New Scope Wizard

12. In the Server name text box, type the name of a DNS server on the network and click Resolve, or type the address of a DNS server in the IP address text box and click Add. Then click Next. The *WINS Servers* page appears.
13. Click Next. The *Activate Scope* page appears.
14. Select Yes, I want to activate this scope now and click Next. The *Completing the New Scope Wizard* page appears.
15. Click Finish. The wizard closes.

CLOSE the DHCP console.

After the role installation and configuration is complete, all DHCP clients on the subnet identified in the scope you created can obtain their IP addresses and other TCP/IP configuration settings via DHCP. You can also use the DHCP console to create additional scopes for other subnets.

Configuring DHCP Options

The *New Scope Wizard* enables you to configure a few of the most commonly used DHCP options as you create a new scope, but you can always configure the many other options at a later time.

The Windows DHCP server supports two kinds of options:

- **Scope options:** Supplied only to DHCP clients receiving addresses from a particular scope.
- **Server options:** Supplied to all DHCP clients receiving addresses from the server.

The *Router* option is a typical example of a scope option, because a DHCP client's default gateway address must be on the same subnet as its IP address. The *DNS Servers* option is typically a server option, because DNS servers do not have to be on the same subnet, and networks often use the same DNS servers for all their clients.

The process of configuring all the options supported by the Windows DHCP server is the same. To configure a scope option, you right-click the *Scope Options* node and, from the context menu, select *Configure Options*. The *Scope Options* dialog box (see Figure 11-3) provides appropriate controls for each available option.

Figure 11-3

The Scope Options dialog box

Right-clicking the *Server Options* node enables you to display the *Server Options* dialog box, which behaves in exactly the same way as the *Scope Options* dialog box.

Creating a Reservation

While DHCP is an excellent TCP/IP configuration solution for most computers on a network, it is not such a good solution for a few components. Domain controllers and DHCP servers themselves, for example, need static IP addresses.

Because the DHCP dynamic allocation method allows for the possibility that a computer's IP address could change, it is not appropriate for these particular roles. However, it is still possible to assign addresses to these computers with DHCP by using manual, instead of dynamic, allocation.

In a Windows DHCP server, a manually allocated address is called a *reservation*. You create a reservation by expanding the scope node, right-clicking the *Reservations* node, and, from the context menu, selecting *New Reservation*. The *New Reservation* dialog box appears.

In this dialog box, you specify the IP address you want to assign and associate it with the client computer's media access control (MAC) address, which is hard-coded into its network interface adapter.

To discover the MAC address of a network interface adapter, run the Ipconfig.exe program with the /all parameter, as shown in Figure 11-4, where the MAC address appears as *Physical Address*.

Figure 11-4

A MAC address in the Ipconfig display

Of course, you also can manually configure the computer's TCP/IP client, but creating a DHCP reservation ensures that your DHCP servers manage all your IP addresses. In a large enterprise, where various administrators might be dealing with DHCP and TCP/IP configuration issues, the IP address that one technician manually assigns to a computer might be included in a DHCP scope by another technician, resulting in potential addressing conflicts. Reservations create a permanent record of the IP address assignment on the DHCP server.

Using PXE

The Windows operating systems include a DHCP client that can configure the IP address and other TCP/IP settings of computers with an operating system already installed. However, it is also possible for a bare metal computer—that is, a computer with no operating system—to use DHCP.

The ***Pre-boot Execution Environment (PXE)*** is a feature built into many network interface adapters that enables them to connect to a DHCP server over the network and obtain TCP/IP client settings, even when the computer has no operating system. Administrators typically use this capability to automate the operating system deployment process on large fleets of computers.

In addition to configuring the IP address and other TCP/IP client settings on the computer, the DHCP server can also supply the workstation with an option specifying the location of a boot file that the system can download and use to start the computer and initiate a Windows operating system installation. A PXE-equipped system downloads boot files using the Trivial File Transfer Protocol (TFTP), a simplified version of the FTP protocol that requires no authentication.

USING PXE WITH WDS

Windows Server 2012 R2 includes a role called Windows Deployment Services (WDS), which enables you to manage image files that remote computers can use to start up and install Windows. For a PXE adapter to access WDS images, the DHCP server on the network must have a custom PXEClient option (option 60) configured with the string "PXEClient." This indicates that the server can also provide option 66, Boot Server Host Name, and option 67, Bootfile Name.

The PXE client on the workstation typically needs no configuration, except possibly to change the boot device order, so that the computer attempts a network boot before using the local devices.

In a properly configured WDS installation of Windows 8, the client operating system deployment process proceeds as follows:

1. The client computer starts and, finding no local boot device, attempts to perform a network boot.
2. The client computer connects to a DHCP server on the network from which it obtains a DHCPOFFER message containing an IP address and other TCP/IP configuration parameters, plus the 60, 66, and 67 PXEClient options identifying the WDS server.
3. The client connects to the WDS server and is supplied with a boot image file, which it downloads using the Trivial File Transfer Protocol (TFTP).
4. The client loads Windows PE and the Windows Deployment Services client from the boot image file onto a RAM disk (a virtual disk created out of system memory) and displays a boot menu containing a list of the install images available from the WDS server.
5. The user on the client computer selects an install image from the boot menu, and the operating system installation process begins.
6. From this point, the setup process proceeds just like a manual installation.

■ Deploying a DHCP Relay Agent

THE BOTTOM LINE

Because they rely on broadcast transmissions, DHCPv4 clients can only access DHCP servers on the local network, under normal circumstances. However, it is possible to create a DHCP infrastructure in which one server provides addresses for multiple subnets. To do this, you must install a DHCP relay agent on every subnet that does not have a DHCP server on it.

Many routers can function as DHCP relay agents, but in situations where they cannot, you can configure a Windows Server 2012 R2 computer to function as a relay agent by using the following procedure.

DEPLOY A DHCP RELAY AGENT

GET READY. Log on to Windows Server 2012 R2, using an account with Administrative privileges.

1. In the *Server Manager* window, click Manage and then click Add Roles and Features. The *Add Roles and Features Wizard* appears, displaying the *Before you begin* page.
2. Click Next. The *Select Installation Type* page appears.
3. Leave the *Role-based or feature-based installation* radio button selected and click Next. The *Select Destination Server* page appears.
4. Select the server on which you want to install the roles and/or features and click Next. The *Select Server Roles* page appears.
5. Select the Remote access check box. An *Add features that are required for Remote Access* dialog box appears.
6. Click Add Features. Then click Next. The *Select features* page appears.
7. Click Next. The *Remote Access* page appears.
8. Click Next. The *Role Services* page appears.
9. Select the Routing check box. The *Add features that are required for Routing* page appears.
10. Click Add Features. Then click Next. The *Web Server Role (IIS)* page appears.
11. Click Next. The *Confirm installation selections* page appears.
12. Click Install. The *Installation progress* page appears as the wizard installs the role.
13. Click the Open the Getting Started Wizard link. The *Configure Remote Access – Getting Started Wizard* appears.
14. Click Deploy VPN only. The *Routing and Remote Access* console appears.
15. Right-click the server node and, on the context menu, select Configure and Enable Routing and Remote Access. The *Routing and Remote Access Server Setup Wizard* launches.
16. Click Next to bypass the *Welcome* page. The *Configuration* page appears, as shown in Figure 11-5.

Figure 11-5

The *Configuration* page of the Routing and Remote Access Server Setup Wizard

17. Select Custom configuration and click Next. The *Custom Configuration* page appears.
18. Select the LAN routing check box and click Next. The *Completing the Routing and Remote Access Server Setup Wizard* page appears.
19. Click Finish. A *Routing and Remote Access* message box appears, prompting you to start the service.
20. Click Start Service.
21. Expand the IPv4 node. Then, right-click the General node and, in the context menu, select New Routing Protocol. The *New Routing Protocol* dialog box appears.
22. Select DHCP Relay Agent and click OK. A *DHCP Relay Agent* node appears, subordinate to the IPv4 node.
23. Right-click the DHCP Relay Agent node and, on the context menu, select New Interface. The *New Interface for DHCP Relay Agent* dialog box appears.
24. Select the interface to the subnet on which you want to install the relay agent and click OK. The *DHCP Relay Properties* sheet for the interface appears, as shown in Figure 11-6.

TAKE NOTE*

You can also create a relay agent for DHCPv6 by adding a routing protocol to the IPv6 node

Figure 11-6

The *DHCP Relay Properties* sheet for a selected interface

25. Leave the *Relay DHCP packets* check box selected and configure the following settings, if needed:
    - Hop-count threshold specifies the maximum number of relay agents that DHCP messages can pass through before being discarded. The default value is 4 and the maximum value is 16. This setting prevents DHCP messages from being relayed endlessly around the network.
    - Boot threshold specifies the time interval (in seconds) that the relay agent should wait before forwarding each DHCP message it receives. The default value is 4 seconds. This setting enables you to control which DHCP server processes the clients for a particular subnet.
26. Click OK.
27. Right-click the DHCP Relay Agent node and, on the context menu, select Properties. The *DHCP Relay Agent Properties* sheet appears.

28. Type the IP address of the DHCP server to which you want the agent to relay messages and click Add. Repeat this step to add servers, if necessary.
29. Click OK.

CLOSE the *Routing and Remote Access* console.

At this point, the server is configured to relay DHCP messages to the server addresses you specified.

Business Case Scenarios

Scenario 11-1: Configuring DHCP Servers

After deploying a large number of wireless laptop computers on the network, Taylor, the IT director at Contoso, Ltd. decides to use DHCP to enable the laptop users to move from one subnet to another without having to manually reconfigure their IP addresses. Soon after the DHCP deployment, however, Taylor notices that some of the IP address scopes are being depleted, resulting in some computers being unable to connect to a new subnet. What can Taylor do to resolve this problem without altering the network's subnetting?

Scenario 11-2: Maximizing Lease Availability

You are configuring DHCP scope options for Contoso, Ltd. The company has a limited number of IP addresses available for clients, and it wants to configure DHCP to maximize IP address availability. Choose all of the following actions that will accomplish this objective:

a. Set long lease durations for IP addresses.
b. Set short lease durations for IP addresses.
c. Configure a DHCP option to automatically release an IP address when the computer shuts down.
d. Create DHCP reservations for all portable computers.

12 LESSON

Deploying and Configuring the DNS Service

Understanding the DNS Architecture

THE BOTTOM LINE

The Domain Name System (DNS) is a crucial element of both Internet and Active Directory communications.

All TCP/IP communication is based on IP addresses. Each computer on a network has at least one network interface, which is called a ***host***, in TCP/IP parlance, and each host has an IP address that is unique on that network. Every datagram transmitted by a TCP/IP system contains the sending computer's IP address and the intended recipient's IP address. However, when users access a shared folder on the network or a website on the Internet, they do so by specifying or selecting a host name, not an IP address. This is because names are easier to remember and use than IP addresses.

For TCP/IP systems to use these friendly host names, they must have some way to discover the IP address associated with a specific name. In the early days of TCP/IP networking, each computer had a list of names and their equivalent IP addresses, called a ***host table***. At that time, there were few enough computers on the fledgling Internet for the maintenance and distribution of a single host table to be practical.

Today, millions of computers are on the Internet, and the idea of maintaining and distributing a single file containing names for all of them is absurd. Rather than a host table stored on every computer, TCP/IP networks today use DNS servers to convert host names into IP addresses. This conversion process is referred to as ***name resolution***. The resulting solution was the Domain Name System (DNS).

Creating a DNS Standard

When the developers of what became the Internet recognized the increasing impracticality of the host table, they set about devising a solution that would not only solve their immediate maintenance and distribution problems, but would also remain a viable solution for decades to come.

At its core, the DNS is still a list of names and their equivalent IP addresses, but the method for creating, storing, and retrieving the names is different from those in a host table. The DNS consists of three elements, as follows:

- **The DNS name space:** The DNS standards define a tree-structured name space in which each branch of the tree identifies a ***domain***. Each domain contains a collection of ***resource records*** that contain host names, IP addresses, and other information. Query operations are attempts to retrieve specific resource records from a particular domain.
- **Name servers:** A DNS server is an application running on a server computer that maintains information about the domain tree structure and (usually) contains authoritative

information about one or more specific domains in that structure. The application is capable of responding to queries for information about the domains for which it is the authority, and also of forwarding queries about other domains to other name servers. This enables any DNS server to access information about any domain in the tree.

- **Resolvers:** A ***resolver*** is a client program that generates DNS queries and sends them to a DNS server for fulfillment. A resolver has direct access to at least one DNS server and can also process referrals to direct its queries to other servers when necessary.

In its most basic form, the DNS name resolution process consists of a resolver submitting a name resolution request to its designated DNS server. When the server does not possess information about the requested name, it forwards the request to another DNS server on the network. The second server generates a response containing the IP address of the requested name and returns it to the first server, which relays the information in turn to the resolver, as shown in Figure 12-1. In practice, however, the DNS name resolution process can be considerably more complex, as you learn in the following sections.

Figure 12-1

DNS servers relay requests and replies to other DNS servers

DNS Naming

To facilitate the continued growth of the namespace, the developers of the DNS created a two-tiered system, consisting of domain names and host names. The basic principle is that the administrators of individual networks obtain domain names from a centralized authority, and then assign the host names within that domain themselves. This process enables administrators to assign host names without worrying about duplication, as long as each host name is unique within its domain.

The domain name part of a DNS name is hierarchical and consists of two or more words, separated by periods. The DNS namespace takes the form of a tree that, much like a file system, has its root at the top. Just beneath the root is a series of top-level domains, and beneath each top-level domain is a series of second-level domains, as shown in Figure 12-2. At minimum, the complete DNS name for a computer on the Internet consists of a host name, a second-level domain name, and a top-level domain name, written in this order and separated by periods. The complete DNS name for a particular computer is called its ***fully qualified domain name (FQDN)***.

Figure 12-2

The DNS domain hierarchy

Unlike an IP address, which places the network identifier first and follows it with the host, the notation for an FQDN places the host name first, followed by the domain name, with the top-level domain name last. In the example cited previously, the FQDN *www.contoso.com* consists of a host (or computer) called *www* in the *contoso.com* domain. In the contoso.com domain name, *com* is the top-level domain and *contoso* is the second-level domain. Technically, every FQDN should end with a period, representing the root of the DNS tree, as follows:

```
www.contoso.com.
```

However, the period is rarely included in FQDNs today.

Understanding the DNS Domain Hierarchy

The hierarchical nature of the DNS namespace is designed to make it possible for any DNS server on the Internet to locate the authoritative source for any domain name, by using a minimum number of queries. This efficiency results from the domains at each level of the hierarchy are responsible for maintaining information about the domains at the next lower level.

The authoritative source for any domain is the DNS server (or servers) responsible for maintaining that domain's resource records. Each level of the DNS domain hierarchy has name servers responsible for the individual domains at that level.

At the top of the DNS hierarchy are the root name servers. The ***root name servers*** are the highest-level DNS servers in the entire namespace, and they maintain information about the top-level domains. All DNS server implementations are preconfigured with the IP addresses of the root name servers, because these servers are the ultimate source for all DNS information. When a computer attempts to resolve a DNS name, it begins at the top of the namespace hierarchy with the root name servers and works down the levels until it reaches the authoritative server for the domain in which the name is located.

TOP-LEVEL DOMAINS

Just beneath the root name servers are the top-level domains (TLDs). The original DNS name space called for six ***generic top-level domains (gTLDs),*** dedicated to specific purposes, as follows:

- *com:* Commercial organizations
- *edu:* Four-year, degree-granting educational institutions in North America
- *gov:* United States government institutions
- *mil:* United States military applications
- *net:* Networking organizations
- *org:* Noncommercial organizations

The *edu*, *gov*, and *mil* domains are reserved for use by certified organizations, but the *com*, *org*, and *net* domains are called ***global domains,*** because organizations anywhere in the world can register second-level domains within them.

SECOND-LEVEL DOMAINS

Each top-level domain has its own collection of second-level domains. Individuals and organizations can purchase these domains for their own use. For the payment of an annual fee, you can purchase the rights to a second-level domain.

To use the domain name, you must supply the registrar with the IP addresses of two DNS servers that you want to be the authoritative sources for information about the domain. A DNS server is a software program that runs on a computer. DNS server products are available

for all the major network operating systems. The DNS servers do not need to be located on the registrant's network; many companies outsource their Internet server hosting chores and use their service provider's DNS servers.

SUBDOMAINS

After you purchase the rights to a second-level domain, you can create as many hosts as you want in that domain, by creating new resource records on the authoritative servers. You can also create as many additional domain levels as you want. The only limitations to the subdomains and hosts you can create in your second-level domain are as follows:

- Each individual domain name can be no more than 63 characters long.
- The total FQDN (including the trailing period) can be no more than 255 characters long.

For the convenience of users and administrators, most domain names do not approach these limitations.

Understanding DNS Communications

Although all Internet applications use DNS to resolve host names into IP addresses, this name resolution process is easiest to see when you use a web browser to access an Internet site.

When you type a URL containing a DNS name (such as *www.microsoft.com*) into the browser's *Address* box and press the *Enter* key, you might see a message that says something like, "Finding Site: www.microsoft.com." Then, a few seconds later, you might see a message that says, "Connecting to," followed by an IP address. It is during this interval that the DNS name resolution process occurs.

From the client's perspective, the procedure that occurs during these few seconds consists of the application sending a query message to its designated DNS server that contains the name to be resolved. The server replies with a message containing the IP address corresponding to that name. Using the supplied address, the application can transmit a message to the intended destination. When you examine the DNS server's role in the process, you see the procedure's complexity.

Comprehending DNS Server Caching

The DNS name resolution process might seem long and complex, but in many cases, it isn't necessary for the client's DNS server to send queries to the servers for each domain specified in the requested DNS name. That is, DNS servers are capable of retaining the information they learn about the DNS name space in the course of their name resolution procedures and storing it in a cache on the local drive.

A DNS server that receives requests from clients, for example, caches the addresses of the requested systems, as well as the addresses for authoritative servers of particular domains. The next time that a client requests the resolution of a previously resolved name, the server can respond immediately with the cached information, as shown in Figure 12-3. In addition, if a client requests another name in one of the same domains, the server can send a query directly to an authoritative server for that domain, and not to a root name server. Thus, the names in commonly accessed domains generally resolve more quickly because one of the servers along the line has information about the domain in its cache, whereas names in obscure domains take longer because the entire request/referral process is needed.

Figure 12-3

Name caching enables the second name resolution request for the same name to bypass the referral process

NEGATIVE CACHING

In addition to storing information that aids in the name resolution process, most modern DNS server implementations are also capable of negative caching. ***Negative caching*** occurs when a DNS server retains information about names that do not exist in a domain. If, for example, a client sends a query to its DNS server containing a name in which the second-level domain does not exist, the top-level domain server will return a reply containing an error message to that effect. The client's DNS server will then retain the error message information in its cache. The next time a client requests a name in that domain, the DNS server will be able to respond immediately with its own error message, without consulting the top-level domain.

CACHE DATA PERSISTENCE

Caching is a vital element of the DNS architecture, because it reduces the number of requests sent to the root name and top-level domain servers, which, being at the top of the DNS tree, are the most likely to act as a bottleneck for the whole system. However, caches must be purged eventually, and there is a fine line between effective and ineffective caching.

Because DNS servers retain resource records in their caches, it can take hours or even days for changes made in an authoritative server to be propagated around the Internet. During this period, users might receive incorrect information in response to a query. If information remains in server caches too long, then the changes that administrators make to the data in their DNS servers take too long to propagate around the Internet. If caches are purged too quickly, then the number of requests sent to the root name and top-level domain servers increases precipitously.

The amount of time that DNS data remains cached on a server is called its *Time To Live (TTL).* Unlike most data caches, the TTL is not specified by the administrator of the server where the cache is stored. Instead, the administrators of each authoritative DNS server specify how long the data for the resource records in their domains or zones should be retained in the servers where it is cached. This enables administrators to specify a TTL value based on the volatility of their server data. On a network where changes in IP addresses or the addition of new resource records is frequent, a lower TTL value increases the likelihood that clients will receive current data. On a network that rarely changes, you can use a longer TTL value, and minimize the number of requests sent to the parent servers of your domain or zone.

To modify the TTL value for a zone on a Windows Server 2012 DNS server, right-click the zone, open the Properties sheet, and click the *Start Of Authority (SOA)* tab. On this tab, you can modify the TTL for this record setting from its default value of one hour.

Using DNS Forwarders

DNS servers send recursive queries to other servers when you configure a server to function as a forwarder.

On a network running several DNS servers, you might not want all the servers sending queries to other DNS servers on the Internet. If the network has a slow connection to the Internet, for example, several servers transmitting repeated queries might use too much of the available bandwidth.

To prevent this, most DNS implementations enable you to configure one server to function as the forwarder for all Internet queries generated by the other servers on the network. Any time that a server has to resolve the DNS name of an Internet system and fails to find the needed information in its cache, it transmits a recursive query to the forwarder, which is then responsible for sending its own iterative queries over the Internet connection. After the forwarder resolves the name, it sends a reply back to the original DNS server, which relays it to the client.

To configure forwarders on a Windows Server 2012 R2 DNS server, use the following procedure.

CONFIGURE FORWARDERS

GET READY. Log on to Windows Server 2012 R2 domain controller by using an account with administrative privileges.

1. In the *Server Manager* window, click Tools > DNS. The *DNS Manager* console appears.
2. Right-click the server node and, from the context menu, select Properties. The server's Properties sheet appears.
3. Click the Forwarders tab.
4. Click Edit. The Edit Forwarders dialog box appears.
5. Type the name or address of the DNS server you want to function as a forwarder and press Enter. The system validates the name or address by connecting to the DNS server.
6. Click OK to close the Edit Forwarders dialog box and add the servers to the Forwarders tab.
7. Click OK to close the server's Properties sheet.

CLOSE the *DNS Manager* console.

Designing a DNS Deployment

THE BOTTOM LINE

All the DNS information in the preceding sections might at first seem gratuitous, but understanding the structure of the DNS and how the clients and servers communicate is crucial to creating an effective DNS deployment plan.

Every computer on a TCP/IP network needs access to a DNS server, but this does not mean that you must deploy your own DNS servers on your network. Internet service providers (ISPs) nearly always include the use of their DNS servers into their rates, and in some cases, it might be better to use other DNS servers, rather than run your own.

When designing a DNS deployment, you should first determine what DNS services your network requires. Consider the information in the following sections as you create your design.

Resolving Internet Names

If you provide your network users with access to the Internet, as most organizations do, then every user must have at least one DNS server address specified in its TCP/IP configuration settings. If you use DHCP servers to assign IP addresses to the network computers, you can configure the servers to configure the clients' DNS server addresses as well.

For Internet name resolution purposes, the only functions required of the DNS server are the capability to process incoming queries from resolvers and send its own queries to other DNS servers on the Internet. A DNS server that performs only these functions is known as a ***caching-only server***, because it is not the authoritative source for any domain and hosts no resource records of its own.

Installing your own caching-only DNS server is a simple matter, or you can use the DNS servers supplied by your ISP. The important factor to consider in this decision is the amount of traffic generated by the server's query process. In the DNS name resolution process, the client resolver and its DNS server exchange one query message and one reply. If the clients on your local network use the DNS servers on your ISP's network, then your Internet connection has to handle only these two messages, as shown in Figure 12-4.

Figure 12-4

Using an ISP's caching-only DNS server

If, however, you install a DNS server on your local network, the recursive queries the server receives from clients cause it to send numerous iterative queries to various other DNS servers on the Internet. These multiple message exchanges must all pass over the Internet connection, as shown in Figure 12-5. When you have hundreds or thousands of clients using the DNS server, the amount of iterative query traffic the server generates can overburden your Internet connection or greatly increase its cost.

Figure 12-5

Using your own caching-only DNS server

As a general rule, if your network requires no DNS services other than name resolution, you should consider using off-site DNS servers.

Hosting Internet Domains

If you host a domain on the Internet, you must pay an annual fee to register a second-level domain name with a commercial registrar and supply it with the IP addresses of your DNS servers. These servers are the authoritative source for information about your domain. Therefore, they must have registered IP addresses and be accessible from the Internet at all times.

The two main reasons for registering an Internet domain name are to host web servers and to create e-mail addresses. The authoritative DNS servers for the domain must have resource records that can provide Internet users with the IP addresses of your web servers and e-mail servers. If the authoritative DNS servers are offline, Internet users might be unable to access your web servers, and e-mail messages destined for your domain could bounce back to their senders.

As with name resolution, the DNS servers you use to host your domain can be computers on your own network or servers supplied by a commercial entity. The DNS servers that host your domain do not need to be located in that domain, nor do they need to be supplied by the registrar from whom you obtained your domain name. You can usually pay an additional fee to your domain registrar and have them host the domain on their servers, or you can use you ISP's servers, also for an additional fee.

Creating Internet Domains

THE BOTTOM LINE

Designing a DNS namespace for your organization's Internet presence is usually the easiest part of deploying DNS. Most organizations register a single second-level domain and use it to host all their Internet servers.

In most cases, the selection of a second-level domain name depends on what is available. A large portion of the most popular top-level domain, *com*, is already depleted, and you might find that the name you want to use is already taken. In this case, you have three alternatives:

- Choose a different domain name.
- Register the name in a different top-level domain.
- Attempt to purchase the domain name from its current owner.

Some organizations maintain multiple sites on the Internet, for various reasons. Your organization might be involved in several separate businesses that warrant individual treatment, or your company might have independent divisions with different sites. You might also create different sites for retail customers, wholesale customers, and providers. Whatever the reason, the following two basic ways can help you implement multiple sites on the Internet:

- **Register a single second-level domain name and then create multiple subdomains beneath it:** For the price of a single domain registration, you can create as many third-level domains as you need, and you can also maintain a single brand across all your sites. For example, a company called *Contoso Pharmaceuticals* might register the contoso.com domain, and then create separate websites for doctors and patients, in domains called *doctors.contoso.com* and *patients.contoso.com*.
- **Register multiple second-level domains:** If your organization consists of multiple, completely unrelated brands or operations, this is often the best solution. You must pay a separate registration fee for each domain name, however, and you must maintain a separate DNS namespace for each domain. A problem might also arise when you try to integrate your Internet domains with your internal network. You can select one of your second-level domains to integrate with your internal namespace, or you can leave your internal and external namespaces completely separate, as discussed later in this lesson.

Deploying a DNS Server

THE BOTTOM LINE

The process of deploying a DNS server on a Windows Server 2012 R2 computer is a matter of installing the DNS Server role, by using the Add Roles and Features Wizard in Server Manager. The actual installation requires no additional input; there are no additional pages in the wizard and no role services to select.

After you install the DNS Server role, the computer is ready to perform caching-only name resolution services for any clients that have access to it. The role also installs the DNS Manager console, shown in Figure 12-6, which you use to configure the DNS server's other capabilities. To configure the server to perform other services, consult the following sections.

Figure 12-6

The DNS Manager console

Creating Zones

A ***zone*** is an administrative entity you create on a DNS server to represent a discrete portion of the DNS namespace.

Administrators typically divide the DNS namespace into zones to store them on different servers and to delegate their administration to different people. Zones always consist of entire domains or subdomains. You can create a zone that contains multiple domains, as long as those domains are contiguous in the DNS namespace. For example, you can create a zone containing a parent domain and its child, because they are directly connected, but you cannot create a zone containing two child domains without their common parent, because the two children are not directly connected.

You can divide the DNS namespace into multiple zones and host them on a single DNS server, although there is usually no persuasive reason to do so. The DNS server in Windows Server 2012 R2 can support as many as 200,000 zones on a single server, although it is hard to imagine a scenario that would require that many. In most cases, an administrator creates multiple zones on a server and then delegates most of them to other servers, which then become responsible for hosting them.

Every zone consists of a zone database, which contains the resource records for the domains in that zone. The DNS server in Windows Server 2012 R2 supports three zone types, which specify where the server stores the zone database and what kind of information it contains. These zone types are as follows:

- **Primary zone:** creates a primary zone that contains the master copy of the zone database, where administrators make all changes to the zone's resource records. If the *Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller)* check box is cleared, the server creates a primary master zone database file on the local drive. This is a simple text file that is compliant with most non-Windows DNS server implementations.

- **Secondary zone:** creates a duplicate of a primary zone on another server. The secondary zone contains a backup copy of the primary master zone database file, stored as an identical text file on the server's local drive. You cannot modify the resource records in a secondary zone manually; you can update them only by replicating the primary master zone database file, using a process called a ***zone transfer***. You should always create at least one secondary zone for each file-based primary zone in your namespace, both to provide fault tolerance and to balance the DNS traffic load.
- **Stub zone:** creates a copy of a primary zone that contains the key resource records that identify the authoritative servers for the zone. The stub zone forwards or refers requests. When you create a stub zone, you configure it with the IP address of the server that hosts the zone from which you created the stub. When the server hosting the stub zone receives a query for a name in that zone, it either forwards the request to the host of the zone or replies with a referral to that host, depending on whether the query is recursive or iterative.

The DNS was designed long before Active Directory, so most of the Internet relies on primary and secondary zones using text-based database files. The most common DNS server implementation on the Internet is a UNIX program called *bind* that uses these databases.

However, for DNS servers supporting internal domains, and especially AD DS domains, using the Windows DNS server to create a primary zone and store it in Active Directory is the recommended procedure. When you store the zone in the AD DS database, you do not need to create secondary zones or perform zone transfers, because AD DS takes the responsibility for replicating the data, and your backup solution used to protect Active Directory protects the DNS data.

USING ACTIVE DIRECTORY-INTEGRATED ZONES

When you are running the DNS server service on a computer that is an AD DS domain controller and you select the *Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller)* check box while creating a zone in the *New Zone Wizard*, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the AD DS database. Storing the DNS database in Active Directory provides several advantages, including ease of administration, conservation of network bandwidth, and increased security.

In Active Directory-integrated zones, the zone database is replicated automatically to other domain controllers, along with all other Active Directory data. Active Directory uses a multiple master replication system so that copies of the database are updated on all domain controllers in the domain. You can modify the DNS resource records on any domain controller hosting a copy of the zone database, and Active Directory will update all of the other domain controllers automatically. You don't need to create secondary zones or manually configure zone transfers, because Active Directory performs all database replication activities.

By default, Windows Server 2012 R2 replicates the database for a primary zone stored in Active Directory to all the other domain controllers running the DNS server in the AD DS domain where the primary is located. You can also modify the scope of zone database replication to keep copies on all domain controllers throughout the enterprise, or on all domain controllers in the AD DS domain, whether or not they are running the DNS server. You can also create a custom replication scope that copies the zone database to the domain controllers you specify.

Active Directory conserves network bandwidth by replicating only the DNS data that has changed since the last replication, and by compressing the data before transmitting it over the network. The zone replications also use the full security capabilities of Active Directory, which are considerably more robust than those of file-based zone transfers.

CREATING AN ACTIVE DIRECTORY ZONE

To create a new primary zone and store it in Active Directory, use the following procedure.

CREATE AN ACTIVE DIRECTORY ZONE

GET READY. Log on to Windows Server 2012 R2 domain controller using an account with administrative privileges.

1. In the *Server Manager* window, click Tools > DNS. The *DNS Manager* console appears.
2. Expand the server node and select the Forward Lookup Zones folder.
3. Right-click the Forward Lookup Zones folder and, from the context menu, select New Zone. The *New Zone Wizard* appears.
4. Click Next to bypass the *Welcome* page. The *Zone Type* page appears, as shown in Figure 12-7.

Figure 12-7

The *Zone Type* page of the New Zone Wizard

5. Leave the *Primary Zone* option and the *Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller)* check box selected and click Next. The *Active Directory Zone Replication Scope* page appears.
6. Click Next. The *Zone Name* page appears.
7. Specify the name you want to assign to the zone in the Zone Name text box and click Next. The *Dynamic Update* page appears.
8. Select one of the following options:
   - Allow only secure dynamic updates
   - Allow both nonsecure and secure dynamic updates
   - Do not allow dynamic updates
9. Click Next. The *Completing the New Zone Wizard* page appears.
10. Click Finish. The wizard creates the zone.

CLOSE the *DNS Manager* console.

After you create a primary zone, you can create resource records that specify the names of the hosts on the network and their equivalent IP addresses.

Creating Resource Records

When you run your own DNS server, you create a resource record for each host name that you want to be accessible by the rest of the network.

There are several different types of resource records used by DNS servers, the most important of which are as follows:

- **SOA (Start of Authority):** indicates that the server is the best authoritative source for data concerning the zone. Each zone must have an SOA record, and only one SOA record can be in a zone.
- **NS (Name Server):** identifies a DNS server functioning as an authority for the zone. Each DNS server in the zone (whether primary master or secondary) must be represented by an NS record.
- **A (Address):** provides a name-to-address mapping that supplies an IPv4 address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.
- **AAAA (Address):** provides a name-to-address mapping that supplies an IPv6 address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.
- **PTR (Pointer):** provides an address-to-name mapping that supplies a DNS name for a specific address in the *in-addr.arpa* domain. This is the functional opposite of an A record, used for reverse lookups only.
- **CNAME (Canonical Name):** creates an alias that points to the *canonical* name (that is, the "real" name) of a host identified by an A record. Administrators use CNAME records to provide alternative names by which systems can be identified.
- **MX (Mail Exchanger):** identifies a system that directs e-mail traffic sent to an address in the domain to the individual recipient, a mail gateway, or another mail server.

To create a new Address resource record, use the following procedure.

CREATE AN ADDRESS RESOURCE RECORD

GET READY. Log on to Windows Server 2012 R2 using an account with Administrative privileges.

1. In the *Server Manager* window, click Tools > DNS. The *DNS Manager* console appears.
2. Expand the server node and select the Forward Lookup Zones folder.
3. Right-click the zone in which you want to create the record and, from the context menu, select New Host (A or AAAA). The *New Host* dialog box appears, as shown in Figure 12-8.

Figure 12-8

The New Host dialog box

4. In the Name text box, type the host name for the new record. The FQDN for the record appears.

5. In the IP address text box, type the IPv4 or IPv6 address associated with the host name.
6. Select the following check boxes, if necessary:
   - Create associated pointer (PTR) record creates a reverse name lookup record for the host in the in-addr.arpa domain
   - Allow any authenticated use to update DNS records with the same owner name enables users to modify their own resource records
7. Click Add Host. The new resource record is created in the zone you selected.

CLOSE the *DNS Manager* console.

To create a PTR record for a new host, you can select the *Create associated pointer (PTR) record* check box in the *New Host* dialog box, but that will only be effective if a reverse lookup zone already exists on the server. To create the zone, you follow the same procedure described previously, but select the *Reverse Lookup Zones* folder. This causes the *New Zone Wizard* to add a *Reverse Lookup Zone Name* page like the one shown in Figure 12-9.

Figure 12-9

The *Reverse Lookup Zone Name* page in the New Zone Wizard

A second page then appears, as shown in Figure 12-10, in which you supply the Network ID that the wizard uses to create the zone.

Figure 12-10

The second *Reverse Lookup Zone Name* page in the New Zone Wizard

After the zone is created, you can either create PTR records along with A or AAAA records, or create a new PTR record by using the interface shown in Figure 12-11.

Figure 12-11

The New Resource Record dialog box

Configuring DNS Server Settings

After you install a DNS server and create zones and resource records on it, you can alter settings to modify its behavior.

The following sections describe some of these settings.

CONFIGURING ACTIVE DIRECTORY DNS REPLICATION

To modify the replication scope for an Active Directory-integrated zone, open the zone's Properties sheet in the *DNS Manager* console, and in the *General* tab, click the *Change button for Replication: All DNS Servers In the Active Directory Domain* to display the *Change Zone Replication Scope* dialog box. The options are the same as those in the New Zone Wizard.

CONFIGURING ROOT HINTS

Every DNS server must be able to contact the root name servers to initiate name resolution processes. Most server implementations, including Microsoft DNS Server, are preconfigured with the names and addresses of multiple root name servers. These are called *root hints*.

The 13 root name server names are located in a domain called *root-servers.net*, and are named using letters of the alphabet. The servers are scattered around the world on different subnets, to provide fault tolerance.

To modify the root hints on a Windows Server 2012 DNS server, right-click the server node, open the Properties sheet, and click the *Root Hints* tab, as shown in Figure 12-12. On this tab, you can add, edit, or remove root hints from the list provided.

Figure 12-12

The Root Hints tab on a DNS server's Properties sheet

Business Case Scenarios

Scenario 12-1: Deploying DNS Servers

Harold is a freelance networking consultant who has designed a network for a small company with a single location. The owner of the company wants to use an Active Directory domain, so Harold installs a Windows Server 2012 R2 domain controller with the Active Directory Domain Services and DNS Server roles. Harold also uses DHCP to configure all of the workstations on the network to use the DNS services provided by the domain controller.

Soon after the installation, however, the owner of the company reports extremely slow Internet performance. After examining the traffic passing over the Internet connection, you determine that it is being flooded with DNS traffic. What can you do to reduce the amount of DNS traffic passing over the internet connection?

Scenario 12-2: Regulating DNS Traffic

Ralph is an enterprise administrator for Wingtip Toys, which has recently expanded its customer service division by adding 100 workstations. All of the workstations on the company network are configured to use a server on the perimeter network as their primary DNS server and a server on their ISP's network as a secondary. As a result of the expansion, Internet performance has slowed down perceptibly, and a Network Monitor trace indicates that there is a disproportionate amount of DNS traffic on the link between the perimeter network and the ISP's network. What are two ways that Ralph can reduce the amount of DNS traffic passing over the Internet connection?

Installing Domain Controllers

LESSON 13

Introducing Active Directory

THE BOTTOM LINE

A directory service is a repository of information about the resources—hardware, software, and human—connected to a network. Users, computers, and applications throughout the network can access the repository for various purposes, including user authentication, storage of configuration data, and even simple white pages–style information lookups. ***Active Directory Domain Services (AD DS)*** is the directory service that Microsoft first introduced in Windows 2000 Server and has upgraded in each successive server operating system release, including Windows Server 2012 R2.

AD DS is a directory service that enables you to create organizational divisions called domains. A ***domain*** is a logical container of network components, hosted by at least one server designated as a ***domain controller***. The domain controllers for each domain replicate their data among themselves for fault tolerance and load-balancing purposes.

Understanding Active Directory Architecture

Active Directory is a hierarchical directory service, based on the domain, that is scalable in both directions.

In AD DS, you can subdivide a domain into organizational units and populate it with objects. You can also create multiple domains and group them into sites, trees, and forests. As a result, AD DS provides a highly flexible architecture that can accommodate the smallest and the largest organizations, as well as provide various design options.

The following sections examine the components you can use to design and build an Active Directory structure.

UNDERSTANDING OBJECTS AND ATTRIBUTES

An AD DS domain is a hierarchical structure that takes the form of a tree, much like a file system. The domain consists of objects, each of which represents a logical or physical resource. Objects come in two basic classes: container objects and leaf objects. A ***container object*** can have other objects subordinate to it, whereas a ***leaf object*** cannot have subordinate objects.

The container objects essentially form the branches of the tree, with the leaf objects growing on the branches.

The domain itself is a container object, as are the organizational unit objects within the domain. Leaf objects can represent users, computers, groups, applications, and other resources on the network.

Every object consists of ***attributes***, which store information about the object. A container object has, as one of its attributes, a list of all the other objects it contains. Leaf objects have attributes that contain information about the specific resource the object represents. Some attributes are created automatically, such as the globally unique identifier (GUID) that the domain controller assigns to each object when it creates it, whereas you must supply information for other attributes manually.

UNDERSTANDING DOMAINS

The domain is the fundamental component of the Active Directory architecture. You can zoom into a domain and create a hierarchy within it, and you can zoom out and create a hierarchy out of multiple domains. In AD DS, domains function by default as the boundaries for virtually all directory functions, including administration, access control, database management, and replication. You begin the process of designing an Active Directory infrastructure by deciding what domains to create, and you begin deploying AD DS by creating your first domain.

ZOOMING IN: ORGANIZATIONAL UNITS

While the domain is the fundamental division in the Active Directory service, the extreme scalability that AD DS provides can result in domains containing many thousands of objects. When domains grow this large, dividing the security and administrative responsibility for the domain among several divisions or departments can become necessary. To make this possible, you can create objects within a domain called organizational units.

An ***organizational unit (OU)*** is a container object that functions in a subordinate capacity to a domain, something like a subdomain, but without the complete separation of security policies. As container objects, OUs can contain other OUs, as well as leaf objects. You can apply separate Group Policy settings to an OU and delegate the administration of an OU as needed. However, an OU is still part of the domain and still inherits policies and permissions from its parent objects.

ZOOMING IN: GROUPS

Group objects are not containers, as OUs are, but they perform a similar function, with important differences. Groups are not full-fledged security divisions, as OUs are; you cannot apply Group Policy settings to a group object directly. However, group members—which can be leaf objects, such as users or computers, as well as other groups—inherit permissions assigned to that group.

One of the most important differences between groups and OUs is that group memberships are independent of the domain's tree structure. A group can have members located anywhere in the domain and, in some cases, can have members from other domains.

ZOOMING OUT: DOMAIN TREES

When designing an AD DS infrastructure, you might, in some cases, want to create multiple domains. Active Directory scales upward from the domain, just as easily as it scales downward.

Active Directory uses the Domain Name System (DNS) naming conventions for its domains. You can create an Active Directory domain using the registered domain name you use on the Internet, or you can create an internal domain name, without registering it.

When you create your first domain on an Active Directory network, you are, in essence, creating the root of a ***domain tree***. You can populate the tree with additional domains as long as they are part of the same contiguous namespace (see Figure 13-1). These subdomains are said to be part of the same tree as *contoso.com* because they use the same top- and second-level domain names.

Figure 13-1

An internal Active Directory domain tree

You can add as many domains to the tree as you need, using any number of levels, as long as you conform to the DNS naming limitations, which call for a maximum of 63 characters per domain name and 255 characters for the fully qualified domain name (FQDN).

ZOOMING OUT: FORESTS

An organization might want to use multiple domains that cannot be part of the same tree, because they are not contiguous. For example, a single corporation might run two operations out of the same facilities, each with its own Internet domain name, such as *contoso.com* and *adatum.com*. You can create two separate Active Directory domains using these two names, but they cannot be parts of the same tree, because one is not subordinate to the other. You can, however, create two separate domain trees and join them together in a parent structure called a ***forest***.

An Active Directory forest consists of one or more separate domain trees, which have the same two-way trust relationships between them as two domains in the same tree. When you create the first domain on an Active Directory network, you are in fact creating a new forest, and that first domain becomes the ***forest root domain***. Therefore, if you create the *contoso.com* domain first, that domain becomes the root of the *contoso.com* forest. When you create the *adatum.com* domain in the same forest, it retains its status as a separate domain in a separate tree, but it is still considered part of the *contoso.com* forest.

It is important to understand that separate trees in the same forest still have trust relationships between them, even though they do not share a domain name. If you want to create two domains completely separate from one another, you must create each one in a separate forest.

INTRODUCING THE GLOBAL CATALOG

Domains also function as the hierarchical boundaries for the AD DS database. A domain controller maintains only the part of the database that defines that domain and its objects. However, Active Directory clients still need a way to locate and access the resources of other domains in the same forest. To make this possible, each forest has a ***global catalog***, which lists all objects in the forest, along with a subset of each object's attributes.

To locate an object in another domain, Active Directory clients perform a search of the global catalog first. This search provides the client with the information it needs to find the object in the specific domain that contains it. Thus, the global catalog prevents the client from having to search all domains in the forest.

Deploying Active Directory Domain Services

THE BOTTOM LINE To create a new domain, or to add a domain controller to an existing domain, you must install the Active Directory Domain Services role on a Windows Server 2012 R2 computer, and then run the *Active Directory Domain Services Configuration Wizard*.

To use a Windows Server 2012 R2 computer as a domain controller, you must configure it to use static IP addresses, not addresses supplied by a Dynamic Host Configuration Protocol (DHCP) server. If you are creating a domain in an existing forest, or adding a domain controller to an existing domain, you also must configure the computer to use the DNS server that hosts the existing forest or domain, at least during the Active Directory installation.

Installing the Active Directory Domain Services Role

Although the Active Directory Domain Services role does not actually convert the computer into a domain controller, installing it prepares the computer for the conversion process.

To install the Active Directory Domain Services role, use the following procedure.

INSTALL THE ACTIVE DIRECTORY DOMAIN SERVICES ROLE

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the *Server Manager*'s Manage menu, select Add Roles and Features. The *Add Roles and Features Wizard* appears, displaying the *Before you begin* page.
2. Click Next. The *Select Installation Type* page appears.
3. Leave the *Role-based or feature-based installation* radio button selected and click Next. The *Select Destination Server* page appears.
4. Select the server that you want to promote to a domain controller and click Next. The *Add Roles and Features Wizard* displays the *Select server roles* page.
5. Select the Active Directory Domain Service role. The *Add features that are required for Active Directory Domain Services?* page appears.
6. Click Add Features to accept the dependencies, and then click Next. The *Select features* page appears.
7. Click Next. The *Active Directory Domain Services* page appears, displaying information about the role.
8. Click Next. A *Confirm installation selections* page appears.
9. Select from the following optional functions, if desired:
   - Restart the destination server automatically if desired causes the server to restart automatically when the installation is complete, if the selected roles and features require it.
   - Export configuration settings creates an XML script documenting the procedures performed by the wizard, which you can use to install the same configuration on another server using Windows PowerShell.
   - Specify an alternate source path specifies the location of an image file containing the software needed to install the selected roles and features.

10. Click Install. The *Installation progress* page appears, as shown in Figure 13-2. After the role is installed, a *Promote this server to a domain controller* link appears.

Figure 13-2

The *Installation progress* page in the *Add Roles and Features Wizard*

PAUSE. Leave the wizard open.

After you install the role, you can proceed to run the *Active Directory Domain Services Installation Wizard*. The wizard procedure varies, depending on what function the new domain controller will serve. The following sections describe the procedures for the most common types of domain controller installations.

Creating a New Forest

When beginning a new AD DS installation, you first need to create a new forest, which you do by creating the first domain in the forest, the forest root domain.

To create a new forest, use the following procedure.

CREATE A NEW FOREST

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges and install the Active Directory Domain Services role, as described earlier in this lesson.

1. On the *Installation progress* page that appears at the end of the Active Directory Domain Services role installation procedure, click the Promote this server to a domain controller hyperlink. The *Active Directory Domain Services Configuration Wizard* appears, displaying the *Deployment Configuration* page.

2. Select the Add a new forest option and, in the Root domain name text box, type the name of the domain you want to create.
3. Click Next. The *Domain Controller Options* page appears, as shown in Figure 13-3.

Figure 13-3

The *Domain Controller Options* page of the *Active Directory Domain Services Configuration Wizard*

4. Make changes on the *Domain Controller Options* page, as needed:
   - If you plan to add domain controllers running earlier versions of Windows Server to this forest, select the earliest Windows version you plan to install from the Forest functional level drop-down list.
   - If you plan to add domain controllers running earlier versions of Windows Server to this domain, select the earliest Windows version you plan to install from the Domain functional level drop-down list.
   - If you do not already have a DNS server on your network, leave the Domain Name System (DNS) server check box selected. If you have a DNS server on the network and the domain controller is configured to use that server for DNS services, clear the check box.
5. In the Password and Confirm password text boxes, type the password you want to use for Directory Services Restore Mode (DSRM) and click Next. The *DNS options* page appears, with a warning that a delegation for the DNS server cannot be created, because the DNS Server service is not installed yet.
6. Click Next. The *Additional Options* page appears displaying the NetBIOS equivalent of the domain name you specified.
7. Modify the name, if desired, and click Next. The *Paths* page appears.
8. Modify the default locations for the AD DS files, if desired, and click Next. The *Review Options* page appears.
9. Click Next. The *Prerequisites Check* page appears, as shown in Figure 13-4.

Figure 13-4

The *Prerequisites Check* page of the *Active Directory Domain Services Configuration Wizard*

The wizard performs a number of environment tests to determine whether the system can function as a domain controller. The results can appear as cautions, which enable the procedure to continue, or warnings, which require you to perform certain actions before the server can be promoted.

10. After the system passes all the prerequisite checks, click Install. The wizard creates the new forest and configures the server to function as a domain controller.

RESTART the computer.

With the forest root domain in place, you can now proceed to create additional domain controllers in that domain, or add new domains to the forest.

Adding a Domain Controller to an Existing Domain

Every Active Directory domain should have a minimum of two domain controllers.

To add a domain controller to an existing Windows Server 2012 R2 domain, use the following procedure.

ADD A DOMAIN CONTROLLER TO AN EXISTING DOMAIN

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges and install the Active Directory Domain Services role, as described earlier in this lesson.

1. On the *Installation progress* page that appears at the end of the Active Directory Domain Services role installation procedure, click the Promote this server to a domain controller hyperlink. The *Active Directory Domain Services Configuration Wizard* appears, displaying the *Deployment configuration* page.
2. Select the Add a domain controller to an existing domain option and then click Select.
3. If you are not logged on to an existing domain in the forest, a *Credentials for deployment operation* dialog box appears, in which you must supply administrative credentials for the domain to proceed. After you are authenticated, a *Select a domain from the forest* dialog box appears.
4. Select the domain to which you want to add a domain controller and click OK. The selected domain name appears in the *Domain* field.
5. Click Next. The *Domain Controller Options* page appears, as shown in Figure 13-5.

Figure 13-5

The *Domain Controller Options* page of the *Active Directory Domain Services Configuration Wizard*

6. Select or clear the check boxes on the *Domain Controller Options* page as needed:
   - If you want to install the DNS Server service on the computer, leave the Domain Name System (DNS) server check box selected. Otherwise, the DNS server the computer is configured to use will host the domain.
   - Leave the Global Catalog (GC) check box selected if you want the computer to function as a global catalog server. This is essential if you are deploying the new domain controller at a site that does not already have a GC server.
   - Select the Read only domain controller (RODC) check box to create a domain controller that administrators cannot use to modify AD DS objects.
7. In the Site Name drop-down list, select the site where the domain controller will be located.

8. In the Password and Confirm Password text boxes, type the password you want to use for Directory Services Restore Mode (DSRM) and click Next. The *Additional Options* page appears, as shown in Figure 13-6.

Figure 13-6

The *Additional Options* page of the *Active Directory Domain Services Configuration Wizard*

9. To use the Install From Media (IFM) option, select the Install from media check box.
10. In the Replicate from drop-down list, select the existing domain controller that the server should use as a data source. Then click Next. The *Paths* page appears.
11. Modify the default locations for the AD DS files, if desired, and click Next. The *Review Options* page appears.
12. Click Next. The *Prerequisites Check* page appears.
13. After the system passes all the prerequisite checks, click Install. The wizard configures the server to function as a domain controller.

RESTART the computer.

The domain controller is now configured to service the existing domain. If the new domain controller is located in the same site as another, AD DS replication between the two begins automatically.

Installing AD DS on Server Core

In Windows Server 2012 R2, you can now install Active Directory Domain Services on a computer running the Server Core installation option and promote the system to a domain controller, all by using Windows PowerShell.

In Windows Server 2008 and Windows Server 2008 R2, the accepted method for installing AD DS on a computer using the Server Core installation option is to create an answer file and load it from the command prompt using the Dcpromo.exe program with the /unattend parameter.

In Windows Server 2012 and Windows Server 2012 R2, running Dcpromo.exe with no parameters no longer launches the *Active Directory Domain Services Configuration Wizard*. However, administrators who have already invested considerable time into developing answer files for unattended domain controller installations can continue to execute them from the command prompt, although doing so also produces a warning that *The dcpromo unattended operation is replaced by the ADDSDeployment module for Windows PowerShell*.

For AD DS installations on Server Core, Windows PowerShell is now the preferred method. As with the wizard-based installation, the Windows PowerShell procedure occurs in two phases: first, you must install the Active Directory Domain Services role; then, you must promote the server to a domain controller.

Installing the Active Directory Domain Services role via Windows PowerShell is no different from installing any other role. In an elevated Windows PowerShell session, use the following command:

```
Install-WindowsFeature –name AD-Domain-Services
-IncludeManagementTools
```

After you install the role, promoting the server to a domain controller is somewhat more complicated. The ADDSDeployment Windows PowerShell module includes separate cmdlets for the three deployment configurations covered in the previous sections:

- Install-AddsForest
- Install-AddsDomainController
- Install-AddsDomain

Each of these cmdlets has a great many possible parameters to support the many configuration options you find in the Active Directory Domain Services Configuration Wizard. In its simplest form, the following command would install a domain controller for a new forest called *adatum.com*:

```
Install-AddsForest -DomainName “adatum.com”
```

The defaults for all the cmdlet’s other parameters are the same as those in the *Active Directory Domain Services Configuration Wizard*. Running the cmdlet with no parameters steps through the options, prompting you for values. You can also display basic syntax information using the Get-Help command, as shown in Figure 13-7.

Figure 13-7

Syntax for the Install-AddsForest cmdlet in Windows PowerShell

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> get-help install-addsforest

NAME
    Install-ADDSForest

SYNTAX
    Install-ADDSForest -DomainName <string> [-SkipPreChecks] [-SafeModeAdministratorPassword <securestring>]
    [-CreateDnsDelegation] [-DatabasePath <string>] [-DnsDelegationCredential <pscredential>] [-NoDnsOnNetwork]
    [-DomainMode <DomainMode> {Win2008 | Win2008R2 | Win2012 | Win2012R2 | Default}] [-DomainNetbiosName <string>]
    [-ForestMode <ForestMode> {Win2008 | Win2008R2 | Win2012 | Win2012R2 | Default}] [-InstallDns] [-LogPath <string>]
    [-NoRebootOnCompletion] [-SkipAutoConfigureDns] [-SysvolPath <string>] [-Force] [-WhatIf] [-Confirm]
    [<CommonParameters>]
```

Using Install from Media (IFM)

Earlier in this lesson, in the procedure for installing a replica domain controller, the *Additional Options* page of the *Active Directory Domain Services Configuration Wizard* included an *Install from media* check box. This option enables you to streamline the process of deploying replica domain controllers to remote sites.

Normally, installing a domain controller on an existing domain creates the AD DS database structure, but it has no data until the server can receive replication traffic from the other domain controllers. When the domain controllers for a particular domain are well connected, such as by a local area network (LAN), replication occurs automatically and almost immediately after the new domain controller is installed.

When you install a domain controller at a remote location, however, the connection to the other domain controllers is most likely a wide area network (WAN) link, which is typically slower and more expensive than a LAN connection. In this case, the initial replication with the other domain controllers can be much more of a problem. The slow speed of the WAN link might cause the replication to take a long time and might flood the connection, delaying regular traffic. If the domain controllers are located in different AD DS sites, no replication occurs until an administrator creates and configures the required site links.

By using a command-line tool called Ndtsutil.exe, you can avoid these problems by creating domain-controller installation media that include a copy of the AD DS database. By using this media when installing a remote domain controller, the data is installed along with the database structure, and no initial replication is necessary.

To create Install From Media (IFM) media, you must run the Ntdsutil.exe program on a domain controller running the same version of Windows that you intend to deploy. The program is interactive, requiring you to enter a sequence of commands such as the following:

- `Ntdsutil`-launches the program.
- `Activate instance ntds`-focuses the program on the installed AD DS instance.
- `Ifm`-switches the program into IFM mode.
- `Create Full|RODC <path name>`-creates media for either a full read/write domain controller or a read-only domain controller and saves it to the folder specified by the path name variable.

TAKE NOTE*

The Ntdsutil.exe create command also supports parameters that include the contents of the SYSVOL volume with the AD DS data. The Windows Server 2012 R2 version of the program adds a nodefrag parameter, which speeds up the media creation process by skipping the defragmentation.

When you execute these commands, the Ntdsutil.exe program creates a snapshot of the AD DS database, mounts it as a volume to defragment it, and then saves it to the specified folder, along with a copy of the Windows Registry (see Figure 13-8).

After you create the IFM media, you can transport it to the servers you intend to deploy as domain controllers by any convenient means. To use the media, you run the *Active Directory Domain Services Configuration Wizard* in the usual way, select the *Install from media* check box, and specify the path to the location of the folder.

Figure 13-8

An Ntdsutil.exe command sequence

Upgrading Active Directory Domain Services

Introducing Windows Server 2012 R2 onto an existing AD DS installation is easier than it has ever been in previous versions of the operating system.

You can upgrade an AD DS infrastructure in two ways. You can upgrade the existing down-level domain controllers to Windows Server 2012 R2, or you can add a new Windows Server 2012 R2 domain controller to your existing installation.

As noted in Lesson 1, "Installing Servers," the upgrade paths to Windows Server 2012 R2 are few. You can upgrade a Windows Server 2008 or Windows Server 2008 R2 domain controller to Windows Server 2012 R2, but no earlier versions are upgradable.

In the past, if you wanted to add a new domain controller to an existing AD DS installation based on previous Windows versions, you had to run the Adprep.exe program to upgrade the domains and forest. Depending on the installation's complexity, this could involve logging on to various domain controllers with different credentials, locating different versions of Adprep.exe, and running the program several times using /domainprep parameter for each domain and the /forestprep parameter for the forest.

In Windows Server 2012 R2, the Adprep.exe functionality has been fully incorporated into Server Manager in the *Active Directory Domain Services Configuration Wizard*. When you install a new Windows Server 2012 R2 domain controller, you have to supply only appropriate credentials, and the wizard takes care of the rest.

Adprep.exe, still included with the operating system, supports the old preparation method, if you prefer it, but you have no compelling reason to use it.

Deploying Active Directory IaaS on Windows Azure

In addition to running Windows Server 2012 R2 on physical computers and locally-hosted virtual machines, Microsoft's Windows Azure service enables administrators to run Windows Server 2012 R2 on cloud-based virtual machines provided by Microsoft. This capability, called Infrastructure as a Service (IaaS), enables administrators to run applications in the cloud while maintaining full control over the virtual machines themselves.

Windows Azure resources can be self-contained in the cloud, and administrators can create a virtualized AD DS forest to organize and manage them. It is also possible to configure Windows Azure resources as an extension to the existing physical and virtual resources hosted on a private network. For example, after creating a virtual network in the Windows Azure cloud and connecting it to your private network with a site-to-site link using a virtual private networking (VPN) device, you can create a Windows Server 2012 R2 virtual machine in the cloud and configure it as a domain controller for an existing domain.

The process of installing AD DS on a Windows Azure virtual machine and promoting it to a domain controller is no different from that of a private network server. You use the Add Roles and Features Wizard to install the AD DS role and then use the Active Directory Domain Services Configuration Wizard to configure the domain controller. The complicated part of the process is the configuration of the virtual network infrastructure to allow communication between the cloud network and your physical network.

Windows Azure is an idea platform for AD DS domain controllers because it provides IP address consistency in a new way. Windows Azure virtual machines must obtain IP addresses from DHCP servers – you cannot assign static IP addresses to them – but unlike standard DHCP address leases that can expire, causing the address to change, a cloud VM retains its IP address lease for its lifetime.

Removing a Domain Controller

With the loss of Dcpromo.exe, the process of demoting a domain controller has changed, and it is not immediately intuitive.

To remove a domain controller from an AD DS installation, you must begin by running *the Remove Roles and Features Wizard*, as shown in the following procedure.

REMOVE A REPLICA DOMAIN CONTROLLER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Server Manager's Manage menu, select Remove Roles and Features. The *Remove Roles and Features Wizard* appears, displaying the *Before you begin* page.

2. Click Next. The *Select Destination Server* page appears.
3. Select the server that you want to demote from a domain controller and click Next. The *Remove Server Roles* page appears.
4. Clear the Active Directory Domain Services check box. A *Remove features that require Active Directory Domain Services* dialog box appears.
5. Click Remove Features. A *Validation Results* dialog box appears.
6. Click the Demote this domain controller hyperlink. The *Active Directory Domain Services Configuration Wizard* appears, displaying the *Credentials* page.
7. Click Change to supply alternative credentials for demoting the domain controller, if necessary.
8. Select the Force the removal of this domain controller check box and click Next. The *New Administrator Password* page appears.
9. In the Password and Confirm Password text boxes, type the password you want the server to use for the local Administrator account after the demotion. Then click Next. The *Review Options* page appears.
10. Click Demote. The wizard demotes the domain controller and restarts the system.
11. Log on using the local Administrator password you specified earlier.
12. From the Manage menu, select Remove Roles and Features. The *Remove Roles and Features Wizard* appears as before, displaying the *Before you begin* page.
13. Click Next. The *Select Destination Server* page appears.
14. Select the server that you want to demote from a domain controller and click Next. The *Remove Server Roles* page appears.
15. Clear the Active Directory Domain Services check box. A *Remove features that require Active Directory Domain Services* dialog box appears.
16. Click Remove Features, and then click Next. The *Remove Features* page appears.
17. Click Next. The *Confirm Removal Selections* page appears.
18. Click Remove. The wizard removes the role.

CLOSE the wizard and restart the server.

Configuring the Global Catalog

As noted earlier, the global catalog is an index of all AD DS objects in a forest that prevents systems from having to perform searches among multiple domain controllers.

The importance of the global catalog varies depending on the size of your network and its site configuration. For example, if your network consists of a single domain, with domain controllers all located at the same site and well connected, the global catalog serves little purpose other than universal group searches. You can make all your domain controllers global catalog servers, if you want. The searches will be load balanced, and the replication traffic likely will not overwhelm the network.

However, if your network consists of multiple domains with domain controllers located at multiple sites connected by WAN links, the global catalog configuration is critical. If at all possible, you do not want users performing AD DS searches that must reach across slow, expensive WAN links to contact domain controllers at other sites. Placing a global catalog server at each site is recommended in this case. The initial replication might generate a lot of traffic, but the savings in the long run should be significant.

When you promote a server to a domain controller, you have the option of making the domain controller a global catalog server. If you decline to do so, however, you can make any domain controller a global catalog server using the following procedure.

CREATE A GLOBAL CATALOG SERVER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Server Manager's Tools menu, select Active Directory Sites and Services. The *Active Directory Sites and Services* console appears.
2. Expand the site where the domain controller you want to function as a global catalog server is located. Then expand the Servers folder and select the server you want to configure, as shown in Figure 13-9.

Figure 13-9

The Active Directory Sites and Services console

3. Right-click the NTDS Settings node for the server and, from the context menu, select Properties. The *NTDS Settings Properties* sheet appears.
4. Select the Global Catalog check box and click OK.

CLOSE the *Active Directory Sites and Services* console.

Troubleshooting DNS SRV Registration Failure

The Domain Name System (DNS) is essential to the operating of Active Directory Domain Services. To accommodate directory services such as AD DS, a special DNS resource record was created that enables clients to locate domain controllers and other vital AD DS services.

When you create a new domain controller, one of the most important parts of the process is the registration of the server in the DNS. This automatic registration is the reason an AD DS network must have access to a DNS server that supports the Dynamic Updates standard defined in RFC 2136.

If the DNS registration process fails, computers on the network cannot locate that domain controller, the consequences of which can be serious. Computers will be unable to use that domain controller to join the domain; existing domain members will be unable to log on; and other domain controllers will be unable to replicate with it.

DNS problems are, in most cases, due to general networking faults or DNS client configuration error. When troubleshooting these problems, you should first try pinging the DNS server, and then make sure that the TCP/IP client configuration has the correct addresses for the DNS servers it should be using.

To confirm that a domain controller has been registered in the DNS, open a command-prompt window with administrative privileges and enter the following command:

```
dcdiag /test:registerindns /dnsdomain:<domain name> /v
```

A successful result appears, as shown in Figure 13-10.

Figure 13-10

A successful dcdiag test

Business Case Scenarios

Scenario 13-1: Creating AD DS Domains

Robert is designing a new Active Directory Domain Services infrastructure for a company called Litware, Inc., which has its headquarters in New York and two additional offices in London and Tokyo. The London office consists only of sales and marketing staff; it does not have its own IT department. The Tokyo office is larger, with representatives from all of the company departments, including a full IT staff. The Tokyo office is connected to the headquarters using a 64 Kbps demand-dial link, and the London office has a 512-Kbps frame relay connection. The company has registered the litware.com domain name, and Robert has created a subdomain called inside.litware.com for use by Active Directory.

Based on this information, design an Active Directory infrastructure for Litware, Inc. that is as economical as possible, specifying how many domains to create, what to name them, how many domain controllers to install, and where. Explain each of your decisions.

Scenario 13-2: Using Install from Media (IFM)

As you prepare some remote sites for domain controllers, you need the most efficient way to deploy replica DCs. You learn about Install from Media checkbox on the Additional Options page of the Active Directory Domain Services Configuration Wizard. Outline the steps taken in the interactive IFM wizard.

Creating and Managing Active Directory Users and Computers

LESSON 14

Creating User Objects

THE BOTTOM LINE

The user account is the primary means by which people using an Active Directory Domain Services (AD DS) network access resources.

Resource access for individuals takes place through their individual user accounts. To gain access to the network, prospective network users must authenticate to a network with a specific user account. Authentication is the process of confirming a user's identity by using a known value such as a password, a smart card, or a fingerprint. When a user supplies a name and password, the authentication process validates the credentials supplied in the logon against information that is stored within the AD DS database. Do not confuse authentication with authorization, which is the process of confirming that an authenticated user has the correct permissions to access one or more network resources.

The following two types of user accounts run on Windows Server 2012 R2 systems:

- ***Local users*** can access only resources on the local computer and are stored in the local ***Security Account Manager (SAM)*** database on the computer where they reside. Local accounts are never replicated to other computers, nor do these accounts provide domain access. A local account configured on one server cannot be used to access resources on a second server; you need to configure a second local account in that case.
- ***Domain users*** can access AD DS or network-based resources, such as shared folders and printers. Account information for these users is stored in the AD DS database and replicated to all domain controllers within the same domain. A subset of the domain user account information is replicated to the global catalog, which is then replicated to other global catalog servers throughout the forest.

By default, two built-in user accounts are created on a computer running Windows Server 2012 R2: the Administrator account and the Guest account. Built-in user accounts can be local accounts or domain accounts, depending on whether the server is a standalone server or a domain controller. In the case of a standalone server, the built-in accounts are local accounts on the server itself. On a domain controller, the built-in accounts are domain accounts that are replicated to each domain controller.

Creating Single Users

For some administrators, creating individual user accounts is a daily task, and there are many ways to go about it.

Windows Server 2012 R2 redesigned the Active Directory Administrative Center (ADAC) application, first introduced in Windows Server 2008 R2, to fully incorporate new features such as the Active Directory Recycle Bin and fine-grained password policies. You can also use the tool to create and manage AD DS user accounts.

To create a single user account with the Active Directory Administrative Center, use the following procedure.

CREATE A USER WITH ACTIVE DIRECTORY ADMINISTRATIVE CENTER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Active Directory Administrative Center. The *Active Directory Administrative Center* console appears, as shown in Figure 14-1.

Figure 14-1

The Active Directory Administrative Center console

2. In the left pane, find the domain in which you want to create the user object and select a container in that domain.
3. In the Tasks pane, under the container name, click New > User. The *Create User* window appears, as shown in Figure 14-2.

Figure 14-2

The *Create User window* in the Active Directory Administrative Center console

4. Type the user's name in the Full Name field and an account name in the User SamAccountName Logon field.
5. Type an initial password for the user in the Password and Confirm password fields.
6. Supply information for any of the optional fields on the page you want.
7. Click OK. The user object appears in the container.

CLOSE the *Active Directory Administrative Center* console.

USING DSADD.EXE

For administrators more comfortable with the traditional command prompt, the Dsadd.exe program can create new user objects by using the syntax shown in Figure 14-3.

Figure 14-3

Syntax of the Dsadd.exe program

To create a user by using the Dsadd.exe utility, you must know the distinguished name (DN) for the user and the user's login ID, also known as the ***SAM account name*** attribute within AD DS. The distinguished name of an object signifies its location within the Active Directory structure. For example, in the distinguished name **cn=Elizabeth Andersen,ou=Research,dc=adatum,dc=com**, the "cn" refers to the common name for Elizabeth Andersen's user account, which resides in the Research OU, which resides in the adatum.com domain.

Creating User Templates

In some cases, you need to create single users on a regular basis, but the user accounts contain so many attributes that creating them individually becomes time-consuming.

One way to speed up the process of creating complex user objects is to use the New-ADUser cmdlet or the Dsadd.exe program and retain your commands in a script or batch file. However, if you prefer a graphical interface, you can do roughly the same thing by creating a user template.

A user template is a standard user object containing boilerplate attribute settings. To create a new user with these settings, you copy the template to a new user object and change the name and any other attributes that are unique to the user.

To create a user template with the Active Directory Users and Computers console, use the following procedure.

CREATE A USER TEMPLATE

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Active Directory Users and Computers. The *Active Directory Users and Computers* console appears.
2. In the left pane, find the domain in which you want to create the user object and select a container in that domain.
3. From the Action menu, select New > User. The *New Object – User Wizard* appears.
4. Type Default Template, or a similarly descriptive name, in the Full Name field and an account name in the User logon name field.
5. Click Next. The second page of the *New Object – User Wizard* appears.
6. Type an initial password for the user in the Password and Confirm password fields.
7. Clear the *User must change password at next logon* check box.
8. Select the Account is disabled check box and click Next. A confirmation page listing the settings you configured appears.
9. Click Finish. The wizard creates the user object and closes.
10. Locate the user you just created in the console and double-click it to open its Properties sheet.
11. Modify the attributes on the various tabs with values common to all the users you create.
12. Click OK.

CLOSE the *Active Directory Users and Computers* console.

To use the template, right-click the *Default Template* user object and, from the context menu, select *Copy*. The *Copy Object – User Wizard* appears.

Enter the required unique information for the user and clear the *Account is disabled* check box before clicking *OK*. The wizard creates a new user object with all the attributes you configured in the template.

Creating Multiple Users

Administrators sometimes have to create hundreds or thousands of user objects, which makes the single object creation procedures impractical.

The previous sections in this lesson describe the procedures for creating single users and group objects by using the graphical user interface (GUI) and some of the available command-line tools in Windows Server 2012 R2. The following sections examine some of the mechanisms for automating the creation of large numbers of Active Directory objects.

USING CSVDE.EXE

Some applications such as Microsoft Excel can generate a number of users, along with their accompanying information, to add to the AD DS database. In these cases, you can export information from the applications by saving it to a file in ***Comma-Separated Values (CSV)*** format. CSV format also can be used to import information into and export it from other third-party applications. For example, you might need to export user account information to a file for use in another third-party application, such as a UNIX database. CSVDE.exe provides this capability as well.

A CSV file is a plain text file that consists of records, each on a separate line that are divided into fields and separated by commas. The format saves database information in a universally understandable way.

The CSVDE.exe command-line utility enables you to import or export Active Directory objects. It uses a CSV file that is based on a header record, which identifies the attribute contained in each comma-delimited field. The ***header record*** is the first line of the text file that uses proper attribute names. To import into AD DS, the attribute names in the CSV file must match the attributes allowed by the Active Directory schema. For example, to import a list of people and telephone numbers as users into the Active Directory database, you need to create a header record that accurately reflects the object names and attributes you want to create. Review the following attributes that are commonly used for creating user accounts.

- *dn* specifies the distinguished name of the object so that the object can be properly placed in Active Directory.
- *samAccountName* populates the SAM account field
- *objectClass* specifies the type of object to be created, such as user, group, or OU.
- *telephoneNumber* populates the Telephone Number field.
- *userPrincipalName* populates the User Principal Name field for the account.

As you create your CSV file, you must order the data to reflect the sequence of the attributes in the header record. If fields and data are out of order, you will either encounter an error when running the CSVDE.exe utility or you might not get accurate results in the created objects. The following header record example uses the previously listed attributes to create a user object.

```
dn,samAccountName,userPrincipalName,telephoneNumber,
objectClass
```

A data record conforming to this header record appears as follows:

```
"cn=Elizabeth
Andersen,ou=Research,dc=adatum,dc=com",eander,eander@
adatum.com,586-555-1234,user
```

After you add a record for each account you want to create, save the file using .csv as the extension. You then use the following command syntax to run the CSVDE.exe program and import the file.

```
csvde.exe -i -f <filename.csv>
```

The -i switch tells CSVDE.exe that this operation will import data. The -f switch specifies the .csv file containing the records to be imported.

USING LDIFDE.EXE

LDIFDE.exe is a utility that has the same basic functionality as CSVDE.exe and provides the capability to modify existing records in Active Directory. For this reason, LDIFDE.exe is a more flexible option. Consider an example where you need to import 200 new users into your AD DS structure. In this case, you can use CSVDE.exe or LDIFDE.exe to import the users. However, you can use LDIFDE.exe to modify or delete the objects later, whereas CSVDE.exe does not provide this option.

You can use any text editor to create the LDIFDE.exe input file, which is formatted according to the ***LDAP Data Interchange Format (LDIF)*** standard. The format for the data file containing the object records you want to create is significantly different from CSVDE.exe. The following example shows the syntax for a data file to create the same user account discussed in the CSVDE.exe example.

```
dn: "cn=Elizabeth
Andersen,ou=Research,dc=adatum,dc=com"

changetype: add
ObjectClass: user
SAMAccountName: eander
UserPrincipalName: eander@adatum.com
telephoneNumber: 586-555-1234
```

By using LDIFDE.exe, you can specify one of three actions to perform with the LDIF file:

- *Add* creates new objects using the LDIF records.
- *Modify* modifies existing object attributes using the LDIF records.
- *Delete* deletes existing objects using the LDIF records.

After creating the data file and saving it using the .LDF file extension, use the following syntax to execute the LDIFDE.exe program.

```
ldifde –i –f <filename.ldf>
```

The next example illustrates the LDIF syntax to modify the telephone number of an existing user object. Note that the hyphen in the last line is required for the file to function correctly.

```
dn: "cn=Elizabeth
Andersen,ou=Research,dc=adatum,dc=com"

changetype: modify
replace: telephoneNumber
telephoneNumber: 586-555-1111
-
```

Creating Computer Objects

THE BOTTOM LINE

Because an AD DS network uses a centralized directory, you need a way to track the computers that are part of the domain. To do this, Active Directory uses computer accounts, which are realized in the form of computer objects in the Active Directory database. You might have a valid Active Directory user account and a password, but if your computer is not represented by a computer object, you cannot log on to the domain.

Computer objects are stored in the Active Directory hierarchy just as user objects are, and they possess many of the same capabilities, such as the following:

- Computer objects consist of properties that specify the computer's name, where it is located, and who is permitted to manage it.
- Computer objects inherit group policy settings from container objects such as domains, sites, and organizational units.
- Computer objects can be members of groups and inherit permissions from group objects.

When a user attempts to log on to an Active Directory domain, the client computer establishes a connection to a domain controller to authenticate the user's identity. However, before the user authentication occurs, the two computers perform a preliminary authentication using their respective computer objects, to ensure that both systems are part of the domain. The NetLogon service running on the client computer connects to the same service on the domain controller, and then each one verifies that the other system has a valid computer account. When this validation is completed, the two systems establish a secure communications channel between them, which they can then use to begin the user authentication process.

The computer account validation between the client and the domain controller is a genuine authentication process using account names and passwords, just as when a user authenticates to the domain. The difference is that the passwords used by the computer accounts generate automatically and keep hidden. You can reset a computer account, but you do not need to supply passwords for everyone.

What all this means for administrators is that, in addition to creating user accounts in the domain, they have to make sure that the network computers are part of the domain as well. Adding a computer to an AD DS domain consists of two steps:

- **Creating a computer account:** You create a computer account by creating a new computer object in Active Directory and assigning the name of an actual computer on the network.
- **Joining the computer to the domain:** When you join a computer to the domain, the system contacts a domain controller, establishes a trust relationship with the domain, locates (or creates) a computer object corresponding to the computer's name, alters its security identifier (SID) to match the computer object, and modifies its group memberships.

How these steps are performed, and who performs them, depends on the way in which you deploy computers on your network. You can create new computer objects in many ways, but how you elect to do this depends on several factors, including the number of objects you need to create, where you will be when creating the objects, and what tools you prefer to use.

Generally speaking, you create computer objects when you deploy new computers in the domain. After an object represents a computer and joins to the domain, any user in the domain can log on from that computer. For example, you do not need to create new computer objects or rejoin computers to the domain when employees leave the company and new hires start using their computers. However, if you reinstall the operating system on a computer, you must create a new computer object for it (or reset the existing one), because the newly installed computer will have a different SID.

The creation of a computer object must always occur before the corresponding computer can join the domain, although it sometimes does not appear that way. You can use the following two basic strategies for creating Active Directory computer objects:

- Create the computer objects in advance by using an Active Directory tool, so that the computers can locate the existing objects when they are in the domain.
- Begin the joining process first and let the computer create its own computer object.

In each case, the computer object exists before the joining takes place. In the second strategy, the joining process appears to begin first, but the computer creates the object before the joining process begins.

When you have a number of computers to deploy, particularly in different locations, you might prefer to create the computer objects in advance. For large numbers of computers, you can automate the computer object creation process by using command-line tools and batch files.

Computer objects have relatively few attributes, and in most cases, you will most likely just supply them with a name, which can be up to 64 characters long. This name must match the name of the computer joined with the object.

Managing Active Directory Objects

THE BOTTOM LINE

After you create user and computer objects, you can manage them and modify them in many of the same ways that you created them.

Double-clicking any object in the ADAC or the Active Directory Users and Computers console opens the Properties sheet for that object. The windows appear different, but they contain the same information and provide the same capability to alter the object attributes.

Joining Computers to a Domain

The process of joining a computer to a domain must occur at the computer itself and be performed by a member of the computer's local Administrators group.

After logging on, you join a computer running Windows Server 2012 R2 to a domain from the *Computer Name* tab in the System Properties sheet. You can access the System Properties sheet from Server Manager, by clicking the *Computer name or domain* hyperlink on the server's *Properties tile*, from the *Control Panel*.

On a computer that is not joined to a domain, the Computer Name tab displays the name assigned to the computer during the operating system installation, and the name of the workgroup to which the system currently belongs (which is WORKGROUP, by default). To join the computer to the domain, click *Change* to display the *Computer Name Changes* dialog box.

In this dialog box, the Computer name field enables you to change the name assigned to the computer during installation. Depending on whether you have already created a computer object, observe the following precautions:

- To join a domain in which you have already created a computer object for the system in AD DS, the name in this field must match the name of the object exactly.
- If you intend to create a computer object during the joining process, the name in this field must not already exist in the domain.

When you select the *Domain* option button and enter the name of the domain the computer will join, the computer establishes contact with a domain controller for the domain and a second *Computer Name Changes* dialog box appears, which prompts you for the name and password of a domain user account with permission to join the computer to the domain.

After you authenticate with the domain controller, the computer is welcomed to the domain and you are instructed to restart the computer.

CREATING COMPUTER OBJECTS WHILE JOINING

You can join a computer to a domain whether or not you have already created a computer object for it. After the computer authenticates to the domain controller, the domain controller scans the Active Directory database for a computer object with the same name as the computer. If it does not find a matching object, the domain controller creates one in the Computers container, using the name supplied by the computer.

To create the computer object automatically in this manner, you might expect that the user account you specify when connecting to the domain controller must have object creation privileges for the Computers container, such as membership in the administrators group. However, this is not always the case.

Domain users also can create computer objects themselves through an interesting, indirect process. The Default Domain Controllers Policy GPO grants a user right called *Add Workstations To The Domain* to the Authenticated Users special identity. Any user who is successfully authenticated to Active Directory is permitted to join up to ten workstations to the domain, and create 10 associated computer objects, even if the user does not possess explicit object creation permissions.

With Add Workstations To The Domain user right, "workstations" is the operative word. Authenticated users can add up to 10 workstations to the domain, but not servers.

JOINING A DOMAIN WHILE OFFLINE

It is typical for you to join computers to domains while the computers are connected to the network and have access to a domain controller. However, there are situations in which you might want to set up computers without access to a domain controller, such as a new branch office installation. In these cases, it is possible to perform an offline domain join, by using a command-line program called *Djoin.exe*.

The offline domain join procedure requires you to run the Djoin.exe program twice, once on a computer with access to a domain controller, and then again on the computer to be joined. When connected to the domain controller, the program gathers computer account metadata for the system to be joined and saves it to a file. The syntax for this phase of the process is as follows:

```
djoin /provision /domain <domain name>
/machine <computer name> /savefile <filename.txt>
```

You then transport the metadata file to the computer to be joined and run Djoin.exe again, specifying the name of the file. The program saves the metadata from the file to the computer, so that the next time it has access to a domain controller, the system is automatically joined to the domain. The syntax for the second phase of the process is as follows:

```
djoin /requestODJ /loadfile <filename.txt>
/windowspath %SystemRoot% /localos
```

Managing Disabled Accounts

Disabling a user account prevents anyone from using it to log on to the domain until an administrator with the appropriate permissions enables it again.

You can disable user accounts manually, to prevent their use while preserving all their attributes, but it is also possible for a system to automatically disable them. For example, repeated violations of password policy settings can disable an account, to prevent intruders from making further attack attempts.

To disable or enable a user or computer account in ADAC or Active Directory Users and Computers, you simply right-click the object and select *Disable* or *Enable* from the context menu. You can also disable and enable multiple accounts by selecting multiple objects and right-clicking.

To disable or enable a user or computer account with Windows PowerShell, use the following cmdlet syntax:

```
Disable-ADAccount –Identity <account name>
Enable-ADAccount –Identity <account name>
```

■ Business Case Scenarios

Scenario 14-1: Creating User Objects

You are a network administrator who is in the process of building an Active Directory network for a company called Fabrikam, Inc., and you have to create user objects for the 75 users in the Inside Sales department. You have already created the fabrikam.com domain and an OU called Inside Sales for this purpose. The Human Resources department has provided you with a list of the users' names and has instructed you to create the account names by using the first initial and the last name. Each user object must also have the value Inside Sales in the Department property and Fabrikam, Inc. in the Company property. Using the first name in the list, Oliver Cox, as an example, which of the following command-line formats would enable you to create the 75 user objects, with the required property values?

a. dsadd "Oliver Cox" –company "Fabrikam, Inc." –dept "Inside Sales"
b. dsadd user CN=Oliver Cox,CN=Inside Sales,DC=fabrikam,DC=com –company Fabrikam, Inc. –dept Inside Sales
c. dsadd –company "Fabrikam, Inc." –dept "Inside Sales" "CN=Oliver Cox,CN=Inside Sales,DC=fabrikam,DC=com"
d. dsadd user "CN=Oliver Cox,CN=Inside Sales,DC=fabrikam,DC=com" –company "Fabrikam, Inc." –dept "Inside Sales"

Scenario 14-2: Considering Security Guidelines

You are preparing a new branch office with new computers. You would like to join the computers to the domain. Unfortunately, the branch office network is available. How would you proceed?

Creating and Managing Active Directory Groups and Organizational Units

LESSON 15

Working with Organizational Units

THE BOTTOM LINE

OUs can be nested to create a design that enables administrators to take advantage of the natural inheritance of the Active Directory hierarchy. You should limit the number of nested OUs, because too many levels can slow the response time to resource requests and complicate the application of Group Policy settings.

When you install Active Directory Domain Services (AD DS), there is only one OU in the domain, by default: the Domain Controllers OU. The domain administrator must create all other OUs.

You can find another type of container object in a domain, called a *container*. For example, a newly created domain has several container objects, including one called *Users*, which contains the domain's predefined users and groups, and another called *Computers*, which contains the computer objects for all the systems joined to the domain.

Unlike organizational units, you cannot assign Group Policy settings to computer objects, nor can you delegate their administration. You also cannot create new container objects by using the standard Active Directory administration tools, such as the Active Directory Users and Computers console. You can create container objects by using scripts, but there is no compelling reason to do so. Organizational units are the preferred method of subdividing a domain.

Creating OUs

The OU is the easiest object type to create in the AD DS hierarchy. You need only supply a name for the object and define its location in the Active Directory tree.

To create an organizational unit object by using the Active Directory Administrative Center, use the following procedure.

CREATE AN OU WITH ACTIVE DIRECTORY ADMINISTRATIVE CENTER

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Active Directory Administrative Center. The *Active Directory Administrative Center* console appears.
2. In the left pane, right-click the object beneath which you want to create the new OU and, from the context menu, select New > Organizational Unit. The *Create Organizational Unit* window appears, as shown in Figure 15-1.

Figure 15-1

The *Create Organizational Unit* window in the Active Directory Administrative Center console

3. In the Name field, type a name for the OU and add any optional information you want.
4. Click OK. The organizational unit object appears in the container.

CLOSE the *Active Directory Administrative Center* console.

Creating an OU in the Active Directory Users and Computers console works in a similar way, although the *New Object – Organizational Unit* dialog box is different in appearance, as shown in Figure 15-2.

Figure 15-2

The *New Object – Organizational Unit* dialog box in the Active Directory Users and Computers console

After you create an OU, you can double-click it to open its Properties sheet, in which you can modify its attributes, or right-click it and select *Move*, to open the *Move* dialog box.

Using OUs to Delegate Active Directory Management Tasks

Creating OUs enables you to implement a decentralized administration model, in which others manage portions of the AD DS hierarchy, without affecting the rest of the structure.

Delegating authority at a site level affects all domains and users within the site. Delegating authority at the domain level affects the entire domain. However, delegating authority at the OU level affects only that OU and its subordinate objects. By granting administrative authority over an OU structure, as opposed to an entire domain or site, you gain the following advantages:

- **Minimal number of administrators with global privileges:** By creating a hierarchy of administrative levels, you limit the number of people who require global access.
- **Limited scope of errors:** Administrative mistakes, such as a container deletion or group object deletion, affect only the respective OU structure.

The ***Delegation of Control Wizard*** provides a simple interface you can use to delegate permissions for domains, OUs, or containers. AD DS has its own system of permissions, much like those of NTFS and printers. The Delegation of Control Wizard is essentially a front-end interface that creates complex combinations of permissions based on specific administrative tasks.

The wizard interface enables you to specify the users or groups to which you want to delegate management permissions and the specific tasks you want them to be able to perform. You can delegate predefined tasks or create custom tasks that enable you to be more specific.

DELEGATE ADMINISTRATIVE CONTROL OF AN OU

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Active Directory Users and Computers. The *Active Directory Users and Computers* console appears.

2. Right-click the object over which you want to delegate control, and click Delegate Control. The *Delegation of Control Wizard* appears, displaying the *Welcome* page.
3. Click Next. The *Users or Groups* page appears.
4. Click Add. The *Select Users, Computers, or Groups* dialog box appears.
5. Type the name of the user or group to which you want to delegate control of the object, and click OK. The user or group appears in the *Selected users and groups* list.
6. Click Next. The *Tasks to Delegate* page appears with the following options:
   - **Delegate the following common tasks:** This option enables you to choose from a list of predefined tasks.
   - **Create a custom task to delegate:** This option enables you to be more specific about the task delegation.
7. Select Create a custom task to delegate and click Next. The *Active Directory Object Type* page appears, displaying the following options.
   - **This folder, existing objects in this folder, and creation of new objects in this folder:** This option delegates control of the container, including all its current and future objects.
   - **Only the following objects in the folder:** This option enables you to select specific objects to be controlled. You can select *Create selected objects in this folder* to allow selected object types to be created, or select *Delete selected objects in this folder* to allow selected object types to be deleted.
8. Select This folder, existing objects in this folder, and creation of new objects in this folder and click Next. The *Permissions* page appears, as shown in Figure 15-3.

Figure 15-3

The Permissions page of the Delegation of Control Wizard

9. Set the delegated permissions according to your needs for the user or group to which you delegate control. You can combine permissions from all three of the following options:
   - **General:** displays general permissions, which are equal to those displayed on the *Security* tab in an object's properties. For example, selecting Full Control for general permissions is inclusive of all property rights as well.

- **Property-specific:** displays permissions that apply to specific attributes or properties of an object. If you select the Read permission using the General option, all read-specific properties are selected.
- **Creation/deletion of specific child objects:** displays permissions that apply to creation and deletion permissions for specified object types.

10. Click Next. The *Completing the Delegation of Control Wizard* page appears.
11. Click Finish.

CLOSE the *Active Directory Users and Computers* console.

In this procedure, you grant permissions over a portion of Active Directory to a specified administrator or group of administrators. Although you can use the *Delegation of Control Wizard* to grant permissions, you cannot use it to modify or remove permissions. To perform these tasks, you must use the interface provided in the *Security* tab in the AD DS object's Properties sheet.

Working with Groups

THE BOTTOM LINE

Since the early days of the Microsoft server operating system, administrators have used ***groups*** to manage network permissions. Groups enable you to assign permissions to multiple users simultaneously. A group can be defined as a collection of user or computer accounts that functions as a security principal, in much the same way that a user does.

In Windows Server 2012 R2, when a user logs on to Active Directory, an ***access token*** is created that identifies the user and all the user's group memberships. Domain controllers use this access token to verify a user's permissions when the user attempts to access a local or network resource. By using groups, you can grant multiple users the same permission level for resources on the network. If, for example, you have 25 users in the graphics department who need access to a color printer, you can either assign each user the appropriate permissions for the printer, or you can create a group containing the 25 users and assign the appropriate permissions to the group. By using a group object to access a resource, you accomplish the following:

- When users need access to the printer, you can add them to the group. Once added, the user receives all permissions assigned to this group. Similarly, you can remove users from the group when you want to revoke their access to the printer.
- You need to make only one change to modify the level of access to the printer for all the users. Changing the group's permissions changes the permission level for all group members. Without the group, you need to modify all 25 user accounts individually.

Users can be members of more than one group. In addition, groups can contain other Active Directory objects, such as computers, and other groups in a technique called ***group nesting***. Group nesting describes the process of configuring one or more groups as members of another group. For example, consider a company that has two groups: marketing and graphic design. Graphic design group members have access to a high-resolution color laser printer. If the marketing group personnel also need access to the printer, you can add the marketing group as a member of the graphic design group. This gives the marketing group members the same permission to the color laser printer as the members of the graphic design group.

Working with Default Groups

Although there are many situations in which you might create groups to organize users or computers and then assign permissions, there are several built-in security groups that the system creates when you install AD DS on Windows Server 2012 R2. Many of the built-in groups have predefined user rights that enable their members to perform certain system-related tasks, such as backup and restore. You can add accounts to the default groups, to grant users the same rights, in addition to any resource access permissions the groups possess.

The default groups are located in the Built-in and Users container objects in AD DS. The list of predefined groups in these containers varies depending on the installed services. For example, installing the Dynamic Host Configuration Protocol (DHCP) server role creates two new groups in the Users container, called *DHCP Administrators* and *DHCP Users*.

All the default groups are security groups. Active Directory does not include any default distribution groups. The Built-in container, holds domain local groups, and the Users container has groups of various scopes.

You can view the groups described in the Built-in and Users containers and manage their memberships by using the *Active Directory Administrative Center* or *Active Directory Users and Computers*. The only difference between these groups and the ones you create yourself is that you cannot delete the default groups.

Nesting Groups

As discussed previously, *group nesting* is the term used when groups are added as members of other groups. For example, when you make a global group a member of a universal group, it is nested within the universal group.

Group nesting reduces the number of times you need to assign permissions to users in different domains in a multidomain forest. For example, if you have multiple child domains in your AD DS hierarchy, and the users in each domain need access to an enterprise database application located in the parent domain, the simplest way to set up access to this application is as follows:

1. Create global groups in each domain that contain all users needing access to the enterprise database.
2. Create a universal group in the parent domain. Include each location's global group as a member.
3. Add the universal group to the required domain local group to assign the necessary permission to access and use the enterprise database.

This traditional approach to group nesting in AD DS is often referred to using the mnemonic *AGUDLP*: you add **A**ccounts to **G**lobal groups, add those global groups to **U**niversal groups, add universal groups to **D**omain **L**ocal groups, and, finally, assign **P**ermissions to the domain local groups.

For example, the Backup Operators group enables members to perform backups on the computers in the domain, because the Backup Operators group receives the *Backup files and directories* user right through the Default Domain Controllers Policy and Local Security Policy GPOs.

You can use the same method to create your own domain local groups, which you delegate administrative tasks and user rights for particular OUs. Then, after creating global groups (or universal groups, for forest-wide assignments) and adding them to the domain local groups, the structure is in place.

For example, if you run a single-domain enterprise and want to grant the manager of your Boston office the ability to back up the computers at that site, you could use a procedure like the following:

1. Create an OU for the branch office called *Boston*.
2. Create a domain local group called *Boston Backup*.
3. Create a GPO called *Boston OU Backup* and grant the Boston Backup group the *Backup files and directories* user right.
4. Link the GPO to the Boston OU.
5. Create a global group called *Boston Office Managers*.
6. Add the Boston Office Managers group to the Boston Backup group as a member.

All that remains is to add the user account for the Boston branch manager to the Boston Office Managers global group. If the manager goes on vacation or leaves the company, the administrator at the central office just has to add another user from the Boston office to the Boston Office Managers group in order to grant someone else the rights to perform backups.

This procedure grants one user the rights needed to perform one task at one site. Obviously, it is not efficient to delegate every task individually this way. A more efficient method is for enterprise administrators to organize their lists of tasks into groups, which they or others will assign to IT staffers. Microsoft refers to these groups as management roles and has published lists of recommended roles for service management and data management tasks, as shown in Table 15-1.

Table 15-1

Active Directory Management Roles

Service Management Roles	Data Management Roles
Forest Configuration Operators	Business Unit Administrators
Domain Configuration Operators	Account Administrators
Security Policy Administrators	Workstation Administrators
Service Administration Managers	Server Operators
Domain Controller Administrators	Resource Administrators
Backup Operators	Security Group Administrators
Schema Administrators	Help Desk Operators
Replication Management Administrators	Application-Specific Administrators
Replication Monitoring Operators	
DNS Administrators	

Creating Groups

The procedure for creating groups in Active Directory Administrative Center or Active Directory Users and Computers is similar to that of creating organizational units.

When you create a group, you must specify a name for the group object. The name you select can be up to 64 characters long and must be unique in the domain. You must also choose a group type and a group scope. Figure 15-4 shows the Create Group window in Active Directory Administrative Center.

Figure 15-4

Creating a group in Active Directory Administrative Center

The New Object – Group dialog box in Active Directory Users and Computers is slightly different in appearance, but contains the same basic controls, as shown in Figure 15-5.

Figure 15-5

Creating a group in Active Directory Users and Computers

Although the graphical AD DS utilities are a convenient tool for creating and managing groups individually, they are not the most efficient method for creating large numbers of security principals. The command-line tools included with Windows Server 2012 R2 enable you to create and manage groups in large numbers by using batch files or other types of scripts, as discussed in Lesson 14, "Creating and Managing Active Directory Users and Computers." Some of these tools are discussed in the following sections.

Managing Group Memberships

Unlike the Active Directory Administrative Center, which enables you to specify a group's members as you create the group, in Active Directory Users and Computers, you must create the group object first, and then add members to it.

To add members to a group, you select it in the console and, from the *Action* menu, select *Properties* to open the group's Properties sheet, and then select the *Members* tab.

By using the *Members* tab, you can add objects to the group's membership list. On the *Member Of* tab, you can add the group to the membership list of another group. For both of these tasks, you use the standard *Select Users, Contacts, Computers, Service Accounts, or Groups* dialog box.

After you enter or find the objects you want to add, click *OK* to close the Properties sheet and add the objects to the group's membership list.

MANAGING GROUP MEMBERSHIP USING GROUP POLICY

It is also possible to control group memberships by using Group Policy. When you create Restricted Groups policies, you can specify the membership for a group and enforce it, so that no one can add or remove members.

To create Restricted Groups policies, use the following procedure.

CREATE A RESTRICTED GROUPS POLICY

GET READY. Log on to the server running Windows Server 2012 R2 using an account with administrative privileges.

1. From the Tools menu in the *Server Manager* window, select Group Policy Management. The *Group Policy Management* console appears.
2. Create a new Group Policy object (GPO) and link it to your domain.
3. Open the GPO in the *Group Policy Management Editor* and browse to the Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups folder, as shown in Figure 15-6.

Figure 15-6

The Restricted Groups folder in the Group Policy object

4. Right-click the Restricted Groups folder and from the context menu, select Add Group. The *Add Group* dialog box appears.
5. Type or browse to add a group object and click OK. The group appears in the *Restricted Groups* folder and a Properties sheet for the policy appears, as shown in Figure 15-7.

Figure 15-7

The Properties sheet for a Restricted Groups policy

6. Click one or both of the Add buttons to add objects that should be members of the group, or other groups of which the group should be a member.
7. Click OK.

CLOSE the *Group Policy Management Editor* and *Group Policy Management* consoles.

The members you specify for a group in a Restricted Groups policy are the only members permitted to remain in that group. The policy does not prevent you from modifying the group membership by using other tools, but the next time the system refreshes its group policy settings, the group membership list will be overwritten by the policy.

Converting Groups

As group functions change, you might need to change a group object from one type to another.

For example, you might have created a distribution group that contains 100 members from multiple departments working on the same project for the purpose of sending e-mail messages. As the project progresses, members might need to access a common database. By converting the distribution group to a security group and assigning permissions to the group, you can provide the project members with access to the common database without having to create a new group and add 100 members to it again.

To change the type of a group, open the group's Properties sheet in the *Active Directory Administrative Center* or the *Active Directory Users and Computers* console. On the *General* tab, you can modify the *Group Type* option and click *OK*.

The process for changing the group's scope is the same, except that you select one of the *Group Scope* options on the *General* tab. The AD DS utilities enable you to perform only permissible scope changes. Table 15-2 lists the scope changes that are permitted.

Table 15-2

Active Directory Group Scope Conversion Restrictions

	To Domain Local	To Global	To Universal
From Domain Local	Not applicable	Not permitted	Permitted only when the domain local group does not have other domain local groups as members
From Global	Not permitted	Not applicable	Permitted only when the global group is not a member of another global group
From Universal	No restrictions	Permitted only when the universal group does not have other universal groups as members	Not applicable

Business Case Scenarios

Scenario 15-1: Administering Groups for Humongous Insurance

You are a network administrator for Humongous Insurance. Humongous Insurance has a multidomain forest. The forest root is humongousinsurance.com. There are also two child domains named west.humongousinsurance.com and east.humongousinsurance.com. The company has approximately 7,000 users, 7,000 client workstations, and 100 servers.

All domains are Windows Server 2013 domains. The forest root domain has 10 domain controllers. Five of those domain controllers are configured as DNS servers and two are configured as global catalog servers. The West domain has three domain controllers. Two of those domain controllers are configured as DNS servers. One of those domain controllers is configured as a global catalog server. The East domain has two Windows Server 2012 R2 domain controllers and three Windows 2008 domain controllers.

The forest root domain is located in College Station, Texas. The East domain is located in Gainesville, Florida. The West domain is located in San Diego, California. An Active Directory site is configured for each of these locations. The site for College Station is named Main_Site. The Gainesville site is named East_Site. The San Diego site is named West_Site.

You are one of several network administrators assigned to handle the forest root domain and College Station site. Your manager, Jean Trenary, has called a meeting of all network and desktop administrators. She wants to address several issues.

1. Jean says four internal auditors are in the forest root domain. Two internal auditors are in each of the child domains. Each set of internal auditors has been placed in a global group within each domain. These groups are named IA_Main, IA_East, and IA_West

after their respective locations. Jean wants all of the members of these groups to be able to access a common set of resources in the Main domain, while still segregating the auditors' ability to access other resources in domains other than their own. What is the recommended way to configure the groups to allow the desired functionality?

2. The network administrators from the West domain want to know why everyone always recommends placing global groups into universal groups, instead of placing the users directly into the universal groups. What should you tell them?
3. Jean approves a plan to hire assistants for each domain to create and manage user accounts. How can you give the assistants the immediate ability to help in this way, without making them domain administrators?
4. Two employees have been hired to back up data and manage printers for the Main_Site. Which built-in groups will give these users the permissions they require to manage the domain controllers? How should you set up their accounts and group memberships?

Scenario 15-2: Planning GPOs for Tailspin Toys

Tailspin Toys is running a single Windows Server 2012 R2 Active Directory domain with multiple OUs configured for each of its 12 locations. An administrator at each location is responsible for managing GPOs and user accounts. You are the enterprise administrator responsible for planning the infrastructure. For each of the following challenges, document your options and be prepared to share them with other students.

1. Administrators located at each location should be able to create new GPOs and edit any that they have created. They should not be able to change or delete GPOs that they have not created. What are your options for providing this functionality?
2. All users in each location are currently in one OU. Certain group policies should only apply to users in some departments and not others. What options should you consider that will allow group policies to be applied to only the necessary users?
3. Although you have created a domain-wide policy that enforces restrictions on administrative tools, you do not want those settings to apply to users for which you have delegated administrative permissions on each location's OU. What are your options to solve this?

Creating Group Policy Objects

LESSON 16

Introducing Group Policy

THE BOTTOM LINE

Group Policy is a mechanism for controlling and deploying operating system settings to computers all over your network. Group Policy consists of user and computer settings for the various Microsoft Windows operating systems, which the systems implement during computer startup and shutdown and user logon and logoff. You can configure one or more Group Policy objects (GPOs) and then use a process called ***linking*** to associate them with specific Active Directory Domain System (AD DS) objects. When you link a GPO to a container object, all the objects in that container receive the settings you configured in the GPO. You can link multiple GPOs to a single AD DS container or link one GPO to multiple containers throughout the AD DS hierarchy.

You can use Group Policy objects to manage any or all of the following types of settings:

- Registry-based policies, such as user desktop settings and environment variables, provide a consistent, secure, manageable working environment that addresses the users' needs and the organization's administrative goals. As the name implies, these settings modify the Windows Registry.
- Software installation policies ensure that users always have the latest versions of applications. If application files are inadvertently deleted, the policies can make repairs without user intervention.
- ***Folder redirection*** enables users to store local files on a network drive for backup, making them accessible from anywhere on the network.
- Offline file storage works with folder redirection to provide local file caching. This enables users to access their files even when the network is inaccessible.
- Scripts, including logon, logoff, startup, and shutdown commands, can assist in configuring the user environment.
- Windows Deployment Services (WDS) assists in rebuilding or deploying workstations quickly and efficiently in an enterprise environment.
- Microsoft Internet Explorer settings provide quick links and bookmarks for user accessibility, in addition to browser options, such as proxy use, acceptance of cookies, and caching options.
- Security settings protect resources on computers in the enterprise.

Depending on the organization's needs, you can choose which features and settings to implement. For example, you can create a policy for a public access computer in a library that configures the desktop environment with a proprietary library-access system.

In addition, you can disable the capability to write to the computer's hard drive. As you determine the needs of different users and address the needs within corporate security and computing policies, you can plan the best methods to implement Group Policy.

Group Policies can be linked to sites, domains, or organizational units (OUs) to apply the settings to all users and computers within the Active Directory containers. However, an advanced technique, called ***security filtering***, enables you to apply GPO settings to only one or more users or groups within a container by selectively granting the "Apply Group Policy" permission to one or more users or security groups.

Understanding Group Policy Objects

Group Policy objects (GPOs) contain the Group Policy settings to deploy to user and computer objects within a site, domain, or organizational unit. To deploy a GPO, you must associate it with the container to which it is deployed. This association links the GPO to the desired Active Directory Domain Services object. Administrative tasks for Group Policy include creating GPOs, specifying where they are stored, and managing the AD DS links.

There are three types of GPOs: ***local GPOs***, ***domain GPOs,*** and ***starter GPOs***.

LOCAL GPOS

All Windows operating systems have support for local Group Policy objects, sometimes known as LGPOs. Windows versions since Windows Server 2008 R2 and Windows Vista can support ***multiple local GPOs***. This enables you to specify a different local GPO for administrators or to create specific GPO settings for one or more local users configured on a workstation. This capability is particularly valuable for computers in public locations such as libraries and kiosks, which are not part of an Active Directory infrastructure.

Older Windows releases (prior to Windows Vista) can support only one local GPO, and the settings in that local GPO can apply only to the computer, not to individual users or groups.

Local GPO settings are stored on the local computer in the %systemroot%/System32/GroupPolicy folder.

A local GPO has the following characteristics:

- Local GPOs contain fewer options than domain GPOs. They do not support folder redirection or Group Policy software installation. Fewer security settings are available.
- When a local and a nonlocal (Active Directory-based) GPO have conflicting settings, the local GPO settings are overwritten by those of the nonlocal GPO.

DOMAIN GPOS

Nonlocal GPOs are created in Active Directory and are linked to sites, domains, or OUs. After linked to a container, the settings in the GPO are applied to all users and computers within the container by default. The content of each nonlocal GPO is stored in the following two locations:

- ***Group Policy container (GPC)*** is an Active Directory object that stores the properties of the GPO.
- ***Group Policy template (GPT)*** is located in the Policies subfolder of the SYSVOL share; the GPT is a folder that stores policy settings, such as security settings and script files.

STARTER GPOS

Starter GPOs is a feature introduced in Windows Server 2008. A starter GPO is a template for the creation of domain GPOs based on a standard collection of settings. When you create a new GPO from a starter GPO, all the policies in the starter are automatically copied to the new GPO as its default settings.

Configuring a Central Store

In Windows Server 2008 and Windows Vista, Microsoft replaced the token-based administrative template (ADM) files used with previous versions of Group Policy with an XML-based file format (***ADMX***). Administrative templates are the files defining the registry-based settings that appear in Group Policy objects.

Earlier Windows versions created a copy of the ADM files for each GPO you created and placed it in the SYSVOL volume of a domain controller. A large Active Directory installation could easily have dozens of GPOs, and each copy of the ADM files required 4 megabytes of storage. The result was a condition called ***SYSVOL bloat***, in which hundreds of megabytes of redundant information was stored on SYSVOL volumes, which had to be replicated to all the domain controllers for the domain.

To address this problem, Group Policy tools can now access the ADMX files from a ***Central Store***, a single copy of the ADMX files stored on domain controllers. To use a Central Store, however, you must create the appropriate folder in the SYSVOL volume on a domain controller.

By default, tools such as the Group Policy Management console save the ADMX files to the \%systemroot%\PolicyDefinitions folder, which on most computers is C:\Windows\PolicyDefinitions. To create a Central Store, you must copy the entire PolicyDefinitions folder to the same location as the Group Policy templates, that is, %systemroot%\SYSVOL\sysvol\<*domain name*>\Policies, or, in UNC notation, \\<*domain name*>\SYSVOL\<*domain name*>\Policies.

■ Using the Group Policy Management Console

THE BOTTOM LINE

The ***Group Policy Management console*** is the Microsoft Management Console (MMC) snap-in that you use to create Group Policy objects and manage their deployment to Active Directory Domain Services objects. The ***Group Policy Management Editor*** is a separate snap-in that opens GPOs and enables you to modify their settings.

There are several different ways of working with these two tools, depending on what you want to accomplish. You can create a GPO and then link it to a domain, site, or OU, or create and link a GPO in a single step. Windows Server 2012 R2 implements the tools as the Group Policy Management feature, and installs them automatically with the Active Directory Domain Services role. You can install the feature manually on a member server by using the Add Roles and Features Wizard in Server Manager. It is also included in the Remote Server Administration Tools package for Windows workstations.

Creating and Linking Nonlocal GPOs

If, as recommended previously, you leave the default GPOs unaltered, the first steps in deploying your own customized Group Policy settings are to create one or more new Group Policy objects and link them to appropriate AD DS objects.

To use the Group Policy Management console to create a new GPO and link it to an organizational unit object in AD DS, perform the following procedure.

CREATE AND LINK A GPO TO AN OU

GET READY. Log on to a domain controller running Windows Server 2012 R2, using an account with domain Administrator privileges. The Server Manager console appears.

1. Open the Active Directory Administrative Center and create an OU called "Sales" in your domain.
2. From the Tools menu, select Group Policy Management. The Group Policy Management console appears, as shown in Figure 16-1.

Figure 16-1

The Group Policy Management console

3. Expand the forest container and browse to your domain. Then expand the domain container and select the Group Policy Objects folder. The GPOs that currently exist in the domain appear in the *Contents* tab, as shown in Figure 16-2.

Figure 16-2

Contents of the Group Policy Objects folder

4. Right-click the Group Policy Objects folder and, from the context menu, select New. The *New GPO* dialog box appears.
5. In the Name text box, type a name for the new GPO and, if desired, select a *Source Starter GPO* from the drop-down list and click OK. The new GPO appears in the Contents list.
6. In the left pane, right-click the domain, site, or OU object to which you want to link the new GPO and, from the context menu, select Link an existing GPO. The *Select GPO* dialog box appears.
7. Select the GPO you want to link to the object and click OK. The GPO appears on the object's *Linked Group Policy Objects* tab.

CLOSE the Group Policy Management console.

You can also create and link a GPO to an AD container in a single step, by right-clicking an object and selecting Create a GPO in this Domain and Link it here from the context menu.

If you link a GPO to a domain object, it applies to all users and computers in the domain. On a larger scale, if you link a GPO to a site that contains multiple domains, the Group Policy settings are applied to all the domains and the child objects beneath them. This process is referred to as ***GPO inheritance***.

Using Security Filtering

By default, linking a GPO to a container causes all the users and computers in that container to receive the GPO settings. The act of creating the link grants the Read and Apply Group Policy permissions for the GPO to the users and computers in the container.

In actuality, the system grants the permissions to the Authenticated Users special identity, which includes all the users and computers in the container. However, by using a technique called security filtering, you can modify the default permission assignments so that only certain users and computers receive the permissions and, consequently, the settings in the GPO.

To modify the default security filtering configuration for a GPO, select it in the left pane of the Group Policy Management console, as shown in Figure 16-3 . In the Security Filtering area, you can use the Add and Remove buttons to replace the Authenticated Users special identity with specific user, computer, or group objects. Of the users and computers in the container to which the GPO is linked, only those you select in the Security Filtering pane receive the settings from the GPO.

Figure 16-3

Security filtering in the Group Policy Management console

Managing Starter GPOs

Starter GPOs are templates that create multiple GPOs with the same set of baseline Administrative Templates settings.

You create and edit starter GPOs just as you would any other Group Policy object. In the Group Policy Management console, you right-click the Starter GPOs folder and, from the context menu, select New to create a blank starter GPO. You can then open the starter GPO in the Group Policy Management Editor and configure any settings you want to carry over to the new GPOs you create.

After you create and edit your starter GPOs, you can create new GPOs from them in two ways. You can right-click a starter GPO and select New GPO from Starter GPO from the context menu, or you can create a new GPO in the usual manner described previously and select the starter GPO in the Source Starter GPO drop-down list. This process copies the settings from the starter GPO to the new GPO, which you can continue to edit from there.

Configuring Group Policy Settings

Group Policy settings enable you to customize the configuration of a user's desktop, environment, and security settings. The settings are divided into two subcategories: Computer Configuration and User Configuration. The subcategories are referred to as Group Policy nodes. A node is a parent structure that holds all related settings. In this case, the node is specific to computer configurations and user configurations.

Group Policy nodes provide a way to organize the settings according to where they are applied. The settings you define in a GPO can be applied to client computers, users, or member servers and domain controllers. The application of the settings depends on the container to which you link the GPO. By default, all objects within the container to which you link the GPO are affected by the GPO's settings.

The Computer Configuration and the User Configuration nodes contain three subnodes, or extensions, that further organize the available Group Policy settings. Within the Computer Configuration and User Configuration nodes, the subnodes are as follows:

- **Software Settings:** The Software Settings folder located under the Computer Configuration node contains Software Installation settings that apply to all users who log on to a domain using a specific computer. These settings are applied before any user is allowed to log on. Rather than being computer specific, the Software Settings folder located under the User Configuration node contains Software Installation settings applied to users designated by the Group Policy, regardless of the computer from which they log on.
- **Windows Settings:** The Windows Settings folder located under the Computer Configuration node in the Group Policy Management Editor contains security settings and scripts that apply to all users who log on to Active Directory Domain Services from that specific computer. This means that the settings are computer specific. The Windows Settings folder located under the User Configuration node contains settings related to folder redirection, security settings, and scripts that apply to specific users. The computer from which a user logs on does not affect these policy settings; the policies are applied regardless of the user's log on location.
- **Administrative Templates:** Windows Server 2012 R2 includes thousands of Administrative Template policies, which contain all registry-based policy settings. Administrative Templates are files with the .admx extension. They are used to generate the user interface for the Group Policy settings that you can set by using the Group Policy Management Editor. The Windows Server 2012 R2 .admx files are based on the eXtensible Markup Language (XML), unlike the Windows 2003 .adm files, which are token-based text files.

■ Creating Multiple Local GPOs

THE BOTTOM LINE

Computers that are members of an AD DS domain benefit from flexibility when it comes to Group Policy configuration. Standalone (non-AD DS) systems can achieve some of the flexibility, as long as they are running at least Windows Vista or Windows Server 2008 R2. These operating systems enable you to create multiple local GPOs that provide different settings for users, based on their identities.

Windows systems supporting multiple local GPOs have the following three layers of Group Policy support:

- **Local Group Policy:** Identical to the single local GPO supported by older operating system versions, the Local Group Policy layer consists of both Computer and User

settings and applies to all system users, administrative or not. Because this is the only local GPO that includes computer settings, you must use this GPO to apply Computer Configuration policies.

- **Administrators and Non-administrators Group Policy:** This layer consists of two GPOs, one of which applies to members of the local Administrators group and one that applies to all users that are not members of the local Administrators group. This enables you to easily create user settings that distinguish between administrative and non-administrative users. Unlike the Local Group Policy GPO, this layer does not include computer settings.
- **User-specific Group Policy:** This layer consists of GPOs that apply to specific local user accounts created on the computer. These GPOs can apply to individual users only, not to local groups. These GPOs also do not have computer configuration settings.

Windows applies the local GPOs in the order listed here. The Local Group Policy settings are applied first, then either the Administrators or Non-administrators GPO, and finally any user specific GPOs. As with nonlocal GPOs, the settings processed later can overwrite any earlier settings with which they conflict.

In the case of a system that is also a member of a domain, the three layers of local GPO processing come first and are followed by the standard order of nonlocal Group Policy application.

To create local GPOs, you use the Group Policy Object Editor, which is an MMC snap-in provided on all Windows computers, as in the following procedure.

CREATE LOCAL GPOS

GET READY. Log on to a Windows computer, using an account with Administrator privileges. The Server Manager console appears.

1. Open the Run dialog box and, in the Open text box, type mmc and click OK. An empty MMC console appears.
2. Click File > Add/Remove Snap-in. The *Add or Remove Snap-ins* dialog box appears.
3. Select Group Policy Object Editor from the *Available snap-ins* list and click Add. The *Select Group Policy Object* page appears.
4. To create the Local Group Policy GPO, click Finish. To create a secondary or t*ertiary GPO,* click Browse. The *Browse for a Group Policy Object* dialog box appears.
5. Click the Users tab, as shown in Figure 16-4.

Figure 16-4

The Users tab of the *Browse for a Group Policy Object* dialog box

6. To create a secondary GPO, select either Administrators or Non-Administrators and click OK. To create tertiary GPO, select a user and click OK. The Group Policy object appears on the *Select Group Policy Object* page.
7. Click Finish. The snap-in appears in the *Add or Remove Snap-ins* dialog box.
8. Click OK. The snap-in appears in the MMC console, as shown in Figure 16-5.

Figure 16-5

A Group Policy Object Editor console

9. Click File > Save As. A *Save As* combo box appears.
10. Type a name for the console, to save it in the Administrative Tools program group.

CLOSE the MMC console.

You can now open this console to configure the settings in the GPO you created. A Local Group Policy GPO has both Computer Configuration and User Configuration settings, whereas the secondary and tertiary GPOs have only User Configuration settings.

Business Case Scenarios

Scenario 16-1: Creating Device Restrictions

After a recent incident in which an employee left the company with a substantial amount of confidential data, the IT director has given Alice the task of implementing Group Policy settings that prevent all users except administrators and members of the Executives group from installing any USB devices. Alice creates a GPO called Device Restrictions for this purpose and links it to the company's single domain object. The GPO contains the following settings:

- Allow administrators to override Device Installation Restriction policies—Enabled
- Prevent installation of devices not described by other policy sessions—Enabled

What else must Alice do to satisfy the requirements of her assignment?

Scenario 16-2: Deploying a GPO

Ralph has a number of Group Policy settings that he must deploy to the workstations of his firm's department managers, so they can run a timesheet application for their hourly employees. He has created a GPO containing those settings, and has named it HourlyTime. After linking the GPO to his company domain object in Active Directory Domain Services, Ralph quickly receives a number of trouble tickets referred to him from the help desk. The salaried employees are complaining that the application they use to file their weekly expenses has stopped working. Ralph's testing eventually establishes that it is the settings in the HourlyTime GPO that are causing the expense voucher application to malfunction. How can Ralph deploy the HourlyTiime GPO to the department managers only, without interfering with the other application?

Configuring Security Policies

LESSON 17

Configuring Security Policies Using Group Policy

THE BOTTOM LINE

In Lesson 16, "Creating Group Policy Objects," you learned how to create and deploy Group Policy objects (GPOs) by linking them to Active Directory Domain Services (AD DS) objects. This lesson focuses on configuring the settings in the Group Policy objects themselves, and particularly on the ones that can help secure your network.

It is important for administrators to know the difference between user and computer settings. In addition to learning about these settings and categorizing them based on where you apply them, this lesson also looks at the default Group Policy refresh process and how to invoke a manual refresh of Group Policy objects when necessary.

One of the primary aims of Group Policy is to provide centralized management of security settings for users and computers. Most of the settings that pertain to security are found in the Windows Settings folder within the Computer Configuration node of a GPO. You can use security settings to govern how users are authenticated to the network, the resources they are permitted to use, group membership policies, and events related to user and group actions recorded in the event logs. Table 17-1 briefly describes some of the security settings that you can configure within the Computer Configuration node.

Table 17-1

Computer Configuration Node Security Settings

Setting	Description
Account Policies	Includes settings for Password Policy, Account Lockout Policy, and Kerberos Policy. A domain-wide policy, such as the Default Domain Policy GPO, also includes Kerberos Policy settings. Prior to Windows Server 2008, you could configure only Password Policy and Account Lockout Policy settings at the domain level. Starting with Windows Server 2008, you can configure Fine-Grained Password Policies that enable you to specify multiple password policies in a single domain.
Local Policies	Contains three subcategories that pertain to the local computer policies: Audit Policy, User Rights Assignment, and Security Options.
Event Log Policy	These settings pertain to Event Viewer logs, their maximum size, retention settings, and accessibility.
Restricted Groups Policy	This setting gives you control over the Members property and the Members Of property for specific security groups.

(continued)

Table 17-1

(continued)

Setting	Description
System Services Policy	These settings can be used to define the startup mode and access permissions for all system services. You can configure each service to be disabled, to start automatically, or to start manually.
Registry and File System Policies	These settings configure access permissions and audit settings for specific registry keys or file system objects.
Wired Network (IEEE 802.3) Policies	Enables you to create policies specifying authentication settings for computers on wired networks running Windows Vista or later.
Windows Firewall with Advanced Security	Enables you to create inbound and outbound firewall filters and distribute them to network computers.
Network List Manager Policies	Specifies whether unidentified networks should be designated as public or private, causing them to receive a specific group of firewall rules.
Wireless Network (IEEE 802.11) Policies	Enables the creation of policies for IEEE 802.11 wireless networks. Settings include preferred networks and authentication types, in addition to other security-related options.
Public Key Policies	This node includes options to create an Encrypted File System (EFS), automatic certificate request, trusted root certificates, and an enterprise trust list.
Software Restriction Policies	This policy can specify software that you want to run on computers, and that you want to prevent from running, because it might pose a security risk to the computer or organization.
Network Access Protection	Enables you to create policies to configure Network Access Protection clients.
Application Control Policies	Configures access control policies for applications using AppLocker.
IP Security Policies on Active Directory	Includes policy settings that enable you to define mandatory rules applicable to computers on an IP-based network.
Advanced Audit Policy Configuration	Provides more granular audit policy settings than the Audit Policy node found under Local Policies.

Policy settings in the Computer Configuration node apply to a computer; it does not matter who logs on to it. You can apply more Computer Configuration security settings than settings to a specific user. Table 17-2 describes the security settings that you can apply within the User Configuration node of a Group Policy object.

Table 17-2

Security Settings Applied in the User Configuration Node

Setting	Description
Public Key Policies	Includes the Enterprise Trust policy that enables you to list the trusted sources for certificates. Also, auto-enrollment settings can be specified for the user within this node.
Software Restriction Policies	This policy can be used to specify software that you want to run for the user. Specifically, it can be used to disallow applications that might pose a security risk if run.

Defining Local Policies

Local Policies enable you to set user privileges on the local computer that govern what users can do on the computer and determine whether the system should track them in an event log. Tracking events that take place on the local computer, a process referred to as ***auditing***, is another important part of monitoring and managing activities on a computer running Windows Server 2012 R2.

The Local Policies node of a GPO has three subordinate nodes: User Rights Assignment, Security Options, and Audit Policy. As discussed in the following sections, keep in mind that Local Policies are local to a computer. When they are part of a GPO in Active Directory, they affect the local security settings of computer accounts to which the GPO is applied.

PLANNING AND CONFIGURING AN AUDIT POLICY

The Audit Policy section of a GPO enables you to log successful and failed security events, such as logon events, account access, and object access. You can use auditing to track both user activities and system activities. Planning to audit requires that you determine the computers to be audited and the types of events you want to track.

When you consider an event to audit, such as account logon events, you must decide whether to audit successful logon attempts, failed logon attempts, or both. Tracking successful events enables you to determine how often users access network resources. This information can be valuable when planning your resource usage and budgeting for new resources. Tracking failed events can help you determine when security breaches occur or are attempted. For example, if you notice frequent failed logon attempts for a specific user account, you might want to investigate further. The policy settings available for auditing are shown in Figure 17-1.

Figure 17-1

Audit Policies in the Default Domain Policy

When an audited event occurs, Windows Server 2012 R2 writes an event to the security log on the domain controller or the computer where the event took place. If it is a logon attempt or other Active Directory–related event, the event is written to the domain controller. If it is a computer event, such as a drive access, the event is written to the local computer's event log.

Implementation of your plan requires that you specify the categories to be audited and, if necessary, configure objects for auditing. To configure an audit policy, use the following procedure.

CONFIGURE AN AUDIT POLICY

GET READY. Log on to a domain controller running Windows Server 2012 R2, using an account with domain Administrator privileges. The Server Manager console appears.

1. From the Tools menu, select Group Policy Management. The Group Policy Management console appears.
2. Expand the forest container and browse to your domain. Then expand the domain container and select the Group Policy Objects folder. The GPOs that currently exist in the domain appear in the *Contents* tab.
3. Right-click the Default Domain Policy GPO and click Edit. A Group Policy Management Editor window for this policy appears.
4. Browse to the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies node and select Audit Policy. The audit policy settings appear in the right pane.
5. Double-click the Audit Policy setting you want to modify. The Properties sheet for the policy you chose appears.
6. Select the Define This Policy Setting check box.
7. Select the appropriate check box(es) to audit Success, Failure, or both.
8. Click OK to close the setting's Properties sheet.

CLOSE the Group Policy Management Editor and the Group Policy Management console.

You now configured an audit policy in the Default Domain Policy GPO, which will be propagated to all the computers in the domain during the next policy refresh.

Configuring objects for auditing is necessary when you configure either of the two following event categories:

- **Audit Directory Service Access:** logs user access to Active Directory objects, such as other user objects or OUs.
- **Audit Object Access:** logs user access to files, folders, registry keys, and printers.

Each of these event categories requires additional setup steps, which are described in the following procedure.

CONFIGURE AN ACTIVE DIRECTORY OBJECT FOR AUDITING

GET READY. Log on to a domain controller running Windows Server 2012 R2, using an account with domain Administrator privileges. The Server Manager console appears.

1. From the Tools menu, select Active Directory Users and Computers. The *Active Directory Users and Computers* console appears.
2. From the View menu, select Advanced Features.
3. Browse to the object that you want to audit. Right-click the object and, from the context menu, select Properties. The object's Properties sheet appears.
4. Click the Security tab, and then click Advanced. The *Advanced Security Settings* dialog box for the object appears.
5. Select the Auditing tab.
6. Click Add. The *Auditing Entry* page for the object appears.
7. Click Select a Principal. The *Select User, Computer, Service Account, or Group* dialog box appears. Select the users or groups to be audited for Active Directory object access and click OK. The users or groups appear in the *Auditing Entry* dialog box for the object, as shown in Figure 17-2.

Figure 17-2

The Auditing Entry dialog box for an object

8. From the *Type* drop-down list, specify whether you want to audit failures, successes, or both.
9. From the *Applies to* drop-down list, specify which descendent objects should be audited.
10. Select the Permissions and/or Properties you want to audit for this object and click OK. The new Auditing entry appears in the *Advanced Security Settings* dialog box.
11. Create additional auditing entries, if desired, and click OK.
12. Click OK to close the object's Advanced Security Settings dialog box.
13. Click OK to close the object's Properties sheet.

CLOSE the *Active Directory Users and Computers* console.

After you configure the auditing policy and the AD DS objects you want to audit, the systems monitor the objects and create entries in the Security log.

To audit access to objects, such as files and folders, use the following procedure.

CONFIGURE FILES AND FOLDERS FOR AUDITING

GET READY. Log on to a domain controller running Windows Server 2012 R2, using an account with domain Administrator privileges. The Server Manager console appears.

1. Open File Explorer, right-click the file or folder you want to audit and, from the context menu, select Properties. The Properties sheet for the file or folder appears.

2. Click the Security tab, and then click Advanced. The *Advanced Security Settings* dialog box appears.
3. Click the Auditing tab.
4. Click Add. The *Auditing Entry* page appears.
5. Click Select a Principal. The *Select User, Computer, Service Account, or Group* dialog box appears. Select the users or groups to be audited for Active Directory object access and click OK. The users or groups appear in the *Auditing Entry* dialog box for the object.
6. From the *Type* drop-down list, specify whether you want to audit failures, successes, or both.
7. From the *Applies to* drop-down list, specify which descendent objects should be audited.
8. Select the basic permissions you want to audit for this object and click OK. The new Auditing entry appears in the *Advanced Security Settings* dialog box.
9. Create additional auditing entries, if desired, and click OK.
10. Click OK to close the object's *Advanced Security Settings* dialog box.
11. Click OK to close the object's Properties sheet.

CLOSE the File Explorer window.

You now configured auditing for files and folders within the Windows operating system.

ASSIGNING USER RIGHTS

The User Rights Assignment settings in Windows Server 2012 R2 are extensive and include settings that pertain to rights users need to perform system-related tasks, as shown in Figure 17-3.

Figure 17-3

User rights assignment settings in a Group Policy object

For example, a user logging on locally to a domain controller must have the Allow Log On Locally right assigned to his or her account or be a member of one of the following AD DS groups:

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

These group memberships enable users to log on locally because Windows Server 2012 R2 assigns the Allow Log On Locally user right to those groups in the Default Domain Controllers Policy GPO by default.

Other similar settings included in this collection are related to user rights associated with system shutdown, taking ownership privileges of files or objects, restoring files and directories, and synchronizing directory service data.

CONFIGURING SECURITY OPTIONS

The Security Options node in a GPO, shown in Figure 17-4, includes security settings related to interactive log on, digital signing of data, restrictions for access to floppy and CD-ROM drives, unsigned driver installation behavior, and logon dialog box behavior.

Figure 17-4

The Security Options node in a GPO

The Security Options category also includes options to configure authentication and communication security within Active Directory through the use of the following settings:

- **Domain controller:** LDAP server signing requirements controls whether LDAP traffic between domain controllers and clients must be signed. This setting can be configured with a value of None or Require signing.
- **Domain member:** Digitally sign or encrypt or sign secure channel data (always) controls whether traffic between domain members and the domain controllers are signed and encrypted at all times.

- **Domain member:** Digitally encrypt secure channel data (when client agrees) indicates that traffic between domain members and the domain controllers is encrypted only if the client workstations are able to do so.
- **Domain member:** Digitally sign secure channel data (when client agrees) indicates that traffic between domain members and the domain controllers is signed only if the client services are able to do so.
- **Microsoft network client:** Digitally sign communications (always) indicates that Server Message Block (SMB) signing is enabled by the SMB signing component of the SMB client at all times.
- **Microsoft network client:** Digitally sign communications (if server agrees) indicates that SMB signing is enabled by the SMB signing component of the SMB client only if the corresponding server service is able to do so.
- **Microsoft network server:** Digitally sign communications (always) indicates that SMB signing is enabled by the SMB signing component of the SMB server at all times.
- **Microsoft network server:** Digitally sign communications (if server agrees) indicates that SMB signing is enabled by the SMB signing component of the SMB server only if the corresponding client service is able to do so.

From this section, you can also enforce the level of NT LAN Manager (NTLM) authentication that is allowed on your network. Although Kerberos is the default authentication protocol in an AD DS network, NTLM authentication is used in certain situations. The original incarnation of NTLM authentication was called LAN Manager (LM) authentication, which is now considered a weak authentication protocol that can easily be decoded by network traffic analyzers. Microsoft has improved NTLM authentication over the years by introducing first NTLM and subsequently NTLMv2.

NTLM authentication levels are controlled by the *Network security: LAN Manager authentication level* security setting, which enables you to select one of the following options:

- Send LM and NTLM responses.
- Send LM and NTLM—use NTLMv2 session security if negotiated.
- Send NTLM response only.
- Send NTLMv2 response only.
- Send NTLMv2 response only. Refuse LM.
- Send NTLMv2 response only. Refuse LM and NTLM.

By allowing only the most stringent levels of NTLM authentication on your network, you can improve the overall communications security of Active Directory.

Using Security Templates

You learned previously how to deploy security and other system configuration settings on a Microsoft Windows network using Group Policy. Windows Server 2012 R2 also includes another mechanism for deploying security configuration settings called security templates.

A ***security template*** is a collection of configuration settings stored as a text file with an .inf extension. Security templates can contain many of the same security parameters as group policy objects. However, security templates present these parameters in a unified interface, enable you to save your configurations as files, and simplify the process of deploying them when and where they are needed.

The settings that you can deploy using security templates include many of the security policies covered in this lesson, including audit policies, user rights assignments, security options, event log policies, restricted groups, and others. By itself, a security template is a convenient way to configure the security of a single system. When you combine it with group policies or scripting, security templates enable you to maintain the security of networks consisting of hundreds or thousands of computers running various Microsoft Windows versions.

Using these tools together, you can create complex security configurations, and mix and match the configurations for each of the various roles computers serve in your organization. When deployed across a network, security templates enable you to implement consistent, scalable, and reproducible security settings throughout the enterprise.

USING THE SECURITY TEMPLATES CONSOLE

Security templates are plain text files that contain security settings in a variety of formats, depending on the nature of the individual settings. For example, many of the security policies are implemented by registry settings, and for these, a template file contains entries such as the following:

```
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
```

Although it is possible to work with security template files directly, by using any text editor, Windows Server 2012 R2 provides a graphical interface that makes the job much easier. To create and manage security templates, you use the Security Templates snap-in for Microsoft Management Console. By default, the Windows Server 2012 R2 Administrative Tools menu does not include an MMC console containing the Security Templates snap-in, so you need to create one by using the MMC Add or Remove Snap-ins dialog box. After you create a new template, the console provides an interface like the one shown in Figure 17-5.

Figure 17-5

The Security Templates snap-in

The left pane of the Security Templates snap-in points to a default folder in which the console stores the template files you create by default. The snap-in interprets any file in this folder with an .inf extension as a security template, even though the extensions do not appear in the console.

When you create a new template in the console, you see a hierarchical display of the policies in the template, as well as their current settings. Many of the policies are identical to those in a GPO, both in appearance and function. You can modify the policies in each template just as you would those in a GPO.

PLANNING A SECURITY TEMPLATE STRATEGY

When planning a security template strategy, think in terms of computer roles, rather than individual computers. It is possible to create a separate template for each computer and customize the settings for that particular computer's needs, but that defeats the purpose of

creating templates in the first place, because it is just as easy to configure each computer manually. By creating templates for specific roles, you can apply them to multiple computers, using combinations in cases where computers perform multiple roles.

CREATING SECURITY TEMPLATES

After the plan for a network's security templates is in place, you can proceed to create the templates. To create a new security template from scratch, use the following procedure.

CREATE A SECURITY TEMPLATE

GET READY. Log on to a Windows computer, using an account with Administrator privileges. The Server Manager console appears.

1. Open the Run dialog box and, in the Open text box, type mmc and click OK. An empty MMC console appears.
2. Click File > Add/Remove Snap-in. The *Add or Remove Snap-ins* dialog box appears.
3. Select Security Templates from the *Available snap-ins* list and click Add. The snap-in appears in the *Add or Remove Snap-ins* dialog box.
4. Click OK. The snap-in appears in the MMC console.
5. Click File > Save As. A *Save As* combo box appears.
6. Type a name for the console, to save it in the Administrative Tools program group.
7. Expand the *Security Templates* node.
8. Right-click the security template search path and, from the context menu, select New Template. A dialog box appears.
9. In the *Template name* field, type a name for the template and click OK. The new template appears in the console.

LEAVE the console open.

When you create a blank security template, there are no policies defined in it. Applying the blank template to a computer has no effect on it whatsoever.

WORKING WITH SECURITY TEMPLATE SETTINGS

Security templates contain many of the same settings as group policy objects, so you are already familiar with some of the elements of a template. For example, security templates contain the same local policy settings described previously; the template is just a different way to configure and deploy the policies. Security templates also provide a means for configuring the permissions associated with files, folders, registry entries, and services.

Security templates have more settings than Local Computer Policy, because a template includes options for both standalone computers and computers that participate in a domain.

Configuring Local Users and Groups

THE BOTTOM LINE

Windows Server 2012 R2 provides two separate interfaces for creating and managing local user accounts: the User Accounts control panel and the Local Users and Groups snap-in for MMC. Both of these interfaces provide access to the same Security Account Manager (SAM) where the user and group information is stored, so any changes you make using one interface will appear in the other.

Microsoft designed the User Accounts control panel and the Local Users and Groups snap-in for computer users with different levels of expertise, and they provide different degrees of access to the Security Account Manager, as follows:

- **User Accounts:** Microsoft designed the User Accounts control panel for relatively inexperienced end users; it provides a simplified interface with limited access to user accounts. With this interface, you can create local user accounts and modify their basic attributes, but you cannot create groups or manage group memberships (except for the Administrators group).
- **Local Users and Groups:** Microsoft includes this MMC snap-in as part of the Computer Management console; it provides full access to local users and groups, as well as all their attributes. Designed more for the technical specialist or system administrator, this interface is not difficult to use, but it does provide access to controls that beginning users generally do not need.

Using the User Accounts Control Panel

Windows Server 2012 R2 creates two local user accounts during the operating system installation process, the Administrator and Guest accounts. The setup program prompts the installer for an Administrator password during the installation, whereas the Guest account is disabled by default.

After the installation process is complete, the system restarts. Because only the Administrator account is available, the computer logs on using that account. This account has administrative privileges, so at this point you can create additional user accounts or modify the existing ones.

CREATING A NEW LOCAL USER ACCOUNT

To create a new user account with the User Accounts control panel, use the following procedure.

CREATE A NEW LOCAL USER ACCOUNT WITH THE CONTROL PANEL

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges. The Server Manager console appears.

1. Open the Control Panel. The Control Panel window appears.
2. Click User Accounts. The User Accounts window appears.
3. Click User Accounts. The *Make changes to your user account* window appears.
4. Click Manage another account. The *Choose the user you would like to change* page appears.
5. Click Add a user account. The *Add a user* page appears.
6. Type a name for the new account in the User name text box, and a password for the account in the Password and Reenter password text boxes.
7. Type a phrase in the Password hint text box and click Next. The system creates the account.
8. Click Finish. The new account appears in the Manage Accounts window.

CLOSE the Manage Accounts window.

By default, this procedure creates standard accounts. To grant a local user administrative capabilities, you must change the account type, by using the interface shown in Figure 17-6.

Figure 17-6

The Change Account Type window

What the User Accounts control panel refers to as an account type is actually a group membership. Selecting the Standard user option adds the user account to the local Users group, whereas selecting the Administrator option adds the account to the Administrators group.

Using the Local Users and Groups Snap-In

The User Accounts control panel provides only partial access to local user accounts, and no access to groups other than the Users and Administrators groups. The Local Users and Groups snap-in, on the other hand, provides full access to all the local user and group accounts on the computer.

By default, the Local Users and Groups snap-in is part of the Computer Management console. However, you can also load the snap-in by itself, or create your own MMC console with any combination of snap-ins.

To create a local user account with the Local Users and Groups snap-in, use the following procedure.

CREATE A NEW LOCAL USER ACCOUNT WITH LOCAL USERS AND GROUPS

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges. The Server Manager console appears.

1. From the Tools menu, select Computer Management. The Computer Management console appears.
2. Expand the Local Users and Groups node and click Users. A list of the current local users appears.

3. Right-click the Users folder and, from the context menu, select New User. The New User dialog box appears, as shown in Figure 17-7.

Figure 17-7

The New User dialog box

4. In the User name text box, type the name you want to assign to the user account. This is the only required field in the dialog box.
5. Specify a Full name and a Description for the account, if desired.
6. In the Password and Confirm password text boxes, type a password for the account, if desired.
7. Select or clear the four checkboxes to control the following functions:
   - User must change password at next logon: forces the new user to change the password after logging on for the first time. Select this option to assign an initial password and enable users to control their own passwords after the first logon. You cannot select this option if you selected the *Password never expires* check box. Selecting this option automatically clears the *User cannot change password* check box.
   - User cannot change password: prevents the user from changing the account password. Select this option if you want to retain control over the account password, such as when multiple users log on with the same user account. This option is also commonly used to manage service account passwords. You cannot select this option if you selected the *User must change password at next logon* check box.
   - Password never expires: prevents the existing password from ever expiring. This option automatically clears the *User must change password at next logon* check box. This option is also commonly used to manage service account passwords.
   - Account is disabled: disables the user account, preventing anyone from using it to log on.
8. Click Create. The new account is added to the user list and the console clears the dialog box, leaving it ready for the creation of another user account.
9. Click Close.

CLOSE the Computer Management console.

CREATING A LOCAL GROUP

To create a local group with the Local Users and Groups snap-in, use the following procedure.

CREATE A LOCAL GROUP

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges. The Server Manager console appears.

1. From the Tools menu, select Computer Management. The Computer Management console appears.
2. Expand the Local Users and Groups node and click Groups. A list of local groups appears.
3. Right-click the Groups folder and then, from the context menu, select New Group. The New Group dialog box appears.
4. In the Group name text box, type the name you want to assign to the group. This is the only required field in the dialog box. If desired, specify a Description for the group.
5. Click the Add button. The Select Users dialog box appears.
6. Type the names of the users that you want to add to the group, separated by semicolons, in the text box, and then click OK. The users are added to the Members list. You can also type part of a user name and click Check Names to complete the name or click Advanced to search for users.
7. Click Create to create the group and populate it with the user(s) you specify. The console clears the dialog box, leaving it ready for the creation of another group.
8. Click Close.

CLOSE the Computer Management console.

Local groups have no user-definable attributes other than a members list, so you only can add or remove members when you open an existing group. As noted previously, local groups cannot have other local groups as members. If the computer is a member of a Windows domain, a local group can have domain users and domain groups as members.

Configuring User Account Control

THE BOTTOM LINE

One of the most common Windows security problems arises from the fact that many users perform their everyday computing tasks with more system access than they need. Logging on as Administrator or user that is a member of the Administrators group grants the user full access to all areas of the operating system. This degree of system access is not necessary to run many of the applications and perform many of the tasks users require every day; it is needed only for certain administrative functions, such as installing system-wide software or configuring system parameters.

For most users, logging on with administrative privileges all the time is simply a matter of convenience. Microsoft recommends logging on as a standard user, and to use administrative privileges only when you need them. However, many technical specialists who do this frequently find themselves encountering situations in which they need administrative access. There is a surprisingly large number of common, and even mundane, Windows tasks that require administrative access, and the inability to perform the tasks can negatively affect a user's productivity.

Microsoft addressed this problem by keeping all Windows Server 2012 R2 users from accessing the system using administrative privileges unless the privileges are required to perform the task at hand. The mechanism that does this is called ***User Account Control (UAC)***.

Configuring User Account Control Settings

Windows Server 2012 R2 enables User Account Control by default, but it is possible to configure its properties, or even disable it completely.

In Windows Server 2012 R2, four UAC settings are available through the Control Panel. To configure UAC through the Control Panel, use the following procedure.

CONFIGURE UAC SETTINGS

GET READY. Log on to Windows Server 2012 R2, using an account with Administrator privileges. The Server Manager console appears.

1. Open the Control Panel. The Control Panel window appears.
2. Click System and Security > Action Center. The Action Center window appears.
3. Click Change User Account Control settings. The *User Account Control Settings* dialog box appears, as shown in Figure 17-8.

Figure 17-8

The User Account Control Settings dialog box

4. Adjust the slider to one of the following settings and click OK.
   - Always notify me
   - Notify me only when programs try to make changes to my computer
   - Notify me only when programs try to make changes to my computer (do not dim my desktop)
   - Never notify me

CLOSE the Action Center window.

Although the Control Panel provides some control over UAC, the most granular control over UAC properties is still through the Security Options node in Group Policy and Local Security Policy.

Business Case Scenarios

Scenario 17-1: Understanding Group Policy Planning

You are the administrator for Coho Winery, Inc. a large wine distribution company that has locations in the United States and Canada. In the last six months, Coho Winery, Inc. has purchased several smaller distribution companies. As you integrate them into your forest, you want to allow them to remain autonomous in their management of desktops and security. In the process of making their domains part of your corporate network, you have some policies that you want to become part of their environment, and others that you do not want to implement at this time. As you discuss this with your IT team, your manager asks you to explain which features in Windows Server 2012 R2 enable you to provide the Group Policy flexibility needed by the new Active Directory structure. List several of the features in Windows Server 2012 R2 Group Policy that will enable Coho Winery, Inc. to achieve its postacquisition goals.

Scenario 17-2: Deploying Security Templates

You are a network administrator planning a security template deloyment on a network that consists of 100 workstation. The workstations are all running various versions of Microsoft Windows, broken down as follows:

- Windows 7: 30 workstations
- Windows XP Professional: 40 workstations
- Windows XP Home Edition: 20 workstations
- Windows 2000 Professional: 10 workstations

In the past, some computers on the network have been compromised because end users modified their workstation security configurations. Your task is to deploy your security templates on the workstations in such a way that end users cannot modify them. To accomplish this goal, you decide to use Group Policy to deploy the templates to an Active Directory Domain Services OU object that contains all of the workstations.
Based on the information provided, answer the following questions.

1. How many of the workstations cannot receive their security template settings from a GPO linked to an AD DS container?

2. Which of the following methods can you use to deploy your security templates on the workstations that do not support Group Policy, while still accomplishing your assigned goals?
   a. Upgrade all of the computers that do not support Group Policy to Windows 7.
   b. Run the Security Templates snap-in on each computer and load the appropriate security template.
   c. Create a logon script that uses Secedit.exe to import the security template on each computer.
   d. Run the Security Configuration and Analysis snap-in on each computer and use it to import the appropriate security template.

Configuring Application Restriction Policies

LESSON 18

Installing Software with Group Policy

THE BOTTOM LINE

You can use Group Policy to install, upgrade, patch, or remove software applications when a computer starts, when a user logs on to the network, or when a user accesses a file associated with an application that is not currently on the user's computer.

In addition, you can use Group Policy to fix problems associated with applications. For example, if a user inadvertently deletes a file from an application, Group Policy can launch a repair process that will fix the application. To perform these tasks, Group Policy works together with the Windows Installer Service.

Windows Server 2012 R2 uses the Windows Installer with Group Policy to install and manage software that is packaged into Microsoft Installer files, with an .msi extension.

Windows Installer consists of two components: one for the client-side and another for the server-side. The client-side component is called the *Windows Installer Service*. This client-side component is responsible for automating the installation and configuration of the designated software.

The Windows Installer Service requires a package file that contains all the pertinent information about the software. This package file consists of the following information:

- An ***.msi file***, which is a relational database file that is copied to the target computer system, with the program files it deploys. In addition to providing installation information, this database file assists in the ***self-healing*** process for damaged applications and clean application removal.
- External source files that are required for software installation or removal.
- Summary information about the software and the package.
- A reference point to the path where the installation files are located.

To install software by using Group Policy, you must have Windows Installer–enabled applications. An application that has an approval stamp from Microsoft on its packaging, including the Certified for Windows Server 2012 R2 logo, is Windows Installer–enabled by default. This means the application provides support for Group Policy deployments using an .msi file.

At times, you might need to modify Windows Installer files to better suit the needs of your network. Modifications to .msi files require transform files, which have an .mst extension.

Windows Installer files with the .msp extension serve as patch files. You use ***patch files*** to apply service packs and hotfixes to installed software. Unlike an .msi file, a patch package does not include a complete database. Instead, it contains, at minimum, a database transform procedure that adds patching information to the target installation package database. For this reason, .msp files should be located in the same folder as the original .msi file when you want the patch to be applied as part of the Group Policy software installation.

■ Configuring Software Restriction Policies

THE BOTTOM LINE

The options in the Software Restriction Policies node provide organizations greater control in preventing potentially dangerous applications from running. Software restriction policies are designed to identify software and control its execution. In addition, you can control who is affected by the policies.

The *Software Restriction Policies* node is found in the *Windows Settings\Security Settings* node of the *User Configuration or the Computer Configuration* node of a Group Policy object. By default, the Software Restriction Policies folder is empty. When you create a new policy, two subfolders appear: Security Levels and Additional Rules, as shown in Figure 18-1. The *Security Levels* folder enables you to define the default behavior from which all rules are created. The criteria for each executable program are defined in the Additional Rules folder.

Figure 18-1

The Software Restriction Policies folder

Enforcing Restrictions

Prior to creating any rules that govern the restriction or allowance of executable files, you should understand how the rules work by default. If a policy does not enforce restrictions, executable files run based on the permissions that users or groups have in the NTFS file system.

When considering software restriction policies, you must determine your approach to enforcing restrictions. You can use three basic strategies for enforcing restrictions, as follows:

- **Unrestricted:** enables all applications to run, except those that are specifically excluded.
- **Disallowed:** prevents all applications from running except those that are specifically allowed.
- **Basic User:** prevents any application from running that requires administrative rights, but enables programs to run that only require resources that are accessible by normal users.

The approach you take depends on the needs of your particular organization. By default, the Software Restriction Policies area has an Unrestricted value in the Default Security Level setting.

To modify the *Default Security Level* setting to *Disallowed*, use the following procedure.

MODIFY THE DEFAULT SECURITY LEVEL

GET READY. Log on to a server running Windows Server 2012 R2, using an account with domain Administrator privileges.

1. From the Tools menu in the *Server Manager* console, select Group Policy Management. The *Group Policy Management* console appears.
2. Expand the forest container and browse to your domain. Then expand the domain container and select the Group Policy Objects folder. The GPOs that currently exist in the domain appear in the *Contents* tab.
3. Right-click a GPO and click Edit. A *Group Policy Management Editor* window appears.
4. Browse to the Software Restriction Policies node under either Computer Configuration or User Configuration.
5. Right-click Software Restriction Policies and select New Software Restriction Policies. The folders containing the new policies appear.
6. In the details pane, double-click Security Levels. Note the checkmark on the *Unrestricted* icon, which is the default setting.
7. Right-click the Disallowed security level and, from the context menu, select Set As Default. A *Software Restriction Policies* warning message box appears, informing you of the consequences of more restrictive policies.

CLOSE the *Group Policy Management Editor* and *Group Policy Management* consoles.

You have now modified the Default Security Level for a software restriction policy.

Configuring Software Restriction Properties

Within the *Software Restriction Policies* folder, you can configure three specific properties to provide additional settings that apply to all policies when implemented.

These three properties are enforcement, designated file types, and trusted publishers, as described in the following sections.

ENFORCEMENT

As shown in Figure 18-2, Enforcement properties enable you to determine whether the policies apply to all files or whether library files, such as Dynamic Link Library (DLL), are excluded. Excluding DLLs is the default, which is the most practical method of enforcement. For example, if the *Default Security Level* for the policy is set to *Disallowed* and the *Enforcement* properties are set to *All Software Files*, you would need to create a rule that checked every DLL before the program could be allowed or denied. By contrast, excluding DLL files using the default Enforcement property does not require you to define individual rules for each DLL file.

Figure 18-2

Configuring Enforcement properties

DESIGNATED FILE TYPES

The Designated File Types properties within the Software Restriction Policies folder, specify file types that are executable. File types that are designated as executable or program files are shared by all rules, although you can specify a list for a computer policy that is different from one that is specified for a user policy.

TRUSTED PUBLISHERS

Finally, the Trusted Publishers properties enable you to control how systems handle certificate rules. In the Properties dialog box for Trusted Publishers, as shown in Figure 18-3, the first setting enables you to specify which users are permitted to manage trusted certificate sources. By default, local computer administrators have the right to specify trusted publishers on the local computer and enterprise administrators have the right to specify trusted publishers in an OU. From a security standpoint, in a high-security network, users should not be allowed to determine the sources from which certificates can be obtained.

Figure 18-3

Configuring Trusted Publishers properties

In addition, the Trusted Publisher Properties sheet also lets you verify that a certificate has not been revoked. If a certificate has been revoked, the user should not be permitted access to network resources. You have the option of checking either the *Publisher* or the *Timestamp* of the certificate to determine whether it has been revoked.

Using AppLocker

THE BOTTOM LINE

Software restriction policies can be a powerful tool, but they can also require a great deal of administrative overhead. If you elect to disallow all applications except those matching the rules you create, there are a great many programs in Windows Server 2012 R2 that need rules, in addition to the applications you want to install. You must also create the rules manually, which can be an onerous chore.

AppLocker, also known as ***application control policies***, is a Windows feature that is essentially an updated version of the concept implemented in software restriction policies. AppLocker also uses rules, which you must manage, but the process of creating the rules is much easier, thanks to a wizard-based interface.

AppLocker is also more flexible than software restriction policies. You can apply AppLocker rules to specific users and groups and also create rules that support all future versions of an application. The primary disadvantage of AppLocker is that you can apply only the policies to computers running Windows 7 and Windows Server 2008 R2 or later.

Understanding Rule Types

The AppLocker settings are located in Group Policy objects in the Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker container, as shown in Figure 18-4.

Figure 18-4

The AppLocker container in a GPO

In the AppLocker container, four nodes contain the basic rule types, as follows:

- **Executable Rules:** contains rules that apply to files with .exe and .com extensions.
- **Windows Installer Rules:** contains rules that apply to Windows Installer packages with .msi and .msp extensions.
- **Script Rules:** contains rules that apply to script files with .ps1, .bat, .cmd, .vbs, and .js extensions.
- **Packaged app Rules:** contains rules that apply to applications purchased through the Windows Store.

Each of the rules you create in each of these containers can allow or block access to specific resources, based on one of the following criteria:

- **Publisher:** identifies code-signed applications by means of a digital signature extracted from an application file. You can also create publisher rules that apply to all future versions of an application.
- **Path:** identifies applications by specifying a file or folder name. The potential vulnerability of this type of rule is that any file can match the rule, as long as it is the correct name or location.
- **File Hash:** identifies applications based on a digital fingerprint that remains valid even when the name or location of the executable file changes. This type of rule functions much like its equivalent in software restriction policies; in AppLocker, however, the process of creating the rules and generating file hashes is much easier.

Creating Rules Automatically

The greatest advantage of AppLocker over software restriction policies is the capability to create rules automatically.

When you right-click one of the three rules containers and select *Create Rules Automatically* from the context menu, an *Automatically Generate Rules Wizard* appears, as shown in Figure 18-5.

Figure 18-5

The Automatically Generate Executable Rules Wizard

After specifying the folder to be analyzed and the users or groups to which the rules should apply, a *Rule Preferences* page appears, enabling you to specify the types of rules you want to create.

The wizard then displays a summary of its results in the *Review Rules* page, as shown in Figure 18-6, and adds the rules to the container.

Figure 18-6

The Review Rules page of the Automatically Generate Executable Rules Wizard

Creating Rules Manually

In addition to creating rules automatically, you can also do it manually, using a wizard-based interface you activate by selecting *Create New Rule* from the context menu for one of the three rule containers.

The wizard prompts you for the following information:

- **Action:** specifies whether you want to allow or deny the user or group access to the resource. In AppLocker, explicit deny rules always override allow rules.
- **User or group:** specifies the name of the user or group to which the policy should apply.
- **Conditions:** specifies whether you want to create a publisher, path, or file hash rule. The wizard generates an additional page for whichever option you select, enabling you to configure its parameters.
- **Exceptions:** enables you to specify exceptions to the rule you create, using any of the three conditions: publisher, path, or file hash.

■ Business Case Scenarios

Scenario 18-1: Planning Group Policy Software Deployments

Your company, a healthcare organization, is currently working toward compliance with new government standards on patient confidentiality. Your IT department has decided that using software restriction policies with standard user access permissions will help to fulfill the necessary security requirements. You are preparing an implementation plan that is based on user needs and security requirements. Users should not be able to access any programs with the exception of those that are pertinent to their jobs. In addition, the user needs within the organization are as follows:

- Users only need access to e-mail and a patient database.
- The patient database has its own built-in security access system that is configured for each user based on the user's needs within the program.
- All user accounts are located in containers based on the user's office location.

In addition, the following points should be considered in your implementation plan:

- Software restriction policy settings should not affect settings that are already in place within existing GPOs. If problems arise with software restriction policies, they should be easy to rectify, without affecting other security areas.
- Administrator accounts should not be affected by software restrictions.
- Other applications should not be affected by any of the restrictions.

List the key points that should be part of your implementation plan based on the information provided here.

Scenario 18-2: Using AppLocker

Sophie is planning on using AppLocker to control access to applications on a new network she has constructed for the Research and Development department at a major aerospace firm. The software developers in the department have recently deployed a new application called Virtual Wind Tunnel, which is based on government project research and is therefore classified. All of the full-time personnel have sufficient clearance to use the application, but the interns in the department do not. Sophie has placed the user accounts for everyone in the department into a security group called ResDev. The interns are also members of a group called RDint.

How can Sophie use AppLocker to provide everyone in the department with access to the Virtual Wind Tunnel application without changing the group memberships and without having to apply policies to individual users?

19 LESSON

Configuring Windows Firewall

Building a Firewall

THE BOTTOM LINE

You may have locked the door to the computer center in which the servers are located, but the computers are still connected to the network. A network is another type of door, or rather a series of doors, which can allow data out or allow it in. To provide services to your users, some of the doors must be open at least some of the time, but server administrators must make sure that only the right doors are left open.

A ***firewall*** is a software program that protects a computer or a network by allowing certain types of network traffic in and out of the system while blocking others. A firewall is essentially a series of filters that examine the contents of packets and the traffic patterns to and from the network to determine which packets they should allow to pass through the filter.

Some of the hazards that firewalls can protect against are as follows:

- Network scanner applications that probe systems for unguarded ports, which are essentially unlocked doors that attackers can use to gain access to the system.
- Trojan horse applications that open a connection to a computer on the Internet, enabling an attacker on the outside to run programs or store data on the system.
- Attackers that obtain passwords by illicit means, such as social engineering, and then use remote access technologies to log on to a computer from another location and compromise its data and programming.
- Denial of service attacks that use authorized access points to bombard a system with traffic, preventing legitimate traffic from reaching the computer.

The object of a firewall is to permit all the traffic in and out that legitimate users need to perform their assigned tasks, and block everything else. When you work with firewalls, you are not concerned with subjects such as authentication and authorization. These are mechanisms that control who is able to get through the server's open doors. The firewall is all about which doors are left open, and which doors are shut tight.

Understanding Windows Firewall Settings

Windows Server 2012 R2 includes a firewall program called *Windows Firewall*, which is activated by default on all systems.

By default, Windows Firewall blocks most network traffic from entering the computer. Firewalls examine the contents of each packet entering and leaving the computer and comparing the information they find to a series of rules, which specify which packets are allowed to pass through the firewall and which are blocked.

The TCP/IP (Transmission Control Protocol/Internet Protocol) protocols that Windows systems use to communicate function by packaging application data using a series of layered protocols that define where the data comes from and where it is going. The three most important criteria that firewalls can use in their rules are as follows:

- **IP addresses:** identify specific hosts on the network. You can use IP addresses to configure a firewall to allow only traffic from specific computers or networks in and out.
- **Protocol numbers:** specify whether the packet contains TCP or UDP (User Datagram Protocol) traffic. You can filter protocol numbers to block packets containing certain types of traffic. Windows computers typically use UDP for brief message exchanges, such as DNS (Domain Name System) and DHCP (Dynamic Host Configuration Protocol) transactions. TCP packets usually carry larger amounts of data, such as the files exchanged by web, file, and print servers.
- ***Port numbers*:** identify specific applications running on the computer. The most common firewall rules use port numbers to specify the types of application traffic the computer is allowed to send and receive. For example, a web server usually receives its incoming packets to port number 80. Unless the firewall has a rule opening port 80 to incoming traffic, the web server cannot function in its default configuration.

Firewall rules can function in two ways:

- Admit all traffic, except that which conforms to the applied rules
- Block all traffic, except that which conforms to the applied rules

Generally speaking, blocking all traffic by default is the more secure arrangement. From the server administrator's standpoint, you start with a completely blocked system, and then test your applications. When an application fails to function properly because network access is blocked, you create a rule that opens up the ports the application needs to communicate.

This is the method that Windows Firewall uses by default for incoming network traffic. There are default rules preconfigured into the firewall that are designed to admit the traffic used by standard Windows networking functions, such as file and printer sharing. For outgoing network traffic, Windows Firewall uses the other method, allowing all traffic to pass the firewall except that which conforms to a rule.

Using the Windows Firewall Control Panel

THE BOTTOM LINE

The Windows Firewall control panel provides the easiest and safest access to the firewall controls. These controls are usually sufficient for most server administrators, unless the system has special requirements or you work with custom server applications.

When you open the *Windows Firewall* window from the *Control Panel*, as shown in Figure 19-1, you see the following information:

- Whether the computer is connected to a domain, private, or public network
- Whether the Windows Firewall service is currently turned on or off
- Whether inbound and outbound connections are blocked
- The name of the currently active network
- Whether users are notified when a program is blocked

Figure 19-1

The Windows Firewall control panel window

On the left side of the window is a series of links, which provide the following functions:

- **Allow an app or feature through Windows Firewall:** displays the Allowed apps dialog box, in which you can select the applications that can send traffic through the firewall.
- **Change notification settings:** displays the Customize settings dialog box, in which you can adjust the notification settings for each of the three profiles.
- **Turn Windows Firewall on or off:** displays the Customize settings dialog box, in which you can toggle the state of the firewall in each of the three profiles.
- **Restore defaults:** returns all firewall settings to their installation defaults.
- **Advanced settings:** launches the Windows Firewall with Advanced Security console.
- **Troubleshoot my network:** launches the Network and Internet troubleshooter.

Allowing Applications

Sometimes, administrators might be required to modify the firewall settings in other ways, typically because a specific application requires access to a port not anticipated by the firewall's default rules.

To do this, you can use the Allowed Apps dialog box in the Windows Firewall control panel, as shown in Figure 19-2.

Figure 19-2

The Allowed Apps dialog box for Windows Firewall

Opening a port in a server's firewall is an inherently dangerous activity. The more open doors you put in a wall, the more opportunities that intruders can exploit to get in. Windows Firewall provides two basic methods for opening a hole in your firewall: opening a port and allowing an application. Both are risky, but the latter of the two is less so. This is because when you open a port by creating a rule in the Windows Firewall with Advanced Security console, the port stays open permanently. When you allow an application through the firewall using the Control Panel, the specified port is open only while the program is running. When you terminate the program, the firewall closes the port.

To allow an application through the firewall by using Control Panel, use the following procedure.

ALLOW AN APPLICATION

GET READY. Log on to a server running Windows Server 2012 R2, using an account with domain administrator privileges.

1. In the *Server Manager* console, open the Control Panel and click System and Security > Windows Firewall. The *Windows Firewall* window appears.
2. Click Allow an app or feature through Windows Firewall. The *Allowed Apps* dialog box appears.
3. Scroll down in the Allowed apps and features list and select the check box for the application you want to allow through the firewall.
4. Click OK to close the *Allowed Apps* dialog box.

CLOSE the *Windows Firewall* window.

The applications listed on the Allowed Apps dialog box are based on the roles and features installed on the server. Each listed application corresponds to one or more firewall rules, which the Control Panel activates and deactivates as needed.

Unlike earlier versions, the Windows Server 2012 and Windows Server 2012 R2 versions of the Windows Firewall control panel do not provide direct access to port numbers. For more precise control over the firewall, you must use the *Windows Firewall with Advanced Security* console, which you can access by clicking the *Advanced Settings* link in the *Windows Firewall* control panel, or by selecting it from the *Tools* menu in *Server Manager*.

■ Using the Windows Firewall with Advanced Security Console

THE BOTTOM LINE

The Windows Firewall control panel is designed to enable administrators and advanced users to manage basic firewall settings. For full access to the Windows Firewall configuration settings, you must use the *Windows Firewall With Advanced Security* snap-in for the *Microsoft Management* console.

To open the console, open *Server Manager* and, from the *Tools* menu, select *Windows Firewall With Advanced Security*. The *Windows Firewall with Advanced Security* console appears, as shown in Figure 19-3.

Figure 19-3

The *Windows Firewall with Advanced Security* console

Configuring Profile Settings

At the top of the Windows Firewall With Advanced Security console's middle pane, in the Overview section, are status displays for the computer's three network location profiles. If you connect the computer to a different network (which is admittedly not likely with a server), Windows Firewall can load a different profile and a different set of rules.

The default Windows Firewall configuration calls for the same basic settings for all three profiles, as follows:

- The firewall is turned on.
- Incoming traffic is blocked unless it matches a rule.
- Outgoing traffic is allowed unless it matches a rule.

You can change this default behavior by clicking the *Windows Firewall Properties* link, which displays the *Windows Firewall With Advanced Security On Local Computer* dialog box, as shown in Figure 19-4.

In this dialog box, each of the three network location profile has a tab with identical controls that enables you to modify the default profile settings. You can, for example, configure the firewall to shut down completely when it is connected to a domain network, and turn the firewall on with its most protective settings when you connect the computer to a public network. You can also configure the firewall's notification options, its logging behavior, and how it reacts when rules conflict.

Figure 19-4

The *Windows Firewall with Advanced Security on Local Computer* dialog box

Creating Rules

The allowed applications that you can configure in the Windows Firewall control panel are a relatively friendly method for working with firewall rules. In the Windows Firewall With Advanced Security console, you can work with the rules in their raw form.

Selecting either *Inbound Rules* or *Outbound Rules* in the left pane displays a list of all the rules operating in that direction, as shown in Figure 19-5. The rules that are currently operational have a check mark in a green circle, whereas the rules not in force are grayed out.

Figure 19-5

The Inbound Rules list in the Windows Firewall with Advanced Security console

Creating new rules with this interface provides more flexibility than the Windows Firewall control panel. When you right-click the *Inbound Rules* (or *Outbound Rules*) node and select *New Rule* from the context menu, the *New Inbound* (or *Outbound*) *Rule Wizard* takes you through the process of configuring the following sets of parameters:

- **Rule Type:** specifies whether you want to create a program rule, a port rule, a variant on one of the predefined rules, or a custom rule. This selection determines which of the following pages the wizard displays.
- **Program:** specifies whether the rule applies to all programs, to one specific program, or to a specific service. This is the equivalent of defining an allowed application in the Windows Firewall control panel, except that you must specify the exact path to the application.
- **Protocol and Ports:** specifies the network or transport layer protocol and the local and remote ports to which the rule applies. This enables you to specify the exact types of traffic that the rule should block or allow. To create rules in this way, you must be familiar with the protocols and ports that an application uses to communicate at both ends of the connection.
- **Predefined Rules:** specifies which predefined rules defining specific network connectivity requirements the wizard should create.
- **Scope:** specifies the IP addresses of the local and remote systems to which the rule applies. This enables you to block or allow traffic between specific computers.
- **Action:** specifies the action the firewall should take when a packet matches the rule. You configure the rule to allow traffic if it is blocked by default, or block traffic if it is allowed by default. You can also configure the rule to allow traffic only when the connection between the communicating computers is secured using IPsec.
- **Profile:** specifies the profile(s) to which the rule should apply: domain, private, and public.
- **Name:** specifies a name and (optionally) a description for the rule.

The rules you can create by using the wizards range from simple program rules, just like those you can create in the Windows Firewall control panel, to highly complex and specific rules that block or allow only specific types of traffic between specific computers. The more complicated the rules become, however, the more you need to know about TCP/IP communications in general and the specific behavior of your applications. Modifying the default firewall settings to accommodate some special applications is relatively simple, but creating an entirely new firewall configuration is a formidable task.

Importing and Exporting Rules

The process of creating and modifying rules in the Windows Firewall with Advanced Security console can be time-consuming, and repeating the process on multiple computers even more so. Therefore, the console makes it possible for you to save the rules and settings you create by exporting them to a policy file.

A policy file is a file with a .wfw extension that contains all the property settings in a Windows Firewall installation, as well as all of its rules, including the preconfigured rules and the ones you created or modified. To create a policy file, use the following procedure.

EXPORT WINDOWS FIREWALL RULES

GET READY. Log on to a server running Windows Server 2012 R2, using an account with domain administrator privileges.

1. In the *Server Manager* console, select *Windows Firewall With Advanced Security* from the Tools menu. The *Windows Firewall with Advanced Security* console appears.
2. Modify the inbound or outbound firewall rules or create new rules as needed.
3. In the left pane, select the Windows Firewall with Advanced Security on Local Computer node.
4. From the Action menu, select Export Policy. The Save As combo box appears.
5. In the File Name text box, type a name for the policy file and click Save.

CLOSE the Windows Firewall With Advanced Security console.

You can then duplicate the rules and settings on another computer by copying the file and using the *Import Policy* function to read in the contents, as in the following procedure.

IMPORT WINDOWS FIREWALL RULES

GET READY. Log on to a server running Windows Server 2012 R2, using an account with domain administrator privileges.

1. In the *Server Manager* console, select *Windows Firewall With Advanced Security* from the Tools menu. The *Windows Firewall with Advanced Security* console appears.
2. From the *Action* menu, select Import Policy. A message box appears, warning that importing a policy file will overwrite all existing firewall rules.
3. Click Yes. An *Open* combo box appears.
4. Locate and select the policy file you want to import and click Open.

5. A message box appears, stating that the policy was successfully imported.
6. Click OK.

CLOSE the Windows Firewall With Advanced Security console.

Creating Rules Using Group Policy

The Windows Firewall with Advanced Security console makes it possible to create complex firewall configurations, but Windows Firewall is still an application designed to protect a single computer from intrusion. If you have a large number of servers running Windows Server 2012 R2, manually creating a complex firewall configuration on each one can be a lengthy process. Therefore, as with most Windows configuration tasks, administrators can distribute firewall settings to computers throughout the network by using Group Policy.

When you edit a Group Policy object (GPO) and browse to the *Computer Configuration\Policies\Windows Settings\Security Settings\ Windows Firewall with Advanced Security* node, you see an interface, shown in Figure 19-6, which is similar to the Windows Firewall with Advanced Security console.

Figure 19-6

The *Windows Firewall with Advanced Security* node in a Group Policy object

You can configure Windows Firewall properties and create inbound, outbound, and connection security rules, just as you would in the console. The difference is that you can then deploy these settings to computers anywhere on the network by linking the GPO to Active Directory Domain Services object.

When you open a new GPO, the Windows Firewall with Advanced Security node contains no rules at all. The preconfigured rules that you find on every computer running Windows Server 2012 R2 are not there. You can create new rules from scratch to deploy to the network, or you can import settings from a policy file, just as you can in the Windows Firewall with Advanced Security console.

Group Policy does not overwrite the entire Windows Firewall configuration, as importing a policy file does. When you deploy firewall rules and settings by using Group Policy, the rules in the GPO are combined with the existing rules on the target computers. The only exception is when you deploy rules with the same names as existing rules. Then, the GPO settings overwrite these found on the target computers.

Creating Connection Security Rules

Windows Server 2012 R2 also includes a feature that incorporates IPsec data protection into the Windows Firewall. The IP Security (IPsec) standards are a collection of documents that define a method for securing data while it is in transit over a TCP/IP network. IPsec includes a connection establishment routine, during which computers authenticate each other before transmitting data, and a technique called ***tunneling***, in which data packets are encapsulated within other packets, for their protection.

In addition to inbound and outbound rules, the Windows Firewall With Advanced Security console enables you to create connection security rules, by using the New Connection Security Rule Wizard. Connection security rules define the type of protection you want to apply to the communications that conform to Windows Firewall rules.

When you right-click the *Connection Security Rules* node and select *New Rule* from the context menu, the *New Connection Security Rule Wizard* takes you through the process of configuring the following sets of parameters:

- **Rule Type:** specifies the basic function of the rule, such as to isolate computers based on authentication criteria, to exempt certain computers (such as infrastructure servers) from authentication, to authenticate two specific computers or groups of computers, or to tunnel communications between two computers. You can also create custom rules combining these functions.
- **Endpoints:** specifies the IP addresses of the computers that establish a secured connection before transmitting any data.
- **Requirements:** specifies whether authentication between two computers should be requested or required. If required, options include requiring authentication for inbound connections only or for both inbound and outbound connections.
- **Authentication Method:** specifies the type of authentication the computers should use when establishing a connection.
- **Profile:** specifies the profile(s) to which the rule should apply: domain, private, and public.
- **Name:** specifies a name and (optionally) a description for the rule.

■ Business Case Scenarios

Scenario 19-1: Configuring Windows Firewall

Ralph is a junior network administrator at Wingtip Toys, left in change of the IP department while everyone else is out of town at a conference. Ralph receives a call from the company's best customer, reporting that they are unable to place orders through the company's website. Ralph examines the logs for the Windows web server and notices a huge amount of incoming traffic that began that morning.

Ralph suspects that the server is the target of a denial of service (DoS) attack, but he doesn't have access to the network firewall, nor does he know anything about the firewall configuration his company uses. Ralph does have access to the Windows Firewall running on the web server, however. What temporary modifications can he make to that firewall to block the attack and allow the customer to submit orders as they normally do?

Scenario 19-2: Configuring Firewall Rules to Require IPsec Encryption

Alice is responsible for the file server where all of the company payroll and accounting data is stored, and as a result, security is one of her primary concerns. To prevent potential intruders from intercepting sensitive data in transit over the network, Alice wants to ensure that all of the company bookkeepers and accountants use IPsec to encrypt their traffic as they access the financial spreadsheets stored on the server.

Alice has located the inbound firewall rules on the server that enable users to access files using their spreadsheet application. How can she modify those rules to permit access only under the following conditions:

- The user must be a member of the Accounting group.
- The user must be using a computer on the company subnet.
- The user must connect using IPsec encryption.

Microsoft

Introducing Windows Server 2012 R2

Technical Overview

Mitch Tulloch with the Windows Server team

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

Copyright © 2013 Microsoft Corporation

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: 2013945007
ISBN: 978-0-7356-8278-8

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/about/legal/en/us/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
Project Editors: Valerie Woolley and Carol Dillingham
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Copyeditor: Andrew Jones
Indexer: Jean Skipp

Contents

Introduction *ix*

Chapter 1 Cloud OS **1**

The big picture 1

Journey to the Cloud OS 2

Let's begin! 3

Chapter 2 Hyper-V **5**

Previous enhancements to Hyper-V 5

Generation 2 virtual machines 7

Automatic Virtual Machine Activation 11

Remote access over VMBus 12

Cross-version live migration 14

Faster live migration 16

Online VHDX resize 17

Live export 18

More robust Linux support 20

Managing Hyper-V hosts running previous versions of Windows Server 21

Hyper-V Replica enhancements 21

Additional Hyper-V improvements 25

Learn more 25

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:

microsoft.com/learning/booksurvey

Chapter 3 Storage **27**

Previous enhancements to storage 27

Microsoft's vision for storage 29

Building the solution using Windows Server 2012 R2 29

Enabling the solution using System Center 2012 R2 31

Storage Management API 32

Storage QoS 33

iSCSI Target Server enhancements. 34

SMB 3.0 enhancements 36

Data deduplication enhancements 38

Storage Spaces enhancements 39

Storage Spaces in Windows Server 2012 41

Storage Spaces in Windows Server 2012 R2 42

Work Folders 50

Learn more 60

Chapter 4 Failover Clustering **63**

Previous enhancements to Failover Clustering 63

Guest clustering using shared virtual disks 64

Hosting highly available workloads 64

Separating virtual resources from physical infrastructure 65

Understanding shared virtual disks 67

Using shared virtual disks 69

CSV and SoFS enhancements 70

Failover Clustering and SoFS 70

Optimized ownership of CSV disks 71

Increased CSV resiliency 72

Improved CSV cache allocation 73

CSV and other storage features 73

Changes to heartbeat threshold 74
Detecting the health of virtual machines 75
Virtual machine drain on shutdown 78
Dynamic witness 81
Active Directory-detached clustering 82
Learn more 82

Chapter 5 Networking 85

Previous enhancements to networking 85
Virtual RSS 88
Windows NIC Teaming enhancements 90
NIC Teaming in Windows Server 2012 91
NIC Teaming in Windows Server 2012 R2 92
Choosing the right teaming mode 94
Choosing the right load-balancing mode 95
Improved network diagnostics 96
Network diagnostic cmdlets in Windows Server 2012 97
Network diagnostic cmdlets in Windows Server 2012 R2 102
IPAM enhancements 105
IPAM in Windows Server 2012 107
IPAM in Windows Server 2012 R2 107
Hyper-V Network Virtualization enhancements 112
How Hyper-V Network Virtualization works 113
Hyper-V Network Virtualization enhancements in Windows Server 2012 R2 115
Hyper-V Virtual Switch enhancements 119
Hyper-V Virtual Switch in Windows Server 2012 119
Hyper-V Virtual Switch in Windows Server 2012 R2 121
Learn more 121

Chapter 6 Active Directory 123

Previous enhancements to Active Directory 124

Workplace Join 125

Implementing Workplace Join 126

Multi-factor access control 127

Web Application Proxy 127

Implementing Web Application Proxy 128

Improved LDAP search performance. 131

Learn more 136

Chapter 7 Group Policy 137

Previous enhancements to Group Policy 137

Group Policy caching 138

Group Policy Preferences and IPv6 139

New policy settings 142

Start screen 142

Multi-monitor display 143

Apps 144

Sync your settings 145

Work Folders 145

Kerberos authentication 146

Logon scripts 148

Windows Update 149

Windows Runtime apps 149

Microsoft accounts 150

Automatic sign-in 150

Windows SkyDrive 151

Learn more 152

Chapter 8 IIS **153**

Previous enhancements to IIS 153

Dynamic Site Activation 155

Idle Worker Process Page-out 156

Custom IIS logging fields 158

IIS ETW logging 159

Learn more 162

Chapter 9 Remote Desktop Services **165**

Previous RDS enhancements 165

Improved RemoteApp experience 167

DX11.1 support 168

Improved video experience 169

Seamless display handling 169

Quick Reconnect 169

Session Shadowing 170

VDI and data deduplication 172

Restricted Admin mode 173

Learn more 173

Chapter 10 Windows PowerShell **175**

Previous enhancements in Windows PowerShell 3.0 175

Windows PowerShell Desired State Configuration 176

Save-Help 184

Yet more new cmdlets 186

DISM cmdlets 186

DHCP server cmdlets 189

DNS server cmdlets 190
Hardware certification cmdlets 191
Hyper-V cmdlets 191
iSCSI target cmdlets 195
Net TCP/IP cmdlets 196
Network Address Translation cmdlets 196
Network event packet capture cmdlets 197
Network Virtualization cmdlets 197
Physical Computer System View (PCSV) cmdlets 198
Software Inventory Logging cmdlets 198
Start screen cmdlets 198
Windows Deployment Services cmdlets 200
Windows PowerShell Web Access cmdlets 201
Windows Search cmdlets 201

Learn more 202

Chapter 11 Windows Server Essentials 203

Learn more 214

Appendix *215*

Index *217*

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:

microsoft.com/learning/booksurvey

Introduction

This book is intended to provide you with an overview of the new features and enhancements introduced in Windows Server 2012 R2. The intended audience for this book is IT pros who deploy, manage, and maintain Windows Server workloads in data center, private cloud, and hosting provider environments.

We assume that you are at least somewhat familiar with the features and capabilities of the previous platform Windows Server 2012. If you are not familiar with all the new features and enhancements Microsoft introduced previously in Windows Server 2012, we recommend that you first read *Introducing Windows Server 2012 RTM Edition* (Microsoft Press, 2012). This e-book is available as a free download from Microsoft in three formats:

- PDF from *http://aka.ms/682788pdf*
- EPUB from *http://aka.ms/682788epub*
- MOBI from *http://aka.ms/682788mobi*

A key feature of this book is the technical sidebars that have been contributed by Microsoft insiders. These sidebars were written by experts who have been closely involved in the Windows Server 2012 R2 development process and include Program Managers, Support Escalation Engineers, Technical Consultants, Data Center Specialists, and others who work at Microsoft in various capacities.

Acknowledgments

Three groups of people have helped make this book possible, and as the author I'd like to thank them all here. First, the following experts at Microsoft have contributed sidebars that explain and demonstrate different aspects of Windows Server 2012 R2:

- Deepak Srivastava
- Erez Benari
- Gene Chellis
- Jason M. Anderson
- Jeff Butte
- John Marlin
- Justin Turner
- Mark Gehazi
- Nir Ben Zvi

Second, the following Microsoft insiders have peer reviewed various portions of this book to help us ensure our content is as accurate as possible:

- Aanand Ramachandran
- Adam Carter
- Ben Armstrong
- Bryan Matthew
- CJ Williams
- Clinton Ho
- Deepak Srivastava
- Elden Christensen
- Erez Benari
- Gabriel Silva
- Guang Hu
- Jason Gerund
- Jeff Woolsey
- John Savill
- Jose Barreto
- Matthew John
- Raghavendran Gururajan
- Roiy Zysman
- Shivam Garg
- Symon Perriman
- Vijay Tandra Sistla
- Vijay Tewari
- Yang Cao Sun
- Yuheng Cai sun

Finally, I'd also like to thank Valerie Woolley, Content Project Manager at Microsoft Press; Christian Holdener at S4Carlisle Publishing Services; and copyeditor Andrew Jones.

Errata & book support

We've made every effort to ensure the accuracy of this content and its companion content. Any errors that have been reported since this content was published are listed on our Microsoft Press site:

http://aka.ms/introwinsrv2012R2/errata

If you find an error that is not already listed, you can report it to us through the same page.

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

Please note that product support for Microsoft software is not offered through the addresses above.

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*.

CHAPTER 1

Cloud OS

This chapter introduces Windows Server 2012 R2 which is at the heart of Microsoft's revolutionary new Cloud OS platform. The chapter describes five key areas Microsoft focused on when developing Windows Server 2012 R2 and sets the stage for the discussion of the new features and enhancements in Windows Server 2012 R2 that follow in the remaining chapters of this book.

The big picture

Information Technology (IT) is in the midst of a time of rapid change. More and more businesses are seeing cloud computing as a viable option for hosting their applications, services, and data. Some businesses have already implemented private clouds within their own data centers or have begun utilizing cloud services offered by hosting providers. Other businesses are in the process of evaluating the possible benefits they can reap from cloud availability, scalability, mobility, and agility. And for various reasons, some businesses are still skeptical of whether cloud computing is right for them.

But clearly, Microsoft isn't skeptical. In fact, Microsoft is fully committed to the cloud as the computing paradigm of the future. Nowhere is this more obvious than in this latest release of the Windows Server platform. Microsoft firmly believes that cloud computing isn't a trend but rather a golden opportunity for businesses. Why is that?

Because businesses need to become agile in order to survive in today's competitive landscape. And to have an agile business, you need to build your applications and services on a highly available and elastic development platform. Businesses need a uniform model for application lifecycle management with common frameworks across their physical infrastructure, virtual infrastructure, and the cloud. They need a highly scalable, secure identity solution they can use for managing their computing, networking, and storage assets, both on-premises and in the cloud. They need to be able to process, store, and transfer huge amounts of data and perform analytics quickly and easily. And businesses need to be able to do all this in a cost-effective manner.

In other words, what they need is a cloud-optimized business. And that's what Microsoft intends to deliver with their current product release cycle. Because for the first time in their history, Microsoft has synchronized the development cycles of three major platforms:

- **Windows Server** A proven, enterprise-class platform that forms the foundation for building cloud solutions.
- **System Center** An integrated platform that provides a common management experience across private, hosted, and public clouds.
- **Windows Azure** An open and flexible cloud platform for building, deploying, and managing applications and workloads hosted on a global network of Microsoft-managed data centers.

Together, these three platforms comprise Microsoft's vision for a Cloud OS, as shown in Figure 1-1. This book only focuses on one portion of this Cloud OS, namely, Windows Server 2012 R2. It's a key portion, however, because it forms the foundation for businesses to be able to run their applications in private clouds, with service providers, or in the Windows Azure public cloud.

FIGURE 1-1 Microsoft thinks about the cloud in three parts.

Journey to the Cloud OS

To better understand Microsoft's vision for a Cloud OS, start by thinking about how IT has traditionally managed server workloads. In the early days of Windows Server, you deployed and managed lots of physical servers on-premises. Each server had to be individually managed, and this meant performing tasks like configuring storage for them, configuring networking, tuning performance, and so on. Lots of servers meant lots of tasks to perform, and although scripting could automate many of these tasks, such solutions were typically inflexible and difficult to maintain.

Then along came virtualization, and suddenly you saw that you could save money by retiring physical servers after migrating their workloads onto virtualization hosts. But the management paradigm stayed the same, for instead of managing lots of physical servers, you were now managing lots of virtual machines. But proliferation is proliferation whether it's in the physical or virtual realm, and managing thousands of individual virtual machines can be just as challenging as managing physical machines.

Then the concept of cloud computing arrived—with its promises of rapid elasticity, resource pooling, and on-demand self-service. Now, if a business wants to maintain control over its IT resources, it can implement a private cloud solution on-premises using Windows Server and System Center. If scalability is the issue, the business can opt for running its applications, services, or virtual machines in Windows Azure. And if reach and customization are important, the business can use the services of a cloud hosting service provider. Each of these approaches is equally valid, and it's up to the business to decide which to choose based on its needs and constraints.

From Microsoft's perspective, these three approaches (private cloud, service providers, and Windows Azure) are really one and comprise one consistent platform: the Cloud OS. Windows Server forms the foundation; System Center provides the management capability; and Windows Azure delivers the solutions. In other words, cloud is not just something that happens out there; it happens wherever and whenever you need it to optimize your business. That's what Microsoft means by cloud.

For example, do you need Active Directory? You can deploy it on-premises using Windows Server. But Active Directory is already waiting for you in Windows Azure. And with Windows Server 2012 R2 you can even virtualize domain controllers and host them in a service provider's cloud. The choice is yours.

Microsoft wants you to have the choice to implement the cloud computing model that best meets the needs of your business. And the Cloud OS—Windows Server, System Center, and Windows Azure—delivers that kind of choice to customers. Windows Server 2012 R2 is the foundation for all of this, and that's what this book is about.

Let's begin!

In the chapters that follow, we're going to examine what's new and enhanced in Windows Server 2012 R2. Because virtualization is at the heart of how cloud computing works, we're going to start by looking at Hyper-V first. Let's begin!

CHAPTER 2

Hyper-V

Hyper-V virtualization represents the foundation of Microsoft's vision for the cloud operating system. Storage and networking are the walls that help support your virtualization infrastructure. Then, on top of everything, comes management and automation. Together, these different functionalities enable a wide range of cloud solutions that can meet the needs of any business.

But the bottom line is that virtualization is at the core of everything in most IT shops nowadays. For example, when IT wants to deploy a new workload (such as a Microsoft SQL Server machine) the common way of doing this (and it's really a best practice) is to virtualize the workload first instead of deploying the workload on a physical server. As a second example, when IT wants to deploy a new desktop image, the common practice is to create the image in a Hyper-V virtual environment before deploying it onto physical desktop computers.

Windows Server 2012 R2 builds upon the improvements added earlier in Hyper-V on Windows Server 2012 and adds new features and functionality that can deliver greater gains in performance, availability, and agility. This chapter examines what's new in this latest version of Hyper-V, but first we'll briefly review what was previously introduced in Hyper-V on Windows Server 2012.

Previous enhancements to Hyper-V

A lot of powerful new features and capabilities were added to Hyper-V in the previous version of Windows Server, and space doesn't allow us to go into detail concerning each of them. As a quick summary, however, the following enhancements could be characterized as some of the more significant improvements in the platform:

- **Increased scalability and resiliency** Hyper-V hosts running Windows Server 2012 supported up to 320 logical processors and 4 terabytes (TB) of memory, and virtual machines running on these hosts could be configured with 64 virtual processors and 1 TB of memory.
- **New live migration options** Beginning with Windows Server 2012, you could perform a live migration in a nonclustered environment and could perform multiple live migrations simultaneously utilizing higher network bandwidths.

- **Storage migration** Hyper-V in Windows Server 2012 allowed you to move the virtual hard disks used by a virtual machine to different physical storage while the virtual machine remained running.
- **Virtual machines on file shares** Hyper-V in Windows Server 2012 supported using Server Message Block 3.0 (SMB 3.0) file shares as storage for virtual machines. This meant you could store your virtual machine files on a cost-efficient Scale-Out File Server running Windows Server 2012 instead of buying an expensive storage area network (SAN) for this purpose.
- **Extensible virtual switch** Hyper-V on Windows Server 2012 included a new extensible virtual switch that provided an open framework to allow third parties to add new functionality such as packet monitoring, forwarding, and filtering into the virtual switch.
- **Windows PowerShell module** Hyper-V in Windows Server 2012 included a Windows PowerShell module for Hyper-V that provided more than 160 cmdlets for automating Hyper-V management tasks.
- **VHDX format** Hyper-V in Windows Server 2012 included a new virtual hard disk format called VHDX that supported up to 64 TB of storage. The VHDX format also provided built-in protection from corruption stemming from power failures and resisted performance degradation when using some large-sector physical disks.
- **Reclaiming snapshot storage** With Hyper-V in Windows Server 2012, when a virtual machine snapshot was deleted, the storage space that the snapshot consumed before being deleted was made available while the virtual machine was running. This meant that you no longer needed to shut down, turn off, or put the virtual machine into a saved state to recover the storage space. And even more importantly for production environments, differencing disks are now merged with the parent while the virtual machine is running.
- **Improved virtual machine import** The virtual machine import process in Hyper-V in Windows Server 2012 improved to help resolve configuration problems that might otherwise prevent a virtual machine from being imported. In addition, you could import a virtual machine by copying its files manually instead of having to export the virtual machine first.
- **Dynamic Memory improvements** Dynamic Memory was improved in Hyper-V in Windows Server 2012 to include support for configuring minimum memory. In addition, Smart Paging, a new memory management mechanism, was introduced to provide a reliable restart experience for virtual machines configured with less minimum memory than startup memory.
- **Single-root I/O virtualization (SR-IOV)** Hyper-V in Windows Server 2012 allowed you to assign network adapters that supported SR-IOV directly to virtual machines running on the host. SR-IOV maximized network throughput while minimizing network latency and CPU overhead needed for processing network traffic.

- **Virtual Fibre Channel** Hyper-V in Windows Server 2012 allowed you to connect directly to Fibre Channel storage from within the guest operating system that runs in a virtual machine. This allowed you to virtualize workloads and applications that require direct access to Fibre Channel–based storage. It also made guest clustering (clustering directly within the guest operating system) possible when using Fibre Channel–based storage.
- **Hyper-V Replica** Hyper-V in Windows Server 2012 allowed you to replicate virtual machines between storage systems, clusters, and data centers in two sites to provide business continuity and disaster recovery.

Now that we've reviewed the Hyper-V improvements introduced previously in Windows Server 2012, let's move on and examine some of the new capabilities added to Hyper-V in Windows Server 2012 R2.

Generation 2 virtual machines

One of the key ways that Windows Server 2012 R2 advances the Hyper-V virtualization platform is in its support for a new generation of virtual machines. Microsoft refers to these as "Generation 2" virtual machines, and they have the key following characteristics:

- **UEFI-based** Beginning with Windows 8 and Windows Server 2012, Microsoft Windows now supports the Secure Boot feature of the Unified Extensible Firmware Interface (UEFI). This means that UEFI is now part of the Windows 8 and Windows Server 2012 boot architecture, and it replaces the Basic Input/Output System (BIOS) firmware interface used by previous versions of Windows for initiating the boot process. Generation 2 virtual machines comply with the UEFI Secure Boot standard and enable virtual machines to use Secure Boot.
- **Legacy free** In previous versions of Hyper-V, virtual machines used a standard set of emulated hardware devices to ensure compatibility running all versions of Windows. These emulated devices include an AMI BIOS, Intel 440BX chipset motherboard, S3 Trio graphics display adapter, Intel/DEC 21140 network adapter, and so on. With Generation 2 virtual machines, many of these emulated devices have now been removed and replaced with synthetic drivers and software-based devices as summarized in Table 2-1.
- **SCSI boot** Virtual machines in previous versions of Hyper-V needed to boot from integrated development environment (IDE) disks (virtual disks attached to the virtual machine using the IDE controller). Beginning with Windows Server 2012 R2, however, Generation 2 virtual machines can now boot directly from SCSI disks (virtual disks attached to the virtual machine using the SCSI controller). In fact, Generation 2 virtual machines don't even have an IDE controller! Generation 2 virtual machines can also boot from a SCSI virtual DVD.

- **Faster deployment** Network-based installation of a guest operating system onto a Generation 2 virtual machine is significantly faster than for the previous generation of Hyper-V virtual machines for two reasons. First, the Legacy Network Adapter device is no longer required (or even supported) by Generation 2 virtual machines. Instead, you can PXE-boot a Generation 2 virtual machine using a standard network adapter. Second, the SCSI controller performs much better than the legacy IDE controller in the previous generation of virtual machines. The result is that installing a supported guest operating system in a Generation 2 virtual machine takes only about half the time as installing the same guest operating system in a previous generation virtual machine.

TABLE 2-1 Hardware Device Changes in Generation 2 Virtual Machines

Legacy Devices Removed	Replacement Devices	Enhancements
IDE controller	Virtual SCSI controller	Boot from VHDX (64 TB max size, online resize)
IDE CD-ROM	Virtual SCSI CD-ROM	Hot add/remove
Legacy BIOS	UEFI firmware	Secure Boot
Legacy NIC	Synthetic NIC	Network boot with IPv4 & IPv6
Floppy & DMA Controller	No floppy support	
UART (COM Ports)	Optional UART for debugging	Faster and more reliable
i8042 keyboard controller	Software-based input	No emulation—reduced resources
PS/2 keyboard	Software-based keyboard	No emulation—reduced resources
PS/2 mouse	Software-based mouse	No emulation—reduced resources
S3 video	Software-based video	No emulation—reduced resources
PCI Bus	VMBus	
Programmable Interrupt Controller (PIC)	No longer required	
Programmable Interrupt Timer (PIT)	No longer required	
Super I/O device	No longer required	

Because of all these hardware changes, Generation 2 virtual machines only support the following versions of Windows as guest operating systems:

- 64-bit versions of Windows 8 and Windows Server 2012
- 64-bit versions of Windows 8.1 and Windows Server 2012 R2

As Figure 2-1 shows, when you create a new virtual machine in Windows Server 2012 R2 using Hyper-V Manager, you now have the option of choosing whether to create a first-generation virtual machine or a Generation 2 virtual machine. You can also specify which type of virtual machine is to be created by using the New-Generation parameter of the New-VM Windows PowerShell cmdlet in Windows Server 2012 R2.

FIGURE 2-1 A Generation 2 virtual machine can be created using the New Virtual Machine Wizard.

Once the Generation 2 virtual machine has Windows Server 2012 R2 installed as the guest operating system, opening Device Manager reveals the various synthetic and software-based devices attached to the VMBus. Note that unlike first-generation virtual machines, there is no PCI-to-ISA bridge running in ISA mode, no PS/2 keyboard, no PS/2 mouse, no COM ports, and so on. Figure 2-2 compares Device Manager for Generation 1 virtual machines (left) with Device Manager for Generation 2 virtual machines (right).

FIGURE 2-2 A comparison of what Device Manager shows for Generation 1 (left) and Generation 2 (right) virtual machines.

> ***NOTE*** **You cannot change the generation of a virtual machine after you have created the virtual machine.**

The key benefits of using Generation 2 virtual machines, as opposed to Generation 1 virtual machines, are twofold. First, as mentioned previously, new Generation 2 virtual machines can be quickly provisioned because they can boot from a SCSI device or a standard network adapter. This can be useful in scenarios where you need to quickly deploy new virtual machines in order to scale out a cloud-based application to meet rapidly increasing demand.

The second main benefit of Generation 2 virtual machines is in the area of security. Because Generation 2 virtual machines are UEFI-based and support Secure Boot, unauthorized operating systems, drivers, and firmware can be prevented from running when the virtual machine starts. In order for this to apply, however, Secure Boot must be enabled for the virtual machine. As Figure 2-3 shows, you can enable or disable Secure Boot on a Generation 2 virtual machine by opening the Settings of the virtual machine, selecting Firmware under Hardware, and selecting or clearing the Enable Secure Boot check box. By default, Secure Boot is enabled when you create a new Generation 2 virtual machine.

FIGURE 2-3 You can enable or disable Secure Boot in the virtual machine's Settings dialog.

MORE INFO **For a good explanation of UEFI Secure Boot, see the post titled "Protecting the pre-OS environment with UEFI" in the Building Windows 8 blog at** *http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx*.

Automatic Virtual Machine Activation

Starting way back with Windows Server 2003 R2 with Service Pack 2, the Datacenter edition of Windows Server has provided unlimited virtualization rights for servers to allow organizations to deploy as many virtual machines as they need in their environments. But until now this benefit has come with the cost of the administrative overhead of deploying a key management infrastructure for licensing and activating these virtual machines.

Beginning with Windows Server 2012 R2, however, the pain of managing product keys for virtual machines can be greatly alleviated by using new capability called Automatic Virtual Machine Activation (AVMA). The way it works is like this:

1. To start with, the Hyper-V host on which your virtual machines will be deployed must have Windows Server 2012 R2 Datacenter edition installed on it as the host operating system.
2. Next, to avoid having to activate virtual machines and manage their product keys, the virtual machines themselves must have either Windows Server 2012 R2 Standard, Windows Server 2012 R2 Datacenter, or Windows Server 2012 R2 Essentials installed on them as their guest operating system.
3. Once the guest operating system is installed in a virtual machine and the virtual machine is started, you can log on to the virtual machine, open an elevated command prompt, and install the AVMA key in the virtual machine by running this command:

   ```
   slmgr /ipk <AVMA_key>
   ```

   Doing this automatically activates the license for the virtual machine against the host.
4. Alternatively, you can use the AVMA key in an unattend.xml answer file and completely automate the activation of the virtual machine when an unattended installation of the guest operating system is performed on the virtual machine.

AVMA removes a major customer pain point by greatly reducing the time and effort needed by large enterprises and hosters for managing licensing and activation of large numbers of virtual machines in their environment. Regardless of whether your Hyper-V hosts are OEM machines or are running a volume-licensed version of Windows Server activated using Key Management Service (KMS) or Multiple Activation Key (MAK), if the host machine is running Datacenter edition and is activated, then all virtual machines running any Windows Server 2012 R2 edition as a guest operating system are automatically activated.

In addition, this is also completely secure with respect to your existing key management infrastructure since no keys are used to activate the virtual machines. So, if you should copy or move one of your virtual machines to someone else's environment, for example, as part of demonstration purposes, your keys won't be exposed. Of course, the other environment must also be using hosts running an activated copy of a Datacenter edition of Windows Server.

Remote access over VMBus

Virtual Machine Connection (VM Connect) is a tool that you use to connect to a virtual machine running on a Hyper-V host. VM Connect is installed on the host when you add the Hyper-V role to your server. Specifically, if the server is running Windows Server 2012, then the VM Connect is installed with the Hyper-V role provided that either the server with a GUI installation option has been selected or the Minimal Server Interface option has been configured. (VM Connect is not available on Windows Server Core installations of Windows Server.)

The purpose of VM Connect is to enable Hyper-V administrators to directly interact with the guest operating system in a virtual machine from the local console of the host. Although management of most virtual machines is typically performed remotely, using either Remote Desktop Connection (RDC) or Windows PowerShell, there are times when you might need to work with a virtual machine directly on the host, for example, when the virtual network adapter of a virtual machine stops functioning. In such cases, you can use Hyper-V Manager on the host and to connect to the virtual machine, and open its desktop within the VM Connect window to configure or troubleshoot the virtual machine and its guest operating system, even if the virtual machine has no connectivity with your network.

The way that VM Connect works in Windows Server 2012 and earlier is to present you with a bitmap image of the desktop of a virtual machine's guest operating system, which is generated by an emulated video card in the virtual machine. This bitmap image is updated in real time so you can see configuration changes as they happen. VM Connect also provides you with emulated keyboard and mouse devices in the virtual machine, so you can directly control the desktop of the guest operating system. Because VM Connect in Windows Server 2012 and earlier uses bitmap images, certain limitations exist in how you can use VM Connect to interact with the guest operating system. For example, you can copy and paste text between the host machine's desktop and the desktop of the guest operating system, but you can't copy/paste images or files between them.

Beginning with Windows Server 2012 R2, however, VM Connect no longer connects you to the guest operating system using an emulated video card, keyboard, and mouse in the virtual machine. Instead, VM Connect uses Remote Desktop Services (RDS) in the guest operating system of the virtual machine to provide the full RDS experience when you use it to connect to the virtual machine (see Figure 2-4). The result is an enhanced experience that enables you to:

- Copy/paste files between the desktop of the host and the desktop of the guest operating system by using a new Hyper-V integration service.
- Redirect audio on the virtual machine to the host.
- Enable the guest operating system to use smart cards attached to the host.
- Enable the guest operating system to access any USB device attached to the host.

FIGURE 2-4 VM Connect now connects to the virtual machine using RDS in the guest operating system.

All of this is possible even if the virtual machine is not connected to the network. And you can do it with hosts you are managing remotely using Hyper-V Manager or Windows PowerShell. You don't have to be logged on interactively to the host to experience all this new VM Connect functionality.

Cross-version live migration

Windows Server 2012 R2 also includes several significant improvements to live migration that can benefit organizations deploying private cloud solutions built with Windows Server and Microsoft System Center. Live migration was introduced in Windows Server 2008 R2 to provide a high-availability solution for virtual machines running on Hyper-V hosts. Live migration uses the Failover Clustering feature to allow running virtual machines to be moved between cluster nodes without perceived downtime or loss of network connection.

Live migration provides the benefit of increased agility by allowing you to move running virtual machines to the best host for improving performance, achieving better scaling, or ensuring optimal workload consolidation. Live migration also helps increase productivity and reduce costs by allowing you to service your host machines without interruption or downtime for your virtualized workloads.

The ability to perform cross-version live migration between Hyper-V hosts running Windows Server 2012 and Windows Server 2012 R2 is new in Windows Server 2012 R2. Cross-version live migration can be performed using any of the live migration options supported by Windows Server 2012 including:

- Live migration on a failover cluster
- Live migration between failover clusters
- Live migration using a Scale-Out File Server that supports SMB 3.0
- Shared nothing live migration where no shared storage is used for the virtual machines

For organizations that have already begun deploying a private cloud solution based on Windows Server 2012, cross-version live migration means that you will be able to upgrade your private cloud solution from Windows Server 2012 to Windows Server 2012 R2 with zero downtime for the workloads running on your virtual machines. If you can tolerate a brief downtime window for your workloads, you can even choose to perform an in-place upgrade of your existing Hyper-V hosts from Windows Server 2012 to Windows Server 2012 R2.

And unlike previous versions of Windows Server, you don't have to perform a lot of preparatory actions before performing an in-place upgrade of your Hyper-V hosts. For example, you previously had to do things like turn off the virtual machines running on the host, and you also had to delete any snapshots and saved states of the virtual machines. When performing an in-place upgrade of a Hyper-V host from Windows Server 2012 to Windows Server 2012 R2, however, none of these preparatory steps are required, and all of the virtual machine's snapshots and saved states are preserved.

Let's now learn more about this new feature from one of our experts at Microsoft.

Benefits of cross-version live migration

Historically, every new version of Hyper-V has delivered very exciting and advanced features which added lots of value to customers' modern data centers and private/public clouds. In the past, migrating to the latest version of Hyper-V required more planning and some outage to the virtual environment while exporting and importing those virtual machines to the hosts running the latest version of Hyper-V.

With release of Windows Server 2012 R2 Hyper-V, administrators now can live migrate virtual machines from Windows Server 2012 Hyper-V to Windows Server 2012 R2 Hyper-V hosts. Microsoft private cloud administrators are very excited to be able to keep up with the latest innovations and feature improvements in Microsoft Hyper-V without negatively impacting their services and Service Level Agreements (SLAs).

In larger environments, private cloud fabric administrators can certainly take advantage of the Microsoft Hyper-V PowerShell module, and using the Move-VM cmdlet could help them create a sophisticated script and automate this migration according to their internal processes.

And last but not least, the majority of Microsoft Hyper-V environments are configured as Highly Available (HA) using Microsoft Failover Clustering and migrating to Windows Server 2012 R2 Hyper-V requires an administrator to remove each VM as an HA role, live migrate the Windows Server 2012 R2 host that is part of a new Server 2012 R2 Hyper-V cluster, and, preferably, place the VM files on the new Cluster Shared Volume (CSV), then add that VM as an HA role on the new cluster. This process should cause no outages to the virtual machine and of course, if it is needed, an administrator can use Microsoft Failover Cluster and Hyper-V PowerShell cmdlets to automate the entire process. This also could be even easier using Microsoft System Center Virtual Machine Manager (VMM) 2012 R2 as the centralized private cloud management solution.

Please note that this feature has been provided solely for upgrade purposes, and live migration of virtual machines to the previous version Hyper-V hosts will not be supported or possible.

Mark Gehazi
Data Center Specialist, US-SLG STU Infrastructure

Faster live migration

Live migration is also significantly faster in Windows Server 2012 R2 Hyper-V for two reasons. First, a new ability to compress live migration traffic can be used to reduce the amount of data that needs to be sent over the network during a live migration. This live migration compression capability is enabled by default for Hyper-V in Windows Server 2012 R2 and can often halve the time it takes to perform a live migration in a Windows Server 2012 R2 Hyper-V environment, depending on the processing resources available on the host machines for performing the compression operation.

Second, live migration can be faster in Windows Server 2012 R2 Hyper-V because of the ability to use network adapters that have Remote Direct Memory Access (RDMA) together with the SMB Direct and SMB Multichannel features of SMB 3.0. RDMA is a networking technology that enables high-throughput, low-latency communication that minimizes CPU usage on the computers using this technology. RDMA is an industry standard protocol defined in RFC 5040 that works by moving data directly between the memory of the computers involved, bypassing the operating systems on these machines. Examples of types of RDMA-capable network adapter hardware include Infiniband (IB), Internet Wide Area RDMA Protocol (iWARP), and RDMA over Converged Ethernet (RoCE).

SMB Direct, which is short for SMB over Remote Direct Memory Access (SMB over RDMA), is a feature of SMB 3.0 that supports the use of RDMA-capable network adapters. By using SMB Direct, for example, a Hyper-V host is able to access data on a remote SMB 3.0 file server (called a Scale-Out File Server) as quickly and easily as if the data was on local storage on the Hyper-V host. SMB Direct is available only on the Windows Server platform and was introduced in Windows Server 2012. SMB Direct requires that the SMB client and SMB server both support SMB 3.0.

SMB Multichannel is another feature of SMB 3.0 that enables the aggregation of network bandwidth and provides network fault tolerance whenever multiple paths are available between an SMB 3.0 client and an SMB 3.0 server. SMB Multichannel thus enables server applications to take full advantage of all available network bandwidth and be resilient to a network failure. SMB Multichannel is also the feature that is responsible for detecting the RDMA capabilities of network adapters to enable the use of SMB Direct. Once SMB Multichannel has determined that a network adapter is RDMA-capable, it creates multiple RDMA connections (two per interface) for that session. SMB Multichannel is also available only on the Windows Server platform and was introduced in Windows Server 2012, and it requires that the SMB client and SMB server both support SMB 3.0.

When a live migration is performed with virtual machines running on Hyper-V hosts that have RDMA-capable network adapters, SMB Direct and SMB Multichannel enable multiple network interfaces to be used for performing the live migration. This not only results in significantly faster live migrations, but also results in less use of processing resources on the hosts as well. This is different from live migration compression, which utilizes available processor resources on the host to reduce the network load involved in transferring the compressed virtual machine memory across the network.

When would you use live migration compression? A typical scenario would be when the primary constraining factor limiting the speed of live migration is your network bandwidth, but your Hyper-V hosts are not under heavy load as regards processing cycles. When would you use live migration using SMB Direct and SMB Multichannel? A scenario here would be when the primary constraining factor is high processor utilization on your host machines while you have lots of bandwidth available on your network. In general, if the network you are using for performing your live migration is 10 GbE or slower, you probably want to use the compression approach. If your network is faster than 10 GbE, then you should probably be using RDMA-capable network adapters so you can take advantage of the SMB Direct and SMB Multichannel capabilities of Windows Server 2012 and later.

Online VHDX resize

Another new capability of Hyper-V in Windows Server 2012 R2 is the ability to increase or decrease the size of a virtual hard disk attached to a virtual machine while that virtual machine is still running on the host. This means that if the workload running on a virtual machine should require more space, you can expand the virtual hard disk without interrupting any applications accessing the workload. And if you want to reallocate storage space from one virtual machine to another, you can shrink the virtual hard disk attached to the first virtual machine (provided that there is sufficient unpartitioned space on the disk) to free up space for expanding the disk on the second machine.

Online resizing of virtual hard disks requires that these disks be using the newer VHDX virtual hard disk format first introduced in Windows Server 2012. VHDX was designed to address the growing technological demands of today's enterprises and provides greater storage capacity, built-in data protection, and support for large-sector hard disk drives. In addition, online resizing requires that the virtual disk be attached to the virtual machine's SCSI bus.

For example, the following steps use Hyper-V Manager to expand the size of a running virtual machine:

1. In Hyper-V Manager, right-click the virtual machine and select Settings.
2. In the Settings dialog for the virtual machine, click the Hard Drive node under SCSI Controller for the virtual hard disk you want to expand, and then click the Edit button to launch the Edit Virtual Hard Disk Wizard.
3. Select the Expand option on the Choose Action page, click Next, type the new size you want the virtual hard disk to have (see Figure 2-5), and then click Next followed by Finish.

Once you've expanded a virtual hard disk, the option to shrink it will be displayed next time you use the Edit Virtual Hard Disk Wizard. Of course, you can also resize online virtual disks by using Windows PowerShell.

FIGURE 2-5 Virtual hard disks of running virtual machines can now be resized on Windows Server 2012 R2.

Live export

Not only can you now resize virtual hard disks attached to virtual machines while the virtual machines are running, you can also export a running virtual machine. You couldn't do this with virtual machines on Windows Server 2012 or earlier versions of Windows Server. However, with Windows Server 2012 R2 you can use Hyper-V Manager to export a complete copy of a running virtual machine or to export any snapshot of a running virtual machine. And you can use Virtual Machine Manager 2012 R2 to clone a running virtual machine, which basically involves exporting and then importing a virtual machine to create a new virtual machine that is based on the existing virtual machine. And you can even export snapshots (checkpoints) associated with a virtual machine while the virtual machine is running.

One scenario where live export can be helpful is when a running virtual machine in your environment begins to exhibit some instability but is still performing its expected workload. Previously, you had to choose between the lesser of two evils:

- Stop the virtual machine or take it offline and try to troubleshoot the problem. Unfortunately while the virtual machine is stopped or offline, its workload will no longer be available to users, and this can result in loss of either business or productivity.

- Let the virtual machine continue to run and hope it doesn't fail. This approach allows the virtual machine's workload to continue to be available, but instability often ends up with the application or guest operating system crashing, which means a probable interruption in workload will occur. Once again, this is likely to result in loss of either business or productivity.

With live export, however, you can now clone a copy of your unstable virtual machine without shutting the virtual machine down (see Figure 2-6). You can then let your production virtual machine continue to run while you perform troubleshooting steps on the cloned workload to try and see if you can resolve the issue causing the instability. Once you determine how to fix the problem by working with the cloned virtual machine, you might be able to repair your production virtual machine without needing to reboot the guest operating system or restart its running applications, depending on the issue causing the instability.

FIGURE 2-6 Running virtual machines can now be exported or cloned on Windows Server 2012 R2.

Some other scenarios where being able to export running virtual machines can be useful include troubleshooting problems with applications running in virtual machines, performing tests prior to moving a virtual machine from your private cloud to a hosted or public cloud environment (or vice versa), and when you want to duplicate your existing production environment to create a test lab.

More robust Linux support

Hyper-V has supported installing and running various Linux distros or "flavors" in virtual machines for some time now. Linux guest support in Hyper-V is especially desired by hosting providers who often like to provide their customers with a wide range of platform options for running their web applications and services. Linux (and UNIX) support in Hyper-V is also important in the enterprise space where heterogeneous IT solutions are generally the norm.

Because of the needs of these customer segments, Microsoft envisions Hyper-V virtualization as "cross-platform from the metal up" and supports a wide range of Linux distros, as shown in Table 2-2, by providing Linux Integration Services (LIS) for specific versions of popular distros. Microsoft also includes robust Linux/UNIX capabilities across the entire System Center family of products, and also in Windows Azure offerings as well. Linux/UNIX support is an integral part of all of these platforms and is not merely an extension of Windows-centric functionality.

TABLE 2-2 Current Availability of Linux Integration Services for Hyper-V in Windows Server 2012 R2

Distro	Version	LIS Availability
Red Hat Enterprise Linux	5.7, 5.8, 6.0-6.3	Download LIS from Microsoft
	5.9, 6.4	LIS built-in and certified by Red Hat
SUSE Linux Enterprise Server	11 SP2	LIS built-in
CentOS	5.7, 5.8, 6.0-6.3	Download LIS from Microsoft
	5.9, 6.4	LIS built-in
Ubuntu Server	12.04, 12.10, 13.04	LIS built-in
Debian	7.0	LIS built-in

As part of Microsoft's continuing commitment to making Hyper-V the best all-around virtual platform for hosting providers, Linux support for Hyper-V in Windows Server 2012 R2 has now been enhanced in the following ways:

- **Improved video** A virtualized video driver is now included for Linux virtual machines to provide an enhanced video experience with better mouse support.
- **Dynamic Memory** Dynamic Memory is now fully supported for Linux virtual machines, including both hot-add and remove functionality. This means you can now run Windows and Linux virtual machines side-by-side on the same host machine while using Dynamic Memory to ensure fair allocation of memory resources to each virtual machine on the host.
- **Online VHDX resize** Virtual hard disks attached to Linux virtual machines can be resized while the virtual machine is running.
- **Online backup** You can now back up running Linux virtual machines to Windows Azure using the Windows Azure Online Backup capabilities of the in-box Windows

Server Backup utility, System Center Data Protection Manager, or any third-party backup solution that supports backing up Hyper-V virtual machines.

Managing Hyper-V hosts running previous versions of Windows Server

Previously with Hyper-V in Windows Server 2012, if you wanted to manage a previous version Hyper-V host running Windows Server 2008 R2 or Windows Server 2008, you couldn't use the Windows Server 2012 version of Hyper-V Manager to do this. Instead, you would typically establish a Remote Desktop connection from the Windows Server 2012 host to the previous version host to run the previous version of Hyper-V Manager remotely on the previous version host.

Now, however, you can use Hyper-V Manager running on a Windows Server 2012 R2 Hyper-V host to manage hosts running either Windows Server 2012 R2 or Windows Server 2012. This means that you can now deploy the latest version of Hyper-V in your environment without needing to upgrade your Hyper-V management workstation immediately. Alternatively, you can upgrade your management station from Windows 8 to Windows 8.1, install the Remote Server Administration Tools (RSAT) for Windows 8.1, and use your upgraded management workstation to manage both hosts running Windows Server 2012 R2 and hosts running Windows Server 2012.

Note, however, that when you connect to a Windows Server 2012 R2 host from a host running Windows Server 2012 (or a management workstation running Windows 8 with RSAT installed) you will only be able to perform those actions that are supported by Hyper-V in Windows Server 2012.

Hyper-V Replica enhancements

In the short time that Windows Server 2012 has been released, Hyper-V Replica has proven to be one of its most popular features. Hyper-V Replica provides asynchronous replication of virtual machines between two Hyper-V hosts. It's easy to configure and doesn't need either shared storage or any particular storage hardware. Any server workload that you can virtualize on Hyper-V can be replicated using this capability, and replication is encrypted during transmission and works over any IP-based network.

You can use Hyper-V Replica with standalone Hyper-V hosts, failover clusters of hosts, or a mixture of these environments. The host machines can either be physically co-located or widely separated geographically. And they don't need to be in the same domain or even domain-joined at all.

Hyper-V Replica is an ideal technology for organizations that want to add support for disaster recovery to their Hyper-V environment to ensure business continuity. For example, you could use it to provide disaster recovery support for the branch offices by replicating

their virtual machines to hosts at the head office. Another possible scenario would be to have a hosting provider set up a Replica server at their data center to receive replication data from a number of Hyper-V hosts running virtualized workloads on the premises of customers.

In Hyper-V Replica in Windows Server 2012 R2, greater control over the frequency at which data is replicated between hosts is a new feature. In Windows Server 2012, the replication frequency was fixed at every five minutes. Some customers provided feedback that this was not frequent enough for their environment, while others requested the option of performing replication less frequently. So now, as Figure 2-7 shows, there are two new replication frequencies you can choose from besides the default one of five minutes when you enable replication for a server:

- **30 seconds** Choosing this option means that the host in the replica site will never be more than a minute behind the host in the primary site. This option was provided in Windows Server 2012 R2 so that Hyper-V Replica could be used as an alternative to more expensive SAN solutions that have a similar low latency. Organizations that simply need to replicate data as quickly as possible, for example between two data centers in the same metropolitan area, might choose this option.
- **15 minutes** This option was provided especially for organizations that wanted to replicate data over networks that had very high latency or low reliability, for example over a satellite link. To ensure that replication would tolerate network outages and succeed in such scenarios, a long replication window like this can now be chosen when you enable replication on a host in Windows Server 2012 R2, and choosing this option means that the host in the replica site will never be more than an hour behind the host in the primary site.

FIGURE 2-7 Hyper-V Replica in Windows Server 2012 R2 now supports three possible replication frequencies.

A second new capability for Hyper-V Replica in Windows Server 2012 R2 is the introduction of extended replication. This allows a chain of replication to be configured between hosts so that, for example, HOSTA automatically replicates to HOSTB, which automatically replicates to HOSTC. As Figure 2-8 shows, you configure extended replication when you enable replication on a host.

FIGURE 2-8 Hyper-V Replica in Windows Server 2012 R2 now supports extended replication.

One possible use for this new feature would be enterprises that want to do replication both on-premises and to a local hoster. With extended replication, enterprises can do a first-hop replication on-premises and then a second hop offsite, like this:

On-premises host A → On-premises host B → Hosting provider

Another usage scenario might be for hosting providers that provide Hyper-V Replica services to their customers and also want to replicate customer virtual machines to the hoster's backup data center. Extended replication in this scenario would thus be:

Customer site → Primary data center → Secondary data center

These enhancements to Hyper-V Replica in Windows Server 2012 R2 don't just represent new features added to the platform in response to customer requests; they also represent the next steps in Microsoft's vision of offering cloud-scale disaster recoverability solutions based on the Windows Server platform, System Center, and Windows Azure. As Figure 2-9 shows,

another key part of this vision is Windows Azure Hyper-V Recovery Manager, a Windows Azure service that provides orchestration of the replication of private clouds managed using System Center Virtual Machine Manager 2012 R2.

FIGURE 2-9 Hyper-V Replica and Hyper-V Recovery Manager (HRM) are part of Microsoft's vision for cloud-scale disaster recoverability.

For example, by using Hyper-V Recovery Manager together with VMM 2012 R2, you can replicate your organization's primary data center to your disaster recovery site as shown in Figure 2-10. Using Hyper-V Recovery Manager, you can enhance your organization's disaster recovery preparedness by performing failovers of selected virtual machine workloads in your environment to replicate them to your backup site. And the best thing about it is that you can do this at a fraction of the cost of using traditional SAN replication.

FIGURE 2-10 Hyper-V Recovery Manager lets you replicate your organization's primary data center to your disaster recovery site using Windows Azure.

Additional Hyper-V improvements

Hyper-V in Windows Server 2012 R2 also includes support for Quality of Service (QoS) management for virtual hard disks, which allows you to monitor and restrict the Input/Output Operations Per Second (IOPS) for a virtual hard disk attached to a virtual machine. We'll talk about this in Chapter 3, "Storage," since it fits well into the theme of that chapter.

Hyper-V in Windows Server 2012 R2 also now allows guest clustering using shared VHDX files. This new capability is going to be a game changer, especially for hosters who want to maintain separation between their own storage infrastructure and that of their tenants. Since this is related to the topic of clustering, we'll defer discussion of this until we get to Chapter 4, "Failover Clustering" later in this book.

Finally, the Hyper-V Virtual Switch and Hyper-V Network Virtualization have also been enhanced in Windows Server 2012 R2 in a number of important ways. Since this is related to the topic of networking, we'll defer discussion of this to Chapter 5, "Networking" later in this book.

Learn more

You can learn more about the new Hyper-V features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Hyper-V in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn282278.aspx*.
- "Generation 2 Virtual Machine Overview" at *http://technet.microsoft.com/en-us/library/dn282285.aspx*.
- "Automatic Virtual Machine Activation" at *http://technet.microsoft.com/en-us/library/dn303421.aspx*.
- "Online Virtual Hard Disk Resizing Overview" *at http://technet.microsoft.com/en-us/library/dn282286.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "Overview of Windows Server 2012 Hyper-V" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B338*.
- "Understanding Hyper-V Replica: Performance, Networking and Automation" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B373*.
- "Comparing Windows Server Hyper-V and VMware vSphere" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B353*.

CHAPTER 3

Storage

Storage is a key part of any IT infrastructure. For many organizations, storage is also a major cost center that consumes a large portion of the budget of the IT department. Maximizing the performance and efficiency of storage while helping to reduce costs was a major goal of Windows Server 2012, and the numerous new features and capabilities introduced in that platform now provide enterprises with new ways of squeezing the most out of shrinking IT budgets when it comes to storage.

Windows Server 2012 R2 takes these previous enhancements a step further and enables organizations to re-envision how storage infrastructure can be built and managed. This chapter examines the new storage features in Windows Server 2012 R2, focusing mainly on improvements to file- and block-based storage in the platform. The next chapter will build on this one by examining how failover clustering has been enhanced in Windows Server 2012 R2 and how Hyper-V virtualization can benefit from the improvements to storage and failover clustering. But first we'll briefly review some of the storage enhancements that were previously introduced in Windows Server 2012.

Previous enhancements to storage

A number of new storage capabilities were introduced in the previous version of Windows Server, and space doesn't allow us to describe each of them in detail. But as a quick summary, the following might be characterized as some of the more significant storage improvements in the platform:

Storage Spaces Storage Spaces provided storage virtualization capabilities that allow you to group industry-standard disks (such as Serial ATA or Serial Attached SCSI disks) into storage pools. You could then create virtual disks called "storage spaces" or "spaces" from the available capacity in the pools and provision resilient storage volumes as they were needed. This allowed you to make more efficient use of disk capacity, provision storage quickly and easily without impacting users, delegate the administration of storage, and provide cost-effective storage for business-critical applications that make use of low-cost, commodity-based just-a-bunch-of-disks (JBODs).

SMB 3.0 A new version of the Server Message Block (SMB) protocol, a network file sharing protocol that enables applications on a computer to read and write to files and to request services from server programs on a network, was introduced in

Windows Server 2012. These improvements included SMB Direct, SMB Multichannel, SMB Transparent Failover, and other enhancements that enabled new scenarios such as storing Hyper-V virtual machine files and Microsoft SQL Server database files on file shares on an SMB 3.0 file server (called a Scale-out File Server) instead of having to store these files on local storage, Direct Attached Storage (DAS), or a Storage Area Network (SAN) array.

ReFS The new Resilient File System (ReFS) introduced in Windows Server 2012 provided enhanced integrity, availability, scalability, and error protection for file-based data storage. ReFS supported volume sizes up to 18 exabytes and could be especially useful on file servers storing large amounts of data or running disk-intensive applications that require high levels of performance. ReFS in Windows Server 2012 did not support certain NTFS features, however, such as disk quotas.

Data deduplication Data deduplication allowed more data to be stored in less space without compromising the integrity or fidelity of the data stored on the volume. It accomplished this by segmenting files into small, variable-sized chunks, identifying any duplicate chunks present, and maintaining only a single copy of each unique chunk of data. One scenario where this was useful was when data was transferred over the WAN to a branch office using the BranchCache feature of Windows Server 2012.

iSCSI Target Server The iSCSI Target Server provides block storage to servers and applications on the network using the Internet SCSI (iSCSI) standard. When combined with other availability technologies in Windows Server 2012, iSCSI Target Server provided continuously available storage that previously required organizations to purchase expensive, high-end SAN arrays.

ODX Offloaded Data Transfer (ODX) functionality in Windows Server 2012 enabled ODX-capable storage arrays to bypass the host computer and directly transfer data within or between compatible storage devices. The result was to minimize latency, maximize array throughput, and reduce resource usage, such as CPU and network consumption on the host computer. For example, by using ODX-capable storage arrays accessed via iSCSI, Fibre Channel, or SMB 3.0 file shares, virtual machines stored on the array could be imported and exported much more rapidly than they could without ODX capability being present.

Chkdsk Windows Server 2012 introduced a new Chkdsk model that allowed organizations to confidently deploy large, multiterabyte NTFS file system volumes without worrying about their availability being compromised should file system corruption be detected on them. The new version of Chkdsk ran automatically in the background and actively monitored the health state of the file system volume. Should file system corruption be detected, NTFS now instantaneously self-healed most issues online without requiring Chkdsk to run offline. This means that the amount of time needed for running Chkdsk on multiterabyte data volumes can be reduced from hours to only a few seconds, plus in many scenarios you won't even need to take the disk offline and run Chkdsk on it at all.

Storage management improvements Beginning with Windows Server 2012, you could now use the File and Storage Services role in Server Manager to remotely manage multiple file servers running Windows Server 2012, including their storage pools, volumes, shares, and iSCSI

virtual disks, all from a single user interface. You could also use the new Windows PowerShell cmdlets in Windows Server 2012 to automate the same storage management tasks.

Now that we've reviewed the storage improvements introduced previously in Windows Server 2012, let's move on and look at some of the new storage capabilities and enhancements added in Windows Server 2012 R2.

Microsoft's vision for storage

As you can see from the previous section, Windows Server 2012 introduced a lot of new storage features and capabilities to the Windows Server platform. Together with System Center 2012 SP1, Windows Server 2012 provided organizations with a cost-effective solution for building and deploying private clouds using file-based storage access composed of low-cost commodity storage accessed over a standard Ethernet network.

Although the R2 release of Windows Server 2012 adds a number of incremental improvements to both file- and block-based storage and to how storage is managed on the Windows Server platform, it also represents something more. Microsoft's vision and goals with respect to storage for this new release are threefold:

- To greatly reduce the capital and operational storage and available costs for organizations deploying Infrastructure-as-a-Service (IaaS) services for private clouds, hosted clouds, and cloud service providers.
- To disaggregate compute and storage resources so they can be independently managed and scaled at each layer of cloud infrastructure.
- To allow enterprises to build software-defined storage solutions using inexpensive, industry-standard servers, networks, and shared JBOD storage.

With this focus in mind, the incremental improvements to storage capabilities in Windows Server 2012 R2 are designed to specifically target the above three goals.

Building the solution using Windows Server 2012 R2

To understand how Windows Server 2012 R2 can be used to implement the above vision for cloud computing, let's look at an example. Figure 3-1 shows the compute, networking, and storage components of a simple private cloud solution built using the Windows Server platform. You can think of this solution as having four layers as follows:

- **Compute layer** At the top are several Hyper-V hosts joined together in a failover cluster. These hosts use commodity server hardware to provide cost-efficient scale-out capabilities. For example, if the solution needs more processing power to run more workloads running in virtual machines, you can add another commodity server to the Hyper-V cluster. Utilizing the scale-out approach like this is often a more cost-effective solution for organizations than using a scale-up solution that involves only two expensive high-end host machines, where you need to add another processor to each host if you want to run more workloads.

- **Network layer** A low-cost industry-standard Ethernet network is used to connect the Hyper-V cluster that provides compute resources for the solution with the Scale-out File Servers (SoFS) that provide virtualized storage resources for the cloud. This kind of approach can be a lot more cost-effective for many organizations than utilizing a proprietary SAN for their storage layer. That's because you don't need to install expensive host bus adapters (HBAs) in the Hyper-V hosts to enable them to connect to storage volumes (logical unit numbers, or LUNs) provisioned on the SAN. This approach is only possible, however, because of new capabilities in version 3.0 of the SMB protocol that was first introduced in Windows Server 2012.
- **Virtualized storage layer** The virtual machines running on the clustered Hyper-V hosts have their virtual machine files (virtual hard disks, configuration files, snapshots, and so on) stored on SoFS. SoFS was first introduced in Windows Server 2012 and represented clustered file servers that allow you to store server application data, such as Hyper-V virtual machine files or SQL Server database files, on file shares while maintaining a similar level of reliability, availability, manageability, and high performance as using a SAN for storing such files. With a SoFS, all file shares are online on all nodes simultaneously in an active-active cluster configuration. Again, this kind of approach can be much more cost-effective for organizations than using a SAN for storing the virtual machine files for a Hyper-V cluster. And again, using a scale-out approach instead of scale-up can be a more cost-effective solution, and as we'll see in the next chapter, Windows Server 2012 R2 increases the scale-out capabilities of the SoFS role service.

  To enable the virtualization of storage resources, Storage Spaces can be used on SoFS. This allows the physical storage resources for the solution to be pooled together to provide resiliency in case of failure of a storage device. Storage Spaces was also introduced in Windows Server 2012 and provides two types of resiliency—mirroring and parity. Storage devices can be selectively reserved as hot spares so they can automatically replace devices that fail, thus ensuring that the integrity of data is preserved in the event of a power interruption or hardware failure. The storage pools you create using Storage Spaces can be used to provision virtual disks (virtualized storage) on which you can create new volumes and shares for your solution.
- **Physical storage layer** Depending on the performance needs of the workloads running in the solution, the virtual machine files for the Hyper-V clusters can be stored on different types of storage devices. Supported drives include Serial ATA (SATA) and Serial Attached SCSI (SAS) disks, which can be either hard disk drives (HDDs) or solid-state drives (SSDs). These disks can either be internal to the SoFS, directly connected as DAS, or within JBOD enclosures.

FIGURE 3-1 Microsoft's vision for storage can implemented by using Windows Server 2012 Hyper-V, SoFS clusters, and shared JBOD storage.

Although this kind of cloud solution is already possible using Windows Server 2012, the enhancements to virtualization, storage, and networking in Windows Server 2012 R2 now make it possible to optimize such solutions to achieve enterprise-quality levels of performance, reliability, and availability. That's why Windows Server 2012 R2 is being positioned by Microsoft as a cloud-optimized server operating system.

Enabling the solution using System Center 2012 R2

Windows Server 2012 R2 only represents the foundation for a cloud solution. To manage the cloud solution and the workloads running on it, you also need System Center, and in particular you need System Center Virtual Machine Manager (VMM). What truly makes this new release of Windows Server a cloud-optimized operating system is that it represents the first time that Microsoft has synchronized the product release cycles of Windows Server and System Center. The goal of doing this is to ensure that Microsoft can deliver to both its enterprise and service provider customers a completely integrated solution for building and deploying both private and hosted clouds.

To achieve this goal, the R2 release of System Center 2012 (particularly in VMM 2012 R2) also includes numerous enhancements, particularly in the areas of storage performance, provisioning, and management. For example, System Center 2012 R2 now supports:

- Faster enumerations through its Storage Management Initiative - Specification (SMI-S) storage service
- Real-time updates for out-of-band changes using Common Information Model (CIM) indications
- Fibre Channel fabric discovery and zone provisioning
- Support for Hyper-V Virtual Fibre Channel
- ODX optimized virtual machine deployments
- Rapid provisioning using differencing disks

Although the focus of this book is on Windows Server 2012 R2 and its new features and enhancements, System Center 2012 R2 (and particularly VMM) should really be considered the default platform going forward for managing a cloud solution built using Windows Server 2012 R2 as its foundation.

Storage Management API

One of the key storage management improvements introduced in Window Server 2012 and System Center 2012 was the Storage Management application programming interface (SM-API). SM-API is a Windows Management Infrastructure (WMI)–based programming interface that provides a standards-based way of managing storage on the Windows Server platform, and it supersedes the Virtual Disk Service (VDS) API used in previous versions of Windows Server. And in VMM 2012, the new Windows Standards–Based Storage Management service—which utilizes SM-API—replaces the Microsoft Storage Management Service used in previous versions of VMM.

Figure 3-2 shows how SM-API can be used to manage different kinds of storage providers, arrays, and devices by using Server Manager, VMM, or a third-party storage management tool. (You can also use Windows PowerShell to manage storage on Windows Server 2012.) Some examples of different types of storage providers and arrays you can manage using SM-API include:

- Older symmetric multiprocessing (SMP) based internal storage subsystems
- Newer SMI-S-based internal storage subsystems
- SMI-S-based network attached storage (NAS) devices
- SMI-S-compliant Fibre Channel switches on SAN arrays using CIM pass through
- JBODs that are compatible with Storage Spaces using CIM pass through

FIGURE 3-2 SM-API can be used to manage a wide range of storage providers and arrays.

Although SM-API isn't new in this R2 release of Windows Server 2012, it has been enhanced in several ways, and especially in the area of performance. Specifically, the new version of SM-API includes:

- A new architecture that performs enumerations of storage resources 10 times faster than previously
- The addition of remoting and cluster-awareness when managing Storage Spaces
- Support for new Storage Spaces features like write-back caching and storage tiering which are described later in this chapter
- The ability to use VMM to manage Storage Spaces and SoFS using SM-API

Storage QoS

Storage Quality of Service (QoS) is another new feature of file-based storage introduced in Windows Server 2012 R2. Storage QoS is enabled at the VHDX layer and allows you to limit the maximum IOPS allowed to a virtual disk on a Hyper-V host. It can also allow you to set triggers to send notifications when a specified minimum IOPS is not met for a virtual disk. Possible usage scenarios for this feature include:

- Configuring different service-level agreements (SLAs) for different types of storage operations within your infrastructure. For example, a hoster might use this feature to configure Bronze, Silver, and Gold SLAs for storage performance available for different classes of tenants. You can even set alerts that trigger when virtual machines are not getting enough IOPS for storage access.
- Restricting the disk throughput for overactive or disruptive virtual machines within your environment that are saturating the storage array. Hosting providers will especially love this capability since it means they won't have to worry about one tenant consuming excessive storage fabric resources at the expense of other tenants.

As Figure 3-3 shows, Storage QoS can even be configured while the virtual machine is running. This allows organizations to have a lot of flexibility in how they manage access to the storage fabric from workloads running in their cloud environments.

FIGURE 3-3 You can configure Storage QoS for a virtual machine using Hyper-V Manager.

iSCSI Target Server enhancements

Internet Small Computer System Interface (iSCSI) is an industry-standard protocol that allows sharing of block-level storage over a TCP/IP network. Block-level storage is typically used in SANs and is supported by the iSCSI, Fibre Channel, and SAS connection mechanisms. File-level storage involves using network shares on volumes that have been formatted using a file system like NTFS or ReFS.

iSCSI is designed to transmit and receive Small Computer System Interface (SCSI) commands and data encapsulated as TCP packets. This enables servers to utilize storage on an iSCSI-based storage device, such as an iSCSI SAN, even when the servers and SAN are in different locations.

Fibre Channel SANs can be prohibitively expensive for a small or midsized business because they require specialized connection hardware such as HBAs and cabling. By contrast, iSCSI needs no specialized connection hardware or special-purpose cabling because it can use a standard Ethernet network for connecting servers with the storage array. This means that iSCSI storage can be deployed using an organization's existing network infrastructure, which helps keep the cost of the iSCSI approach low.

Beginning with Windows Server 2012, a built-in role service (iSCSI Target Server) and client component (iSCSI Initiator) are included and can be used to implement an iSCSI-based storage solution without the need of purchasing a third-party iSCSI SAN. Using these new features, organizations can deploy iSCSI storage without the need of purchasing any additional storage hardware or software.

Some of the usage scenarios for iSCSI storage include:

- Deploying diskless servers that boot from iSCSI virtual disks over the network
- Providing block storage to applications that require or can benefit from it
- Creating iSCSI storage test environments where you can validate applications before deploying them onto a third-party iSCSI SAN

Because Microsoft iSCSI technologies are based on industry standards, you can also deploy Windows Server–based iSCSI storage solutions together with third-party solutions.

One of the key components of the iSCSI implementation in Windows Server 2012 is iSCSI Target Server, a role service under the File and Storage Services role. In a typical iSCSI storage scenario, an iSCSI initiator (a service running on the server consuming the storage) establishes a session (consisting of one or more TCP connections) with an iSCSI target (an object on the target server that allows an iSCSI initiator to establish a connection with the target server) in order to access an iSCSI virtual disk (storage backed by a virtual hard disk file) on the iSCSI Target Server (the server or device, such as a SAN, that shares storage so that users or applications running on a different server can consume the storage). Figure 3-4 shows how these different iSCSI components work together on the Windows Server platform.

FIGURE 3-4 The basic iSCSI components work together on Windows Server.

In the R2 release of Windows Server 2012, the iSCSI Target Server role service has been enhanced in a couple of important ways:

- VHDX support is now included, which enables the provisioning of larger LUNs up to 64 TB in size. VHDX support also means you can now expand or shrink iSCSI LUNs while they are online (see the section "Online VHDX resize" in Chapter 2, "Hyper-V") and dynamically grow them for greater scalability and flexibility. And VHDX is now the default virtual disk format when creating new iSCSI LUNs.
- iSCSI Target Server can now be fully managed using SMS-S. This means that you can now perform end-to-end management of your iSCSI storage system using VMM.

SMB 3.0 enhancements

SMB 3.0 is at the core of the new SoFS functionality introduced previously in Windows Server 2012 and enables file-based storage solutions (file servers) to provide network storage for servers that have similar performance to expensive, proprietary SAN solutions. Using SMB 3.0 and the Windows Server 2012 platform, organizations can build low-cost scale-out storage fabrics that can meet the needs of a broad range of private and hosted cloud solutions.

Some of the key features of SMB 3.0 include:

- **SMB Scale Out** Allows you to create file shares using Cluster Shared Volumes (CSV) to provide simultaneous access to data files, with direct I/O, through all nodes in a file server cluster. This results in improved utilization of network bandwidth, load balancing of SMB 3.0 clients, and optimized performance for server applications.
- **SMB Transparent Failover** Allows you to perform hardware or software maintenance of nodes in a clustered SMB 3.0 file server (an SoFS) without interruption to server applications storing data on the file shares. If a hardware or software failure occurs on a cluster node, SMB 3.0 clients can transparently reconnect to another cluster node without interruption as well.
- **SMB Direct** Supports using network adapters that have Remote Direct Memory Access (RDMA) capability, which allows them to function at full speed with very low latency and very low CPU utilization. When used with workloads, such as Hyper-V or SQL Server, the result is that a remote SMB 3.0 file server can resemble local storage in its performance.
- **SMB Multichannel** Provides aggregation of network bandwidth and network fault tolerance when multiple paths are available between the SMB 3.0 client and the SMB 3.0 file server. This results in server applications taking full advantage of all available network bandwidth and being more resilient to network failure.
- **SMB Encryption** Provides end-to-end encryption of SMB data to protect data from eavesdropping without the need for configuring Internet Protocol security (IPsec), deploying specialized hardware, or utilizing WAN accelerators. Encryption can be configured on a per share basis or for the entire SMB 3.0 file server.

With the release of version 3.0 of SMB, the SMB protocol has become more than just a network file sharing protocol used for copying files over a network. Some of the additional uses for SMB now include:

- A protocol transport for CSV that enables I/O forwarding between the nodes of a failover cluster.
- A storage protocol that enables Hyper-V hosts to access and run virtual machine files stored on file servers on the network.
- A protocol transport for performing live migrations of virtual machines between clustered and nonclustered Hyper-V hosts.

A number of improvements have been made to SMB 3.0 in Windows Server 2012 R2. For example, the performance of SMB Direct has been enhanced to provide a 50 percent improvement for small IO workloads when used with RDMA-capable network adapters. For example, 8KB data transfers have now increased from about 300K I/O operations per second (IOPS) to about 450K IOPS per interface.

A second improvement is the increased efficiency and density of hosting workloads with small I/Os, for example, when running an online transaction processing (OLTP) database workload inside a virtual machine. SMB Direct in Windows Server 2012 R2 also includes optimizations for using 40 Gbps Ethernet and 56 Gbps InfiniBand for network transport.

SMB connections can also now be managed per share on SoFS instead of per file server as in Windows Server 2012. But we'll defer further discussion of this until we reexamine SoFS in Chapter 4, "Failover Clustering."

Another new feature of SMB 3.0 in Windows Server 2012 R2 is SMB Bandwidth Management. Because SMB now has so many different functions in a network and storage infrastructure built using Windows Server 2012, it now represents a common infrastructure component in many environments. That means it's important to be able to control how much bandwidth SMB uses when it's performing many different tasks within an infrastructure. As Figure 3-5 shows, you can now configure bandwidth limits for different categories of SMB usage. For example, the figure shows that three categories of bandwidth limits have been configured to ensure optimal performance of the various infrastructure components present in this infrastructure:

- **Default** A limit of 100 MB/s has been configured for Hyper-V host 1 to use SMB when performing file copies from the file server used for library storage by VMM 2012 R2.
- **VirtualMachine** No limit has been set for the amount of bandwidth that Hyper-V host 1 can utilize when using SMB to access virtual machine files stored on the SoFS.
- **LiveMigration** A limit of 500 MB/s has been set for SMB to use when performing live migrations of virtual machines from Hyper-V host 1 to Hyper-V host 2.

FIGURE 3-5 SMB 3.0 now supports bandwidth management.

Data deduplication enhancements

Data deduplication was introduced in Windows Server 2012 to help enterprises cope with exponentially increasing growth of data storage in their environments. Data deduplication allows Windows Server 2012 to store more data in less physical space to optimize the capacity of their storage fabric. Data deduplication is highly scalable, resource efficient, and nonintrusive in Windows Server 2012 and can run on multiple volumes simultaneously without affecting other workloads running on the server. Checksums, consistency, and identity validation are used to ensure data integrity, and redundant copies of file system metadata are maintained to ensure data is recoverable in the event of corruption.

Windows Server 2012 R2 includes several important improvements to the way data deduplication works. For example, in the previous version deduplication could only be used with files that are closed, such as virtual machine files stored in the VMM library. With this new release, however, deduplication can now be used even with open virtual hard disk files (both VHD and VHDX) for virtual desktop infrastructure (VDI) scenarios using SMB 3.0 remote storage.

Deduplication in Windows Server 2012 was also incompatible with CSVs. This meant that deduplication couldn't be used to optimize storage of virtual machine files stored on SoFS. This limitation has now been removed in the R2 release of Windows Server 2012 with support for deduplication of data stored on CSVs used by SoFS. For example, Figure 3-6 shows a failover cluster of Hyper-V hosts with the virtual machine files being stored on CSVs used by a two-node SoFS. In order for this scenario to work, SMB 3.0 must be used as the network

storage protocol. Although SoFS running Windows Server 2012 can provide this functionality, using SoFS running Windows Server 2012 R2 enables deduplication to be turned on for the CSVs, which enables space savings as high as 90 percent on the CSVs. This type of space savings can be especially beneficial for Windows Server 2012 or Windows Server 2012 R2 Hyper-V or VDI deployments using remote storage on the Windows Server 2012 R2 SoFS.

FIGURE 3-6 Windows Server 2012 R2 now supports data deduplication on CSV volumes and live VDI image files on SMB 3.0 storage.

Other improvements to data deduplication in Windows Server 2012 R2 include performance enhancements resulting from faster read/write of optimized files and improved optimization speed. Deduplication is supported only for data volumes, however, and not for boot or system volumes. In addition, ReFS volumes do not support using deduplication.

Storage Spaces enhancements

Until Windows Server 2012 was released, implementing storage virtualization required purchasing proprietary third-party SAN solutions that were expensive and required using their own set of management tools. Such solutions also required special training to implement, manage, and maintain them effectively. Storage Spaces, first introduced in Windows Server 2012, was designed to make storage virtualization affordable even for small businesses. Storage Spaces is simple to deploy and manage, and it can provide businesses with shared storage that can grow on demand to meet an organization's changing needs.

Some of the benefits of using Storage Spaces include:

- **Increased scalability** Additional physical storage can easily be added and used to meet increasing business demands.
- **Increased flexibility** New storage pools can be created and existing ones expanded as the need arises.

- **Increased efficiency** Unused storage capacity can be reclaimed to enable more efficient use of existing physical storage resources.
- **Increased elasticity** Storage capacity can be preallocated by using thin provisioning to meet growing demand even when the underlying physical storage is insufficient.
- **Lower cost** Low-cost, commodity-based storage devices can be used to save IT departments money that can be better allocated elsewhere.

To understand how Storage Spaces might be used for private cloud solutions, Figure 3-7 compares a traditional SAN-based storage solution with one built using Storage Spaces in Windows Server 2012. On the left side is a cluster of Hyper-V hosts whose virtual machine files are stored in LUNs on the SAN. These LUNs are backed by enterprise-class SAS disks (which can be HDDs or SSDs) mounted in disk shelves in the SAN chassis. Establishing connectivity between the Hyper-V host cluster and the SAN requires installing Fibre Channel or iSCSI HBAs in these hosts (depending on type of SAN involved) and data is transferred between the SAN and the Hyper-V host cluster using either Fibre Channel or iSCSI as a block-level storage protocol. Proprietary technology is required for this solution in the form of HBAs, cabling, and the SAN chassis.

By comparison, using Storage Spaces on the right requires no use of proprietary technology. Instead, all of the components of this solution can use off-the-shelf commodity-based server hardware. The SAN chassis is replaced with a cluster of file servers running Windows Server 2012 on enterprise-level server system hardware and rack-based JBOD enclosures containing the same kind of enterprise-class SAS disks (HDDs or SSDs) that might be used in the traditional SAN approach. Connectivity between the Hyper-V host cluster requires only a standard Ethernet network (typically 10 GbE) and high-performance network interface cards installed in the Hyper-V hosts and uses SMB 3.0 as a file-based storage protocol. Everything is commodity hardware here, and there's no vendor lock-in as there is with the traditional SAN approach.

FIGURE 3-7 A comparison of traditional SAN storage with one based on Storage Spaces.

Storage Spaces in Windows Server 2012

The reaction when Storage Spaces was announced was somewhat qualified, especially by large enterprises that run workloads requiring the highest levels of performance involving millions of IOPS and massive throughput. The reason for this was because it was initially assumed that the performance of a virtualized storage solution based on Storage Spaces would fall short of what a typical SAN array can deliver. However, Microsoft soon proved its critics wrong with a demonstration performed at TechEd 2012, where a three-node high-performance server cluster was connected to a 24-bay JBOD filled with enterprise-grade SSDs. When Storage Spaces was used to present storage from the JBOD to the cluster nodes, the performance resulted in an aggregate sequential throughput of 12 GB/s and 1.45 million IOPS. When a second JBOD was added to the environment, the IOPS were increased to 2.7 million! Clearly, Storage Spaces is an enterprise-ready storage virtualization technology and its usage scenarios are not limited only to smaller deployments.

The challenge, however, with the Windows Server 2012 version of Storage Spaces is deciding whether you want to optimize performance or storage capacity when building your storage virtualization solution. For example, if you use Storage Spaces to create storage pools backed by low-cost, large-capacity commodity HDDs, you get a capacity-optimized storage solution, but the performance might not be at the level that some of your applications require. This is typically because large-capacity HDDs are optimized for sequential data access, whereas many server applications perform best with random data access. On the other hand, if you create pools using more expensive SSDs, you can easily achieve the kind of random I/O performance your applications require, but you probably won't have enough room in your budget to meet your capacity requirements for storage.

The logical solution is to use a mix of low-cost, large-capacity commodity HDDs together with expensive, high-performance enterprise-class SSDs. Building a Storage Spaces solution along these lines can provide you with the best of both worlds and deliver high levels of IOPS at a relatively low cost compared to using a SAN. This means that there are three ways you can build a virtualized storage solution using Storage Spaces in Windows Server 2012:

- **Capacity-optimized approach** Uses only low-cost, large-capacity commodity HDDs to provide high capacity while minimizing cost per terabyte
- **Performance-optimized approach** Uses only expensive, high-performance enterprise-class SSDs to provide extreme performance, high throughput, and the largest number of IOPS per dollar
- **Balanced approach** Uses a mix of HDDs and SDDs to achieve good performance and reasonable capacity at an acceptable cost

Unfortunately, there's a problem with the balanced approach. This is because although most enterprise workloads have a relatively large data set, the majority of data in this working set is often cold (seldom-accessed) data. Only a minority of data is typically in active use at a given time, and this hot data can be considered the working set for such workloads. Naturally, this working set also changes over time for the typical server workload. Since the working set is small, it would seem natural to place the hot data (the working set) on high-performance

SSDs while keeping the majority of the data (which is cold data) on high-capacity HDDs. But the working set changes over time, so how do you seamlessly ensure that hot data is placed on SSDs and cold data on HDDs when you use Storage Spaces to create pools containing both SSDs and HDDs?

The answer is you couldn't do that with Storage Spaces—until now.

Storage Spaces in Windows Server 2012 R2

As Figure 3-8 shows, the Windows Server 2012 R2 version of Storage Spaces now allows you to create a tiered storage solution that transparently delivers an appropriate balance between capacity and performance that can meet the needs of enterprise workloads. The result is that the workload's most frequently accessed data (the working set) will automatically be stored on the SSD tier while the rest of the workload's data is stored on the HDD tier.

How does Storage Spaces accomplish this? By having the file system actively measure the activity of the workload in the background and then automatically and transparently move data to the appropriate tier (SSD or HDD) depending on how hot or cold the data is determined to be. Storage Spaces in Windows Server 2012 R2 can thus ensure that the workload's hot data is always stored on the SSD tier to take advantage of the high performance of this tier, and its cold data on the HDD tier to make use of the high capacity of this tier. If a portion of the data for a particular file becomes hotter (is accessed more frequently), then it gets moved from the HDD tier to the SSD tier. And if the portion of data becomes cooler (is accessed less frequently), then it gets moved from the SSD tier to the HDD tier.

FIGURE 3-8 Storage Spaces in Windows Server 2012 R2 now supports data tiering.

This seamless movement of data between tiers is configured by default to happen daily in 1 MB chunks, but you also have the option of configuring the scheduled task for this operation to run as frequently as you want. Data moves between tiers in the background and has minimal impact on the performance of the storage space. If needed, you can use Windows PowerShell to assign certain files to a specific tier, thereby overriding the automatic placement of data based on heat. For example, the parent virtual hard disk file for a collection of pooled virtual machines in a VDI environment might be assigned to the SSD tier to ensure the file always remains pinned to this tier. The result of doing this can be to achieve significant improvements in the boot times of the hundreds or thousands of virtual desktops derived from this parent virtual hard disk.

Tiered Storage Spaces is an exciting new capability in Windows Server 2012 R2, and when this book is revised and enlarged in the RTM timeframe, we'll take a closer look at how it can be implemented. But there's one additional new feature of Storage Spaces that we'll briefly describe here, and it's called write-back caching. Whereas the goal of tiering is to balance capacity against performance, the purpose of write-back caching is to smooth out short-term bursts of random writes. Write-back caching integrates seamlessly into tiered volumes and is enabled by default. The write-back cache is located on the SSD tier of a storage space and services smaller, random writes; larger, sequential writes are serviced by the HDD tier. You can also enable write-back caching on non-tiered volumes.

Now let's hear from one of our insiders at Microsoft to learn more about the Storage Spaces enhancements in Windows Server 2012 R2 and watch these new features in action.

Storage Spaces in action

Let's examine the new features of Storage Spaces in Windows Server 2012 R2 and see some of them in action.

Storage tiering

It has been observed that SSDs with 15k speed are expensive and low capacity, but with some good performance and poor $/GB rate. On the other hand, 7.5K drives can give much better capacity at a great $/GB rate, but they're slow. We wanted to give our customers a new way to balance scalability and performance, and we have added tiered storage functionality in Windows Server 2012 R2 Storage Spaces.

Using storage tiering, the most active data (hot data) can be placed on SSD and less active data (cold data) will be placed on normal HDD, and hence it provides great throughput for I/O operations.

Tiered storage helps maximize IOPS/$ because it:

- **Utilizes best characteristics of SSDs and HDDs in single storage**
- **Provides balance between capacity and performance**
- **Allows admins to assign files to specific storage**

When creating a virtual disk, we can assign some capacity from the fast tier and slow tier as well. Windows will automatically analyze the data on your virtual disk to identify hot spots (Most Active Data) and cold spots (Less Active Data) and move them into fast and slow tiers, respectively. This capability is very useful in multiple scenarios and provides maximum throughput. For example:

- Assume we are using Storage Spaces for storing VDI virtual machines. The parent VHDX will be pinned to the fast tier, while the child differential disks live in the slow tier.
- During the boot process, SSD provides the good IOPS bandwidth to reduce logon time.

Write-back cache

The write-back caching feature creates a separate write-back cache for each accelerated volume from available SSDs in the Storage Spaces pool. There are many scenarios when we observe spikes in disk I/O and these can reduce write performance. To overcome this, a virtual disk leverages tiered storage to absorb the spike in write activity. Whenever a spike is detected, the SSDs in the fast tier are used, which offers greater IOPS and can take the pressure that the normal HDD tier cannot.

Dual parity and parity space support for failover clusters

This provides resiliency to **two-disk** failures for archival workloads, while minimizing $/TB and space utilization for resiliency. It also provides:

- Efficient rebuild times
- Windows Clustering support
- Integrated journaling for power fault resiliency

Faster storage space rebuild

A storage space and a RAID array can be configured with the traditional hot spare (one or more). When a disk fails, the other available disk is used to replace it. This will offer more IOPS to normal production storage activity and leave your business less vulnerable during a repair process.

Let's watch this in action. The following is a demo showcasing the dual parity capability and the disk repair process for maximizing uptime. We'll start with a Windows Server 2012 R2 that has seven SSDs of different capacities totaling 230 GB that is direct-attached via SAS to the server:

As you can see, there is only the primordial storage pool:

Now let's use all seven physical disks in the primordial pool to create a new storage pool named StoragePool01:

Note that the total capacity of the StoragePool01 is 225 GB but the free space is only 223 GB because some disk space is reserved by Windows for internal purposes. The capacity of the seven physical disks changes to reflect their addition to the new pool:

Now let's create a new virtual disk with dual parity mode:

As you can see, dual parity mode stores three copies of your data and can protect against simultaneous failure of up to two physical disks in the underlying pool.

Here's a screenshot showing the newly created virtual disk named vdisk01:

The Health Status of the new virtual disk is Healthy while its Operational Status is OK. All seven disks are in use:

Health

Health status: Healthy

Operational status: OK

Storage layout: Parity

Physical disks in use:

Slot	Name	Status	Capacity	Free Space	Bus	Chassis	Media Type
	PhysicalDisk1	OK	19.3 GB	17.0 GB	SAS		SSD
	PhysicalDisk7	OK	49.3 GB	47.0 GB	SAS		SSD
	PhysicalDisk6	OK	49.3 GB	47.0 GB	SAS		SSD
	PhysicalDisk5	OK	29.3 GB	28.0 GB	SAS		SSD
	PhysicalDisk2	OK	19.3 GB	17.0 GB	SAS		SSD
	PhysicalDisk4	OK	29.3 GB	27.0 GB	SAS		SSD
	PhysicalDisk3	OK	29.3 GB	27.0 GB	SAS		SSD

After we created the new virtual disk, we created a new volume E: on it as shown here:

Devices and drives (4)

Floppy Disk Drive (A:)	Floppy Disk Drive		
Local Disk (C:)	Local Disk	29.6 GB	18.3 GB
DVD Drive (D:)	CD Drive		
New Volume (E:)	Local Disk	59.8 GB	59.7 GB

Now let's check out the dual parity capability. First, let's detach two physical disks (disks 1 and 2) from the server to simulate the simultaneous failure of two physical disks. When we do this, Storage Spaces shows a warning message for the pool:

STORAGE POOLS
All storage pools | 1 total

TASKS

Filter

Name	Type	Version	Managed by	Available to	Read-Write Server	Capacity	Free Space
Storage Spaces (1)							
StoragePool01	Storage Pool	Windows Server 2012 R2	SRV01	SRV01	SRV01	225 GB	210 GB

In addition, the two detached physical disks display Unknown for their Bus type:

PHYSICAL DISKS
StoragePool01 on SRV01

TASKS

Filter

Name	Capaci...	Bus	Usage
PhysicalDisk-1 (SRV01)	19.3 GB	Unknown	Automatic
PhysicalDisk-1 (SRV01)	19.3 GB	Unknown	Automatic
PhysicalDisk3 (SRV01)	29.3 GB	SAS	Automatic
PhysicalDisk4 (SRV01)	29.3 GB	SAS	Automatic
PhysicalDisk5 (SRV01)	29.3 GB	SAS	Automatic
PhysicalDisk6 (SRV01)	49.3 GB	SAS	Automatic
PhysicalDisk7 (SRV01)	49.3 GB	SAS	Automatic

The virtual disk also shows a warning message:

The Health Status of the virtual disk has changed from Healthy to Warning, and the Operational Status has changed from OK to Degraded:

However, the volume E: that we created from the virtual disk is still accessible:

As you can see, the dual parity capability of Storage Spaces in Windows Server 2012 R2 can compensate for two-disk failures—the volume created previously is in good status for I/O operations.

Now let's see what happens when we remove a third physical disk from the server to simulate the simultaneous failure of three physical disks. When this is done, the virtual disk is now in a failed state since dual parity only tolerates up to two simultaneous disk failures:

The Health Status for the virtual disk now changes to Unhealthy, and its Operational Status becomes Detached:

Health	
Health status:	Unhealthy
Operational status:	Detached
Storage layout:	Parity

If we had additional disks in the pool and wanted Storage Spaces to automatically compensate for disk failures, these additional disks could be configured in Hot Spare mode as per recommended practices. When this is done, a spare disk will switch to Automatic mode whenever a disk failure is detected to ensure maximum uptime. You can change the existing usage mode of a physical disk to Hot Spare mode either using the Storage Spaces canvas of Server Manager or by using Windows PowerShell as shown here:

```
PS C:\Users\Administrator> Set-PhysicalDisk Physicaldisk1 -Usage hotspare
PS C:\Users\Administrator> Get-PhysicalDisk Physicaldisk1

FriendlyName        CanPool             OperationalStatus   HealthStatus   Usage          Size
------------        -------             -----------------   ------------   -----          ----
PhysicalDisk1       False               OK                  Healthy        Hot Spare  29.25 GB
```

Conclusion

Storage Spaces in Windows Server 2012 supports mirrored storage and single parity, which allows single disk failure, but with Windows Server 2012 R2 two disk failures are supported if you configure the inbuilt dual parity mechanism. Additionally, Windows Server 2012 R2 introduces a parallelized repair process, where the remaining healthy disks move around and take responsibility of data that was stored on the failed disk. It is extremely quick because all disks in the storage space are involved. Hence, Storage Spaces delivers sophisticated storage virtualization capabilities, which empower customers to use industry-standard storage for single computer and scalable multinode deployment.

Deepak Srivastava
Partner Consultant, Microsoft

Work Folders

Work Folders is another new File and Storage Services feature introduced in Windows Server 2012 R2 that can help organizations address the bring your own device (BYOD) scenario that so many of them are currently facing as the modern workplace evolves. Work Folders provides a consistent way for users to access their work files from their personal computers and devices anywhere from centrally managed file servers on the corporate network. Work Folders can also be deployed alongside existing deployments of other Microsoft data synchronization solutions such as Folder Redirection (FR), Offline Files (also known as client-side caching, or CSC), and even home folders.

To learn more about how Work Folders works, how you set it up, and how you use it, let's now hear from some insiders on the team who developed this exciting new feature.

Understanding and implementing Work Folders

During Windows Server 2012 R2 planning, we noticed two converging trends around managing and protecting corporate data:

- Users "I need to work from anywhere on my different devices"
- IT "I'd like to empower my information workers (users) while reducing information leakage and keeping control of the corporate data that is sprawled across devices"

Work Folders is a new file server-based sync solution in Windows Server 2012 R2 and Windows 8.1 that is designed to address these two trends. Work Folders enables IT administrators to provide information workers the ability to sync their work data on all their devices wherever they are while remaining in compliance with company policies. This is done by syncing user data from devices to on-premises file servers, which are now extended to include a new sync protocol.

Work Folders as experienced by an information worker

To show how this works, here's an example of how an information worker, Joe, might use Work Folders to separate his work data from his personal data while having the ability to work from any device. When Joe saves a document on his work computer in the Work Folders directory, the document is synced to an IT-controlled file server. When Joe returns home, he can pick up his Surface RT (where the document is already synced) and head to the beach. He can work on the document offline, and when he returns home the document is synced back with the file server and all of the changes are available to him the next day when he returns to the office.

Look familiar? Indeed, this is how consumer storage services such as SkyDrive and business collaboration services such as SkyDrive Pro work. We kept the user

interaction simple and familiar so that there is little user education required. The biggest difference from SkyDrive or SkyDrive Pro is that the centralized storage for Work Folders is an on-premises file server running Windows Server 2012 R2, but we'll get to that a little later in this post.

Work Folders as experienced by an administrator

IT administrators can use Work Folders to gain more control over corporate data and user devices and centralize user work data so that they can apply the appropriate processes and tools to keep their company in compliance. This can range from simply having a copy of the data if the user leaves the company to a wide range of capabilities such as backup, retention, classification, and automated encryption.

For example, when a user authors a sensitive document in Work Folders on his or her work PC, it gets synced to the file server. The file server then can automatically classify the document based on content, if configured using File Server Resource Manager, and encrypt the document using Windows Rights Management Services before syncing the document back to all the user's devices. This allows a seamless experience for the user while keeping the organization in compliance and preventing leakage of sensitive information.

Capabilities of Work Folders

Our main design focus around Work Folders was to keep it simple for the information workers while allowing IT administrators to use the familiar **low-cost, high-scale** Windows file server with all the rich functionality available on the back end from high availability to comprehensive data management. Some of the functionality provided by Work Folders includes the following:

- It provides a single point of access to work files on a user's work and personal PCs and devices (Windows 8.1 and Windows RT 8.1, with immediate plans to follow up with Windows 7 and iPad support and other devices likely in the future).
- It enables users to access work files while offline and sync with the central file server when the PC or device next has Internet or network connectivity.
- It helps maintain data encryption in transit, as well as at rest, on devices and allow corporate data wipe through device management services such as Windows Intune.
- It uses existing file server management technologies, such as file classification and folder quotas, to manage user data.
- You can configure security policies to instruct user PCs and devices to encrypt Work Folders and use a lock screen password, for example.
- You can implement Failover Clustering together with Work Folders to provide a high-availability solution.

Considerations for Work Folders

When planning for the implementation of Work Folders, you need to be aware of the following considerations:

- Backend storage is provided by on-premises file servers and Work Folders must be stored in local storage on the file server (for example, data can be on local shares on a Windows Server 2012 R2).
- Users sync to their own folder on the file server—there is no support for syncing arbitrary file shares (for example, sync the sales demos share to my device).
- Work Folders doesn't provide collaboration functionality such as sharing sync files or folders with other users (we recommend using SkyDrive Pro if you need document collaboration features).

Comparison between Work Folders and other data sync solutions

The table below compares the different underlying technologies used and intended usage scenarios for Work Folders, FR/CSC, Microsoft SkyDrive, and Microsoft SkyDrive Pro.

Sync solution	Data location	Access protocol	Intended usage scenarios	Support for personal devices
Work Folders	File server	HTTPS	The user's work data	Yes
FR/CSC	File server	SMB (on-premises or VPN)	The user's work data	No
SkyDrive	Public cloud	HTTPS	The user's personal data	Yes
SkyDrive Pro	SharePoint Online in Office 365 or on-premises SharePoint 2013	HTTPS	The user's work data and team work data	Yes

Setting up Work Folders

The following is a brief overview of how to set up and use Work Folders. Note that additional steps are required to enable the client computer to be able to retrieve Work Folders settings and connect to the server across the Internet. For more detailed information see the Work Folders Test Lab Deployment Guide referenced in the Learn More section at the end of this chapter.

Work Folders requires an Active Directory environment. Start by installing the Work Folders role service on a file server running Windows Server 2012 R2. The Work Folders role service is part of the File and iSCSI Services role service for the file and Storage Services role:

Installing the Work Folders role service will also install some components of the IIS (Web Server) role.

A new Work Folders page will be added to the File and Storage Services canvas in Server Manager. To configure Work Folders, you first need to create a sync share, which maps to a local path where all the user folders will be hosted under and to the group of users who can access the sync share:

Creating a sync share simply allows the user to access the data hosted on the file server through the Sync protocol. Selecting the New Sync Share task, as shown previously, launches the New Sync Share Wizard:

If you already have a local path that has been configured as an SMB share, such as a Folder Redirection share, you can simply select the first option, Select By File Share. In this walkthrough, we have selected the Enter A Local Path option to create a new SMB share for the folder C:\SalesShare on the file server.

The next page of the wizard allows us to specify the structure for user folders. There are two options here:

- **Using user alias** This option is selected by default and is compatible with other technologies such as Folder Redirection or home folders. For example, the folder for Karen Berg will be named after her alias kberg.
- **Using a combination of user alias and domain information** This option ensures the uniqueness of the folder name for users across domains. For example, let's say your organization has two users named Karen Berg, one in the hq.contoso.com domain and the other in the research.contoso.com domain. The folder for the first Karen will be named kberg@hq.contoso.com and the folder for the second Karen will be named kberg@research.contoso.com, thus ensuring each Karen has her own unique folder.

By default, all the folders/files under the user folder will be synced to the devices. The **check box** allows the admin to specify a single subfolder to be synced to the devices.

The next page allows you to specify the sync share name and an optional description:

The next page is where you can assign specific security groups for sync share access:

Note that, by default, administrators will not be able to access user data on the file server. If you want to enable administrator access to user data, clear Disable Inherited Permissions And Grant Users Exclusive Access To Their Files.

The next page is where you can configure device policies:

Selecting the Encrypt Work Folders Policy will ensure the document under the work folders on the client devices is encrypted with the Enterprise ID. By default, the Enterprise ID is the user primary SMTP email address (which is also the proxyAddresses attribute of the user object in Active Directory). Encryption using a different key ensures that deleting the user's Work Folder documents will not delete the user's personal documents on the same device.

Selecting the Automatically Lock Screen And Require A Password Policy (this is selected by default) enforces the following policy on the user's device:

- Minimum password length of 6
- Autolock screen set to be 15 minutes or less
- Maximum password retry of 10 or less

If the user's device doesn't meet the configured policies, the user will not be able to set up Work Folders.

Once you've completed the wizard, we can enable the sync share for SMB access by right-clicking the SalesShare folder in Windows Explorer and selecting Share With,

and then Specific People. Then in the File Sharing dialog, add the Sales group and give it Read\Write access, as shown here, and then click Share:

All of the above can also be done of course with Windows PowerShell commands, if desired.

By default, the Work Folders client always **connects** to the file server using SSL, which requires the server to have an SSL certificate installed and configured.

Once Work Folders has been set up on the file server, the user can now set up Work Folders on client computers and devices. For example, on a computer running Windows 8.1 the user would open Control Panel, select System and Security, and then select Work Folders. Doing this displays the Manage Work Folders item as shown here:

The user then provides his or her email address and domain credentials, accepts or changes where the Work Folders will be stored (by default in the user profile), and consents to the configured Work Folders policies being applied.

At this point a new icon labeled Work Folders will be displayed under This PC in Windows Explorer on the user's computer:

At this point Work Folders has been configured on both the server and client sides and is ready for use. To test Work Folders, the user could use two client PCs running Windows 8.1. The user begins by using Notepad to create a new text file named "test" on the first PC and saves the file to the Work Folders location (which, as the previous screenshot shows, has been added under Favorites in Windows Explorer). When the file is saved, Work Folders automatically syncs the file to the Work Folders location on the second PC as shown here:

For a more detailed demonstration of how to configure Work Folders on both the server and client sides, and of how the user can store and access data using Work Folders, see the Work Folders Test Lab Deployment guide, which is referenced in the "Learn more" section at the end of this chapter.

Nir Ben Zvi
Principal Program Manager, WSSC WS PM USA

Learn more

You can learn more about the new storage features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "New and changed functionality in File and Storage Services" at *http://technet.microsoft.com/en-us/library/4cb00829-8d05-4499-8adc-7506e159f857#BKMK_NEW*.
- "What's New for iSCSI Target Server in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn305893.aspx*.
- "What's New for SMB in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/hh831474.aspx*.
- "Storage Quality of Service for Hyper-V" at *http://technet.microsoft.com/en-us/library/dn282281.aspx*.
- "Storage Spaces Overview" at *http://technet.microsoft.com/en-us/library/hh831739.aspx*.
- "Work Folders Overview" at *http://technet.microsoft.com/en-us/library/dn265974.aspx*.

The following Microsoft TechNet and MSDN blog posts also have lots of information about the new storage features and enhancements in Windows Server 2012 R2:

- "Storage Transformation for your Datacenter" at *http://blogs.technet.com/b/windowsserver/archive/2013/06/26/storage-transformation-for-your-datacenter.aspx*.
- "What's New for SMI-S in Windows Server 2012 R2" at *http://blogs.technet.com/b/filecab/archive/2013/07/31/what-s-new-for-smi-s-in-windows-server-2012-r2.aspx*.
- "Introducing Work Folders on Windows Server 2012 R2" at *http://blogs.technet.com/b/filecab/archive/2013/07/09/introducing-work-folders-on-windows-server-2012-r2.aspx*.
- "Work Folders Test Lab Deployment" at *http://blogs.technet.com/b/filecab/archive/2013/07/10/work-folders-test-lab-deployment.aspx*.
- "Work Folders Certificate Management" at *http://blogs.technet.com/b/filecab/archive/2013/08/09/work-folders-certificate-management.aspx*.
- "Extending Data Deduplication to New Workloads in Windows Server 2012 R2" at *http://blogs.technet.com/b/filecab/archive/2013/07/31/extending-data-deduplication-to-new-workloads-in-windows-server-2012-r2.aspx*.
- "Deploying Data Deduplication for VDI storage in Windows Server 2012 R2" at *http://blogs.technet.com/b/filecab/archive/2013/07/31/deploying-data-deduplication-for-vdi-storage-in-windows-server-2012-r2.aspx*.
- "Storage and File Services PowerShell Cmdlets Quick Reference Card for Windows Server 2012 R2 [Preview Edition]" at *http://blogs.technet.com/b/filecab/archive/2013/07/30/storage-and-file-services-powershell-cmdlets-quick-reference-card-for-windows-server-2012-r2-preview-edition.aspx*.

- "Windows Server 2012 R2 Storage: Step-by-step with Storage Spaces, SMB Scale-Out and Shared VHDX (Physical)" at *http://blogs.technet.com/b/josebda/archive/2013/07/31/windows-server-2012-r2-storage-step-by-step-with-storage-spaces-smb-scale-out-and-shared-vhdx-physical.aspx*.
- "Step-by-step for Storage Spaces Tiering in Windows Server 2012 R2" at *http://blogs.technet.com/b/josebda/archive/2013/08/28/step-by-step-for-storage-spaces-tiering-in-windows-server-2012-r2.aspx*.
- "iSCSI Target Server in Windows Server 2012 R2" at *http://blogs.technet.com/b/filecab/archive/2013/07/31/iscsi-target-server-in-windows-server-2012-r2.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "Storage Changes in Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/C9-14*.
- "Reduce Storage Costs with Data Deduplication" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B342*.
- "Storage Spaces: What's New in Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B218*.
- "Storage and Availability Improvements in Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B333*.

CHAPTER 4

Failover Clustering

Both virtualization and storage can only take you so far unless you also add high availability into the mix. Failover Clustering, a key feature of the Windows Server platform, is designed to do just that by providing high availability and scalability to many types of server workloads including Hyper-V hosts, file servers, and different server applications such as Microsoft SQL Server and Microsoft Exchange Server that can run on both physical servers and virtual machines.

Whereas Windows Server 2012 included a number of important enhancements to the Failover Clustering feature, Windows Server 2012 R2 adds even more. This chapter continues the discussion of what's new in Windows Server 2012 R2 by describing several of the key improvements to Failover Clustering functionality in the new platform.

But first let's start by reviewing the Failover Clustering enhancements that were previously introduced in Windows Server 2012.

Previous enhancements to Failover Clustering

Some of the many ways that Failover Clustering was enhanced in Windows Server 2012 include:

- **Improved scalability** Compared with Failover Clustering in Windows Server 2008 R2, the number of cluster nodes supported increased from 16 to 64 in Windows Server 2012. The number of clustered roles or virtual machines also increased from 1,000 to 8,000 (up to 1,024 per node) in the new platform. This increased scalability enabled new scenarios and efficiencies to help IT departments deliver more for the dollar.
- **Cluster Shared Volumes enhancements** Cluster Shared Volumes (CSV) were introduced in Windows Server 2008 R2 to provide common storage for clustered virtual machines. CSV was enhanced in Windows Server 2012 and enabled to provide storage for additional clustered roles such as the new Scale-out File Server (SoFS) feature, which can provide continuously available and scalable file-based (SMB 3.0) server storage for Hyper-V and applications such as SQL Server. CSV could also be integrated with the new Storage Spaces feature of Windows Server 2012 to enable scale-out access to data by virtualizing cluster storage on groups of inexpensive disks (JBODs). CSV in Windows Server 2012 was also integrated

with new SMB 3.0 features like SMB Multichannel and SMB Direct, which allow CSV traffic to stream across multiple networks in the cluster and leverage network adapters that support Remote Direct Memory Access (RDMA). Other CSV improvements in Windows Server 2012 included support for BitLocker Drive Encryption, removal of external authentication dependencies, and improved file backup.

- **Updating failover cluster nodes** Cluster-Aware Updating (CAU) was introduced in Windows Server 2012 to enable software updates to be applied automatically to the host operating system or other system components on the nodes of a failover cluster while maintaining availability during the update process. CAU reduced maintenance time by automating what was previously a very repetitive task.
- **Quorum improvements** New features of the cluster quorum feature in Windows Server 2012 included simplified quorum configuration, support for specifying which cluster nodes had votes in determining quorum, and dynamic quorum, which provides the administrator the ability to automatically manage the quorum vote assignment for a node based on the state of the node.
- **Other enhancements** Some of the many other enhancements to Failover Clustering in Windows Server 2012 included simplified migration of the configuration settings of clustered roles, more robust integration with Active Directory Domain Services, improved cluster validation tests, improved Windows PowerShell support, Node Maintenance Mode, clustered tasks, new clustered roles like iSCSI Target, guest clusters using virtual Fibre Channel, and more. Many of the Hyper-V enhancements in Windows Server 2012 are also relevant to Failover Clustering, for example, virtual machine prioritization, pre-emption to shut down low-priority virtual machines, virtual machine health monitoring, Hyper-V Replica Broker, and so on.

Guest clustering using shared virtual disks

As we mentioned briefly at the end of Chapter 2, Hyper-V in Windows Server 2012 R2 now allows guest clustering using shared VHDX files. This new exciting capability will be especially appreciated by hosters who want to maintain separation between their own storage infrastructure and that of their tenants. Why is that?

Hosting highly available workloads

Consider your typical hoster for a moment. A hoster provides its customer with services that allow them to run their virtual machines in the cloud instead of on location at their company premises. These virtual machines are pretty important to the customers too, since they are typically running server workloads—like SQL Server—that are critical to the operation of the customer's business. In fact, they're so important to the customer that they want the hoster to make sure these workloads are highly available. And since the hoster says it has the infrastructure to do this and wants the customer's business, it agrees.

Now let's say that until today, the customer has been running their virtualized workloads on-premises. To ensure high availability for their workloads, they've been using two types of failover clustering, namely, guest host clustering and guest clustering. First, the customer has been using host clustering, which means running the Failover Clustering feature in the parent partition of two or more Hyper-V hosts. (To understand host clustering, think of making a single virtual machine highly available.) Using host clustering helps you ensure continuous availability in the event of a hardware failure on a host, when you need to apply software updates to the parent partition resulting in a reboot being required, and similar scenarios.

Second, the customer has been using guest clustering, which means running the Failover Clustering feature in the guest operating system of two or more virtual machines. (To understand guest clustering, think of multiple virtual machines in a failover cluster.) Using guest clustering helps you proactively monitor application health and mobility within the guest operating system and protect against application failures, guest operating system problems, host and guest networking issues, and other problem scenarios.

By combining both types of failover clustering like this, the customer has the best of both worlds. In other words, having a cluster of clusters (guest clustering on top of host clustering) gives you the highest level of availability for your virtualized workloads.

But now let's say that the customer wants to move their virtualized workloads into a hosted cloud. So, the customer asks the hoster to provide them with high availability similar to what they've been using on-premises. The hoster agrees but wants to maintain complete separation between the tenant's virtual workloads and the hoster's own physical storage infrastructure.

Separating virtual resources from physical infrastructure

The new guest clustering using shared virtual disks capability of Windows Server 2012 R2 now makes such a scenario possible for hosters. As you'll see in a moment, what this new capability enables you to do is to keep your physical infrastructure layer (computer, storage, and network) and your virtualized resources (tenant virtual machines and the workloads running on them) separate from one another.

This approach can benefit hosters since it allows them to maintain strict control over the physical infrastructure of their cloud while providing great flexibility in how they deliver virtual resources to customers. Specifically, it allows them to provision virtual machines, services, and applications to customers (together with the virtual compute, storage, and network resources needed) while keeping the underlying physical resources opaque to them.

For example, when a customer spins up a new virtual machine, the customer doesn't care which Hyper-V host it's running on, which physical network that host is sitting on, or which logical unit number (LUN) its virtual machine files are stored on. All the customer cares about is that they get the necessary virtualized compute, storage, and network resources they need to run their workload with the performance they desire. The hoster should be able to reallocate, reconfigure, and upgrade their physical infrastructure without interrupting customer workloads or even the customers being aware of it.

With guest clustering in the previous versions of Windows Server, maintaining strict separation of tenant virtual machines and the hoster's physical infrastructure just wasn't possible. That's because in order to implement guest clustering you had to present a LUN to your virtual machines so they could use it as shared storage for the Failover Clustering feature running in the guest operating system of the virtual machines. In Windows Server 2008 R2, you would generally do this by having iSCSI initiators running in the guest operating system to enable connectivity with an iSCSI-based storage device. (You could also use Fibre Channel over Ethernet, or FCoE, for this purpose as well, but the point is that you were still restricted to using NICs to transport the data.) Typically you would host the LUN on an iSCSI SAN, but you could also download and install the free Microsoft iSCSI Target Software from the Microsoft Download Center, install it on a server running Windows Server 2012 R2, and use that server as shared storage for the guest cluster.

Windows Server 2012 made guest clustering easier in two ways. First, the iSCSI Software Target is now an in-box feature integrated into the Failover Clustering feature, and this makes it easier to implement guest clustering using shared iSCSI storage. Second, Windows Server 2012 also includes an in-box Hyper-V Virtual Fibre Channel adapter that allows you to connect directly from within the guest operating system of a virtual machine to LUNs on a Fibre Channel SAN. This means that in Windows Server 2012 you have three choices for the shared storage you'll need if you want to implement guest clustering, namely, iSCSI storage, Fibre Channel storage, or Hyper-V over SMB 3.0.

But the problem with guest clustering in Windows Server 2012 is that it still requires that something in your virtual infrastructure (the guest operating system of the clustered virtual machines) needs to be able to directly connect to something in your physical infrastructure (a LUN on your iSCSI or Fibre Channel SAN). What this effectively does when guest clustering is implemented is to open a hole between the physical infrastructure and the clustered virtual machines as shown in Figure 4-1.

FIGURE 4-1 Hosters like to keep their customers' virtual machines and their own supporting infrastructure separate, but until now guest clustering has required establishing a connection between them.

What's the problem with opening such a hole? For hosters, it basically ties their hands because they can't make changes to their physical storage infrastructure without having it potentially impact the virtualized workloads of the customers that they're hosting. Because

of this, hosters usually decline to implement guest clustering because it limits their ability to separate their physical infrastructure from the tenant's workloads. Customers that want to move workloads into the cloud and have high availability ensured by both host and guest clustering are unable to do this, and this makes them unhappy because they are unable to migrate their workloads into the hoster's cloud to simplify the operations and management of their workloads. So, hosters who want to offer both host and guest clustering to customers can't do this, and they lose out on potential business opportunities.

But now with the new guest clustering using shared VHDX capability of Windows Server 2012 R2, hosters can provide guest clustering to customers without the need of providing direct access by the clustered virtual machines to an iSCSI target or a LUN on a Fibre Channel storage array. This means you can now implement guest clustering for tenant virtual machines running in a hoster's cloud while maintaining complete separation between the hoster's physical storage infrastructure and the virtualized storage resources consumed by the virtual machines (see Figure 4-2). This is an important issue for most hosters because they usually utilize separate networks for providing tenant virtual machine connectivity and storage infrastructure connectivity and, for security and reliability reasons, they want to keep these networks completely separate.

FIGURE 4-2 Guest clustering using shared virtual disks in Windows Server 2012 R2 enables hosters to keep their customers' virtual machines and their own supporting infrastructure separate.

Understanding shared virtual disks

The key to being able to implement guest clustering for tenant virtual machines running in a hoster's cloud is a new capability in Windows Server 2012 R2 that allows a VHDX file (the new virtual hard disk format introduced earlier in Windows Server 2012) to be shared by multiple virtual machines running on one or more Hyper-V hosts. To the hosts, these shared virtual disks look like simple VHDX files attached to multiple virtual machines (each virtual machine already has at least one other virtual hard disk for the guest operating system). To the virtual machines themselves, however, the shared virtual disks appear to be (and behave as if they are) virtual Serial Attached SCSI (SAS) disks that can be used as shared storage for a failover cluster. The virtual machines in a guest cluster can share one or more virtual SAS disks depending on how the cluster is configured. Figure 4-3 shows how the hosts and virtual machines view the shared VHDX files in a guest cluster.

Hyper-V hosts see only a simple VHDX file

Virtual machines see a shared SAS disk

FIGURE 4-3 Hyper-V hosts see shared virtual disks as simple VHDX files, but the guest cluster of virtual machines running on these hosts sees the virtual disks as shared SAS disks.

As in Windows Server 2012, the actual physical storage backing the shared storage volume(s) used by the failover cluster can be implemented using one of two approaches as shown in Figure 4-4:

- Using CSV disks for block storage, for example, by placing the shared VHDX file on a CSV disk provisioned from a virtual disk using Storage Spaces
- Using a SoFS for file storage, which allows the shared VHDX file to be stored on an SMB 3.0 shared folder

Both of these approaches allow the use of low-cost commodity storage instead of more expensive SAN solutions for the shared storage used by the guest cluster. They also allow you to deliver guest clustering using exactly the same infrastructure you use to deliver standalone virtual machines. In other words, you don't need to have specialized storage such as an iSCSI or Fibre Channel SAN or a Windows Server system with the Microsoft iSCSI Target Software installed in order to implement guest clustering.

Cluster Shared Volumes (CSV) for block storage

Scale-out File Server for file storage

FIGURE 4-4 Guest clusters using shared virtual disks can use either CSV disks for block storage or SoFS for file storage.

Using shared virtual disks

Implementing guest clustering using shared virtual disks on Windows Server 2012 R2 is easy:

1. Create a new VHDX file on the volume you will use for shared storage for the cluster.
2. Open the Settings dialog for a virtual machine in Hyper-V Manager.
3. Click the SCSI Controller option under the Hardware category, select Hard Drive, and click Add to add a new hard drive to the controller.
4. Browse to select the VDHX file you created earlier, and then expand the new hard drive under the SCSI Controller to expose the Advanced Features option.
5. Click the Advanced Features option and select the Enable Virtual Hard Disk Sharing check box as shown in Figure 4-5, and then click OK (or Apply) to apply all the changes.
6. Repeat steps 2 through 5 of the above procedure for each virtual machine in the guest cluster.

FIGURE 4-5 Use these settings to share a virtual hard disk.

A few things to consider:

- The shared virtual disk must be a data disk; guest operating system disks cannot be shared.
- The shared virtual disk must use the newer VHDX format; it cannot use the older VHD format.
- The shared virtual disk must be attached to the virtual machine's SCSI controller; it cannot be attached to the IDE controller.
- When performing the above procedure, don't click Apply until you have selected the Enable Virtual Hard Disk Sharing check box. If you do this, you will have to remove the disk from the controller and reselect it in order to share it.

Of course, all this can be done using Windows PowerShell as well.

CSV and SoFS enhancements

At the end of Chapter 3, "Storage," we mentioned that enhancements to CSV in Failover Clustering now result in a more highly optimized rebalancing of how the SoFS feature works, but that since this related to the topic of clustering we'd defer discussing it until this present chapter. This is a fairly significant improvement for SoFS, so let's look at it now together with some other improvements in how CSV works in Windows Server 2012 R2.

Failover Clustering and SoFS

Recall that SoFS is a feature introduced in Windows Server 2012 that allows you to use the Failover Clustering feature to deploy active-active clusters of file servers that can store server application data, such as Hyper-V virtual machine files or SQL Server database files, using file shares instead of using LUNs on a SAN. The key of course is that a SoFS allows you to achieve a similar level of reliability, availability, manageability, and performance as that of a SAN. And since a SoFS can use Storage Spaces, another feature of Windows Server 2012 that allows you to use low-cost commodity disks to create pools of storage from which you can provision resilient volumes, the approach can often be much more cost-effective than using a SAN. That's obviously good news for organizations whose IT budgets are constrained, which probably includes everyone nowadays.

Figure 4-6 illustrates how a SoFS can redirect I/O over SMB to the optimal node. A virtual machine running on a Hyper-V host wants to access a file in a shared folder named Share2 on a two-node SoFS. The nodes of the SoFS are named File Server 1 and File Server 2. When the virtual machine attempts to connect to the share, it might connect to either Share2 on File Server 1 or to Share2 on File Server 2. Let's say that it establishes an SMB connection to Share2 on File Server 1 as shown by the dashed line on the left. Unfortunately, this is not an optimal connection because the file it wants to access is actually located on storage attached to File Server 2. The SoFS detects this situation, however, and it automatically and seamlessly transitions the SMB connection from Share2 on File Server 1 to Share2 on File Server 2 as shown by the dashed arrow at the bottom. From this point until the end of the SMB session,

to provide optimal I/O and throughput, the SMB connection between the virtual machine and Share2 on File Server 2 can use direct I/O as shown by the solid line.

FIGURE 4-6 A SoFS can redirect I/O over SMB to the optimal node.

Optimized ownership of CSV disks

To ensure that a SoFS can deliver SAN-quality throughput and IOPS, Microsoft has made a couple of optimizations in how a SoFS works in Windows Server 2012 R2. We'll begin by considering things from the perspective of CSV. Recall that CSV allow multiple nodes in a failover cluster to simultaneously have read-write access to the same LUN (disk) provisioned as an NTFS volume. This enables clustered roles to fail over quickly from one node to another node without requiring a change in drive ownership or dismounting/remounting a volume. CSV also help simplify managing a large number of LUNs in a large failover cluster. CSV work by providing a general-purpose, clustered file system layered on top of NTFS. Examples of CSV applications can include clustered virtual hard disk (VHD or VHDX) files for clustered Hyper-V virtual machines and scale-out file shares to store application data for the SoFS role.

Consider a failover cluster with a bunch of nodes with a bunch CSV disks, and each CSV disk is backed by a shared LUN exposed through Storage Spaces on a SoFS. Applications running on any node have simultaneous read/write access to the shared LUN even if it is only mounted on one of the cluster nodes. The coordinator node, one of the cluster nodes, handles all synchronization of metadata for file system I/O on the shared LUN and is the only node where NTFS is mounted. An example of such metadata would be the file system changes that occur when a virtual machine running on a Hyper-V cluster is turned off. Such metadata changes are routed over the SMB path to the coordinator node. By contrast, file system I/O that is not metadata is sent directly down the stack to the storage to provide direct I/O performance.

In Windows Server 2012, the Failover Clustering feature handles orchestration of file system changes on CSV disks by performing orchestration separately for each LUN. This meant that if you had eight cluster nodes using four LUNs for shared storage, you had to manually spread the CSV disks across the cluster. Also, Failover Clustering in Windows Server 2012 had no built-in mechanism for ensuring that they stayed spread out. In fact, all of the CSV disks could be owned by a single node.

Failover Clustering in Windows Server 2012 R2, however, now includes a mechanism for fairly distributing the ownership of CSV disks across all cluster nodes based on the number of CSV disks each node owns. Rebalancing ownership of CSV disks happens automatically whenever a new node is added to the cluster, a node is restarted, or a failover occurs.

Another enhancement in Windows Server 2012 R2 is when a workload, such as a virtual machine running on a Hyper-V host, attempts to establish an SMB 3.0 connection with a SoFS, the SoFS will try to determine whether the workload has an optimized I/O path it can use to access the CSV disk using direct I/O. One of the key improvements with Failover Clustering in Windows Server 2012 was that CSV disks could perform more operations in direct I/O mode than occurred in Windows Server 2008 R2. Direct I/O can be used with storage that has Fibre Channel, iSCSI, or SAS connectivity and involves writing directly to a CSV disk. Drivers for devices that can transfer large amounts of data at a time can use direct I/O for those transfers, and using direct I/O for such transfers improves a driver's performance, both by reducing its interrupt overhead and by eliminating the memory allocation and copying operations inherent in buffered I/O.

Increased CSV resiliency

CSV in Windows Server 2012 R2 now has health monitoring of the Server service to help increase the resilience of your Failover Clustering solution. This is important because if the Server service becomes unhealthy on a failover cluster, it can impact the ability of the CSV coordinator node to orchestrate metadata updates and accept I/O requests from other nodes. To protect against this, when the Server service is detected as being unhealthy in a Windows Server 2012 R2 failover cluster, ownership of the CSV is automatically transitioned to another node in the cluster.

Another improvement is that multiple Server service instances are now allowed per failover cluster node. Specifically, you can now have:

- The default instance, which handles incoming traffic from SMB clients that access ordinary file shares.
- A second CSV instance that handles only inter-node CSV traffic such as metadata access and redirected I/O traffic.

Improved CSV cache allocation

The CSV cache enables the server to use system memory as a write-through cache to increase the performance of a Failover Clustering solution. In Windows Server 2012, you could only allocate up to 20 percent of the total physical memory on the server for use by the CSV cache. Now, in Windows Server 2012 R2, you can allocate up to 80 percent of the total physical memory of the server to the CSV cache. This can result in huge performance gains in certain scenarios such as failover clusters of Hyper-V hosts and Scale-out File Server deployments.

Another change with the CSV cache is that it is now enabled by default. Previously in Windows Server 2012, the CSV cache was disabled by default and had to be manually enabled. However, you still need to allocate the size of the block cache you want to reserve. You can do this by using Windows PowerShell. For example, the following command will configure a cache of 512 MB to be reserved on each node of a failover cluster:

```
(Get-Cluster).SharedVolumeBlockCacheSizeInMB = 512
```

After you have modified the amount of memory allocated to the CSV cache, you need to restart each node in the cluster.

CSV and other storage features

CSV in Windows Server 2012 R2 now supports the Resilient File System (ReFS), data deduplication, and parity Storage Spaces. ReFS is a new file system introduced previously in Windows Server 2012 that is designed to maximize the integrity and availability of data by safeguarding against common errors that cause data loss. ReFS can scale to very large volumes and is designed to handle the very large data sets of the future.

Data deduplication and Storage Spaces have been discussed previously in Chapter 2, “Storage,” of this book. By supporting ReFS, data deduplication, and parity Storage Spaces, greater flexibility has been added in Windows Server 2012 R2 in how organizations can implement Failover Clustering solutions.

Changes to heartbeat threshold

Although the goal of failover clustering is to deliver high availability for server workloads, beneath the hood, failover clustering is simply a health detection model. Each and every second, a heartbeat connection is tested between nodes in the cluster. If no heartbeat is heard from a node one second, nothing happens. No heartbeat for two seconds? Nothing happens. Three seconds? Nothing. Four seconds? Nothing. Five seconds?

Five seconds is the default heartbeat threshold for all cluster roles in the Windows Server 2012 version of Failover Clustering. That means if the coordinator node doesn't hear from one of the other cluster nodes in five seconds, it assumes that the other node has failed or is partitioned, so it takes corrective action to remedy the situation and ensure continued availability of the workloads currently running on the failed node.

As an example, let's say you have a single-subnet failover cluster of Hyper-V hosts with virtual machines running on them. VM-A is currently running on HOST-1 and everything is working fine until an unexpected network interruption occurs on the network connecting the nodes. A transient issue with the network switch could be the cause, perhaps because someone tripped over the switch's power cable in the server room and plugged it back in immediately, but the switch took a few seconds to reboot. Whatever the cause of the network interruption, Failover Clustering decides that since the heartbeat threshold had been exceeded for HOST-1, that node must be down, so it assumes that VM-A has become unavailable even though clients are still able to access the workload running on the virtual machine. Since HOST-1 has been determined to have failed, Failover Clustering begins taking remedial action on that node, which terminates any active client connections to the workload. Meanwhile, it starts booting up VM-A on a different node so clients will be able to access the workload again.

What has actually happened here, unfortunately, is that Failover Clustering could be said to have triggered a false failover. Of course, that's not really true—it's the network interruption that caused the problem. The best action in this case would be to ensure that all network cables are physically secured. But what if your network experiences more mysterious transient failures? And what if you, as cluster administrator, can't identify or address these network failures because another section of the IT department oversees the network infrastructure and they aren't cooperative or helpful? For one reason or another, transient network interruptions are sometimes unavoidable for some customers. Yet network interruptions that exceed the heartbeat threshold can cause a cluster to fail over when such action is neither necessary nor desired. What's to be done?

To address this issue, the Windows Server team made a change in Failover Clustering in Windows Server 2012 R2. Instead of the five-second heartbeat threshold used for all clustered roles in Windows Server 2012, the heartbeat threshold has been increased, but only for the Hyper-V clustered role. For Hyper-V cluster nodes on the same subnet, the threshold is now 10 seconds. And for Hyper-V cluster nodes on different subnets, the threshold is now 20 seconds. This reduction of cluster sensitivity to health problems was specifically made to enable Hyper-V clusters to provide increased resiliency to packet loss on unreliable networks. However, increasing the heartbeat threshold like this can have the negative result of greater downtime when a real failure does happen, so administrators also have the option of configuring a lower threshold if they want to. But you shouldn't raise the threshold any higher than 20 seconds or it can cause TCP sessions to unexpectedly terminate. And remember, increasing the heartbeat threshold doesn't fix the underlying network problems you're experiencing—it only masks them.

Detecting the health of virtual machines

Interruptions in the physical network infrastructure of a failover cluster aren't the only types of network problems that can cause problems for clusters. Network disconnections can also occur at the virtual machine level on the clustered Hyper-V hosts. If this happens in Windows Server 2012, the virtual machine continues to run on the cluster node even though the workload on the virtual machine is no longer available to clients.

A new setting called Protected Network in Windows Server 2012 R2 can resolve this kind of problem by automatically moving the virtual machine to a different cluster node if the virtual machine's network becomes disconnected. To enable this capability for a virtual machine running on a Hyper-V host cluster, simply do the following:

1. Open the Settings dialog for a virtual machine in Hyper-V Manager.
2. Expand the Network Adapter node under Hardware, and select the Advanced Features option.
3. Select the Protected Network check box, as shown in Figure 4-7.

FIGURE 4-7 You can now enable the Protected Network setting.

For more information on this new capability and how to configure it using Windows PowerShell, let's now hear from one of our experts at Microsoft.

Configuring virtual machine health protection

In Windows Server 2008 R2 Failover Clustering, we had our first health type check, wherein, if the virtual machine hangs, we would restart it. In Windows Server 2012, we introduced Virtual Machine Monitoring. This monitoring could be set up to monitor specific services running inside of the virtual machine and restart them if necessary.

However, there was still one scenario where Failover Clustering would not react—that was the disconnect of a network. If a network disconnected in previous versions of Failover Clustering, it would remain on the current node and not do

anything. There really was nothing that could be done—from a cluster standpoint—to have it automatically move unless there was an IP address resource also in the group. This was ugly and meant you had IP addresses on the network that would never be utilized.

This has been addressed in Windows Server 2012 R2 Failover Clustering. Now, a component level virtual machine health detector is included. With highly available virtual machines, there is a new thorough (IsAlive) health check that implements checks to the external connectivity of a VM switch to that virtual machine.

This is not something that is enabled as a default and is not for all networks or virtual machines. To configure this, you must first identify which network is your "protected" network. The "protected" network could be the network that the clients will access for their virtual machines.

So let's take this example: I have a highly available virtual machine called Bob and a Hyper-V network called Public that will be my protected network. I would bring up the settings of the virtual machine in Failover Cluster Manager, expand my Network Adapter identified as Public, and go to the Advanced Features. Here is where I can select it to be the Protected Network.

This will also verify that the destination node has the network available. You can configure this for any virtual machine and any network. If you had a virtual machine that you wanted to protect multiple networks, you can. Simply select all the networks that you want. You may not always want to do this on all networks that the virtual machine has.

You can also set this using Windows PowerShell and we'll examine that now.

For example, if I just wanted to turn this off for a specific virtual machine called Acct, the command would be:

```
PS C:\>Get-VMNetworkAdapter -VMName Acct | Where-Object {$_.SwitchName
-eq "Public"} | Set-VmNetworkAdapter -NotMonitoredInCluster False
```

If I wanted to turn it off for all virtual machines that use Public as the network switch, the command would be:

```
PS C:\>Get-VMNetworkAdapter * | Where-Object {$_.SwitchName -eq
"Public"} | Set-VmNetworkAdapter -NotMonitoredInCluster False
```

Keep in mind that the previous commands are only going to work for the highly available virtual machines currently running on the node you run the commands on. If you wanted to execute this against the Acct virtual machine running on a different node, the command would be:

```
PS C:\>Get-ClusterGroup Acct | Get-VM | Get-VMNetworkAdapter |
Where-Object {$_.SwitchName -eq "Private"} | Set-VMNetworkAdapter –
NotMonitoredInCluster False
```

Now that we have the protected network, we are monitoring the health of that network and the connectivity to the machine.

If we lose network connectivity on this network from this node, the cluster is going to check all remaining nodes to see if this network is up. If it is, it is going to do a live migration of the virtual machine to that node. If all other nodes do not have access to the network either, the virtual machine will remain in the current state it is in until the network is reconnected.

The virtual machine live migrations will be queued if there are more VMs affected by a network issue on a host than can be concurrently live migrated. If the disconnected network becomes available again and there are VMs virtual machines in the queue to be live migrated, the virtual machines pending will have the live migrations canceled.

John Marlin
Senior Support Escalation Engineer, Windows CORE TX

Virtual machine drain on shutdown

Previously in Windows Server 2012, if you shut down a node on a failover cluster of Hyper-V hosts running virtual machines without first draining the node, the virtual machines on the node were put into a saved state, moved to other nodes in the cluster, and then resumed. The result was an interruption in the availability of the virtual machines. In addition, if Failover Clustering determined that it was taking too long to save the state of the virtual machines on the node shutting down, the virtual machines might be turned off and then restarted on other nodes. This can not only cause an interruption in the availability of the virtual machines but might also result in data loss for business applications running in the virtual machines.

Failover Clustering in Windows Server 2012 R2 now solves this problem by automatically live migrating all running virtual machines from the node being shut down to other nodes in the cluster. The result of this change is to significantly improve the availability of applications and virtual machines running on failover clusters of Hyper-V hosts.

IMPORTANT **Although the new virtual machine drain on shutdown capability is designed to ensure continued availability of applications and virtual machines running on failover clusters of Hyper-V hosts, Microsoft still recommends that you put a cluster node into maintenance mode or move all virtual machines to other nodes before you shut down the node.**

Let's learn more about this exciting new capability by listening again to one of our experts at Microsoft.

Ensuring virtual machine availability

Windows Server 2012 Failover Clustering introduced the ability to drain resources off of a node. This process was used in cases where a node was to be patched or shut down. When a node is drained, the Cluster service will pause the node, which prevents any new virtual machines (or other workload) from coming to it. It would also automatically move all the virtual machines off to another node.

When these virtual machines moved off, the type of move would depend on the priority setting. Virtual machines that are set as high or medium are live migrated, whereas low priority machines are quick migrated.

These moves are primarily based on preferred owners that may be set on the virtual machine resource as well as to random nodes. The problem with this is that you could run into an issue in which you overload one of the nodes and cause other virtual machines or the virtual machine you moved to fail.

In Windows Server 2012 R2, things were changed for the better with this process.

The first change is with the low priority machines. When a virtual machine is quick migrated, it does go down as it is put in a saved state. Once over on the other machine, it comes out of this saved state. Because it is down, any user(s) connected to it also loses connectivity and must re-establish the connectivity. In Failover Clustering with Windows Server 2012, this has been changed to have the low priority also live migrated.

Since we are now moving all virtual machines using live migration, this allows for the next item that was updated in regard to the virtual machine mobility. As mentioned previously:

"You could run into an issue in which you overload one of the nodes and cause other virtual machines or the virtual machine you moved to fail."

Now, we are being smarter with how things are moved. Before the virtual machines are moved, we will detect resources on the other nodes to better determine where virtual machines are placed. This will provide a better way of preventing failures of virtual machines for the moves and it truly moves the virtual machines to the "best available node."

This change allows for all virtual machines to remain up and connected to users. However, what happens if you were to forget to move virtual machines off or drain a node when the node is to be shut down? When a group is moved by means other than by the administrator, it falls back to the "cluster-controlled action" because the cluster must move it.

The recommendation has always been to move all workloads off of a node before it is shut down. When it is inadvertently forgotten, then connectivity is lost to the virtual machine due to the way the quick migration process works. Once the process starts, there is no stopping it.

So, in the thoughts of virtual machine availability, the next new change for the better was done. When a node is now shut down, it will issue a drain of the node first. The same draining process as described above is what occurs here.

This change is controlled by the cluster common property DrainOnShutdown, which is enabled (1) as a default. This can be changed to being disabled (0), but really, why would you when the name of the game is availability?

John Marlin
Senior Support Escalation Engineer, Windows CORE TX

Dynamic witness

In Failover Clustering, the quorum configuration determines the maximum number of failures that the cluster can sustain and still keep running. In Windows Server 2012, you had to determine when to configure a witness. In addition, you had to manually adjust the quorum configuration if the node membership changed. You needed to do this to keep the total number of votes at an odd number. And you had to do this every time you added or evicted cluster nodes. For example, if you added another node to your cluster, you had to manually adjust the quorum configuration. This is important because if there is an odd number of votes, then the quorum witness doesn't get to vote. But if the witness should have been able to vote and wasn't able to because of misconfiguration, then the possibility exists of the cluster going down because of witness failure.

With Failover Clustering in Windows Server 2012 R2, however, a new feature called dynamic witness allows the quorum witness vote to be dynamically adjusted based on the state of the witness resource. For example, if the witness resource is offline or failed, the cluster sets the witness vote to zero. The cluster thus decides whether to use the witness vote based on the number of voting nodes that are available in the cluster. As a result, Microsoft now recommends that you always configure a quorum witness when implementing a Failover Clustering solution using Windows Server 2012 R2.

A related enhancement to this dynamic quorum functionality is that a failover cluster can now dynamically adjust a running node's vote in order to keep the total number of votes at an odd number. To accomplish this, the cluster first tries to adjust the quorum witness vote through dynamic witness. But if a quorum witness is not available, the cluster can adjust a node's vote directly.

You can also now configure a cluster property that will determine which side of the cluster continues running in the event of a 50 percent node split where neither side would normally have a quorum. Previously, when this happened to a failover cluster running Windows Server 2012, both sides of the cluster would go down. Now, however, one side of the cluster can continue to run in the event of a tie like this.

You can configure this behavior by assigning the LowerQuorumPriorityNodeID cluster common property to a cluster node in your secondary site so that your primary site will continue to run in the event of a tie. You can configure this property using Windows PowerShell as follows:

```
(Get-Cluster).LowerQuorumPriorityNodeID = <node_ID_of_secondary_site)
```

You can determine the node IDs, node names, and node state using this command:

```
Get-ClusterNode | ft
```

Active Directory–detached clustering

One more (and potentially very useful for many customers) new feature of Failover Clustering in Windows Server 2012 R2 is the ability to deploy a failover cluster without any dependencies in Active Directory Domain Services (AD DS) for network names. What this means is that you can now register the cluster network name together with the network names of clustered roles that have client access points on your DNS servers without the need of creating corresponding computer objects in AD DS. This new capability is called Active Directory–detached clustering.

The main benefit of this new option for implementing Failover Clustering is that it can simplify the process of deploying, managing, and maintaining your failover clusters. For example, if you use Active Directory–detached clustering, then you will no longer need permissions to create these computer objects in AD DS or ask your Active Directory administrator to pre-stage the computer objects in AD DS. In addition, you will no longer need to manage and maintain the cluster computer objects for the cluster.

The chance of an administrative error causing your failover cluster to go down can also be reduced if you implement Active Directory–detached clustering in your environment. For example, it has been known to happen in the past that an administrator accidentally deletes a cluster object in Active Directory. Such mistakes, of course, can have disastrous consequences not only for your failover cluster and the workloads running on it, but for your business operations as well.

Note that Active Directory–detached clustering does not mean you don't need Active Directory for your Failover Clustering solution. The nodes in a failover cluster must still be joined to an Active Directory domain. Windows Server does not support deploying failover clusters in a workgroup environment using standalone servers.

Note also that you must use Windows PowerShell to implement Active Directory–detached clustering. For more information on how to do this, see the link on this topic in the "Learn more" section at the end of this chapter.

IMPORTANT **Microsoft does not recommend implementing Active Directory–detached clustering for any scenario that requires Kerberos authentication.**

Learn more

You can learn more about the new Failover Clustering features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Failover Clustering in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn265972.aspx*.
- "Virtual Hard Disk Sharing Overview" at *http://technet.microsoft.com/en-us/library/dn281956.aspx*.

- "Deploy a Guest Cluster Using a Shared Virtual Hard Disk" at *http://technet.microsoft.com/en-us/library/dn265980.aspx*.
- "Deploy an Active Directory-Detached Cluster" at *http://technet.microsoft.com/en-us/library/dn265970.aspx*.

The following Microsoft TechNet and MSDN blog posts also have lots of information about the new Failover Clustering features and enhancements in Windows Server 2012 R2:

- "How to Enable CSV Cache" at *http://blogs.msdn.com/b/clustering/archive/2013/07/19/10286676.aspx*.
- "How to Properly Shutdown a Failover Cluster or a Node" at *http://blogs.msdn.com/b/clustering/archive/2013/08/23/10443912.aspx*.
- "Windows Server 2012 R2 Virtual Machine Recovery from Network Disconnects" at *http://blogs.msdn.com/b/clustering/archive/2013/09/04/10446482.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "Continuous Availability: Deploying and Managing Clusters Using Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B305*.
- "Failover Cluster Networking Essentials" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B337*.
- "Upgrading Your Private Cloud with Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B331*.
- "Application Availability Strategies for the Private Cloud" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B311*.
- "Storage and Availability Improvements in Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B333*.
- "Understanding the Hyper-V over SMB Scenario, Configurations, and End-to-End Performance" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B335*.

CHAPTER 5

Networking

Currently, IT is all about the cloud, and the foundation of cloud computing is infrastructure. If you're an enterprise that's going to build and manage a private cloud, then you'll be dealing with three main kinds of infrastructure: compute, storage, and network. And if you're a hoster creating a cloud for selling services to customers, then you'll be working with the same three building blocks but on a much larger scale and with additional features that are essential for hosting environments such as multitenant isolation, IP address management, and Network Virtualization.

In Chapter 2, "Hyper-V," we looked at Hyper-V improvements in Windows Server 2012 R2. Hyper-V hosts provide the compute infrastructure needed for running virtualized workloads in a cloud infrastructure. In Chapter 3, "Storage," we examined storage improvements in the new platform. Storage Spaces and the Scale-out File Server (SoFS) are two storage technologies that can enable new scenarios and help lower costs when deploying the storage infrastructure for a cloud solution. In Chapter 4, "Failover Clustering," we looked at how the Failover Clustering feature has been enhanced in the platform. Failover clustering enables your compute and storage resources to be highly available, which is essential for today's always-on businesses.

In this chapter, we'll now examine the networking improvements in Windows Server 2012 R2. Networking is the underlying glue that holds your infrastructure together, makes possible the delivery of services, makes remote management a reality, and more.

But first let's begin by reviewing the networking enhancements introduced earlier in Windows Server 2012.

Previous enhancements to networking

Some of the many networking improvements introduced previously in Windows Server 2012 included the following:

- **Dynamic VMQ** Virtual Machine Queue (VMQ) allows a host's network adapter to pass DMA packets directly into the memory stacks of individual virtual machines. The net effect of doing this is to allow the host's single network adapter to appear to the virtual machines as multiple network interface cards (NICs) which then allows each virtual machine to have its own dedicated NIC. Windows Server 2012 improved this by introducing Dynamic VMQ, which dynamically distrib-

uted incoming network traffic processing to host processors, based on processor use and network load. The earlier implementation, which was also called Static VMQ, was removed in Windows Server 2012.

- **Receive Side Scaling** Receive Side Scaling (RSS) allows network adapters to distribute kernel-mode network processing across multiple processor cores in multicore systems. Such distribution of processing enables support of higher network traffic loads than are possible if only a single core is used. RSS was enhanced in Windows Server 2012 to support systems with up to 64 processors, improved scalability across Non-Uniform Memory Access (NUMA) nodes, improved management and diagnostics, and automatic load balancing capabilities for non-TCP traffic such as UDP unicast, multicast, and IP-forwarded traffic.
- **Windows NIC Teaming** Also known as load balancing and failover (LBFO), Windows NIC Teaming enables multiple NICs on a server to be grouped together into a team. This has two purposes: to help ensure availability by providing traffic failover in the event of a network component failure and to enable aggregation of network bandwidth across multiple NICs. Previously, implementing NIC teaming required using third-party solutions from independent hardware vendors (IHVs). Beginning with Windows Server 2012, however, NIC teaming was now an in-box solution that worked across different NIC hardware types and manufacturers.
- **Quality of Service enhancements** Quality of Service (QoS) refers to technologies used for managing network traffic in ways that can meet service level agreements (SLAs) and/or enhance user experiences in a cost-effective manner. For example, by using QoS to prioritize different types of network traffic, you can ensure that mission-critical applications and services are delivered according to SLAs and to optimize user productivity. Windows Server 2012 introduced a number of new QoS capabilities including Hyper-V QoS, which allows you to specify upper and lower bounds for network bandwidth used by a virtual machine, and new Group Policy settings to implement policy-based QoS by tagging packets with an 802.1p value to prioritize different kinds of network traffic.
- **Data Center Bridging** Data Center Bridging (DCB) is an IEEE standard that allows for hardware-based bandwidth allocation for specific types of network traffic, which means that DCB is yet another QoS technology. DCB-capable network adapter hardware can be useful in cloud environments where it can enable storage, data management, and other kinds of traffic all to be carried on the same underlying physical network in a way that guarantees each type of traffic its fair share of bandwidth. Windows Server 2012 supported DCB, provided that you had both DCB-capable Ethernet NICs and DCB-capable Ethernet switches on your network.
- **Dynamic Host Configuration Protocol enhancements** Dynamic Host Configuration Protocol (DHCP) functionality was enhanced in several ways in Windows Server 2012. DHCP Server Failover was introduced as a new approach for ensuring DHCP availability by enabling two DHCP servers to replicate lease information

between them. That way, one of the DHCP servers could assume responsibility for providing addresses to all the clients on a subnet when the other DHCP server became unavailable. Policy-based assignment allowed a DHCP server to evaluate DHCP requests against policies you defined for a specific scope and in a defined processing order.

- **Domain Name System enhancements** Domain Name System (DNS) functionality was also enhanced in several ways in Windows Server 2012. The DNS Server component included improved support for DNS Security Extensions (DNSSEC) including support for DNS dynamic updates in DNSSEC signed zones, automated trust anchor distribution through Active Directory, automated trust anchor rollover, and support for updated DNSSEC standards. The DNS Client component included improved support for Network basic input/output system (NETBIOS) and Link-local multicast name resolution (LLMNR), binding order optimization, and asynchronous DNS caching.
- **IP Address Management** IP Address Management (IPAM) is a new built-in framework introduced in Windows Server 2012 for discovering, monitoring, auditing, and managing the IP address space used on a corporate network. IPAM provided a central and integrated experience for managing IP addresses that could replace manual, work-intensive tools such as spreadsheets and custom scripts that can be tedious, unreliable, and scale poorly.
- **Network virtualization** Network virtualization was introduced in Windows Server 2012 as a way for organizations to keep their own internal IP addresses when moving their servers into a hoster's cloud. Network virtualization works by allowing you to assign two different IP addresses to each virtual machine running on a Windows Server 2012 Hyper-V host: the customer address, which is the IP address that the server had when it resided on the customer's premises before it was migrated into the cloud; and the provider address, which is the IP address assigned by the cloud provider to the server once the server has been migrated to the provider's data center. Network virtualization thus lets the cloud provider run multiple virtual networks on top of a single physical network in much the same way as server virtualization lets you run multiple virtual servers on a single physical server. Network virtualization also isolates each virtual network from every other virtual network, with the result that each virtual network has the illusion that it is a separate physical network. This means that two or more virtual networks can have the exact same addressing scheme, yet the networks will be fully isolated from one another and each will function as if it is the only network with that scheme.
- **BranchCache enhancements** BranchCache allows organizations to increase the network responsiveness of centralized applications that are being accessed from remote offices, with the result that branch office users have an experience similar to being directly connected to the central office. BranchCache was first introduced in Windows Server 2008 R2 and was enhanced in Windows Server 2012 with improved

performance and reduced bandwidth usage, default encryption of cached content, new tools that allowed you to preload cachable content onto your hosted cache servers even before the content was first requested by clients, single instance storage and downloading of duplicated content, and tighter integration with the File Server role.

There were also other networking technologies introduced or improved in Windows Server 2012 that closely relate to other infrastructure components like compute and storage. For example, there was the Hyper-V Extensible Switch, which added new virtual networking functionality to the Hyper-V server role. There was version 3.0 of the Server Message Block (SMB) file-sharing protocol, which enabled new network storage scenarios such as the SoFS. There was single-root I/O virtualization (SR-IOV), which enabled a network adapter to divide access to its resources across various PCIe hardware functions and reduced processing overhead on the host, which can make the network performance of a virtual machine nearly as good as that of a physical computer. And there was a lot more new networking features and capabilities introduced previously in Windows Server 2012.

Many of the above networking features and technologies have now been improved even more in Windows Server 2012 R2. Let's examine some of these enhancements now.

Virtual RSS

Today, enterprise-grade NICs can be extremely fast—so fast in fact that a single processor core of the server won't be able to make full use of the NIC's throughput capability. RSS in Windows Server 2012 helps you get around that by allowing kernel-mode network processing to be spread across multiple cores in a multicore server system. In Windows Server 2012, however, virtual machines were limited to using only one virtual processor for processing network traffic. As a result, virtual machines running on Hyper-V hosts were unable to make use of RSS to utilize the highest possible network traffic loads. To compound the problem, VMQ would affinitize all traffic destined for a virtual machine to one core inside the host for access control list (ACL) and vmSwitch extension processing.

With Windows Server 2012 R2, however, this is no longer a limitation. That's because a new feature called virtual RSS (vRSS) maximizes network utilization for a virtual machine by spreading the processing of the traffic across multiple virtual processors inside the virtual machine and also inside the host. This is demonstrated by Figure 5-1, which shows a virtual machine that has four virtual processors assigned to it. The physical NIC can now spread traffic among available cores inside the host, while the virtual NIC distributes the processing load across the virtual processors inside the virtual machine.

FIGURE 5-1 Virtual Receive Side Scaling (vRSS) is available in Windows Server 2012 R2.

The result of using vRSS is that it is now possible to virtualize network-intensive physical workloads that were traditionally run on bare-metal machines. A typical usage scenario might be a Hyper-V host that has a small number or only one virtual machine running on it, but the applications running in that virtual machine generate a large amount of network traffic. For example, vRSS can be especially useful for virtual network appliances, virtual gateways, file servers, and similar network-intensive applications, because you'll now be able to virtualize them without any network throughput degradation.

A nice thing about vRSS is that it will work on existing network hardware that is VMQ-capable. This means you don't have to upgrade your hardware in order to take advantage of this new capability.

RSS (and vRSS) is disabled by default in Windows Server 2012 and should only be enabled on network-intensive virtual machines. This is because extra processing is required for vRSS to spread the incoming network traffic inside the host. In other words, enabling vRSS trades CPU cycles for network throughput.

You can configure and manage vRSS by using Windows PowerShell commands and scripts. Figure 5-2 shows how to use the Get-NetAdapterRss cmdlet to get all RSS-capable network adapters on a system that have RSS enabled and display their names, interface description, and state. The figure also shows how to use the Get-Command cmdlet to display a list of all cmdlets available for managing RSS and vRSS.

```
Administrator: Windows PowerShell
PS C:\> Get-NetAdapterRss -name * | Where-Object -FilterScript { $_.Enabled } |
Format-List -Property Name,InterfaceDescription,Enabled


Name                  : Ethernet 2
InterfaceDescription  : Broadcom NetXtreme Gigabit Ethernet #2
Enabled               : True

Name                  : Ethernet
InterfaceDescription  : Broadcom NetXtreme Gigabit Ethernet
Enabled               : True



PS C:\> Get-Command *NetAdapterRss

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Function        Disable-NetAdapterRss                              NetAdapter
Function        Enable-NetAdapterRss                               NetAdapter
Function        Get-NetAdapterRss                                  NetAdapter
Function        Set-NetAdapterRss                                  NetAdapter


PS C:\>
```

FIGURE 5-2 You can use Windows PowerShell to manage vRSS.

Windows NIC Teaming enhancements

Windows servers today are often huge beasts with tons of processing power to handle the biggest business workloads. Getting data in and out of such servers requires fat pipes—lots of network bandwidth—and for some environments even a single 10 GbE Ethernet network interface card (NIC) is insufficient and becomes a bottleneck. And what if that NIC fails for some reason? Your enterprise-class server suddenly becomes an expensive paperweight!

NIC teaming can address such problems. Also known as Load Balancing/Failover (LBFO), NIC teaming refers to any technological approach that enables two or more NICs to be linked together to form a team of some kind. Until recently, if you wanted to use NIC teaming, you had to implement a proprietary solution provided by your NIC hardware vendor. But beginning with Windows Server 2012, you now have an in-box solution called Windows NIC Teaming that you can use for implementing NIC teaming on your Windows servers.

NIC teaming can provide two types of benefits for enterprise networks. First, it allows you to aggregate the throughput from multiple network adapters. For example, let's say you have a server system that has two 1 gigabit network adapters configured as a team. The result is that the total throughput of the team is 1 + 1 = 2 gigabits, so teaming network adapters together basically gives your server a bigger "pipe" for sending and receiving traffic over the network the server is connected to.

The second benefit of NIC teaming is that it helps ensure continuous availability of the server's connection to the network by providing fault tolerance. For example, let's say that one of the NICs in the above team fails. If this happens, the throughput drops from 2 gigabits to 1 gigabit, and although such a 50 percent drop in network traffic handling capability could affect the performance of applications running on the server, the good thing is that the server still has some connectivity with the network. Without NIC teaming, failure of a single NIC would have caused the throughput to drop from 1 gigabit to zero, which is probably much worse from a business point of view.

Before Windows Server 2012, if you wanted to make use of NIC teaming, then you had to use third-party NIC teaming software from your network adapter vendor. With the release of Windows Server 2012, however, NIC teaming became a built-in feature called Windows NIC Teaming that makes it possible to team together even commodity network adapters to aggregate throughput and enable fault tolerance.

NIC Teaming in Windows Server 2012

Let's begin with a quick overview of what Windows NIC Teaming is, what kinds of scenarios it can address, and what types of configuration modes it supports. The following short description is excerpted from the free e-book *Introducing Windows Server 2012 RTM Edition* (Microsoft Press, 2012) which has been downloaded over 650,000 times since it was released just over a year ago.

Windows NIC Teaming is the name for the new network adapter teaming functionality included in Windows Server 2012. Network adapter teaming is also known as LBFO and enables multiple network adapters on a server to be grouped together into a team. This has two purposes:

- To help ensure availability by providing traffic failover in the event of a network component failure
- To enable aggregation of network bandwidth across multiple network adapters

Previously, implementing network adapter teaming required using third-party solutions from independent hardware vendors (IHVs). Beginning with Windows Server 2012, however, network adapter teaming is now an in-box solution that works across different NIC hardware types and manufacturers.

Windows NIC Teaming supports up to 32 network adapters in a team in three teaming modes:

- **Static Teaming** Also called Generic Teaming and based on IEEE 802.3ad draft v1, this mode is typically supported by server-class Ethernet switches and requires manual configuration of the switch and the server to identify which links form the team.
- **Switch Independent** This mode doesn't require that the team members connect to different switches; it merely makes it possible.

- **LACP** Also called Dynamic Teaming and based on IEEE 802.1ax, this mode is supported by most enterprise-class switches and allows automatic creation of a team using the Link Aggregation Control Protocol (LACP), which dynamically identifies links between the server and a specific switch. To use this mode, you generally need to enable LACP manually on the port of the switch.

Since a picture is worth a thousand words, Figure 5-3 shows the three teaming modes you can choose from when creating a new team in Windows Server 2012:

FIGURE 5-3 Configuring NIC Teaming in Windows Server 2012.

NIC Teaming in Windows Server 2012 R2

Although NIC Teaming in Windows Server 2012 provided both distribution of network load across NICs in a team and failover support for teamed NICs, network traffic was not distributed across teamed NICs in a balanced fashion. Beginning with Windows Server 2012 R2, however, a new feature called dynamic load balancing automatically and continuously balances traffic across teamed NICs in an equitable fashion.

Figure 5-4 is another thousand-word picture that illustrates this new functionality for NIC Teaming in Windows Server 2012 R2. Previously in Windows Server 2012, you only had two load-balancing modes you could choose from:

- **Address Hash** This algorithm distributes traffic among the teamed NICs by creating a hash from the address components of the packets that comprised a single stream of TCP traffic. The algorithm then assigns packets that have that particular hash value to one of the NICs in the team.
- **Hyper-V Port** This approach distributes traffic among the teamed NICs on the basis of the Mac address or port that a virtual machine uses to connect to the virtual switch on a Hyper-V host.

As you can see from the figure, however, a third load-balancing mode called Dynamic has now been added to NIC Teaming in Windows Server 2012 R2. Not only that, but this new mode is now the default load-balancing mode when you create a new team on the new platform. By using dynamic load balancing, you can now use all members of a NIC team even when the team is in Switch Independent mode.

FIGURE 5-4 Configuring NIC Teaming in Windows Server 2012 R2.

Choosing the right teaming mode

We saw from Figure 5-4 that when you use the UI to create a new NIC team in Windows Server 2012 R2 you have a choice of three teaming modes to choose from:

- Static Teaming
- Switch Independent
- LACP

This is actually a bit confusing because there are really only two types of teaming modes available:

- Switch Independent
- Switch Dependent

The UI doesn't display a mode called Switch Dependent but instead displays two types of switch dependent modes:

- Static Teaming
- LACP

So your choices for teaming mode really look like this:

- Switch Independent
- Switch Dependent
  - Static Teaming
  - LACP

When should you use Switch Independent teaming mode?

Switch Independent is the default teaming mode when you create a new team. This mode assumes that you don't need your Ethernet switches to participate in making NIC teaming happen for your server. In other words, this mode assumes the Ethernet switch isn't even aware that the NICs connected to it are teamed.

Because of this, selecting Switch Independent mode allows you to connect each NIC in a team to a different Ethernet switch on your backbone. However, you can also use this mode when all the NICs in the team are connected to the same Ethernet switch.

One scenario where you could use this functionality is to provide fault tolerance in the case of one of the teamed NICs failing. For example, you could create a team from two NICs (NIC1 and NIC2) on your server and then connect NIC1 to SWITCH1 and NIC2 to SWITCH2. You could then configure NIC1 as the active adapter for the team, and NIC2 as the standby adapter for the team. Then if NIC1 fails, NIC2 will automatically become active and your server won't lose its connectivity with your backbone.

Note that the above approach, which is variously called Active/Passive Teaming or Active/Standby Teaming, provides fault tolerance but not bandwidth aggregation for your server's connection to the network. You can just as easily leave both NICs configured as active and get both fault tolerance and bandwidth aggregation if you prefer, but the choice is up to you.

And when should you use Switch Dependent teaming mode?

You can only use one of the Switch Dependent modes (Static Teaming or LACP) if all of the teamed NICs are connected to the same Ethernet switch on your backbone. Let's consider this next.

Static Teaming (also called Generic Teaming or IEEE 802.3ad teaming) requires configuring both the server and Ethernet switch to get the team to work. Generally, only enterprise-class Ethernet switches support this kind of functionality, and since you need to manually configure it on the Ethernet switch, it requires additional work to get it working. Plus, manually configuring something always increases the odds of configuration errors happening if you make some kind of mistake during the setting up process. If at all possible, try to stay away from following this approach to NIC teaming on Windows Server.

LACP (also called IEEE 802.1ax teaming or dynamic teaming, which should not be confused with the new Dynamic load-balancing mode available for NIC teaming in Windows Server 2012 R2) uses the LACP to dynamically identify the network links between the server and the Ethernet switch. This makes LACP superior to Static Teaming because it enables the server to communicate with the Ethernet switch during the team creation process, thus enabling automatic configuration of the team on both the server and Ethernet switch. But whereas most enterprise-class Ethernet switches support LACP, you generally need to enable it on selected switch ports before it can be used. So LACP is less work to configure than Static Teaming, but still more work to set up than switch independent teaming which is the default option for Windows NIC Teaming.

The bottom line then is that Switch Independent teaming is generally your best choice to select for the teaming mode when creating a new NIC Team for two reasons. First, you don't need to perform any configuration on the Ethernet switch to get it working. And second, you can gain two kinds of fault tolerance:

- Protection against the failure of a NIC in the team
- Protection against the failure of an Ethernet switch connected to a teamed NIC (when you are connecting different teamed NICs to different Ethernet switches)

However, there are a couple of scenarios described later where Switch Dependent teaming might be the best choice if your Ethernet switches support such functionality and you're up to configuring it.

Choosing the right load-balancing mode

Let's say you've chosen Switch Independent teaming as the teaming mode for a new NIC team you're creating. Your next decision is which load-balancing mode you're going to use. As described in the previous section, NIC Teaming in Windows Server 2012 supports two different load-balancing modes: Address Hash or Hyper-V Port. Windows Server 2012 R2 adds a third option for load-balancing mode called Dynamic.

First, when should you use Address Hash load-balancing mode?

The main limitation of the Address Hash load-balancing approach is that inbound traffic can only be received by a single member of the team. The reason for this has to do with the underlying operation of how address hashing uses IP addresses and TCP ports to seed the hash function. So a scenario where this could be the best choice would be if your server was running the kind of workload where inbound traffic is light while outbound traffic is heavy.

Sound familiar? That's exactly what a web server like IIS experiences in terms of network traffic. Incoming HTTP/HTTPS requests are generally short streams of TCP traffic. What gets pumped out in response to such requests, however, can include text, images, and video.

So when should you use Hyper-V Port load-balancing mode?

This load balancing approach affinitizes each Hyper-V port (such as each virtual machine) on a Hyper-V host to a single NIC in the team at any given time. Basically what you get here is no load balancing from the virtual machine's perspective. Each virtual machine can only utilize one teamed NIC at a time, so maximum inbound and outbound throughput for the virtual machine is limited to what's provided by a single physical NIC on the host.

When might you use this form of load balancing? A typical scenario might be if the number of virtual machines running on the host is much greater than the number of physical NICs in the team on the host. Just be sure that the physical NICs can provide sufficient bandwidth to the workloads running in the virtual machines.

This discussion only scratches the surface, however, because there are other scenarios you might encounter when considering NIC teaming as a possible solution. For example, if you implement Windows NIC Teaming on a Hyper-V host and your virtual machines need to be able to utilize bandwidth from more than one NIC in the team, then an option for you (if your Ethernet switch supports it) is to configure LACP or Static Teaming as your teaming mode and Address Hash as your load-balancing mode. This is possible because it's how you configure the Ethernet switch that determines how traffic will be distributed across the team members. This scenario is kind of unusual, however, because typically if you have a virtualized workload that requires high bandwidth for both inbound and outbound traffic (such as a huge SQL Server database workload) then you're probably only going to have one or two virtual machines running on the Hyper-V host.

Finally, when should you use the new dynamic load-balancing mode?

Unfortunately, we can't provide guidance concerning this at the time of writing because the documentation on Windows NIC Teaming hasn't yet been updated. So your best bet for more detailed guidance on implementing NIC teaming in different configurations is to keep a watch on the link to this topic in the "Learn more" section at the end of this chapter.

Improved network diagnostics

Networking problems can bring down your private cloud solution and result in losses for your business. Being able to correctly diagnose networking problems makes it easier to quickly resolve them so you can get your business up and running again.

Windows Server 2012 R2 includes new features in Windows PowerShell that can help you troubleshoot network connection problems when they occur. But before we examine some of these improvements, let's start by briefly reviewing some of the network diagnostic capabilities of Windows PowerShell in the previous version Windows Server 2012.

Network diagnostic cmdlets in Windows Server 2012

If you're experiencing what might be a networking issue with one of your servers, the first thing you probably want to check is the configuration of the network adapters. The Get-NetAdapter cmdlet was first introduced in Windows Server 2012 as a way of retrieving the configuration of all physical network adapters in the server.

For example, let's see what happens when we run this command on a Hyper-V host named HOST30.contosol.com that is running Windows Server 2012 R2:

```
PS C:\> Get-NetAdapter

Name                      InterfaceDescription                    ifIndex Statu
                                                                          s
----                      --------------------                    ------- -----
vEthernet (Broadcom Ne... Hyper-V Virtual Ethernet Adapter #2          18 Up
Ethernet                  Broadcom NetXtreme Gigabit Ethernet          12 Di...
Ethernet 2                Broadcom NetXtreme Gigabit Ethernet #2       13 Up
```

Because this is a Hyper-V host, there are probably some virtual machines running on it. On Hyper-V hosts running Windows Server 2012 and later, you can use the Get-VMNetwork-Adapter cmdlet to collect configuration information for the network adapters for these virtual machines. For example, the following command will retrieve information about all virtual machine network adapters on the host:

```
PS C:\> Get-VMNetworkAdapter *

Name            IsManagementOs VMName       SwitchName
----            -------------- ------       ----------
Network Adapter False          SRV-STANDARD Broadcom NetXtreme Gigabit Ether...
Network Adapter False          SRV2012R2    Broadcom NetXtreme Gigabit Ether...
Network Adapter False          SRV2012R2
Network Adapter False          SRV2012      Broadcom NetXtreme Gigabit Ether...
Network Adapter False          SRV2012      Broadcom NetXtreme Gigabit Ether...
Network Adapter False          Gen2Test     Broadcom NetXtreme Gigabit Ether...
```

You can also use Get-VMNetworkAdapter with the -VMName option to display network adapters for a specific virtual machine on the host.

Another useful network troubleshooting cmdlet introduced previously in Windows Server 2012 is Get-NetIPAddress, which retrieves the IP addresses configured on the system's network adapters. You can use the Get-NetIPAddress cmdlet both on physical servers and within virtual machines. For example, let's run this command on HOST30 described above:

```
PS C:\> Get-NetIPAddress


IPAddress         : fe80::8843:1e98:a8a6:6fab%12
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Deprecated
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : fe80::1905:8ae1:5bfd:7b8e%18
InterfaceIndex    : 18
InterfaceAlias    : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                    Virtual Switch)
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : fe80::5efe:172.16.11.30%14
InterfaceIndex    : 14
InterfaceAlias    : isatap.{3D53D3DC-9209-4C7F-8AAE-AD8ADCBD93FC}
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 128
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Deprecated
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
```

```
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : ::1
InterfaceIndex    : 1
InterfaceAlias    : Loopback Pseudo-Interface 1
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 128
PrefixOrigin      : WellKnown
SuffixOrigin      : WellKnown
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 169.254.111.171
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 16
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 172.16.11.30
InterfaceIndex    : 18
InterfaceAlias    : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                    Virtual Switch)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore
```

```
IPAddress         : 127.0.0.1
InterfaceIndex    : 1
InterfaceAlias    : Loopback Pseudo-Interface 1
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 8
PrefixOrigin      : WellKnown
SuffixOrigin      : WellKnown
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore
```

You can see that Get-NetIPAddress returns a lot of useful info you can parse or pipe into other commands for further processing.

Another useful network troubleshooting cmdlet is Get-NetIPConfiguration which can be used to retrieve usable network interfaces, IP addresses, and DNS servers configured on a system. The key value of Get-NetIPConfiguration is that it gives you the "big picture" of the system's network configuration in a concise way. For example, let's see what happens when we run this command on HOST30 without any further options being specified:

```
PS C:\> Get-NetIPConfiguration


InterfaceAlias       : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                       Virtual Switch)
InterfaceIndex       : 18
InterfaceDescription : Hyper-V Virtual Ethernet Adapter #2
NetProfile.Name      : contoso.com
IPv4Address          : 172.16.11.30
IPv6DefaultGateway   :
IPv4DefaultGateway   : 172.16.11.1
DNSServer            : 172.16.11.50

InterfaceAlias       : Ethernet
InterfaceIndex       : 12
InterfaceDescription : Broadcom NetXtreme Gigabit Ethernet
NetAdapter.Status    : Disconnected
```

To make things even easier, the alias GIP can be used instead of having to type Get-NetIPConfiguration at the command line. For example, let's say we want to retrieve only the DNS Server configuration of the network adapter whose alias begins with "vEthernet" as shown above. Here's how we can do this:

```
PS C:\> $a = GIP 'v*'
PS C:\> $a.DNSServer

InterfaceAlias               Interface Address ServerAddresses  PSComputerName
                             Index     Family
--------------               --------- ------- ---------------  --------------
vEthernet (Broadcom NetXt...        18 IPv6    {}
vEthernet (Broadcom NetXt...        18 IPv4    {172.16.11.50}
```

Get-NetIPConfiguration can also provide verbose output by specifying the -Detailed option as shown here:

```
PS C:\> GIP -Detailed


ComputerName                : HOST30
InterfaceAlias              : vEthernet (Broadcom NetXtreme Gigabit Ethernet
                              #2 - Virtual Switch)
InterfaceIndex              : 18
InterfaceDescription        : Hyper-V Virtual Ethernet Adapter #2
NetAdapter.LinkLayerAddress : 00-24-E8-50-17-F3
NetAdapter.Status           : Up
NetProfile.Name             : contoso.com
NetProfile.NetworkCategory  : DomainAuthenticated
NetProfile.IPv6Connectivity : LocalNetwork
NetProfile.IPv4Connectivity : Internet
IPv6LinkLocalAddress        : fe80::1905:8ae1:5bfd:7b8e%18
IPv4Address                 : 172.16.11.30
IPv6DefaultGateway          :
IPv4DefaultGateway          : 172.16.11.1
NetIPv6Interface.NlMTU      : 1500
NetIPv4Interface.NlMTU      : 1500
NetIPv6Interface.DHCP       : Enabled
NetIPv4Interface.DHCP       : Disabled
DNSServer                   : 172.16.11.50

ComputerName                : HOST30
InterfaceAlias              : Ethernet
InterfaceIndex              : 12
InterfaceDescription        : Broadcom NetXtreme Gigabit Ethernet
NetAdapter.LinkLayerAddress : 00-24-E8-50-17-F4
NetAdapter.Status           : Disconnected
```

Network diagnostic cmdlets in Windows Server 2012 R2

Although the above cdmlets can help you troubleshoot a lot of networking issues, they're sometimes hard to apply in certain situations. So let's now examine some of the network troubleshooting improvements introduced in Windows PowerShell in Windows Server 2012 R2.

For many network admins, the first and most useful improvement is the addition of a new cmdlet named Test-NetConnection that can be used to perform ICMP and TCP connectivity tests. Let's now see this in action. We'll perform all our tests from a Windows PowerShell prompt on server HOST30.contoso.com as before.

First, let's test network connectivity between HOST30 and another server named HOST50 on our network:

```
PS C:\> Test-NetConnection HOST50.contoso.com


ComputerName           : HOST50.contoso.com
RemoteAddress          : 172.16.11.50
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
```

The Test-NetConnection cmdlet can also be used to test network connectivity with hosts on remote networks and over the Internet. For example, let's see if HOST30 can establish network connectivity with the Microsoft Xbox website:

```
PS C:\> Test-NetConnection www.xbox.com


ComputerName           : www.xbox.com
RemoteAddress          : 184.29.219.150
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : True
PingReplyDetails (RTT) : 26 ms
```

The -TraceRoute option can also be used to trace the exact network route used to establish connectivity with the remote site:

```
PS C:\> Test-NetConnection www.xbox.com -TraceRoute


ComputerName           : www.xbox.com
RemoteAddress          : 184.29.219.150
```

```
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : True
PingReplyDetails (RTT) : 29 ms
TraceRoute             : 172.16.11.1
                         142.161.5.200
                         142.161.5.65
                         4.28.68.21
                         4.69.158.146
                         4.69.138.166
                         4.68.111.70
                         184.29.219.150
```

You can also use Test-NetConnection to test connectivity on a specific TCP port by including the -Port option in your command. For example, let's verify that the Xbox website can be accessed on the standard HTTP port which is TCP port 80:

```
PS C:\> Test-NetConnection www.xbox.com -Port 80


ComputerName           : www.xbox.com
RemoteAddress          : 184.29.219.150
RemotePort             : 80
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : True
PingReplyDetails (RTT) : 28 ms
TcpTestSucceeded       : True
```

You can also use an alias like RDP to verify TCP connectivity with the well-known port for the Remote Desktop Protocol, which is TCP port 3389. For example, let's see if HOST30 can establish connectivity to TCP port 3389 on HOST50:

```
PS C:\> Test-NetConnection HOST50 RDP


ComputerName           : HOST50
RemoteAddress          : 172.16.11.50
RemotePort             : 3389
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : True
```

The success of the above test indicates that Remote Desktop is enabled on the server HOST50.

Test-NetConnection also lets you use other aliases besides RDP for testing connectivity with well-known TCP ports. For example, you can also use:

- SMB
- HTTP
- PING

Now let's see what happens when we try the RDP test against the server HOST40 on our network:

```
PS C:\> Test-NetConnection HOST40 RDP
WARNING: Ping to HOST40 failed -- Status: TimedOut


ComputerName           : HOST40
RemoteAddress          : 172.16.11.61
RemotePort             : 3389
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : True
```

Note that RDP connectivity succeeded, but pinging the server failed. This indicates that the server's firewall is active and blocking the inbound ICMP messages that are being sent by HOST30.

The Test-NetConnection cmdlet also supports an -InformationLevel option that allows you to gather more detailed information concerning the connectivity test being performed:

```
PS C:\> Test-NetConnection HOST50 RDP -InformationLevel Detailed


ComputerName             : HOST50
RemoteAddress            : 172.16.11.50
RemotePort               : 3389
AllNameResolutionResults : 172.16.11.50
                           fe80::396f:7162:ab64:fa82
MatchingIPsecRules       :
NetworkIsolationContext  : Private Network
InterfaceAlias           : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                           Virtual Switch)
SourceAddress            : 172.16.11.30
NetRoute (NextHop)       : 0.0.0.0
PingSucceeded            : True
```

```
PingReplyDetails (RTT)   : 0 ms
TcpTestSucceeded         : True
```

Or you can use -InformationLevel to suppress all output except whether the desired test was successful or not:

```
PS C:\> Test-NetConnection HOST40 RDP -InformationLevel Quiet
WARNING: Ping to HOST40 failed -- Status: TimedOut
True
PS C:\>
```

One final note about Test-NetConnection is that you can also run it with no parameters like this:

```
PS C:\> Test-NetConnection


ComputerName           : internetbeacon.msedge.net
RemoteAddress          : 131.253.3.197
InterfaceAlias         : vEthernet (Broadcom NetXtreme Gigabit Ethernet #2 -
                         Virtual Switch)
SourceAddress          : 172.16.11.30
PingSucceeded          : True
PingReplyDetails (RTT) : 49 ms
```

Doing this simply tests whether your server has a network connection with the Internet by testing connectivity with a remote server belonging to the DNS domain msedge.net, which is registered by Microsoft.

Another new network diagnostic cmdlet introduced in Windows Server 2012 R2 is Test-VMNetworkAdapter, which lets you diagnose network connectivity issues in the tenant network of a Hyper-V Virtual Network environment. At the time of writing, the documentation for this cmdlet had not been published, so we'll refer you to the link on this topic in the "Learn more" section of this chapter for more information when it becomes available.

IPAM enhancements

Enterprise networks today tend to be a lot more complex than they were 20 or even 10 years ago. With the advent of virtualization technologies like Hyper-V, network administrators have to deal with both physical networks and virtual networks. Nodes on both kinds of networks need IP addresses in order to be reachable, and these IP addresses can be assigned statically (manually), dynamically using DHCP, dynamically using Automatic Private IP Addressing (APIPA), or more typically, using some combination of these three methods. DNS is also needed in order to provide name resolution services so servers can have easy-to-remember friendly names like SRV-A instead of hard-to-memorize IP addresses like 169.254.115.33.

DHCP simplifies the task of allocating IP addresses to clients on a network (and to servers by using DHCP reservations), but large organizations can have multiple DHCP servers with each server having dozens or more scopes and each scope having its own special set of options. Similarly, DNS simplifies management of fully-qualified domain names (FQDNs) for both servers and clients, but large organizations can have multiple DNS servers with each one authoritative over dozens of zones and each zone containing thousands of resource records.

How does one manage all this? On the Windows Server platform, you can use the DHCP Server snap-in to manage all the DHCP servers in your organization, but the snap-in really isn't efficient when it comes to managing large numbers of DHCP servers. Similarly, you can use the DNS Server snap-in to manage all your DNS servers, but again this snap-in isn't efficient for managing large numbers of DNS servers.

For example, on large networks neither the DHCP snap-in nor DNS snap-in are very useful for helping you get quick answers to any of the following questions:

- Which DHCP servers in my organization manage which blocks of the IP address space?
- Which IP addresses are actually being used at each site where my company has a physical presence?
- Which IP addresses have been assigned to virtual network adapters of virtual machines running on Hyper-V hosts?
- How can I modify a particular scope option for a certain number of scopes residing on several different DHCP servers?
- How can I determine which subnets of an IP address range being managed by a certain DHCP server are not being used?
- How can I determine how many free IP addresses are available for leasing for certain scopes on certain DHCP servers?
- How can I find all scopes that have 95 percent or more of their address pool leased out to clients?
- How can I track all the IP addresses that have been assigned over the last 12 months to a certain server on my network?
- How can I find DNS servers that don't have a certain server option configured?

Administrators of large enterprises often want answers like these—and want them quickly. However, it can be difficult for them to keep track of their IP addressing schemes, DHCP server configurations, and DNS server configurations. Cloud hosting providers can have even greater difficulties keeping track of such information because their environments include both physical and virtual networks, and because of the address space reuse that often happens in multitenant cloud environments.

In the past, most large enterprises and hosters have relied on either spreadsheets, custom software developed in-house, or third-party commercial programs for keeping track of IP addressing schemes, DHCP server configurations, and DNS server configurations. Beginning with Windows Server 2012, however, Microsoft introduced an in-box solution for performing these kinds of tasks. That in-box solution is IPAM.

IPAM in Windows Server 2012

IPAM is an integrated set of tools that helps you plan, deploy, manage, and monitor your IP address infrastructure. IPAM includes functionality for performing address space management in multiserver environments and includes monitoring and network auditing capabilities. IPAM can automatically discover the IP address infrastructure of servers on your network and allows you to manage them from a central interface that is integrated into Server Manager. IPAM is an agentless technology that works together with the Active Directory Domain Services (AD DS), DHCP Server, DNS Server, and Network Policy Server (NPS) roles of the Windows Server platform.

Some of the capabilities of IPAM in Windows Server 2012 include:

- Integrates management of IP addresses, domain names, and device identities
- Organizes, assigns, monitors, and manages static and dynamic IPv4 and IPv6 addresses
- Automatic discovery of domain controllers, DHCP and DNS servers, and dynamic IP addresses in use
- Provides custom IP address space display, reporting, and management
- Tightly integrates with Microsoft DNS and DHCP servers
- Centralizes configuration and update of Microsoft DHCP and DNS servers
- Monitors and manages specific scenario-based DHCP and DNS services
- Tracks and audits changes and provides real-time view of status
- Audits server configuration changes and tracks IP address use

Although IPAM in Windows Server 2012 provided enough functionality for some organizations, other organizations (especially hosters) wanted something more. That something more has now arrived with the enhanced IPAM included in Windows Server 2012 R2.

IPAM in Windows Server 2012 R2

IPAM in Windows Server 2012 R2 represents a significant step forward in simplifying the management of addressing and DNS/DHCP server management both for large enterprises and especially for cloud hosting providers. Let's examine some of these improvements now.

First and perhaps most importantly, IPAM in Windows Server 2012 R2 now allows you to manage your virtual address space in addition to its physical address space. This means that enterprises that have a mixture of physical and virtual environments now have an in-box unified IP address management solution. Figure 5-5 shows the new Virtualized IP Address Space option in the IPAM page of Server Manager and some of the available configuration options.

This enhancement should be especially useful to very large enterprises and to hosters whose networks often consist of multiple data centers in different geographical locations. Such networks typically consist of an underlying fabric layer of infrastructure resources with a multitenant virtual network layered on top.

FIGURE 5-5 You can now manage the Virtualized IP Address Space option for IPAM using Server Manager.

For hosters that have built their cloud using the Windows Server platform, IPAM in Windows Server 2012 R2 offers the additional advantage of tight integration between IPAM and System Center Virtual Machine Manager (VMM) 2012 R2. Because IPAM basically knows everything about your physical network, such as its subnets, virtual LANs (VLANs), and pools, IPAM can make all this information available to VMM for the rapid provisioning of new virtual networks.

Another very important enhancement to IPAM in Windows Server 2012 R2 is the introduction of role-based access control. Role-based access control provides the organization with a mechanism for specifying access to objects and capabilities in terms of the organizational structure. Instead of assigning certain rights and permissions to a user or group of users, role-based access control allows you to assign a certain role instead. The role aligns with the kinds of tasks a certain type of user needs to be able to perform, and assigning the role to a user automatically grants that user all the necessary rights and permissions he or she needs to do the job.

For example, let's say your organization is very large and you have a fairly large IT staff to manage your network. You want to assign the job of being able to manage the IP address space for your network to three individuals, and you want to give the job of managing network infrastructure servers (DHCP and DNS) to two other people. Role-based access control in IPAM now makes doing these things simple.

Role-based access control in IPAM is also highly granular. For example, let's say that you want to allow a junior administrator to be able to manage only a certain DHCP scope on a certain DHCP server. Role-based access control in IPAM allows you to grant such access to the user while preventing her from having any other IP address management capabilities in your organization.

Role-based access control also includes the ability to delegate administrative privileges. This means that a senior administrator can delegate to junior administrators the ability to perform certain kinds of address management tasks in your organization.

To understand how role-based access control is integrated into the capabilities of IPAM, Figure 5-6 shows the basic architecture for how IPAM works. At the top is an administrator whose computer is running Windows 8.1 and has the Remote Server Administration Tools (RSAT) for Windows 8.1 installed. The administrator opens Server Manager on his computer and selects the IPAM page of Server Manager, as shown previously in Figure 5-5. The tasks available for the administrator to perform will depend on the specific role assigned to the administrator—for example, whether he is a network administrator, fabric administrator, system administrator, forensics investigator, and so on.

FIGURE 5-6 An example of how role-based access control is integrated into the capabilities of IPAM in Windows Server 2012 R2.

The IPAM client (in Server Manager) communicates with the IPAM server using Windows Communication Foundation (WCF)—a framework for building service-oriented applications. All communications between the IPAM client and IPAM server must go through the role-based access control component, which controls what tasks the administrator is able to perform.

The IPAM server performs various data-collection tasks including performing server discovery and monitoring, determining the configuration and availability of servers, performing event collection, determining address utilization, checking for expired addresses, and so on. To perform these different tasks, IPAM communicates with the DHCP servers, DNS servers, NPS servers, and domain controllers on your network.

As described earlier, the IPAM server can also communicate with one or more VMM servers. Such communications are made possible by using an IPAM integration plug-in included in VMM 2012 R2.

Although role-based access control should be the way to use IPAM going forward, IPAM in Windows Server 2012 R2 still includes the various IPAM security groups that were used in the previous version of IPAM for granting administrative privileges to users and groups.

The IPAM server stores the information it collects about your organization's network in a database. In the previous version of IPAM in Windows Server 2012, addressing information that was collected could only be stored in the Windows Internal Database (WID). IPAM in Windows Server 2012 R2, however, can now store data in a Microsoft SQL Server database running either on the local IPAM server or on an external server. This means that you can now ensure that the IPAM database is highly available, back the database up more easily, perform custom queries against it using T-SQL, and so on. As Figure 5-7 shows, when you provision a Windows Server 2012 R2 system as an IPAM server, you have the option of using either the WID or a SQL server for storing the data that IPAM collects for your network. The SQL Server database for IPAM must be on SQL Server 2008 R2 or SQL Server 2012.

IPAM in Windows Server 2012 R2 also includes extensive capabilities for allowing you to monitor and manage the activity of the DHCP and DNS servers on your network. For example, IPAM allows you to monitor such things as:

- Server availability
- DHCP Scope utilization
- DNS Zone replication health
- DHCP Failover health

IPAM also enables you to enable/disable features, activate/deactivate entities, allow/deny actions, and so on relating to DNS and DHCP servers.

FIGURE 5-7 IPAM in Windows Server 2012 R2 can now store data in a Microsoft SQL Server database.

In terms of management capability, IPAM in Windows Server 2012 R2 makes it easy for administrators to manage from a central user interface and for a whole organization such things as:

- DHCP servers
- DHCP scopes
- DHCP properties
- DHCP options
- DHCP filters
- DHCP failover relationships
- DHCP policies
- DHCP classes
- DHCP reservations
- DNS resource records

Just imagine how much easier this is compared to using the DHCP or DNS snap-ins for performing such tasks!

IPAM in Windows Server 2012 R2 is also fully integrated with Windows PowerShell. In fact, there is 100 percent parity between what you can do using the IPAM page in Server Manager and the IPAM cmdlets in Windows PowerShell. The IPAM Windows PowerShell provider also facilitates integration with other platforms such as System Center Configuration Manager and the Microsoft Assessment and Planning (MAP) Toolkit. Such integration can simplify and speed the network discovery of the IP address inventory of your network. And you can also leverage an Internet Control Message Protocol (ICMP)–based discovery module for performing network discovery as well.

IPAM in Windows Server 2012 R2 also integrates with Active Directory Domain Services (AD DS). Specifically, IPAM enables synchronization of Active Directory Sites and Subnets information from Active Directory to IPAM. This too makes it quick and easy for IPAM to determine the subnet structure of your organization's network.

IPAM in Windows Server 2012 R2 is clearly a cost-effective, scalable, and customizable solution for unified management of physical and virtual network IP address spaces, and DHCP and DNS services in both enterprise and hoster environments.

Hyper-V Network Virtualization enhancements

Hyper-V Network Virtualization was introduced in Windows Server 2012 as a key part of Microsoft's vision for software-defined networking (SDN). Traditional enterprise networks typically had many different physical networking devices such as Ethernet switches, routers, virtual private networking (VPN) gateways, hardware firewalls, and other kinds of network appliances. And of course they needed lots of wires to connect all the network hosts (servers and appliances) together.

The modern data center network is no longer like that. Instead of dozens of network devices and hundreds or thousands of servers, the modern data center might consist of only a dozen or so very powerful virtualization host systems, a handful of 10 GbE switches, and a couple of perimeter firewalls. Instead of thousands of individual physical servers, you now have thousands of virtual machines running on relatively few Hyper-V hosts. One reason this change is possible is because of server virtualization and consolidation, which enables organizations to virtualize workloads that previously needed to run on physical server systems. Another reason it's possible, however, is because of SDN technologies like network virtualization that allow you to consolidate multiple physical network devices onto a single physical networking device in a similar fashion to how server virtualization lets you consolidate multiple physical servers onto a single physical virtualization host. The basic idea of network virtualization is nothing new, and Hyper-V Network Virtualization is simply Microsoft's implementation of the concept of network virtualization.

How Hyper-V Network Virtualization works

The basic idea behind network virtualization is that it allows multiple virtual machine networks to overlay a cloud hosting provider's underlying physical network (see Figure 5-8). Each virtual machine network, which can be composed of one or more virtual subnets, is independent of all other virtual machine networks and also of the hoster's underlying physical network. In other words, the exact physical location of an IP subnet on the hoster's physical network is decoupled from the virtual network topology of each customer's network.

FIGURE 5-8 Hyper-V Network Virtualization allows multiple virtual machine networks to overlay a cloud hosting provider's underlying physical network.

The benefit of this decoupling is that customers can easily move physical server workloads to a hoster's cloud while preserving the IP addresses and network topology of their workloads. For example, let's say that your organization has three physical servers residing on-premises and having private IP addresses of 192.168.33.45, 192.168.33.46, and 192.168.33.47. You want to virtualize these servers by converting them into virtual machines, which you will move to the hoster's cloud. Your physical servers are currently using 192.168.0.0/16 as their address space, while the hoster uses 10.0.0.0/24 for its physical network.

If the hoster is using Hyper-V hosts running Windows Server 2012, your servers can keep their existing IP addresses in the 192.168.0.0/16 address space when their workloads are moved into the hoster's cloud. This means that your existing clients, which are used to accessing physical servers located on the 192.168.0.0/16 subnet, will still be able to do so with no modifications needed to your routing infrastructure, management platform, or network security policies. All that is required is a gateway be used to connect the physical networks where your clients and the resources they need reside with the virtual network on which your virtualized workloads are running on the hoster's physical network.

The ability of Hyper-V Network Virtualization to preserve your network infrastructure (addressing and subnet scheme) allows existing services to continue to work while being unaware of the physical location of the subnets. The way this works is that network virtualization enables you to assign two different IP addresses to each virtual machine running on a Windows Server 2012 Hyper-V host. These two addresses are:

- **Customer Address (CA)** This is the IP address that the server had when it resided on the customer's premises before it was migrated into the cloud. In the above example, this might be the 192.168.33.45 address for a particular server that the customer wants to move to the cloud.
- **Provider Address (PA)** This is the IP address assigned by the cloud provider to the server once the server has been migrated to the provider's data center. In the above example, this might be 10.44.2.133, or some other address in the 10.0.0.0/24 address space.

The CA for each virtual machine is mapped to the PA for the underlying physical host on which the virtual machine is running. Virtual machines communicate over the network by sending and receiving packets in the CA space. The virtual machine's packets are then encapsulated into new packets that have a PA as source and destination address so they can be routed over the hoster's physical network. The standards-based Network Virtualization Generic Routing Encapsulation (NVGRE) protocol is used by Hyper-V Network Virtualization, in Windows Server 2012, to encapsulate the virtual machine's packet inside a new packet. The header of this new packet has the appropriate source and destination PA, in addition to the virtual subnet ID, which is stored in the Key field of the GRE header. The virtual subnet ID in the GRE header allows hosts to identify the customer virtual machine for any given packet even though the PAs and the CAs on the packets may overlap. In other words, Hyper-V Network Virtualization keeps track of CA-to-PA mappings to enable hosts to differentiate packets for virtual machines of different customers. All virtual machines on the same host can therefore share a single PA, which helps increase network scalability because you only need as few as a single IP address per host, which lowers the burden on switches in the hoster's network.

The result is that Hyper-V Network Virtualization allows the hoster to run multiple customer virtual networks on top of a single underlying physical network in much the same way as server virtualization lets you run multiple virtual servers on a single physical server. Network virtualization isolates each virtual network from every other virtual network so that each virtual network has the illusion that it is a completely separate network. Multiple customers can even use the exact same addressing scheme for their virtual networks; customer networks will be fully isolated from one another and will function as if each network is the only one present with that particular addressing scheme.

Hyper-V Network Virtualization also makes it easier for large enterprise to move server workloads between multiple data centers where overlapping addressing schemes exist between these data centers. Hyper-V Network Virtualization thus provides increased virtual machine mobility across data centers, hosting provider clouds, and Windows Azure.

Hyper-V Network Virtualization enhancements in Windows Server 2012 R2

Although Windows Server 2012 provided the base functionality for implementing network virtualization, Windows Server 2012 R2 includes some new features and enhancements that not only make network virtualization easier to implement and manage but also provide customers with a more comprehensive and integrated SDN solution.

One key enhancement with Hyper-V Network Virtualization in Windows Server 2012 R2 is that it can now dynamically learn the IP addresses on the virtual machine networks. This improvement provides several new benefits such as increasing the high availability options available when deploying a network virtualization solution. For example, with Hyper-V Network Virtualization in Windows Server 2012 R2, you can now use guest clustering inside a virtual network, something you couldn't do before using Hyper-V Network Virtualization in Windows Server 2012. Another benefit is that you can now deploy domain controllers, DNS servers, and DHCP servers as virtual machines on your virtual network running on top of your cloud hoster's physical network infrastructure.

Hyper-V Network Virtualization in Windows Server 2012 R2 also includes several performance enhancements over how this technology worked in Windows Server 2012. For example, you now have the option to be able to load balance NVGRE traffic across multiple NICs. This means that customers who move their workloads into a hoster's cloud now have new options for load-balancing network traffic and providing failover capability to ensure the availability of the virtual network at all times.

Another performance improvement with Hyper-V Network Virtualization in Windows Server 2012 R2 involves work Microsoft is doing with network hardware vendor partners to help bring new network adapter hardware to market that has the capability of offloading NVGRE processing from the host system's processor to the network adapter. These NVGRE Task Offload Enabled NICs will soon be available and should provide significantly better performance for Hyper-V Network Virtualization solutions over current network adapters that don't let you offload NVGRE processing from the host system's processors to the adapter. Emulex is one such network adapter hardware vendor, and you can read its analysis of the performance gains that can be achieved using NVGRE Task Offload Enabled NICs on its blog at *http://o-www.emulex.com/blogs/labs/2013/06/03/benefits-network-virtualization-offload-technologies-optimize-performance-nvgre/.*

The architecture of the Hyper-V Extensible Switch has also been modified in Windows Server 2012 R2 to provide new functionality for customers that implement Hyper-V Network Virtualization solutions. Microsoft introduced the Hyper-V Extensible Switch in Windows Server 2012 to provide new capabilities for tenant isolation, traffic shaping, protection against malicious virtual machines, and hassle-free troubleshooting. The Hyper-V Extensible Switch was also designed to allow third parties to develop plug-in extensions to emulate the full capabilities of hardware-based switches and support more complex virtual environments and solutions. It does this by allowing custom Network Driver Interface Specification (NDIS) filter

drivers (called *extensions*) to be added to the driver stack of the virtual switch. This means that networking independent software vendors (ISVs) can create extensions that can be installed in the virtual switch to perform different actions on network packets being processed by the switch.

The Hyper-V Extensible Switch supports three kinds of extensions:

- **Capturing extensions** These can capture packets to monitor network traffic but cannot modify or drop packets.
- **Filtering extensions** These are like capturing extensions but also can inspect and drop packets.
- **Forwarding extensions** These allow you to modify packet routing and enable integration with your physical network infrastructure.

The Hyper-V Extensible Switch also lets you use the built-in Wfplwfs.sys filtering extension of the Windows Filtering Platform (WFP) to intercept packets as they travel along the data path. Networking ISVs can use this functionality to develop applications that can perform packet inspection on a virtual network.

In Windows Server 2012, however, the Hyper-V Extensible Switch was layered above Hyper-V Network Virtualization functionality as shown on the left in Figure 5-9. This meant that capturing, filtering, or forwarding extensions installed in the switch could only see the CA packets, that is, the packets that the virtual machine sees on its virtual network. The extensions could not see or manipulate the PA packets, that is, the packets that the Hyper-V host sees on the hosting provider's underlying physical network.

However, in Windows Server 2012 R2 network virtualization, functionality now resides in the Hyper-V Extensible Switch, as shown on the right in Figure 5-8. This means that third-party extensions can now process network packets using either CA or PA addresses as desired. This enables new types of scenarios, such as hybrid forwarding, whereby Hyper-V Network Virtualization forwards the network virtualization traffic while a third-party extension forwards non-network virtualization traffic. Another possibility might be a networking ISV developing a firewall application that drops certain kinds of packets on the customer's network and other types of packets on the provider's network. It also allows third-party ISVs to use the Hyper-V Extensible Switch to implement their own network virtualization solutions using Hyper-V instead of needing to use the in-box Hyper-V Network Virtualization approach from Microsoft.

Finally, if you wanted to implement a network virtualization solution using Hyper-V in Windows Server 2012, you needed to use third-party gateway products to do this. That's because Windows Server 2012 doesn't include an in-box gateway, and a gateway is needed to provide connectivity between virtual machines running on the virtual network and resources on physical networks at local or remote sites. The result is that Hyper-V Network Virtualization by itself in Windows Server 2012 creates virtual subnets that are separated from the rest of the network the way islands are separated from the mainland.

FIGURE 5-9 A comparison of the architecture of the Hyper-V Extensible Switch in Windows Server 2012 and Windows Server 2012 R2.

Beginning with Windows Server 2012 R2, however, Hyper-V Network Virtualization now includes an in-box component called Windows Server Gateway (WSG), a virtual machine-based software router that allows cloud hosters to route data center and cloud network traffic between virtual and physical networks including the Internet. WSG can be used to route network traffic between physical and virtual networks at the same physical location or at multiple different physical locations. This allows organizations to implement new kinds of scenarios. For example, if your organization has both a physical network and a virtual network at the same location, you can now deploy a Hyper-V host configured with a WSG virtual machine and use it to route traffic between your virtual and physical networks. As a second example, if your virtual networks reside in a hoster's cloud built using Hyper-V in Windows Server 2012 R2, the hoster can now deploy a WSG that allows you to create a VPN connection between your VPN server and the hoster's WSG to allow your users to connect to your organization's virtual resources in the cloud using the VPN connection.

WSG is fully integrated with Hyper-V Network Virtualization in Windows Server 2012 R2 and allows routing of network traffic, even when multiple customers are running tenant networks in the same data center. To deploy WSG, you should use a dedicated Hyper-V host that runs only WSG and no other virtual machines. You can also deploy WSG on a failover cluster of Hyper-V hosts to create a highly available WSG solution to provide failover protection against network outages or hardware failure.

As Figure 5-10 shows, the WSG of Hyper-V Network Virtualization in Windows Server 2012 R2 can be used to implement three types of gateway solutions:

- Implementing a multitenant-aware VPN for site-to-site connectivity, for example, to allow an enterprise to span a single virtual network across multiple data centers in different geographical locations.
- Performing multitenant-aware network address translation (NAT) for Internet access from a virtual network.
- Providing a forwarding gateway for in-data center physical machine access from a virtual network.

FIGURE 5-10 Windows Server Gateway implements three types of solutions.

Hyper-V Virtual Switch enhancements

The Hyper-V Virtual Switch is the software-based layer-2 network switch on Hyper-V hosts. Windows Server 2012 previously added many new capabilities to the Hyper-V Virtual Switch, perhaps most importantly by making the switch extensible, but also other improvements for tenant isolation, traffic shaping, protection against malicious virtual machines, and hassle-free troubleshooting. Let's review these earlier improvements before describing the new ones introduced in Windows Server 2012 R2.

Hyper-V Virtual Switch in Windows Server 2012

Versions of Hyper-V earlier than Windows Server 2012 allowed you to implement complex virtual network environments by creating virtual network switches that worked like physical layer-2 Ethernet switches. You could create external virtual networks to provide VMs with connectivity with externally located servers and clients, internal networks to allow VMs on the same host to communicate with each other as well as the host, or private virtual networks (PVLANs) that you could use to completely isolate all VMs on the same host from each other and allow them to communicate only via external networks.

The Hyper-V Virtual Switch introduced in Windows Server 2012 facilitated the creation of virtual networks that could be implemented in even more ways to provide greater flexibility in how you could design your virtualized infrastructure. For example, you could configure a guest operating system within a virtual machine to have a single virtual network adapter associated with a specific switch or multiple virtual network adapters (each associated with a different switch), but you couldn't connect the same switch to multiple network adapters.

Extensibility was added to the Hyper-V Virtual Switch in Windows Server 2012 in several ways. First, you could install custom Network Driver Interface Specification (NDIS) filter drivers (called extensions) into the driver stack of the virtual switch. For example, you could create an extension that captures, filters, or forwards packets to extensible switch ports. Specifically, the extensible switch allows for using the following kinds of extensions:

- **Capturing extensions** These can capture packets to monitor network traffic but cannot modify or drop packets
- **Filtering extensions** These are like capturing extensions but also can inspect and drop packets
- **Forwarding extensions** These allow you to modify packet routing and enable integration with your physical network infrastructure

Second, you can use the capabilities of the Windows Filtering Platform (WFP) by using the built-in Wfplwfs.sys filtering extension to intercept packets as they travel along the data path of the extensible switch. You might use this approach, for example, to perform packet inspection within your virtualized environment.

These different extensibility capabilities of the Hyper-V Virtual Switch were intended primarily for Microsoft partners and independent software vendors (ISVs) so they could update their existing network monitoring, management, and security software products so they could work not just with physical hosts, but also with VMs deployed within any kind of virtual networking environment that you might possibly create using Hyper-V in Windows Server 2012.

In addition, being able to extend the functionality of the Hyper-V networking by adding extensions made it easier to add new networking functionality to Hyper-V without needing to replace or upgrade the switch. You'd also be able to use the same tools for managing these extensions that you use for managing other aspects of Hyper-V networking, namely the Hyper-V Manager console, Windows PowerShell, and Windows Management Instrumentation (WMI). And because these extensions integrate into the existing framework of Hyper-V networking, they automatically work with other capabilities, like Live Migration.

A number of other advanced capabilities were also integrated by Microsoft into the Hyper-V Virtual Switch in Windows Server 2012 to help enhance security, monitoring, and troubleshooting functionality. These additional capabilities included the following:

- **DHCP guard** Helps safeguard against Dynamic Host Configuration Protocol (DHCP) man-in-the-middle attacks by dropping DHCP server messages from unauthorized VMs pretending to be DHCP servers
- **MAC address spoofing** Helps safeguard against attempts to use ARP spoofing to steal IP addresses from VMs by allowing VMs to change the source media access control (MAC) address in outgoing packets to an address that is not assigned to them
- **Router guard** Helps safeguard against unauthorized routers by dropping router advertisement and redirection messages from unauthorized VMs pretending to be routers
- **Port mirroring** Enables monitoring of a VM's network traffic by forwarding copies of destination or source packets to another VM being used for monitoring purposes
- **Port ACLs** Helps enforce virtual network isolation by allowing traffic filtering based on MAC or IP address ranges
- **Isolated VLANs** Allows segregation of traffic on multiple VLANs to facilitate isolation of tenant networks through the creation of PVLANs
- **Trunk mode** Allows directing traffic from a group of VLANs to a specific VM
- **Bandwidth management** Allows guaranteeing a minimum amount of bandwidth and/or enforcing a maximum amount of bandwidth for each VM
- **Enhanced diagnostics** Allows packet monitoring and event tracing through the extensible switch using ETL and Unified Tracing

Hyper-V Virtual Switch in Windows Server 2012 R2

Besides adding the vRSS capability described earlier in this chapter, Windows Server 2012 R2 builds on the many improvements added to the Hyper-V Virtual Switch in the previous Windows Server version by adding other new capabilities:

- **Enhanced extended port ACLs** Hyper-V Virtual Switch Extended Port ACLs now allow you to specify the socket port number when you create new port ACL rules. You can also configure unidirectional port rules and include a timeout parameter. These improvements make port ACLs more useful for safeguarding data center resources in multitenant cloud environments and for enforcing security policies for tenants.
- **Dynamic load balancing of network traffic** The Hyper-V Virtual Switch now automatically performs dynamic load balancing in order to move traffic streams between different NICs within a NIC team in order to share the network traffic load as equitably as possible. Previously in Windows Server 2012, the Hyper-V Virtual Switch provided simultaneous failover and load distribution capabilities, but it didn't ensure load distribution for teamed NICs in a balanced manner.
- **Coexistence with third-party forwarding extensions** To better support Hyper-V Network Virtualization scenarios in multitenant environments, the Hyper-V Virtual Switch now allows third-party forwarding extensions installed on the switch to forward packets for either the customer address space or the physical address space using hybrid forwarding. Third-party forwarding extensions can also apply other policies, such as ACLs and QoS, to both the NVGRE and the non NVGRE-encapsulated traffic.
- **Improved network tracing** To better enable troubleshooting problems that might arise, network traces now contain switch and port configuration information.

Learn more

You can learn more about the new Failover Clustering features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Networking in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn313100.aspx*.
- "What's New in Hyper-V Network Virtualization in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn383586.aspx*.
- "What's New in Hyper-V Virtual Switch in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn343757.aspx*.
- "Windows Server Gateway" at *http://technet.microsoft.com/en-us/library/dn313101.aspx*.

The following Microsoft TechNet and MSDN blog posts also have lots of information about the new Failover Clustering features and enhancements in Windows Server 2012 R2:

- "What's New in Hyper-V Network Virtualization in R2" at *http://blogs.technet.com/b/networking/archive/2013/07/31/what-s-new-in-hyper-v-network-virtualization-in-r2.aspx*.
- "New Networking Diagnostics with PowerShell in Windows Server R2" at *http://blogs.technet.com/b/networking/archive/2013/07/31/new-networking-diagnostics-with-powershell-in-windows-server-r2.aspx*.
- "Drive Up Networking Performance for Your Most Demanding Workloads with Virtual RSS" at *http://blogs.technet.com/b/networking/archive/2013/07/31/drive-up-networking-performance-for-your-most-demanding-workloads-with-virtual-rss.aspx*.
- "Hyper-V Extensible Switch Enhancements in Windows Server 2012 R2" at *http://blogs.technet.com/b/networking/archive/2013/07/31/hyper-v-extensible-switch-enhancements-in-windows-server-2012-r2.aspx*.
- "Transforming Your Datacenter—Networking in the R2 Release" at *http://blogs.technet.com/b/networking/archive/2013/07/31/transforming-your-datacenter-networking.aspx*.
- "Cloud Scale Multitenant Networking Stack" at *http://blogs.technet.com/b/networking/archive/2013/08/03/cloud-scale-multitenant-networking-stack-and-service.aspx*.
- "Enable the Forwarding Function on Windows Server Gateway: A Use Case Study" at *http://blogs.technet.com/b/networking/archive/2013/09/06/enable-forwarding-function-on-windows-server-gateway-a-use-case-study.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "What's New in Windows Server 2012 R2 Networking" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B216*.
- "Networking for Cloud Services in Windows Server 2012 R2" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B376*.

CHAPTER 6

Active Directory

Active Directory is the core identity and access control technology used for the IT infrastructure of most businesses today. Active Directory on the Windows Server platform collectively consists of the following server roles:

- **Active Directory Domain Services (AD DS)** Provides organizations with a scalable, secure, and manageable infrastructure for user and resource management and support for directory-enabled applications like Microsoft Exchange Server.
- **Active Directory Federation Services (AD FS)** Provides organizations with simple and secure identity federation and web single sign-on (SSO) capabilities.
- **Active Directory Lightweight Directory Services (AD LDS)** Provides an implementation of the Lightweight Directory Access Protocol (LDAP) so organizations can deploy a directory service that doesn't include the dependencies and domain-related restrictions of AD DS.
- **Active Directory Rights Management Services (AD RMS)** Provides organizations with tools for implementing and managing encryption, certificates, and authentication so they can implement reliable information protection solutions.
- **Active Directory Certificate Services (AD CS)** Enables organizations to implement a public key infrastructure (PKI) so they can deploy and manage public key cryptography, digital certificates, and digital signature capabilities for users and devices.

Microsoft has steadily enhanced the identity and access capabilities of the Windows Server platform over the years, and Windows Server 2012 R2 adds some exciting new capabilities we'll examine in a moment. But first let's briefly review how Active Directory was enhanced in the previous platform of Windows Server 2012.

Previous enhancements to Active Directory

Microsoft added a number of new features and enhancements to Active Directory in Windows Server 2012 that helped simplify the task of deploying, managing, and maintaining an Active Directory environment. Some of the key enhancements to AD DS included:

- Virtualizing domain controllers in previous versions of Windows Server sometimes resulted in problems with the logical clocks used by domain controllers to determine relative levels of convergence. Beginning with Windows Server 2012, however, virtual domain controllers employed a unique identifier called the virtual machine GenerationID. This unique identifier is exposed by the hypervisor to the virtual machine's address space within its BIOS so it can be made available to the guest operating system. When the guest operating system of a virtual domain controller boots, the current value of this identifier is compared with the value stored in AD DS. If a mismatch is detected, a rollback takes place to ensure that the virtual domain controller will properly converge with other domain controllers in the forest. The result of this improvement is to make virtualizing domain controllers safe for enterprises who want to implement this kind of scenario.
- Beginning with Windows Server 2012, organizations were able to deploy replica virtual domain controllers by cloning existing virtual domain controllers. The cloning process involved creating a copy of the existing source virtual domain controller, authorizing the source domain controller in AD DS, and using Windows PowerShell to create a configuration file for performing the domain controller promotion operation.
- The process for deploying domain controllers was also made faster and more flexible in Windows Server 2012. The Dcpromo.exe wizard of previous versions of Windows Server was replaced with a new Active Directory Domain Services Configuration Wizard built entirely upon Windows PowerShell. This redesign provides a number of benefits. For example, you can now install the AD DS server role binaries remotely using Server Manager or with the new AD DS PowerShell cmdlets. You can also install the binaries on multiple servers at the same time. Adprep.exe is also integrated into the Active Directory installation process to make it easier to prepare your existing Active Directory environment for upgrading to Windows Server 2012. And the Active Directory Domain Services Configuration Wizard performs validation to ensure that the necessary prerequisites have been met before promoting a server to a domain controller.
- The Active Directory Administrative Center (ADAC) that was first introduced in Windows Server 2008 R2 as a central management console for Active Directory administrators was also enhanced in Windows Server 2012 with new GUI elements for managing the Active Directory Recycle Bin and fine-grained password policies. In addition, a feature called Windows PowerShell History Viewer was added to help you quickly create Windows PowerShell scripts to automate Active Directory administration tasks by viewing and utilizing the Windows PowerShell commands underlying any actions performed using the user interface of ADAC.

Let's now look at some of the new capabilities in Active Directory in Windows Server 2012 R2.

Workplace Join

One of the key Active Directory enhancements in Windows Server 2012 R2 is called Workplace Join. Basically, what this means is that companies can now provide an SSO experience for all workplace-joined devices, which at present includes Windows and iOS devices.

The way it works is that users join their personal devices to their workplace by making their devices known to the company's Active Directory. The goal of doing this is to allow users to be able to easily and securely access resources and services on the company network so they can perform their job better.

Workplace Join associates the device with the user and enables a better user experience by providing a seamless second factor authentication. Users sign in once from any application running on their workplace-joined devices. They are not prompted for credentials by every company application when they are using their workplace-joined devices. This provides both the user and the company with some major benefits in the areas of usability and security, namely:

- Usability is enhanced because the user no longer has to repeatedly enter his or her credentials into the device to access resources on the company network.
- Security is enhanced because the risks involved in saving passwords with each application on the user's device are avoided.

When a user's device is workplace-joined, the attributes of the device are stored in Active Directory and can be retrieved to issue security tokens for the applications running on the user's device. This enables the company to grant the appropriate rights and permissions for the user's application to securely access company resources and services.

Workplace Join enables new scenarios for organizations that want to take advantage of bring-your-own-device (BYOD) to enhance user productivity. As Figure 6-1 shows, Workplace Join represents a middle-of-the-road approach to device manageability and security for enterprises.

FIGURE 6-1 Workplace Join represents a middle-of-the-road approach to device manageability and security for enterprises.

Implementing Workplace Join

Workplace Join uses the new capabilities of the AD FS role in Windows Server 2012 R2. Specifically, AD FS now includes a new service called the Device Registration Service that creates a device object in Active Directory when the user registers the device at a special website on the corporate network. The attributes of the device object are then used to provide conditional access to resources the user tries to access and to applications the user tries to run.

The steps for implementing Workplace Join are fairly straightforward but you'll need three servers to set things up. Here's a quick summary:

1. You need a domain controller running Windows Server 2012 R2.
2. You need to create a Group Managed Service Account (GMSA) account, which is basically a service account that can be used across a domain environment.
3. You need to obtain a server SSL certificate from a certificate authority (CA) and install it on a second server running Windows Server 2012 R2.
4. You need to install and configure the AD FS role on the second server.
5. You need to enable and configure the Device Registration Service on the second server.
6. You need to perform some additional tasks on your DNS server.
7. You need to install the IIS (Web Server) role and the Windows Identity Foundation feature on a third server running Windows Server 2012 R2.
8. You need to install the Windows Identity Foundation SDK on the third server.
9. You need to perform some additional steps involving IIS configuration and using the AD FS Management console.

Now you're all ready to go. Let's say a user wants to join his iPhone to your corporate network. Here's all the user needs to do:

1. Install an SSL certificate on his phone by browsing to a website specified by your administrator.
2. Open Safari on his phone and navigate to a web page by opening a special URL on your corporate network.
3. Log on to the web page using his domain credentials.
4. Accept the prompt to install a profile on his phone.
5. Re-enter his PIN to unlock his phone.

That's basically it and you can find more detail concerning the above steps in the Microsoft TechNet articles listed in the "Learn more" section at the end of this chapter.

Multi-factor access control

The AD FS server role has been enhanced in Windows Server 2012 R2 to support multi-factor access control that includes user, device, location, and authentication data. The result is that organizations that use AD FS can now control access to network resources based on such things as:

- User identity
- Group membership
- Network location
- Whether the device is workplace-joined
- Whether multi-factor authentication (MFA) has been performed

Access can be permitted or denied based on any of the above.

Multi-factor access control provides organizations with greater flexibility in how they craft their authorization policies. A rich claims language is provided, and Windows PowerShell can be used for more advanced claims scenarios.

Other enhancements include:

- A global authentication policy that can be applied to all applications and services that are secured by AD FS. The global policy can also be used to enable device authentication for seamless second-factor authentication.
- A simple and intuitive GUI-based AD FS MMC snap-in that is easy to use.
- Windows PowerShell support for automating mundane tasks.
- Support for custom MFA providers for organizations that leverage third-party MFA methods.

Web Application Proxy

Web Application Proxy is a new role service of the Remote Access server role in Windows Server 2012 R2 (see Figure 6-2). With a Web Application Proxy your organization can publish applications for external access, for example, in order to make your on-premises web resources available over the Internet so users outside your organization can access applications and services running on servers inside your corporate network.

FIGURE 6-2 Installing the Web Application Proxy role service of the Remote Access server role.

Web Application Proxy works by acting as both a reverse proxy and an AD FS proxy. In the previous version of Windows Server 2012, a role service called Federation Proxy Service was available for installation when you installed the AD FS server role. In Windows Server 2012 R2, this role service has been removed from the AD FS role and moved to the Remote Access role, and additional reverse proxy functionality has been added. Because you cannot install both Web Application Proxy and AD FS on the same server, remote access solutions based on Windows Server 2012 R2 are now made more secure by controlling authentication and authorization policies separately in AD FS.

Web Application Proxy works with any kind of user device. This means for example that Web Application Proxy can be used to enable your users to work from home or on the road using their personal computer, tablet, or smartphone. And because Web Application Proxy also provides reverse proxy functionality, the experience from the user's point of view is the same as if her device was connecting directly to the server running the application.

Implementing Web Application Proxy

Web Application Proxy is typically deployed on a server in the perimeter network of your organization (see Figure 6-3). Placing the Web Application Proxy on your perimeter network affords greater security because of the double nature of the firewall protection being provided.

FIGURE 6-3 Deploying a Web Application Proxy on your perimeter network.

Once you've deployed and configure AD FS in your environment and have installed Web Application Proxy on the perimeter network server, your next step is to configure the Web Application Proxy. The Web Application Proxy Configuration Wizard shown in Figure 6-4 can be used for this purpose. Configuring the Web Application Proxy involves providing information that can be used to connect Web Application Proxy with your AD FS server.

FIGURE 6-4 Configuring the Web Application Proxy.

Once Web Application Proxy has been configured, you can use the Remote Access Management console to publish your internal applications so external users can access them via Web Application Proxy. Applications are published by using the Publish New Application Wizard. On the Preauthentication page, as shown in Figure 6-5, you choose which method Web Application Proxy should use for preauthentication. The options here are either Pass-through, which simply forwards all requests to the backend application server without performing any preauthentication, or AD FS, which redirects all requests to your federation server. If you choose AD FS, requests that have been successfully preauthenticated are then forwarded to the backend server.

FIGURE 6-5 You can publish an application using Web Application Proxy.

After choosing the preauthentication method you wish to use for publishing applications, you then specify the relying party. Since we selected AD FS as the preauthentication method, the relying party is the Device Registration Service (see Figure 6-6).

FIGURE 6-6 A continued look at publishing an application using Web Application Proxy.

The Publishing Settings page allows you to specify a name, external URL, external certificate, and backend server URL for the application you are publishing. Once you've completed the wizard, the internal application will be accessible for external users to access provided they have been properly authorized to do so.

Improved LDAP search performance

Lightweight Directory Access Protocol (LDAP) is the industry-standard protocol used by Active Directory clients when performing searches against the directory. To query AD DS, the client composes a search query using the LDAP syntax and then submits it to the directory for processing. One of the many under-the-hood improvements introduced in Windows Server 2012 R2 is some changes to the LDAP query optimizer algorithm. As the following sidebar contributed by one of our Microsoft insiders shows, these changes can result in better performance for even complex queries against AD DS.

LDAP query optimizer changes

The LDAP query optimizer algorithm was reevaluated and further optimized in Windows Server 2012 R2. The result is a performance improvement in LDAP search efficiency and LDAP search time of complex queries.

These improvements in the performance of searches are a result of improvements in the mapping from LDAP query to ESE query. LDAP filters beyond a certain level of complexity prevent optimized index selection, resulting in drastically decreased performance (1000x or more). This change alters the way in which we select indices for LDAP queries to avoid this problem.

Background

The ability to search Active Directory is one of the core services provided by domain controllers. Many services and line-of-business applications rely on this service. Business operations can cease to a halt if this feature is not available. As a core and heavily used service, it is imperative that domain controllers handle LDAP search traffic efficiently.

The LDAP query optimizer algorithm attempts to make LDAP searches efficient as possible by mapping LDAP search filters to a result set that can be satisfied via records already indexed in the database. This algorithm was reevaluated and further optimized. The result is the performance improvement in LDAP search efficiency and LDAP search time of complex queries.

Details of change

An LDAP search contains a location (NC head, OU, Object) within the hierarchy to begin the search, a search filter, and a list of attributes to return. The search process can be summarized as follows:

1. Simplify the search filter, if possible.
2. Select a set of index keys that will return the smallest covered set.
3. Perform one or more intersections of index keys to reduce the covered set.
4. For each record in the covered set, evaluate the filter expression as well as the security. If the filter evaluates to TRUE and access is granted, then return this record to the client.

The LDAP query optimization work modifies steps 2 and 3 so as to reduce the size of the covered set. More specifically, the current implementation selects duplicate index keys and performs redundant intersections.

- Select a set of index keys that will return the smallest covered set.
- Perform one or more intersections of index keys to reduce the covered set.

Sample results using the old algorithm

The target of the inefficient LDAP search in the following example is a Windows Server 2012 domain controller. The search completes in approximately 44 seconds as a result of failing to find a more efficient index.

```
   adfind -b dc=blue,dc=contoso,dc=com -f "(| (& (|(cn=justintu)
(postalcode=80304) (userprincipalname=justintu@blue.contoso.com))
(|(objectclass=person) (cn=justintu)) )
(&(cn=justintu)(objectclass=person)))" -stats >>adfind.txt

Using server: WINSRV-DC1.blue.contoso.com:389

…<removed search results>

Statistics
================================
Elapsed Time: 44640 (ms)
Returned 324 entries of 553896 visited - (0.06%)

Used Filter:
 ( |  ( &  ( |  (cn=justintu)  (postalCode=80304)
(userPrincipalName=justintu@blue.contoso.com) )  ( |
(objectClass=person)  (cn=justintu) ) )  ( &  (cn=justintu)
(objectClass=person) ) )

Used Indices:
 DNT_index:516615:N

Pages Referenced          : 4619650
Pages Read From Disk      : 973
Pages Pre-read From Disk  : 180898
Pages Dirtied             : 0
Pages Re-Dirtied          : 0
Log Records Generated     : 0
Log Record Bytes Generated: 0
```

Sample results using the new algorithm

Here we repeat the exact same search as above but target a Windows Server 2012 R2 domain controller. The same search completes in less than a second due to the improvements in the LDAP query optimizer algorithm.

```
   adfind -b dc=blue,dc=contoso,dc=com -f "(| (& (|(cn=justintu)
(postalcode=80304) (userprincipalname=dhunt@blue.contoso.com))
(|(objectclass=person) (cn=justintu)) )
(&(cn=justintu)(objectclass=person)))" -stats >>adfindBLUE.txt
```

```
Using server: winblueDC1.blue.contoso.com:389

….<removed search results>

Statistics
================================
Elapsed Time: 672 (ms)
Returned 324 entries of 648 visited - (50.00%)

Used Filter:
 ( |  ( &  ( |  (cn=justintu)  (postalCode=80304)
(userPrincipalName=justintu@blue.contoso.com) )  ( |
(objectClass=person)  (cn=justintu) ) )  ( &  (cn=justintu)
(objectClass=person) ) )

Used Indices:
 idx_userPrincipalName:648:N
 idx_postalCode:323:N
 idx_cn:1:N

Pages Referenced          : 15350
Pages Read From Disk      : 176
Pages Pre-read From Disk  : 2
Pages Dirtied             : 0
Pages Re-Dirtied          : 0
Log Records Generated     : 0
Log Record Bytes Generated: 0
```

Optimization of paged queries

The handling of paged queries was changed completely.

From a sample paged query that gets 112 out of 10,000+ groups based on a CN filter and a page size of 6:

```
   Statistics
================================
Elapsed Time: 0 (ms)
Returned 112 entries of 113 visited - (99.12%)

Used Filter:
( |  ( &  ( |  (cn=SFU-GRP-Test73*)  (userPrincipalName=add-t*) )  ( |
(objectClass=person)  (objectClass=group) (cn=add-t*) ) )
( &  (cn=add-t*)  (objectClass=person) ) )

Used Indices:
idx_cn:113:N
```

```
idx_cn:1:N
idx_userPrincipalName:1:N

Pages Referenced          : 3223
Pages Read From Disk      : 0
Pages Pre-read From Disk  : 0
Pages Dirtied             : 0
Pages Re-Dirtied          : 0
Log Records Generated     : 0
Log Record Bytes Generated: 0
…
Filter Breakdown:

(
(|
   (&
     (|
       (cn=SFU-GRP-Test73*)
       (userPrincipalName=add-t*)
     )
     (|
       (objectClass=person)
       (objectClass=group)
       (cn=add-t*)
     )
   )
   (&
     (cn=add-t*)
     (objectClass=person)
   )
)
)
```

In the network frames, the cookie is just 6 bytes now in contrast to several hundred bytes before controls:

```
   ControlType: 1.2.840.113556.1.4.319 (LDAP_PAGED_RESULT_OID_STRING)

31 2E 32 2E 38 34 30 2E 31 31 33 35 35 36 2E 31 2E 34 2E 33 31 39 01 01
FF 04 0F 30 84 00 00 00 09 02 01 06 04 04 33 0B 00 00 01
1.2.840.113556.1.4.319..ÿ..0„.........3....
```

This means we can now optimize paged queries just like non-paged queries.

Justin Turner
Support Topic Lead for Active Directory, Windows DSYS TX

Learn more

You can learn more about the new Active Directory features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Active Directory in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn268294.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "Understanding Access and Information Protection" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B207*.
- "Identity Infrastructure Fundamentals and Essential Capabilities" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/ATC-B209*.
- "Enable Work from Anywhere without Losing Sleep: Remote Access with the Web Application Proxy and VPN Solutions" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B333*.
- "Active Directory Enables User Productivity and IT Risk Management Strategies Across a Variety of Devices" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B204*.

CHAPTER 7

Group Policy

For many organizations, Group Policy is the key technology they utilize to lock down their environments. Composed of thousands of different policy settings and dozens of categories of preference items, a thorough knowledge of what Group Policy can do and how to configure, optimize and maintain its operations is an essential part of the administrator's job.

Previous enhancements to Group Policy

Group Policy received a lot of new functionalities in Windows Server 2012 and Windows 8. Some of the more important enhancements included:

- **Remote Group Policy update** Windows Server 2012 enabled the use of the Group Policy Management Console (GPMC) to refresh the computer and user Group Policy settings (including security settings) on all remote computers in an organizational unit (OU). It did this by scheduling a task that ran an update.exe on the remote computers. You could also use the Invoke-GPUpdate Windows PowerShell cmdlet to automate the remote Group Policy update. These functionalities helped when you needed to push out a new Group Policy setting immediately to users or computers in your environment.
- **Group Policy infrastructure status** You could use the GPMC to view the status of Active Directory and SYSVOL replication for all Group Policy Objects (GPOs) or for a selected GPO. This included viewing the security descriptors, GPO version details, and number of GPOs listed in Active Directory and SYSVOL for each domain controller. This functionality was helpful for monitoring and diagnosing replication issues related to Group Policy at the domain level.
- **Fast Startup** Computers running Windows 8 and later are configured by default to use Fast Startup, a new boot mode that is a hybrid of traditional cold boot and resuming from hibernate. Fast Startup closes all user sessions on shutdown, but hibernates the kernel session instead of closing it. This enabled Windows 8 computers to shut down and start up more quickly than in previous versions of Windows. Although Fast Startup can help speed up Group Policy processing, some policy settings or scripts processed during startup or shutdown might not be applied when Fast Startup is enabled.

- **New Group Policy starter GPOs** Windows Server 2012 included two new starter GPOs that can make configuring Group Policy firewall port requirements a lot easier. These starter GPOs are named Group Policy Reporting Firewall Ports and Group Policy Remote Update Firewall Ports. You could import these starter GPOs when you created a new GPO for this purpose.
- **Local Group Policy support for Windows RT** Group Policy can be used to manage devices that run Windows RT. By default, the Group Policy Client service was disabled on Windows RT devices and must be enabled and configured to start automatically using the Services snap-in.

Additionally, there were lots of new policy settings and preferences added to Group Policy in Windows Server 2012, including settings and preferences for Internet Explorer 10 and many other Windows components and capabilities.

As far as enhancements in Windows Server 2012 R2 go, this time around it's more of a fine-tuning of Group Policy capabilities rather than a lot of new functionality. Let's examine some of the changes now.

Group Policy caching

One of the key enhancements in Windows Server 2012 R2 is policy caching, which can significantly reduce the amount of time it takes to process Group Policy on a client. Policy caching works by having the client download the policy from a domain controller and save a copy of the policy to a local store on the client. Then, when the next Group Policy processing occurs, the client can apply the policy cached in the local store instead of having to download the policy again from the network.

By speeding up Group Policy processing, policy caching can shorten boot times for clients. This can be especially helpful in scenarios where the network connection experiences latency or is connecting from off-premises over the Internet, for example, in a DirectAccess scenario. Note that policy caching only works when Group Policy is running in synchronous mode.

Policy caching is disabled by default in Windows Server 2012 R2. To enable and configure policy caching, configure the following policy setting named Enable Group Policy Caching For Servers as shown in Figure 7-1. This policy setting can be found under:

Computer Configuration\Policies\Administrative Templates\System\Group Policy

FIGURE 7-1 The new Enable Group Policy Caching For Servers policy setting.

Group Policy Preferences and IPv6

Another important area where Group Policy has been enhanced in Windows Server 2012 R2 is in regards to Internet Protocol version 6 (IPv6) support. An increasingly important part of the job of the Windows Server administrator is to prepare the organization's network for migration to IPv6. The reasons for this include the exponential growth of the Internet, the proliferation of mobile devices that need to be able to connect to the corporate network, and the exhaustion of the IPv4 address space. Windows Server 2012 included a number of new IPv6 capabilities such as built-in support for NAT64/DNS64 when implementing DirectAccess, new Windows PowerShell cmdlets that supersede the Netsh.exe command-line utility of earlier Windows versions, and improved Internet connectivity by marking well-known IPv6 Internet resources Windows can't reach as unreachable so that in the future only IPv4 is used for connecting to them.

With Windows Server 2012 R2, however, IPv6 has now made more inroads into Group Policy functionality on the platform. For example, you can now specify an IPv6 address when using item-level targeting with Group Policy Preferences (GPP). This allows you to configure

the scope of individual preference items so they apply only to computers that have a specific IPv6 address range. For example, here's how you might use this capability to use a GPO to apply a certain power plan to computers running Windows 7 or later whose IPv6 addresses fall within the address range 2001:DB8:3FA9:/48:

1. Open the GPO in the Group Policy Management Editor and expand Computer Configuration | Preferences | Control Panel Settings | Power Options.
2. Right-click Power Options and select New | Power Plan (at least Windows 7).
3. In the New Power Plan Properties dialog, click the Common tab, select the Item-level Targeting check box, and click Targeting.
4. In the Targeting Editor, click New Item | IP Address Range.
5. Select the Use IPv6 check box, as shown in Figure 7-2, and specify the IPv6 address and prefix length.

FIGURE 7-2 Item-level targeting now supports IPv6 addresses.

Support for IPv6 has been introduced into other areas of Group Policy as well. For example, when you create a new TCP/IP Printer preference item, you can specify an IPv6 address of the network printer, as shown in Figure 7-3.

FIGURE 7-3 You can now specify an IPv6 address for a network printer.

Another example of IPv6 support in Group Policy can be found when you create a new VPN Connection preference item, as shown in Figure 7-4.

FIGURE 7-4 You can now specify an IPv6 address when creating a new VPN connection.

New policy settings

Finally, as one might expect, there are a number of new policy settings available for Group Policy in Windows Server 2012 R2. Although the sections below don't cover all of these new policy settings, the ones described will definitely be of interest for administrators to learn. Some of these policy settings are specific to Windows 8.1 client computers, whereas others are applicable to both clients and servers. The policy settings have been roughly grouped together according to the areas of functionality to which they apply.

Start screen

There are several new policy settings that can be used for customizing the behavior of the Start screen only on computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1. The ones we'll look at here are:

- Start Screen Layout
- Force a specific Start background
- Force a specific background and accent color
- Show the Apps view automatically when the user goes to Start

Start Screen Layout

This policy setting specifies the Start screen layout for users and is located at:

Computer Configuration\Start Menu and Taskbar

User Configuration\Start Menu and Taskbar

This setting lets you specify the Start screen layout for users and prevents them from changing its configuration. The Start screen layout you specify must be stored in an XML file that was generated by the Export-StartLayout Windows PowerShell cmdlet.

To use this setting, you must first manually configure a device's Start screen layout to the desired look and feel. Once you are done, run the Export-StartLayout Windows PowerShell cmdlet on that same device. The cmdlet will generate an XML file representing the layout you configured.

Once the XML file is generated and moved to the desired file path, type the fully qualified path and name of the XML file. You can type a local path, such as C:\StartLayouts\myLayout.xml or a UNC path, such as \\Server\Share\Layout.xml. If the specified file is not available when the user logs on, the layout won't be changed. Users cannot customize their Start screen while this setting is enabled.

If you disable this setting or do not configure it, the Start screen layout won't be changed and users will be able to customize it.

Force a specific Start background

This policy setting forces the Start screen to use a specific background and is located at:

Computer Configuration\Control Panel\Personalization

Specifically, it forces the Start screen to use one of the available backgrounds, 1 through 20, and prevents the user from changing it.

If this setting is set to zero or not configured, then Start uses the default background and users can change it.

If this setting is set to a nonzero value, then Start uses the specified background and users cannot change it. If the specified background is not supported, the default background is used.

Force a specific background and accent color

This policy setting forces Windows to use the specified colors for the background and accent. It is located at:

Computer Configuration\Control Panel\Personalization

When configuring this policy setting, the color values are specified in hex as #RGB.

By default, users can change the background and accent colors.

If this setting is enabled, the background and accent colors of Windows will be set to the specified colors and users cannot change those colors. This setting will not be applied if the specified colors do not meet a contrast ratio of 2:1 with white text.

Show the Apps view automatically when the user goes to Start

This policy setting allows the Apps view to be opened by default when the user goes to Start. It is located at:

User Configuration\Start Menu and Taskbar

If you enable this policy setting, the Apps view will appear whenever the user goes to Start. Users will still be able to switch between the Apps view and the Start screen.

If you disable or don't configure this policy setting, the Start screen will appear by default whenever the user goes to Start, and the user will be able to switch between the Apps view and the Start screen. Also, the user will be able to configure this setting.

Multi-monitor display

There is an additional policy setting for the Start screen that only applies when the user is using a multimonitor display. This policy setting also applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Show Start on the display the user is using when they press the Windows logo key

This policy setting allows the Start screen to appear on the display the user is using when they press the Windows logo key. It is located at:

User Configuration\Start Menu and Taskbar

If you enable this policy setting, the Start screen will appear on the display the user is using when they press the Windows logo key.

If you disable or don't configure this policy setting, the Start screen will always appear on the main display when the user presses the Windows logo key. Users will still be able to open Start on other displays by pressing the Start button on that display. Also, the user will be able to configure this setting.

Apps

There are a couple of new policy settings that deal with how apps are displayed and searched for from the Start screen:

- Do not show recent apps when the mouse is pointing to the upper-left corner of the screen
- Search just apps from the Apps view

These new policy settings apply only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Do not show recent apps when the mouse is pointing to the upper-left corner of the screen

This policy setting allows you to prevent the last app and the list of recent apps from appearing when the mouse is pointing to the upper-left corner of the screen. It is located at:

User Configuration\Windows Components\Edge UI

If you enable this policy setting, the user will no longer be able to switch to recent apps using the mouse. The user will still be able to switch apps using touch gestures, keyboard shortcuts, and the Start screen.

If you disable or don't configure this policy setting, the recent apps will be available by default and the user can configure this setting.

Search just apps from the Apps view

This policy setting prevents the user from searching apps, files, and settings (and the web if enabled) when the user searches from the Apps view. It is located at:

User Configuration\Start Menu and Taskbar

This policy setting is only applied when the Apps view is set as the default view for Start.

If you enable this policy setting, searching from the Apps view will only search the list of installed apps.

If you disable or don't configure this policy setting, the user can configure this setting.

Sync your settings

There is one new Group Policy setting that can be used to configure the behavior of how Sync Your Settings works for users. This new policy setting applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Do not sync Start settings

This policy setting can prevent the "Start layout" group from syncing to and from this PC. This turns off and disables the "Start layout" group on the "sync your settings" page in PC settings. It is located at:

Computer Configuration\Windows Components\Sync your settings

If you enable this policy setting, the "Start layout" group will not be synced.

If you do not set or disable this setting, syncing of the "Start layout" group is on by default and configurable by the user.

Use the option "Allow users to turn start syncing on" so that syncing is turned off by default but not disabled.

Work Folders

As described previously in Chapter 3, "Storage," Work Folders is a new storage feature introduced in Windows Server 2012 R2 that can help your organization address bring-your-own device (BYOD) scenarios typical of the modern workplace. There are two new Group Policy settings you can use to configure the behavior of this new feature:

- Force automatic setup for all users
- Specify Work Folders settings

Both of these new policy settings apply only to computers running Windows 8.1 or Windows RT 8.1.

Force automatic setup for all users

This policy setting specifies whether Work Folders should be set up automatically for all users of the affected computer. It is located at:

Computer Configuration\Windows Components\Work Folders

If you enable this policy setting, Work Folders will be set up automatically for all users of the affected computer. This prevents users from choosing not to use Work Folders on the computer; it also prevents them from manually specifying the local folder in which Work Folders store files. Work Folders will use the settings specified in the "Specify Work Folders settings" policy setting in User Configuration\Administrative Templates\Windows Components\WorkFolders. If the "Specify Work Folders settings" policy setting does not apply to a user, Work Folders is not automatically set up.

If you disable or do not configure this policy setting, Work Folders uses the "Force automatic setup" option of the "Specify Work Folders settings" policy setting to determine whether to automatically set up Work Folders for a given user.

Specify Work Folders settings

This policy setting specifies the Work Folders server for affected users, as well as whether or not users are allowed to change settings when setting up Work Folders on a domain-joined computer. It is located at:

User Configuration\Windows Components\Work Folders

If you enable this policy setting, affected users receive Work Folders settings when they sign in to a domain-joined PC.

The "Work Folders URL" (see Figure 7-5) can specify either the URL used by the organization for Work Folders discovery, or the specific URL of the file server that stores the affected users' data.

The "Force automatic setup" option specifies that Work Folders should be set up automatically without prompting users. This prevents users from choosing not to use Work Folders on the computer; it also prevents them from manually specifying the local folder in which Work Folders stores files. By default, Work Folders is stored in the "%USERPROFILE%\Work Folders" folder. If this option is not specified, users must use the Work Folders Control Panel item on their computers to set up Work Folders.

If this policy setting is disabled or not configured, no Work Folders settings are specified for the affected users, though users can manually set up Work Folders by using the Work Folders Control Panel item.

Kerberos authentication

There are three new policy settings related to how Kerberos authentication can be performed in Active Directory environments:

- Request compound authentication
- Always send compound authentication first
- Restrict delegation of credentials to remote servers

These new policy settings apply only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Request compound authentication

This policy setting allows you to configure a domain controller to request compound authentication. It is located at:

Computer Configuration\System\KDC

If you enable this policy setting, domain controllers will request compound authentication. The returned service ticket will contain compound authentication only when the account is explicitly configured. This policy should be applied to all domain controllers to ensure consistent application of this policy in the domain.

If you disable or do not configure this policy setting, domain controllers will return service tickets that contain compound authentication any time the client sends a compound authentication request regardless of the account configuration.

NOTE **For a domain controller to request compound authentication, the policy "KDC support for claims, compound authentication, and Kerberos armoring" must be configured and enabled.**

Always send compound authentication first

This policy setting controls whether a device always sends a compound authentication request when the resource domain requests compound identity. It is located at:

Computer Configuration\System\Kerberos

If you enable this policy setting and the resource domain requests compound authentication, devices that support compound authentication always send a compound authentication request.

If you disable or do not configure this policy setting and the resource domain requests compound authentication, devices will send a non-compounded authentication request first, and then a compound authentication request when the service requests compound authentication.

NOTE **For a domain controller to request compound authentication, the policies "KDC support for claims, compound authentication, and Kerberos armoring" and "Request compound authentication" must be configured and enabled in the resource account domain.**

Restrict delegation of credentials to remote servers

This policy setting is used to configure restricted mode. It is located at:

Computer Configuration\System\Credentials Delegation

When running in restricted mode, participating apps do not expose credentials to remote computers (regardless of the delegation method). Restricted mode may limit access to resources located on other servers or networks beyond the target computer because credentials are not delegated. Participating apps include Remote Desktop Client.

If you enable this policy setting, restricted mode is enforced and participating apps will not delegate credentials to remote computers.

If you disable or do not configure this policy setting, restricted mode is not enforced and participating apps can delegate credentials to remote computers.

> ***NOTE*** **To disable most credential delegation, it may be sufficient to deny delegation in Credential Security Support Provider (CredSSP) by modifying Administrative template settings (located at Computer Configuration\Administrative Templates\System\Credentials Delegation).**

Logon scripts

There is one new Group Policy setting that can be used to configure the behavior of how logon scripts are processed in your environment. This new policy setting applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Configure Logon Script Delay

This policy setting allows you to configure how long the Group Policy client waits after logon before running scripts. It is located at:

Computer Configuration\System\Group Policy

By default, the Group Policy client waits five minutes before running logon scripts. This helps create a responsive desktop environment by preventing disk contention.

If you enable this policy setting, Group Policy will wait for the specified amount of time before running logon scripts.

If you disable this policy setting, Group Policy will run scripts immediately after logon.

If you do not configure this policy setting, Group Policy will wait five minutes before running logon scripts.

Enter “0” to disable Logon Script Delay.

Windows Update

There is one new Group Policy setting that can be used to configure the behavior of how Windows Update works in your environment. This new policy setting applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Do not connect to any Windows Update Internet locations

This policy setting is located at:

Computer Configuration\Windows Components\Windows Update

Enabling this policy will disable that functionality and may cause connection to public services such as the Windows Store to stop working.

Even when Windows Update is configured to receive updates from an intranet update service, it will periodically retrieve information from the public Windows Update service to enable future connections to Windows Update, and other services like Microsoft Update or the Windows Store.

NOTE **This policy applies only when this PC is configured to connect to an intranet update service using the "Specify intranet Microsoft update service location" policy.**

Windows Runtime apps

There is one new Group Policy setting that can be used to configure the behavior of Windows runtime apps for your environment. This new policy setting applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Allow Windows Runtime apps to revoke enterprise data

This policy setting is located at:

User Configuration\Windows Components\File Revocation

Windows Runtime applications can protect content which has been associated with an enterprise identifier (EID), but can only revoke access to content it protected. To allow an application to revoke access to all content on the device that is protected by a particular enterprise, add an entry to the list on a new line that contains the enterprise identifier, separated by a comma, and the Package Family Name of the application. The EID must be an internet domain belonging to the enterprise in standard international domain name format. An example value might be:

Contoso.com,ContosoIT.HumanResourcesApp_m5g0r7arhahqy

If you enable this policy setting, the application identified by the Package Family Name will be permitted to revoke access to all content protected using the specified EID on the device.

If you disable or do not configure this policy setting, the only Windows Runtime applications that can revoke access to all enterprise-protected content on the device are Windows Mail and the user-selected mailto protocol handler app. Any other Windows Runtime application will only be able to revoke access to content it protected.

> ***NOTE*** **File revocation applies to all content protected under the same second level domain as the provided enterprise identifier. So, revoking an enterprise ID of mail.contoso.com will revoke the user's access to all content protected under the contoso.com hierarchy.**

Microsoft accounts

There is one new Group Policy setting that can be used to configure the behavior of Microsoft accounts for users. This new policy setting applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Allow Microsoft accounts to be optional

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. It is located at:

Computer Configuration\Windows Components\App runtime

User Configuration\Windows Components\App runtime

If you enable this policy setting, Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

If you disable or do not configure this policy setting, users will need to sign in with a Microsoft account.

> ***NOTE*** **This policy only affects Windows Store apps that support it.**

Automatic sign-in

An interesting new Group Policy setting is now available to configure what happens if Windows initiates a restart while the user is logged on to his or her computer. This new policy setting applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

Sign-in last interactive user automatically after a system-initiated restart

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system. It is located at:

Computer Configuration\Windows Components\Windows Logon Options

If you enable or do not configure this policy setting, the device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.

If you disable this policy setting, the device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts.

Windows SkyDrive

Two new Group Policy settings can be used to configure the behavior of Windows SkyDrive for users:

- Prevent the usage of SkyDrive for file storage
- Save documents and pictures to the local PC by default

These new policy settings apply only to computers running Windows 8.1 or Windows RT 8.1.

Prevent the usage of SkyDrive for file storage

This policy setting lets you prevent apps and features from working with files on SkyDrive. It is located at:

Computer Configuration\Windows Components\SkyDrive

If you enable this policy setting, the following happens:

- Users can't access SkyDrive from the SkyDrive app and file picker.
- Windows Store apps can't access SkyDrive using the WinRT API.
- SkyDrive doesn't appear in the navigation pane in File Explorer.
- SkyDrive files aren't kept in sync with the cloud.
- Users can't automatically upload photos and videos from the camera roll folder.

If you disable or do not configure this policy setting, apps and features can work with SkyDrive file storage.

Save documents and pictures to the local PC by default

This policy setting lets you select the local PC as the default save location. It does not prevent apps and users from saving files on SkyDrive. It is located at:

Computer Configuration\Windows Components\SkyDrive

If you enable this policy setting, files will be saved locally by default. Users will still be able to change the value of this setting to save to SkyDrive by default. They will also be able to open and save files on SkyDrive using the SkyDrive app and file picker, and Windows Store apps will still be able to access SkyDrive using the WinRT API.

If you disable or do not configure this policy setting, users with a connected account will save files to SkyDrive by default.

Learn more

You can learn more about the new Group Policy features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Group Policy in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn265973.aspx*.

CHAPTER 8

IIS

The Web Server (IIS) role in Windows Server 2012 R2 provides a modular and extensible platform for reliably hosting websites, services, and applications. IIS enables businesses to share information with users on the Internet, a corporate intranet, or a company extranet. IIS is a secure and easy-to-manage unified web platform that integrates IIS, ASP.NET, FTP services, PHP, and Windows Communication Foundation (WCF).

Previous enhancements to IIS

IIS 8.0 in Windows Server 2012 introduced a number of new capabilities that made the Microsoft web server a highly scalable and elastic platform for cloud computing. The results were beneficial to a wide spectrum of customers ranging from an enterprise hosting line of business (LOB) applications or a cloud-hosting provider managing a multitenant public cloud. Some of the significant improvements made to IIS 8 in Windows Server 2012 included:

- **NUMA-aware scalability** Non-Uniform Memory Architecture (NUMA) was designed to overcome the scalability limits of the traditional symmetric multiprocessing (SMP) architecture, where all memory access happens on the same shared memory bus. SMP works well when you have a small number of CPUs, but it doesn't when you have dozens of them competing for access to the shared bus. NUMA alleviated such bottlenecks by limiting how many CPUs could be on any one memory bus and connecting them with a high-speed interconnection. To utilize these capabilities, IIS in Windows Server 2012 introduced NUMA-aware scalability, which worked by intelligently affinitizing worker processes to NUMA nodes. On NUMA-aware hardware, IIS will try to assign each worker process in a web garden to a different NUMA node to achieve optimal performance.
- **Server Name Indication** Before Windows Server 2012, you could use host headers in IIS to support hosting multiple HTTP websites using only a single shared IP address. Moreover, if you wanted these websites to use HTTPS, then you had a problem because you couldn't use host headers with HTTPS since IIS didn't support that. Instead, you had to assign multiple IP addresses to your web server and bind a different IP address to each HTTPS site, which incurred a lot

of management overhead for IIS administrators. However, IIS 8 in Windows Server 2012 supported Server Name Indication (SNI), which allowed a virtual domain name to be used to identify the network end point of an SSL/TSL connection. This meant IIS could host multiple HTTPS websites, each with their own SSL certificate, bound to the same shared IP address. SNI thus provided increased scalability for web servers hosting multiple SSL sites, and it helped cloud hosting providers to better conserve the dwindling resources of their pool of available IP addresses.

- **SSL central store** Before Windows Server 2012, managing SSL certificates on servers in IIS web farms was time consuming because the certificates had to be imported into every server in the farm, which made scaling out a farm by deploying additional servers a complex task. Replicating certificates across IIS servers in a farm was further complicated by the need to manually ensure that certificate versions were in sync with each another. IIS in Windows Server 2012 solved this problem by introducing a central store for storing SSL certificates on a file share on the network instead of in the certificate store of each host.
- **CPU throttling** IIS in Windows Server 2012 allowed you to configure an application pool to throttle the CPU usage so that it could not consume more CPU cycles than a user-specified threshold. You could also configure IIS to throttle an application pool when the system was under load, and this allowed your application pool to consume more resources than your specified level when the system was idle because the Windows kernel would only throttle the worker process and all child processes when the system came under load.
- **Application Initialization** When users try to open a website in their web browser, and then have to wait for several seconds or longer for the site to respond, they get frustrated. Before Windows Server 2012, the delay that occurred when a web application was first accessed was because the application needed to be loaded into memory before IIS could process the user's request and return a response. With the introduction of Application Initialization in IIS 8, however, application pools could now be prestarted instead of having to wait for a first request to arrive for a web application in the pool. Administrators could choose which applications should be preloaded on their IIS servers, and IIS could even be configured to return a static "splash page" while the application was being initialized so the user felt the website being accessed was responding instead of failing to respond.
- **Dynamic IP address filtering** Before Windows Server 2012, IIS could use static IP filtering to block requests from specific clients. This functionality was of limited usefulness, however, since it meant that you had to first discover the IP address of the offending client, and then manually configure IIS to block that address. Also, IIS offered no choice as to what action it would take when it blocked a client—an HTTP 403.6 status message was always returned to the offending client. IIS 8, however, introduced a new capability called dynamic IP address filtering, which allowed you to configure an IIS server to block access for any IP address that exceeded a specified

number of concurrent requests or exceeded a specified number of requests within a given period of time. You could also configure how IIS responded when it blocked an IP address—for example, by aborting the request instead of returning HTTP 403.6 responses to the client.

By contrast, the improvements made to IIS 8.5 in Windows Server 2012 R2 are targeted at a different audience, namely, website administrators who are highly focused on scalability and manageability. Such improvements are increasingly important in today's world. In fact, both Microsoft's public website and the Windows Azure platform are deeply tied to IIS.

Dynamic Site Activation

One of the key scalability goals Microsoft has for IIS 8.5 is enabling cloud-hosting providers to host more sites on a single IIS server. In Windows Server 2012 and earlier, when IIS starts up on a host, the Windows Activation Service (WAS) loads the entire configuration for IIS. This configuration can be very large if several thousand sites are being hosted on the server, which is typical in many hoster environments. Because of this, loading the IIS configuration can consume a lot of memory on the server, which can impact the performance of other options, such as initializing worker processes for web applications.

To address this issue, the WAS component has been redesigned in IIS to better handle large configurations and improve the memory efficiency of the IIS startup process. In addition, the HTTP protocol stack (Http.sys) now uses a single catch-all request queue and binding to be used by WAS for initializing the worker processes associated with each of the sites running on the IIS server. The result of this change is that when WAS starts up, it no longer has to create thousands of request queues and bindings in Http.sys—one for each of the thousands of worker processes associated with each of the thousands of sites running on the server. The WAS component can now examine a client request in this queue and determine which site and worker process should handle that request. WAS then creates a queue for the request, registers the binding, and spins up the worker process for the site to start the site.

This new functionality is called Dynamic Site Activation, and it addresses the issue of being "config-bound" which hosters who run large numbers of sites on IIS servers can experience. By default, if an IIS 8.5 server is hosting 100 or more sites, this new WAS functionality is used. If the server is hosting fewer than 100 sites, however, the old method of creating separate queues and bindings for each site is still used since such a scenario has only a relatively small configuration that can load quite easily without undue memory being needed. This functionality can be tuned by modifying the *dynamicRegistrationThreshold* parameter using the IIS Configuration Editor, as shown in Figure 8-1. Note that you must restart WAS after changing this parameter for the change to take effect.

FIGURE 8-1 The Configuration Editor configures Dynamic Site Activation.

Idle Worker Process Page-out

A second scalability issue that can be experienced on IIS servers hosting large numbers of sites has to do with cold requests. A cold request is a request that comes for a worker process that has not yet been started. The cold request has to wait for IIS to initialize, for the appropriate framework (for example, .NET or PHP) to initialize, for the associated site to initialize, and so on. As a result, the response time to cold requests with previous versions of IIS sometimes left something to be desired.

This issue was partly addressed with IIS 8 in Windows Server 2012 where static sites responded much more quickly (typically a few hundred milliseconds) to cold requests than for IIS 7 in Windows Server 2008 R2. However, there was only a small performance improvement in IIS 8 for dynamic sites with managed code, with such sites typically taking several seconds to start in response to cold requests, largely because of the time needed to load the application framework needed by the site. From the perspective of the hoster's customers, however, taking several seconds to launch their LOB web application can be viewed negatively as unacceptable and poor performance.

To improve the start time for dynamic sites in response to cold requests, a module called Application Initialization, was included in IIS 8 in Windows Server 2012 that allowed the administrator to preload the application framework needed for a dynamic site so that the site could respond to a cold request in a few hundred milliseconds instead of several seconds. However, this module is not useful for hosters because such preloaded application

frameworks consume additional memory for each site configured to use them. Since the IIS servers of a hoster are typically hosting thousands of sites and are usually memory-bound (assume at least 100 MB needed per dynamic site), such preloading application frameworks for all sites hosted on a server just wasn't feasible. IIS can partly address this problem by killing idle worker processes after a default of 20 minutes of inactivity, and WAS can halve this time interval if it determines that memory pressure has reached 80 percent on the server.

IIS 8.5 in Windows Server 2012 R2 now takes a different perspective on how to address the problem of cold request delays for dynamic sites. A new feature called Idle Worker Process Page-out, saves memory by allowing an idle worker process to be paged to disk so that the worker process is removed from memory. The page-out feature can be made to perform even better by utilizing a solid state disk (SSD) for the paging file of an IIS server. The result is that memory pressure can now be greatly reduced for servers hosting thousands of dynamic sites and the response time to cold requests for these sites can be significantly improved.

Idle Worker Process Page-out is not enabled by default in IIS 8.5. Instead, worker processes simply terminate idle worker processes. You can enable Idle Worker Process Page-out by opening the Advanced Settings dialog for an application pool in IIS Manager and changing the value of the Idle Time-out Action setting from Terminate to Suspend, as shown in Figure 8-2. You can also enable Idle Worker Process Page-out at the server level, and although doing this won't affect the configuration of existing sites, any new sites that are created will inherit this setting.

FIGURE 8-2 You can enable Idle Worker Process Page-out through Advanced Settings.

Custom IIS logging fields

Another set of enhancements made in IIS 8.5 is in the area of logging. IIS logging can be used for monitoring and tracking IIS activity and for troubleshooting and debugging IIS when problems occur. One frequent request from customers who use IIS is for the ability to log more kinds of IIS activities.

To address such requests, IIS 8.5 now allows administrators to specify that additional custom fields be logged by IIS in addition to the standard W3C logging fields. This is illustrated by Figure 8-3, which shows the list of additional sources that can be logged for Request Header. Additional custom fields can also be added for Response Header and for Server Variables. In addition to the prepopulated fields for the variables and headers, the administrator can manually specify custom sources.

FIGURE 8-3 You can add custom fields for IIS logging.

A common scenario where this could come in handy is when the web server is front-ended by networking equipment such as a proxy or load balancer. In such a situation, the IIS logs can not accurately track client IP addresses because the IP captured by Http.sys is the

proxy or load balancer's IP. Network hardware that proxy HTTP requests usually have the ability to store the original client IP in the custom header X-FORWARDED-FOR, and so the administrator can record it as a custom Response Header and thus record the original IP of the clients.

Note that the custom logging is limited to a total of 64 KB, and if the administrator defines custom fields which exceed that, they will be truncated. This means that care must be taken when deciding which fields to collect. Note also that when enhanced logging is enabled, IIS creates log files with _x appended to their name to indicate that these files are enhanced logging fields.

IIS ETW logging

Another useful enhancement to logging in IIS 8.5 is the ability of the IIS logging mechanism to send data through Event Tracing for Windows (ETW). ETW is a tracing and logging mechanism that is part of the operating system, and many Windows components and applications take advantage of it to standardize their output for the purpose of debugging or troubleshooting. If an application or component uses ETW, administrators can use it to collect the info using a multitude of techniques and tools that are publicly available. This way, administrators, application developers, and support personnel can collect traces or logs in real time, and without complicated setup requirements or specific tools. This can be particularly useful for servers that are very busy, because as you'll see soon, the real-time data can be easily filtered.

Let's now hear from one of our Microsoft insiders about how to configure ETW logging in IIS 8.5.

Configuring IIS ETW Logging

To facilitate ETW logging, IIS has a new service—W3C Logging Service (w3logsvc), which was created to handle both the enhanced logging of custom fields we discussed earlier and ETW. As part of this new design, the logging service can send data to either ETW or the text-based log files, or both. Once the logging service sends the data to ETW, the administrator can hook into the same ETW provider and collect the data.

Enabling ETW logging

By default, IIS doesn't use ETW, so to enable it, follow these steps:

1. **Open the IIS management console.**
2. **Click the server you wish to manage.**
3. **Navigate down to the site that you want to configure.**

4. Open the Logging configuration item in the Feature View pane.
5. Configure IIS for either ETW Event Only or Both Log File And ETW Event.

Once you configure this and initiate traffic to the appropriate website, you should be able to see that the w3logsvc service has started.

The ETW provider for IIS's logging is named Microsoft-Windows-IIS-Logging, and any application that is designed to interact with ETW providers can retrieve the data. One specific application that was designed for system administrators is Message Analyzer. Message Analyzer was developed by Microsoft as a next-generation replacement for Network Monitor, and it provides similar functionality, with the addition of several functions, one of which is the ability to connect to ETW providers.

At the time of writing, Message Analyzer is available in Beta 3, and by the time this book is published, a final version should be available. Head over to *http://blogs.technet.com/b/messageanalyzer/* to find out the current release and for a download link.

Collecting ETW events

Once you have installed Message Analyzer on your IIS server, follow these steps to collect the ETW events from IIS:

1. Launch Message Analyzer.
2. Click the Capture / Trace button.
3. In the top-right corner, in the Search And Add Providers input box, type in Microsoft-windows-IIS-logging
4. Click start-with to start the capture.

Once the capture is running, it will show an event for every request received by IIS, and the event details will show the data collected by the logging service. For example, in the screenshot below you can see that the field C_ip contains the connecting client's IP address. This means that if you need to troubleshoot a specific client that's connecting to a busy server, you can simply filter the output to show only data from that specific IP or a group of IPs.

Message Analyzer is a very advanced tool, and it allows you to easily configure filters. It even includes an easy to use time-slider, which allows you to view only the requests that were received during a particular time frame. To learn more about Message Analyzer and how to take advantage of its plethora of features, take a look at the Message Analyzer Operating Guide: *http://technet.microsoft.com/en-us/library/jj649776.aspx*.

Another tool that can connect to an ETW provider is Performance Monitor, which is included with Windows Server. Additional tools and techniques are discussed here: *http://blogs.msdn.com/b/oanapl/archive/2009/08/05/etw-event-tracing-for-windows-what-it-is-and-useful-tools.aspx*. In fact, you can even write your own tool to connect to ETW providers, although this is beyond the scope of this book.

Erez Benari
Program Manager for IIS from the Windows Azure team at Microsoft

Learn more

You can learn more about the new features and enhancements in IIS 8.5 by checking out the following resources on IIS.NET:

- "Dynamic Website Activation in IIS 8.5" at *http://www.iis.net/learn/get-started/whats-new-in-iis-85/dynamic-site-activation-in-iis85*.

- "Idle Worker Process Page-Out in IIS 8.5" at *http://www.iis.net/learn/get-started/whats-new-in-iis-85/idle-worker-process-page-out-in-iis85*.
- "Enhanced Logging for IIS 8.5" at *http://www.iis.net/learn/get-started/whats-new-in-iis-85/enhanced-logging-for-iis85*.
- "Logging to Event Tracing for Windows in IIS 8.5" at *http://www.iis.net/learn/get-started/whats-new-in-iis-85/logging-to-etw-in-iis-85*.
- "Fine-tuning Dynamic Worker-Process Page-out on IIS 8.5" at *https://blogs.iis.net/erez/archive/2013/08/28/fine-tuning-dynamic-worker-process-page-out-on-iis-8-5.aspx*.

Be sure also to check out the following video from TechEd 2013 on Channel 9:

- "Internet Information Services: What's New in Window Server 2012 R2" *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B303*.

CHAPTER 9

Remote Desktop Services

Way back in the mainframe age of computers, dumb terminals ruled the roost. Users keyed their data into a "green screen" terminal and it was sent over the wire to the mainframe. Once the user's commands had been processed, the results were then transmitted back over the wire to the terminal, where they were displayed in bright green on black background. This client/server architecture of dumb terminals and terminal servers can still be seen in operation when you watch classic movies like *Billion Dollar Brain* by Michael Caine.

Terminal servers have come a long way since then. Microsoft first introduced its own version of this architecture way back in 1996 with Windows NT 4.0 Terminal Server edition, and it provided users with session-based desktops they could access remotely as if they were logged on interactively. Then, as successive versions of Windows Server were released, Terminal Services was enhanced in many ways and rebranded as Remote Desktop Services (RDS). Today, RDS is a staple for organizations that want to deploy a wide range of remote work solutions including virtual desktops, RemoteApp programs, and session-based desktops. In fact, RDS can even enable users to securely run business applications over the Internet as if they were sitting at a computer on the company LAN.

Previous RDS enhancements

A big change introduced in Windows Server 2012 was how RDS could be easily deployed in different kinds of scenarios. When you added the RDS role in Windows Server 2012, you first had a choice of choosing two deployment options:

- **Standard** This option provides you with more flexibility concerning how you deploy different RDS role services to different servers and is intended for production environments.
- **Quick Start** This option deploys all the RDS role services required on a single computer using mostly the default options and is intended mainly for test environments.

Once you've selected the appropriate deployment option for your environment, you're next choice is which type of RDS scenario you want to implement:

- **Virtual machine-based desktop deployment** Lets remote users connect to virtual desktops running on a Remote Desktop Virtualization Host to access applications installed on these virtual desktops (and also RemoteApp programs if session virtualization is also deployed).
- **Session-based desktop deployment** Lets remote users connect to sessions running on a Remote Desktop Session Host to access session-based desktop and RemoteApp programs.

That's not all, though, because there were a number of other significant enhancements to RDS in Windows Server 2012, such as:

- **RemoteFX enhancements** RemoteFX was first introduced in Windows Server 2008 R2 as a way of delivering a full Windows experience using Remote Desktop Protocol (RDP) across a wide variety of client devices. RemoteFX uses host-side rendering to enable graphics to be rendered on the host instead of the client by utilizing the capabilities of a RemoteFX-capable graphics processing unit (GPU) on the host. RemoteFX vGPU uses GPU virtualization to expose a virtual graphics device to a virtual machine running on a RemoteFX-capable host so that multiple virtual desktops could share the single GPU on the host. RemoteFX functionality was enhanced for RDS in Windows Server in a lot of ways with support included for multitouch gestures and manipulations in remote sessions; improved multimonitor support; dynamic adaptation to changing network conditions by using multiple codecs to optimize how content is delivered; optimization of performance when sending traffic over a wide area network (WAN) by choosing between TCP or UDP (called RemoteFX for WAN); integration throughout the RDS role services instead of being installed as its own separate role service; and more.
- **Enhanced USB Redirect** USB redirection from within RDS was first introduced in Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1 to support VDI scenarios. USB Redirect occurs at the port protocol level and enables redirection of a wide variety of different types of universal serial bus (USB) devices, including printers, scanners, webcams, Voice over Internet Protocol (VoIP) headsets, and biometric devices. RDS in Windows Server 2012 enhanced this capability with support for USB Redirect for Remote Desktop Session Host (RD Session Host) to enable new kinds of scenarios for businesses that implement session virtualization solutions. In addition, USB Redirect for Remote Desktop Virtualization Host (RD Virtualization Host) no longer requires installing the RemoteFX 3D Video Adapter on the virtual machine in order to work.
- **User Profile Disks** Before Windows Server 2012, preserving user state information for sessions and virtual desktops required using Windows roaming technologies like roaming user profiles (RUP) and Folder Redirection (FR). But implementing RUP and FR added more complexity to deployments. RDS in Windows Server 2012 simplifies session-based and VDI deployments with the introduction of User Profile Disks, which store user data and settings for sessions and virtual desktops in a separate VHD file that can be stored on a network share.

RDS in Windows Server 2012 R2 isn't a radical change from what it was in Windows Server 2012, but it does have some exciting new features and enhancements that can make managing remote sessions easier, provide a richer user experience, and allow you to get the best possible value from VDI.

Improved RemoteApp experience

In previous versions of RDS, when you opened a RemoteApp program and dragged it around on the desktop, only an outline of the program's window was displayed. And if you hovered the mouse pointer over the taskbar icon of a RemoteApp program, no thumbnail preview was displayed—only the generic icon associated with the program.

In Windows Server 2012 R2, however, the RemoteFX graphics capability has been enhanced in several ways. For example, dragging around a RemoteApp program now drags the entire contents of the program's window. And as Figure 9-1 shows, hovering over the taskbar icon of the RemoteApp program displays a live thumbnail preview of the program.

FIGURE 9-1 Hovering over the taskbar icon of a RemoteApp program now displays a live thumbnail preview of the program.

As Figure 9-2 shows, these advanced graphics capabilities of RemoteFX in Windows Server 2012 R2 can be configured using Group Policy. RemoteFX advanced graphics functionality is enabled by default, but you can use this policy setting or disable it if some of your published applications don't support them.

FIGURE 9-2 Advanced graphics for RDS can be controlled using Group Policy.

DX11.1 support

RemoteFX virtual graphics processing unit (vGPU) in Windows Server 2012 R2 also now supports DX11.1 enhanced graphics display capabilities. This means that graphics intensive applications relying on DX11.1 features can now be run in virtualized environments. The requirements for doing this are as follows:

- The system must have DX11.1 capable graphics processing unit (GPU) card.
- The host must be running on Windows 8.1 or Windows Server 2012 R2.
- The virtual machines must be Generation 1 not Generation 2.

In addition, RemoteFX running on Non-Uniform Memory Access (NUMA) based systems will also experience improved scaling capabilities.

Improved video experience

Delivering a quality video experience over RDP has traditionally been a challenge because of the large amount of bandwidth utilized. This is especially true when RDS is being used to stream video content over a WAN connection.

One way of boosting performance in such situations is to compress the video content before streaming it to remote clients. RDS in Windows Server 2012 R2 now has improved codecs that can deliver significantly better video performance especially in WAN scenarios. You can now achieve bandwidth savings of up to 50 percent compared with using RDS in the previous version Windows Server 2012.

Seamless display handling

Improvements made in both Windows 8.1 and Windows Server 2012 R2 now allow RDS to handle a wide variety of display-handling operations. These include:

- Adding or removing monitors
- Adding or removing projectors
- Adding or removing docking stations
- Rotating devices or monitors

RDS can handle these operations for both remote sessions and RemoteApp programs. For example, on tablet devices a remote desktop session will now automatically rotate as you rotate the device.

RDS also allows you to change the display resolution in a remote desktop session and have the session window resize itself properly so you won't have to use the scroll bars to get to the taskbar and charms. This also works in multimonitor scenarios.

The result of all these enhancements is to bring RDS user experience even closer to being on par with that of local devices.

Quick Reconnect

Another new feature of RDS in Windows Server 2012 R2 is called Quick Reconnect. In previous versions of Windows Server, reconnecting to a remote desktop session over a slow or unreliable network connection could sometimes take up to a minute. With RDS in Windows Server 2012 R2, however, reconnecting to disconnected sessions will typically take no more than five seconds even over slow connections. The user will also no longer be stuck seeing that uninformative grey screen when the remote desktop client is trying to reconnect to a previously disconnected session, and instead, will see a more informative message.

Session Shadowing

A frequent request from Microsoft customers who use RDS is to add the ability for administrators to shadow the sessions of remote users. The good news is that this kind of shadowing capability is now an in-box feature of RDS in Windows Server 2012 R2.

To see how Session Shadowing works, Figure 9-3 shows the connections in Server Manager to a Remote Desktop Session Host running Windows Server 2012 R2. In previous versions of RDS, if you right-clicked a remote session, you only got three options: Disconnect, Send Message, and Log Off. But in RDS in Windows Server 2012 R2 there is now a fourth context menu option called Shadow, which enables administrators to shadow the session of a connected remote user.

FIGURE 9-3 The new Shadow option provides administrators with the ability to shadow a remote session.

Selecting the Shadow option opens the Shadow dialog shown in Figure 9-4. This dialog offers administrators two options for shadowing the remote session:

- **View** This option allows the administrator only to view what the user is doing in his session.
- **Control** This option allows the administrator to view the user's session and also take control of the session and perform actions on the user's desktop.

FIGURE 9-4 You can view or control remote sessions.

By default, the Prompt For User Consent check box is selected in the Shadow dialog. This means that when the administrator clicks OK to close the dialog, the user's screen dims and a message bar is displayed across his or her screen, as shown in Figure 9-5.

FIGURE 9-5 The user must accept the prompt to allow shadowing of his session.

Let's pause for a few notes at this point:

- By default, Group Policy is configured to require user consent to shadow requests. In many organizations, this might be the correct approach to ensure the privacy of employees. Be sure to consult your legal and human resources departments before changing this policy setting.
- To shadow a remote user, the user doesn't need to be connected to a full remote desktop session. Administrators can even shadow individual RemoteApp programs as remote users work with them.
- Shadowing functionality is also built into the Remote Desktop Client client (Mstsc.exe). By including the /shadow parameter and specifying the remote session when you use mstsc to launch the Remote Desktop Client from the command line, an administrator can use the client to view or control the remote user's session.

To continue now with our walkthrough of shadowing, if the user clicks No in the message bar on her screen, the administrator will not be able to shadow the user's session. If she clicks Yes, the message bar disappears and the user's screen is no longer dimmed, and she can continue with her work as usual. Meanwhile, a new window appears on the RDS administrator's desktop showing the appearance of the shadowed user's desktop in real time, as shown in Figure 9-6.

FIGURE 9-6 What shadowing a user's session might look like.

Once the administrator is finished shadowing the session, he can simply close the shadow window.

VDI and data deduplication

Windows Server 2012 previously introduced a feature called data deduplication that allowed more data to be stored in less physical disk space. Data deduplication is highly scalable and is designed to safeguard the reliability and integrity of your data.

New in RDS in Windows Server 2012 R2 is the ability to use data deduplication with actively running personal desktop collections in virtual desktop interface (VDI) environments. To implement this feature, the desktop virtual hard disks (VHDs) must be stored on a file server running Windows Server 2012 R2 and accessed by using Server Message Block (SMB) version 3.0. The benefit provided by this new capability is that you are able to dramatically reduce the storage requirements for personal VDI scenarios.

Restricted Admin mode

Restricted Admin mode is a new optional mode you can use when launching the Remote Desktop Connection client (mstsc.exe) from the command line. When you specify the Restricted Admin switch with mstsc.exe in order to connect to a remote desktop host running Windows Server 2012 R2, your credentials are not sent to the host. If the RDS server verifies that your user account has administrator rights and supports Restricted Admin mode, the connection attempt succeeds. Otherwise, the connection attempt fails.

Restricted Admin mode does not send your credentials to the RDS server as plaintext or any other reusable forms. It works only if the client and server are running either Windows Server 2012 R2 or Windows 8.1.

Learn more

You can learn more about the new Remote Desktop Services features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Remote Desktop Services in Windows Server 2012 R2" at *http://technet.microsoft.com/en-us/library/dn283323.aspx*.

The following Microsoft TechNet and MSDN blog posts also have lots of information about the new Remote Desktop Services features and enhancements in Windows Server 2012 R2:

- "What's New in Remote Desktop Services for Windows Server 2012 R2" at *http://blogs.msdn.com/b/rds/archive/2013/07/09/what-s-new-in-remote-desktop-services-for-windows-server-2012-r2.aspx*.
- "Lowering the Cost of Storage for VDI Using Windows Server 2012 R2 with Data Deduplication" at *http://blogs.msdn.com/b/rds/archive/2013/08/07/lowering-the-cost-of-storage-for-vdi-using-windows-server-2012-r2-with-data-deduplication.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "What's New in Windows Server 2012 Virtual Desktop Infrastructure and Remote Desktop Services?" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B350#fbid=_9VugRgK7SS*.
- "Designing a Virtual Desktop Infrastructure Architecture for Scale and Performance on Windows Server 2012" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B314#fbid=Wp7AXxNqBsG*.
- "VDI Smackdown 2013 Edition" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B345#fbid=80k1afViSd5*.
- "Optimizing Windows 8 for Virtual Desktop Infrastructure" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B330#fbid=Wp7AXxNqBsG*.
- "Windows Server 2012 Desktop Virtualization (VDI) on Dell Active Infrastructure" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B393#fbid=Wp7AXxNqBsG*.

CHAPTER 10

Windows PowerShell

Windows PowerShell has become the de facto platform for automating the administration of Windows-based environments. Built on top of the common language runtime (CLR) and the Microsoft .NET Framework, Windows PowerShell has brought a whole new paradigm for configuring and managing Windows servers in enterprise environments. Windows Server 2012 R2 introduces the latest iteration of the platform, Windows PowerShell 4.0, and it has some exciting new capabilities we'll look at. But first let's begin by briefly reviewing what was introduced in Windows PowerShell 3.0 in Windows Server 2012.

Previous enhancements in Windows PowerShell 3.0

Windows PowerShell 3.0 in Windows Server 2012 previously introduced numerous new capabilities that helped bring added flexibility and power for managing cloud and multiserver environments to the platform. Some of the key enhancements that were added to Windows PowerShell 3.0 included the following:

- **New architecture** Windows PowerShell 3.0 was built upon the Windows Management Framework 3.0, which introduced a new Windows Management Instrumentation (WMI) provider model that reduces dependency on COM, a new application programming interface (API) for performing standard Common Information Model (CIM) operations, and the capability of writing new Windows PowerShell cmdlets in native code. Windows Management Framework 3.0 also introduced improvements that made WinRM connections more robust to support long-running tasks and be more resilient against transient network failure.
- **Disconnected sessions** Windows PowerShell 3.0 introduced persistent user-managed sessions (PSSessions) that are not dependent upon the session in which they were created. By using the New-PSSession cmdlet, you can create and save a session on a remote server and then disconnect from the session. The Windows PowerShell commands in the session on the remote server will then continue to execute, even though you are no longer connected to the session. If desired, you can reconnect later to the session from the same or a different computer.

- **Windows PowerShell Workflow** Windows PowerShell Workflow lets you create workflows using Windows PowerShell or the Extensible Application Markup Language (XAML) and run the workflows as if they were Windows PowerShell cmdlets. This enables Windows PowerShell to use the capabilities of the Windows Workflow Foundation to create long-running management activities that can be interrupted, suspended, restarted, repeated, and executed in parallel. Windows PowerShell workflows are especially valuable in cloud computing environments because they help you automate administrative operations by building in repeatability and by increasing robustness and reliability. They also help increase your servers-to-administrators ratio by enabling a single administrator to execute a workflow that runs simultaneously on hundreds of servers.
- **Scheduled jobs** Windows PowerShell 2.0 previously had the concept of background jobs, which can be scheduled to run asynchronously in the background. Windows PowerShell 3.0 introduced cmdlets such as Start-Job and Get-Job that can be used to manage these jobs. You can also easily schedule jobs using the Windows Task Scheduler. This means that you, as the administrator, can now have full control over when Windows PowerShell scripts execute in your environment.
- **Windows PowerShell Web Access** Windows PowerShell Web Access lets you manage the servers in your private cloud from anywhere, at any time, by running Windows PowerShell commands within a web-based console. Windows PowerShell Web Access acts as a gateway to provide a web-based Windows PowerShell console that you can use to manage remote computers. This lets you run Windows PowerShell scripts and commands even on computers that don't have Windows PowerShell installed. All your computer needs is an Internet connection and a web browser that supports JavaScript and accepts cookies.
- **Show-Command** Windows PowerShell 3.0 includes a new cmdlet called Show-Command that displays a GUI for a command with a simpler overview of any Windows PowerShell cmdlet. This capability can make it much easier to understand the syntax of a cmdlet, as opposed to using the Get-Help cmdlet.
- **More cmdlets** Windows Server 2012 introduced hundreds of new Windows PowerShell cmdlets that help you manage almost every aspect of your private cloud environment. Note that some of these cmdlets are available only when a particular server role or feature is installed on the system.

Now let's examine some of the key enhancements that Windows Server 2012 R2 brings with version 4.0 of Windows PowerShell.

Windows PowerShell Desired State Configuration

Probably the most exciting improvement in version 4.0 of Windows PowerShell is Windows PowerShell Desired State Configuration (DSC), a powerful new management paradigm you can use to deploy and manage the configuration data for software services and also the

environment in which these services will be running. The best way we can learn about this new feature is by sitting back and listening to one of our Microsoft insiders explain it and demonstrate how it works.

Managing the data center using Desired State Configuration

IT professionals worldwide are advancing to the cloud with a goal of delivering IT as a service much like that of a utility company. The intent is that delivered services are uniform and easy to use and work with the flip of a switch. In the world of Infrastructure as a Service (IaaS), the challenge is not always how to get there. It is how to stay there.

Today, the world embraces cloud services. The tools and technologies allow us to deploy to private, service provider, and public clouds. But once the systems are deployed there, how do we ensure that they function as expected? How do we ensure that someone does not inadvertently modify a critical setting that renders the service unusable or impaired?

In the past, one solution was to implement an IT Service Management framework to provide process management. For example, in the healthcare industry, a system would be put into production only after it was "validated." The validation process stated that the system would perform an action in repeatable fashion given the same input. The result should never have a deviation. Computer systems would be rigorously documented and tested to ensure they met the appropriate compliance measurements. Once deployed, the systems would be periodically tested by using a series of test protocols. If a system failed, IT professionals were left to evaluating change control documentation and traditional troubleshooting methods to identify what changed.

Some IT organizations began to leverage early automation capabilities (in the form of various scripting languages) to provide a post-execution check after a system was installed. If the organization was fortunate enough to have Microsoft System Center Configuration Manager, they could leverage Desired Configuration Manager (DCM). Similar to the early automation scripts, early versions of DCM could only report on the configuration of a system. The output of the report would tell you that a configuration item (CI) did not match the source template. Although this was greatly beneficial, it did not resolve issues when the configuration did drift from the source template.

In today's data center, this means that you may have gotten to the cloud, but with configuration drift, you may not be able to stay there. To address this, Microsoft updated the Desired Configuration Manager feature of System Center Configuration Manager to become Compliance Settings.

Compliance settings can now apply remediation to configuration drift. See "SCCM 2012 Settings Management – the M in DCM Truly Becomes Management" at *http://technet.microsoft.com/en-us/video/sccm-2012-settings-management-the-m-in-dcm-truly-becomes-management.aspx* and "Compliance Settings in Configuration Manager" at *http://technet.microsoft.com/library/gg681958.aspx*.

This is great, but what if you do not have Configuration Manager in your environment? There are many scenarios where you have the need for monitoring and remediation but Configuration Manager 2012 is not an available option.

Fortunately a solution exists! Windows PowerShell 4.0 now includes Desired State Configuration (DSC). DSC is a new management platform that consists of a suite of language extensions and providers in the form of Windows PowerShell cmdlets along with a host service that is capable of providing the ability to retrieve a configuration, test a configuration, and apply a configuration to a single or set of systems.

Web server example

For this example, you manage a commerce application where the front-end web servers reside in a DMZ or provider cloud. The consistent configuration state of the front-end web servers is key to having a healthy system. Let's face it; the transactions executed on the servers directly impact your company revenue. The health and functionality of the servers have a lot of impact on your company brand. To monitor and maintain the state of the servers, you implement DSC. As the following diagram shows, DSC has four main pieces:

1. **Configuration Instance Document** The Windows PowerShell script that generates the definition of the desired state.
2. **MOF file** The Managed Object Format (MOF) file that contains the compiled definition of the desired state.
3. **Local Configuration Manager** The DSC engine on the client system that executes against the MOF to retrieve the current configuration, compare the current configuration to the MOF, and/or apply the settings defined in the MOF.
4. **Desired State Configuration Pull Server (optional)** The repository for the definition of the desired state. If clients are configured to execute a PULL instead of receiving a PUSH, the DSC Pull Server hosts the configuration and client data required to remediate.

To begin, you need to ensure Windows PowerShell Remoting is enabled on all involved systems (Enable-PSRemoting). I highly recommend leveraging group policy to put this in place. Group policy has been helping IT professionals enforce policy for more than a decade. It is a perfect complement to your DSC implementation.

> ***NOTE*** In addition to requiring PSRemoting, DSC applies only to x64 bit system with Windows PowerShell 4.0.

Next, generate the Configuration Instance Document. This Windows PowerShell script contains the definition and execution order of what should exist on the target machine. In this example, your front-end web server requires IIS installed, a set of files (content), an application installed (setup file such as an MSI) as well as specific registry keys. The Configuration Instance Document is a script that contains a configuration block of code. That configuration block contains:

- **Node(s)** A specific target system; defined as "localhost"; or any targeted node system (defined in a hash table).
- **Resource(s)** The actual configuration items that you are looking for as well as their dependencies. For example, the application that must be present has a prerequisite of IIS. Two resources would be specified: a resource name that contains Web-Server and the resource name that contains the application MSI. The application resource would have a dependency set for the resource that defines Web-Server (see *http://technet.microsoft.com/en-us/library/dn249921.aspx*).

DSC is extremely extensible and modular. Your script can be very simple or be scaled out. In Windows PowerShell, you create functions and modules for tasks that you call frequently or leverage from multiple scripts. In DSC you can separate configuration data and your logic as well to make it more modular.

You can control the actions of the Local Configuration Manager. Windows PowerShell DSC cmdlets Get-DscLocalConfigurationManager and Set-DscLocalConfigurationManager are used to call the Local Configuration Manager engine. Using the Windows PowerShell DesiredStateConfigurationSettings keyword in a script, you can generate a separate MOF file that contains an instruction set for the Local Configuration Manager engine. The MOF-generating script can change the functionality of the engine from receiving configuration information via a PUSH to executing a PULL from a DSC server. You can change frequency so that it refreshes its configuration data:

Once the script is built, review it to ensure you have the external dependencies set up:

```
   Configuration CommerceConfig
{
   # A Configuration block can have zero or more Node blocks
   Node "FE-WEB-01"
   {
      # Next, specify one or more resource blocks

      # WindowsFeature is one of the built-in resources you can use in a
Node block
      # This example ensures the Web Server (IIS) role is installed
      WindowsFeature CommerceSite
      {
          Ensure = "Present" # To uninstall the role, set Ensure to
"Absent"
          Name = "Web-Server"
      }
```

```
      # File is a built-in resource you can use to manage files and
directories
      # This example ensures files from the source directory are present
in the destination directory
      File CommerceSite
      {
         Ensure = "Present"  # You can also set Ensure to "Absent"
         Type = "Directory" # Default is "File"
         Recurse = $true
         SourcePath = $WebsiteFilePath # This is a path that has web
files
         DestinationPath = "C:\inetpub\wwwroot" # The path where we want
to ensure the web files are present
         Requires = "[WindowsFeature]CommerceSite"  # This ensures that
MyRoleExample completes successfully before this block runs
      }
   }
}

$WebsiteFilePath = "\\2012R2PREVIEW\CommerceSiteSource\SiteData"
CommerceConfig
```

Does your web server require file content? If so, did you set up a share for that content to be pulled from? Your DSC Pull Server might make a good repository for these items. In the example above, the share is \\2012R2PREVIEW\CommerceSiteSource; however, the data is located in \SiteData. The path specified for files cannot be the root of a share, but must be a folder underneath that share.

Execute the Configuration Instance Document (your Windows PowerShell script) to generate the MOF file containing the configuration instructions:

```
FEWebServer-DSC.ps1

Configuration CommerceConfig
{
   # A Configuration block can have zero or more Node blocks
   Node "FE-WEB-01"
   {
      # Next, specify one or more resource blocks

      # WindowsFeature is one of the built-in resources you can use in a Node block
      # This example ensures the Web Server (IIS) role is installed
      WindowsFeature CommerceSite
      {
          Ensure = "Present" # To uninstall the role, set Ensure to "Absent"
```

```
PS C:\scripts> .\FEWebServer-DSC.ps1


    Directory: C:\scripts\CommerceConfig


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         8/31/2013  11:10 AM       1770 FE-WEB-01.mof


PS C:\scripts> |
```

Now comes the really cool part—deploying the DSC job to the client system. The –Path switch points to the directory where the MOF file exists (on the system where the script is being executed from):

```
Administrator: Windows PowerShell
PS C:\scripts> Start-DscConfiguration -ComputerName FE-WEB-01 -Path C:\Scripts\CommerceConfig

Id  Name   PSJobTypeName   State    HasMoreData  Location   Command
--  ----   -------------   -----    -----------  --------   -------
18  Job18  Configuratio... Running  True         FE-WEB-01  Start-DscConfiguration...


PS C:\scripts>
```

If you include the –Wait and –Verbose switches, you can see the progress of the job (and any errors if they occur):

```
DSCEngine
   Applying Configuration
   [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                ]
   00:00:02 remaining.

   Set
```

Check the Operational and Debug event logs for DSC. You can find these logs in Event Viewer under Applications And Services Logs | Microsoft | Windows | Desired State Configuration or Applications And Services Logs | Microsoft | Windows | DSC.

You can then test the applied configuration. The test compares the desired state configuration to the target system and returns a "True" or "False" result:

```
Select Administrator: Windows PowerShell
PS C:\scripts> $TargetServer = New-CimSession -ComputerName FE-WEB-01
PS C:\scripts> Test-DscConfiguration -CimSession $TargetServer
True
PS C:\scripts>
```

As a verification test, delete a few files from the web server content directory C:\inetpub\wwwroot and perform the test. Note that the returned result is "False." Execute the same DscConfiguration job run previously. Complete the test and now you can see the returned result is again "True" because the issues were remediated:

```
Administrator: Windows PowerShell
PS C:\scripts> Test-DscConfiguration -CimSession $TargetServer
False
PS C:\scripts> Start-DscConfiguration -ComputerName FE-WEB-01 -Path C:\Scripts\CommerceConfig

Id  Name   PSJobTypeName   State    HasMoreData  Location   Command
--  ----   -------------   -----    -----------  --------   -------
57  Job57  Configuratio... Running  True         FE-WEB-01  Start-DscConfiguration...


PS C:\scripts> Test-DscConfiguration -CimSession $TargetServer
True
PS C:\scripts>
```

Your environment and requirements define how far you extend DSC. For example, if you have Microsoft System Center Orchestrator or an existing automation tool within your environment, you may choose to leverage that to manage checking state and performing remediation if necessary.

If that is not an available option, you may choose to switch the client from receiving a PUSH to now autoremediating via a PULL to extract its MOF file from a Desired State Configuration Pull Server. This is a web service utilizing the ODATA IIS extension. The DSC Pull Server can be set up on Windows Server 2008 R2, 2012, or 2012 R2. For Windows Server 2008 R2 and 2012, you can install the role through a set of Windows PowerShell commands that essentially install all of the necessary components. In Windows Server 2012 R2, the DSC Pull Server is a feature:

Advancements in Windows PowerShell continue to transform the data center landscape. Features like DSC demonstrate how the push toward IaaS is not only achievable, but is here to stay.

Jeff Butte
Senior Consultant, US Public Sector

Save-Help

One small but potentially very useful improvement in Windows PowerShell 4.0 is a new cmdlet that allows you to save help for Windows PowerShell modules installed on remote computers. Once again, let's hear from an expert inside Microsoft about how this works and why it can be useful.

Save-Help for the disconnected Windows PowerShell world

We live in an increasingly connected world. You can now get almost everything online. However, what if you are not online . . . ever? While the world continues to weave more connectivity, there are networks that will never connect to the Internet. Organizations have determined that for reasons of risk and/or security, physical separation from the Internet is a key requirement.

Cyber-crime has risen to a level that our countries are developing national strategies to combat it. Companies operate isolated networks to protect their most critical or valuable resources from data exfiltration by Advanced Persistent Threats. Governments operate isolated networks for the purpose of protecting their nation's secrets. Manufacturing or transportation systems may be isolated to ensure that neither intentional nor accidental connectivity risks human life or the financial well-being of a company. Then again, the reason for isolation may be as simple as protecting production networks from development networks.

Regardless of the reason, disconnected networks exist and they continue down the path toward a private cloud. Organizations are realizing the benefits gained from simple data center automation to advanced IaaS. They are extending those gains through their environments, including their disconnected ones.

If you are one of the lucky ones performing data center automation in a high-security, disconnected network, you have undoubtedly experienced the scenario where you need a Windows PowerShell example to help you along and there are none to be found—because you have no help files.

Save-Help was introduced in Windows PowerShell 3.0. It downloads and saves the newest help files to a directory or path you specify. These help files can be copied to the isolated network and then be imported (Update-Help) to Windows PowerShell on the isolated systems.

This was a fantastic way to keep the help files current, but it does have limitations. Fortunately, the Windows Management Framework 4 with Windows PowerShell 4.0 solves several of those.

Previously, Save-Help worked only for modules that were installed locally. To obtain the help files you required, a common method involved building a reference

machine where you loaded all of the software stacks on the machine so that you could export out all of the Windows PowerShell module's help files. This was time consuming, wasted resources, and was frequently fraught with errors.

With Windows PowerShell 4.0, you can now avoid all of that extra work effort. From a single machine, you can remotely connect to other systems that have those modules you are looking for loaded and download the help. There are three remote connectivity options: Invoke-Command, New-PSSession, and the new CimSession.

The method utilizing Invoke-Command is very effective. Before you save the help files, you can utilize Invoke-Command to Update-Help, ensuring that you have the most current version.

In the example that follows, the Windows PowerShell is executed from a workstation. The commands are invoked against the remote server CM2012SP1PRI. The files are then saved to a directory on the workstation. Here are the commands:

```
Invoke-Command -ComputerName CM2012SP1PRI -ScriptBlock { Update-Help
-Module ActiveDirectory -Force }
$varModule = Invoke-Command -ComputerName CM2012SP1PRI -ScriptBlock {
Get-Module -Name ActiveDirectory -ListAvailable }
Save-Help -Module $varModule -DestinationPath C:\SavedHelp
```

And here are the commands being executed:

The saved help files are then located in the specified directory:

The files can then be copied to the disconnected network using removable media.

Windows PowerShell 4.0 also supports a "pull" method. The method requires you to start on the isolated network. Connect to a system that has the module that requires a help file update. Using Export-CliXml, you can deserialize the PSModuleInfo object of that module to disk. That object can be transported on removable media to an Internet-connected system. Save-Help can be run on the Internet-connected system against the deserialized PSModuleInfo to download the most current help. The help files can then be transported back to the isolated network. This method, however, is not recommended for use on high-security networks where there is concern of data exfiltration on removable media.

If you are a serious Windows PowerShell user who authors your own module, you can also author updatable help. For more information, see "Updatable Help Authoring: Step-by-Step" at *http://msdn.microsoft.com/en-us/library/windows/desktop/hh852735(v=vs.85).aspx*.

Jeff Butte
Senior Consultant, US Public Sector

Yet more new cmdlets

As you might expect, Windows PowerShell 4.0 introduces yet more new cmdlets you can use for configuring and managing various aspects of client and server, especially those running Windows Server 2012 R2 and Windows 8.1. The sections that follow include descriptions of some of the new cmdlets you might find useful for your environment along with some usage examples.

DISM cmdlets

Deployment Image Servicing and Management (DISM) is a command-line platform you can use to mount and service Windows images for purposes of deployment. Windows Server 2012 introduced a DISM PowerShell module that contained 22 different cmdlets. Windows Server 2012 R2 expands the DISM module with more cmdlets including the following ones for managing various aspects of Windows image (.wim) files.

Add-WindowsImage

The Add-WindowsImage cmdlet adds an additional image to an existing image (.wim) file. Add-WindowsImage compares new files to the resources in the existing .wim file, specified by the Name parameter and the ImagePath parameter, and stores only a single copy of each

unique file so that each file is only captured once. The .wim file can have only one assigned compression type. Therefore, you can only append files with the same compression type.

The Add-WindowsImage cmdlet does not apply to virtual hard disk (VHD) files.

> ***IMPORTANT*** **It's important to note that you'll need to ensure you have enough disk space before you run Add-WindowsImage. If you run out of disk space while the image is being appended, you might corrupt the .wim file.**

Here is an example:

```
PS C:\>Add-WindowsImage -ImagePath c:\imagestore\custom.wim -CapturePath d:\ -Name
"Drive D"
```

This command adds files from d:\"Drive D" to the existing image at c:\imagestore\custom.wim.

Expand-WindowsImage

The Expand-WindowsImage cmdlet applies an image to a specified location. This cmdlet does not apply to VHD files.

Here is an example:

```
PS C:\>Expand-WindowsImage -ImagePath c:\imagestore\custom.wim -ApplyPath d:\ -Index 1
```

This command adds files from d:\"Drive D" to the existing image at c:\imagestore\custom.wim.

Export-WindowsImage

The Export-WindowsImage cmdlet exports a copy of the specified image to another image file. The source and destination files must use the same compression type.

You can also optimize an image by exporting to a new image file with Export-WindowsImage. When you modify an image, DISM stores additional resource files that increase the overall size of the image. Exporting the image will remove unnecessary resource files.

This cmdlet does not apply to VHD files.

Here is an example:

```
PS C:\>Export-WindowsImage -SourceImagePath C:\imagestore\custom.wim -SourceIndex 1
-DestinationImagePath c:\imagestore\export.wim -DestinationName "Exported Image"
```

This command exports the image at Index 1 of the file C:\imagestore\custom.wim to the file c:\imagestore\export.wim with the name Exported Image.

Get-WindowsImageContent

The Get-WindowsImageContent cmdlet displays a list of the files and folders in a specified image. This cmdlet does not apply to VHD files.

Here is an example:

```
PS C:\>Get-WindowsImageContent -ImagePath c:\imagestore\install.wim -Index 1
```

This command lists the files and folders in the first image in c:\imagestore\install.wim.

New-WindowsImage

The New-WindowsImage cmdlet captures an image of a drive to a new WIM file. Captured directories include all subfolders and data. You cannot capture an empty directory. A directory must contain at least one file. This cmdlet does not apply to VHD files.

Here is an example:

```
PS C:\>New-WindowsImage -ImagePath c:\imagestore\custom.wim -CapturePath d:\ -Name
"Drive D"
```

This command captures the Drive D image in the WIM file located on d:\ and saves to the file c:\imagestore\custom.wim.

Remove-WindowsImage

The Remove-WindowsImage cmdlet deletes the specified volume image from a WIM file that has multiple volume images. This cmdlet deletes only the metadata entries and XML entries. It does not delete the stream data and does not optimize the WIM file. This command-line option does not apply to VHD files.

Here is an example:

```
PS C:\>Remove-WindowsImage -ImagePath c:\imagestore\custom.wim -Index 1 -CheckIntegrity
```

This command removes the first image in c:\imagestore\custom.wim.

Split-WindowsImage

This option creates the .swm files in the specified directory, naming each file the same as the specified path_to_swm, but with an appended number. For example, if you set path_to_swm as c:\Data.swm, this option creates a Data.swm file, a Data2.swm file, a Data3.swm file, and so on, defining each portion of the split .wim file and saving it to the C:\ directory.

If a single file is larger than the value specified in the -FileSize parameter, one of the split .swm files that results will be larger than the value specified in the -FileSize parameter, in order to accommodate the large file.

This cmdlet does not apply to VHD files.

Here is an example:

```
PS C:\>Split-WindowsImage -ImagePath c:\imagestore\install.wim -SplitImagePath c:\
imagestore\splitfiles\split.swm -FileSize 1024 -CheckIntegrity
```

This command uses the image from c:\imagestore\install.wim to create a split.swm file, a split2.swm file, a split3.swm file, and so on, defining each portion of the split .wim file with a maximum size of 1024 MB and saving it to the C:\imagestore\splitfiles\ directory.

DHCP server cmdlets

Windows Server 2012 introduced the ability to configure and manage your Dynamic Host Configuration Protocol (DHCP) servers using Windows PowerShell. This capability has been enhanced in several ways in Windows Server 2012 R2.

Multicast support

New cmdlets have been added that allow you to configure and manage multicast scopes, exclusions, leases, and statistics for DHCP servers running Windows Server 2012 R2. The new cmdlets for this functionality include:

- Add-DhcpServerv4MulticastExclusionRange
- Add-DhcpServerv4MulticastScope
- Get-DhcpServerv4MulticastExclusionRange
- Get-DhcpServerv4MulticastLease
- Get-DhcpServerv4MulticastScope
- Get-DhcpServerv4MulticastScopeStatistics
- Remove-DhcpServerv4MulticastExclusionRange
- Remove-DhcpServerv4MulticastLease
- Remove-DhcpServerv4MulticastScope
- Set-DhcpServerv4MulticastScope

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

DNS credentials management

New cmdlets have been added that allow you to configure and manage the credentials a DHCP server uses to register or deregister client records on a DNS server. The new cmdlets for this functionality are:

- Get-DhcpServerDnsCredential
- Remove-DhcpServerDnsCredential
- Set-DhcpServerDnsCredential

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Add-DhcpServerSecurityGroup

The Add-DhcpServerSecurityGroup cmdlet adds security groups to the DHCP server. The cmdlet adds the DHCP Users and DHCP Administrators security groups.

Here is an example:

```
PS C:\> Add-DhcpServerSecurityGroup -ComputerName "DhcpServer03.Contoso.com"
```

This command adds the security groups DHCP Users and DHCP Administrators to the DHCP server named DhcpServer03.Contoso.com.

Repair-DhcpServerv4IPRecord

The Repair-DhcpServerv4IPRecord cmdlet reconciles inconsistent DHCP lease records in the database for the DHCP Server service for the specified DHCP scopes. Specify the ReportOnly parameter to view the inconsistent records without repairs.

Here is an example:

```
PS C:\> Repair-DhcpServerv4IPRecord -ScopeId 10.10.10.0 -ReportOnly
```

This command gets inconsistent DHCP client records for the scope 10.10.10.0. The command specifies the ReportOnly parameter. Unlike the previous example, this command makes no changes to inconsistent records.

DNS server cmdlets

Windows Server 2012 added extensive Windows PowerShell support for configuring and managing DNS servers. Several new cmdlets have been added to the DNS Server module in Windows Server 2012 R2. These new cmdlets are designed to help you configure and manage DNSSEC in your DNS server environment. The new cmdlets for this functionality include:

- Add-DnsServerSigningKey
- Disable-DnsServerSigningKeyRollover
- Enable-DnsServerSigningKeyRollover
- Get-DnsServerSigningKey
- Invoke-DnsServerSigningKeyRollover
- Remove-DnsServerSigningKey
- Set-DnsServerSigningKey
- Step-DnsServerSigningKeyRollover

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Hardware certification cmdlets

New in Windows PowerShell 4.0 are cmdlets relating to the Windows Hardware Certification Kit (HCK). These cmdlets can be used to create HCK project definition files and test collection files, create test summary reports, merge test results in different ways, and export/import test collections in XML format. The new cmdlets for this functionality include:

- Export-HwCertTestCollectionToXml
- Import-HwCertTestCollectionFromXml
- Merge-HwCertTestCollectionFromHckx
- Merge-HwCertTestCollectionFromXml
- New-HwCertProjectDefinitionFile
- New-HwCertTestCollection
- New-HwCertTestCollectionExcelReport

You can search Microsoft TechNet if you need more information about these cmdlets.

Hyper-V cmdlets

There are several new cmdlets you can use for managing various aspects of a Hyper-V environment running on Windows Server 2012 R2. The sections that follow include descriptions of some of the new cmdlets you might find useful for your environment along with some usage examples.

Test-VMNetworkAdapter

The Test-VMNetworkAdapter cmdlet tests connectivity between virtual machines by using Internet Control Message Protocol (ICMP) Ping packets. Ping verifies IP-level connectivity to another TCP/IP computer by sending ICMP Echo Request messages.

Here is an example:

```
PS C:\> Test-VMNetworkAdapter –VMName "ContosoVM01" –Receiver –SenderIPAddress
"10.20.20.5" –ReceiverIPAddress "10.20.20.6" –VMNetworkAdapterName "ContosoNic01"
```

This command tests connectivity by using the virtual network adapter named ContosoNic01. The command targets the receiver virtual machine.

Virtual machine firmware cmdlets

The following cmdlets can be used to view or modify the firmware configuration of virtual machines:

- Get-VMFirmware
- Set-VMFirmware

Virtual network adapter isolation cmdlets

The following cmdlets can be used to view or modify the isolation settings for virtual network adapters:

- Get-VmNetworkAdapterIsolation
- Set-VmNetworkAdapterIsolation

Virtual network adapter routing domains

The following cmdlets can be used to configure and manage routing domains and virtual subnets for virtual network adapters:

- Add-VmNetworkAdapterRoutingDomainMapping
- Get-VMNetworkAdapterRoutingDomainMapping
- Remove-VMNetworkAdapterRoutingDomainMapping
- Set-VmNetworkAdapterRoutingDomainMapping

Copy-VMFile

The Copy-VMFile cmdlet can be used to copy files to virtual machines.

Debug-VM

The Debug-VM cmdlet debugs a virtual machine. This deserves more explanation, so let's hear now from another one of our insiders at Microsoft concerning this cmdlet.

Windows Server 2012 R2 Hyper-V and debugging virtual machines

Debugging operating systems and applications running on them is always an important part of software development lifecycle management, particularly when dealing with operating system or kernel mode driver issues. There also could be situations during troubleshooting when a snapshot of a system's state and the contents of its memory in the form of a full or kernel memory dump of the operating system might be required.

On a Windows Server operating system running directly on hardware, administrators and developers have used hardware NMI (Non-Maskable Interrupt), Keyboard "Right Ctrl+Scroll+Scroll," or Live Debug using Remote Null Mode and 1394 (Firewire) cable techniques to freeze the operating system in time and generate a Kernel or Full System Memory dump. NMI is usually a useful troubleshooting method when a system is completely unresponsive and software crash dump or other methods could not be leveraged at all. This is particularly useful for diagnosing systems that have deadlocked due to kernel or user mode components.

When running workloads in Hyper-V virtual machines, the same need for generating memory dumps arises from time to time and administrators might need to initiate some sort of memory dump during troubleshooting, Kernel mode application, or driver development process.

Using windbg

One method that has been available in Hyper-V since the first release has been the use of windbg (Debugging Tools for Windows) over virtual COM port name pipe and using the ".dump /f" to generate a full memory dump. This method is very similar to Remote Debugging using Null Mode or Firewire cable in the physical environment, and there are requirements to have the debug settings configured in the virtual machine's BCD (Boot Configuration Data) store and to attach the debugger during the boot. This also could incur an extended outage to the services running on the virtual machine while the debug session is active. Capturing memory dump also fully freezes the operating system and it might take a while (depends on the size of RAM in the virtual machine and if this is a Kernel memory dump or full memory dump) to transfer the memory dump over the cable to the remote debugger PC.

Please see the following blog post for more information: "Configuring a Hyper-V VM for Kernel Debugging" at *http://blogs.msdn.com/b/ntdebugging/archive/2011/12/30/configuring-a-hyper-v-vm-for-kernel-debugging.aspx*.

Using VM2DMP

Another utility that was published on MSDN and that has been used in the field is VM2DMP.exe (Hyper-V VM State to Memory Dump Converter), a command-line tool that converts the saved state of a Hyper-V virtual machine to a full memory dump file compatible with Debugging Tools for Windows. This utility that is compatible with Windows Server 2008 R2 could be used to convert the memory contents of a virtual machine at a point of time to a full memory dump file.

You can find the VM2DMP.exe tool at *http://archive.msdn.microsoft.com/vm2dmp*.

Using Debug-VM

With the release of Windows Server 2012 R2 Hyper-V and its extensive Windows PowerShell integration, there's a new Windows PowerShell cmdlet called Debug-VM that can inject NMI to the virtual machine from the local or remote PC, given the user has been granted local Hyper-V administrator privilege on the Windows Server 2012 R2 Hyper-V hosting that virtual machine.

The following examples are two different syntaxes that can be used;

```
Debug-VM -Name VMName [-ComputerName HostName] [-Force]
-InjectNonMaskableInterrupt
```

```
Debug-VM -VM VMName [-ComputerName HostName>] [-Force]
-InjectNonMaskableInterrupt
```

Here are three examples of using this command:

```
PS C:\> debug-vm -VM WS2012R2 -InjectNonMaskableInterrupt

PS C:\> debug-vm -Name WS2012R2 -InjectNonMaskableInterrupt

PS C:\> debug-vm -VM WS2012R2 -ComputerName HV-Dev-2630.contoso.com
-InjectNonMaskableInterrupt -Force
```

Executing this cmdlet against a virtual machine or set of virtual machines will initiate a memory dump of the system and, depending on the debug settings of the operating system, a respective memory dump could be collected upon the virtual machine restart. The following is an example of the Windows Server 2012 R2 Virtual Machine console after sending the NMI command via Debug-VM cmdlet:

NMI support and Linux virtual machines on Hyper-V

With the wide range of Linux virtual machine support on Windows Server 2012 R2 Hyper-V, if a Linux system enters a complete unresponsive state, administrators and developers can panic the system by using the Debug-VM cmdlet. The syntax is exactly the same as mentioned above for Linux virtual machines.

In order to check successful execution within the Linux virtual machine, you may run the following command inside the terminal:

```
Localhost:~ # cat /proc/interrupts|grep NMI
                      1     Non-maskable interrupts
```

For more information, see the blog post "Enabling Linux Support on Windows Server 2012 R2 Hyper-V" at *http://blogs.technet.com/b/virtualization/archive/2013/07/24/enabling-linux-support-on-windows-server-2012-r2-hyper-v.aspx*.

Ideally, kernel or complete memory dump file debugging should be the last resort after all the standard troubleshooting methods have been exhausted. Instantiating this process on a production server could be harmful and extreme care must be used. Since you do not have to make any registry changes or reboots to enable this behavior inside Windows Server 2012 R2, please make sure to try these commands only on test and exposable virtual machines unless you've been instructed by Microsoft Support and you are aware of its consequences.

Mark Gehazi
Data Center Specialist, US-SLG STU Infrastructure

iSCSI target cmdlets

Several new cmdlets have been added in Windows Server 2012 R2 to make configuring and managing Internet Small Computer System Interface (iSCSI) target servers and iSCSI virtual disks easier. The new cmdlets for this functionality include:

- Export-IscsiTargetServerConfiguration
- Import-IscsiTargetServerConfiguration
- Resize-IscsiVirtualDisk
- Stop-IscsiVirtualDiskOperation

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Net TCP/IP cmdlets

Three new cmdlets have been added in Windows Server 2012 R2 for performing various Net TCP/IP-specific tasks:

- Get-NetCompartment
- Test-NetConnection
- Find-NetRoute

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Network Address Translation cmdlets

Windows Server 2012 R2 has some new cmdlets you can use for managing various aspects of a Network Address Translation (NAT) environment. The cmdlets for this functionality are:

- Add-NetNatExternalAddress
- Add-NetNatStaticMapping
- Disable-NetNatTransitionConfiguration
- Enable-NetNatTransitionConfiguration
- Get-NetNat
- Get-NetNatExternalAddress
- Get-NetNatGlobal
- Get-NetNatSession
- Get-NetNatStaticMapping
- Get-NetNatTransitionConfiguration
- Get-NetNatTransitionMonitoring
- New-NetNat
- New-NetNatTransitionConfiguration
- Remove-NetNat
- Remove-NetNatExternalAddress
- Remove-NetNatStaticMapping
- Remove-NetNatTransitionConfiguration
- Set-NetNat
- Set-NetNatGlobal
- Set-NetNatTransitionConfiguration

Network event packet capture cmdlets

Windows Server 2012 R2 has a number of new cmdlets you can use for managing network packet filtering. For a list of the cmdlets available, type the following command:

```
Get-Command *NetEvent*
```

Network Virtualization cmdlets

Windows Server 2012 R2 adds Windows PowerShell support for configuring and managing a Network Virtualization environment. The cmdlets for this functionality are:

- Get-NetVirtualizationCustomerRoute
- Get-NetVirtualizationGlobal
- Get-NetVirtualizationLookupRecord
- Get-NetVirtualizationProviderAddress
- Get-NetVirtualizationProviderRoute
- New-NetVirtualizationCustomerRoute
- New-NetVirtualizationLookupRecord
- New-NetVirtualizationProviderAddress
- New-NetVirtualizationProviderRoute
- Remove-NetVirtualizationCustomerRoute
- Remove-NetVirtualizationLookupRecord
- Remove-NetVirtualizationProviderAddress
- Remove-NetVirtualizationProviderRoute
- Select-NetVirtualizationNextHop
- Set-NetVirtualizationCustomerRoute
- Set-NetVirtualizationGlobal
- Set-NetVirtualizationLookupRecord
- Set-NetVirtualizationProviderAddress
- Set-NetVirtualizationProviderRoute

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Physical Computer System View (PCSV) cmdlets

New in Windows Server 2012 R2 are some cmdlets you can use for remotely managing certain aspects of Intelligent Platform Management Interface (IPMI) and Web Services-Management (WSMAN) devices. The cmdlets for this functionality are:

- Get-PcsvDevice
- Restart-PcsvDevice
- Set-PcsvDeviceBootConfiguration
- Start-PcsvDevice
- Stop-PcsvDevice

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Software Inventory Logging cmdlets

Windows Server 2012 R2 adds some cmdlets you can use for managing Software Inventory Logging. The cmdlets for this functionality are:

- Get-SilComputer
- Get-SilData
- Get-SilLogging
- Get-SilSoftware
- Get-SilUalAccess
- Get-SilWindowsUpdate
- Publish-SilData
- Set-SilLogging
- Start-SilLogging
- Stop-SilLogging

Start screen cmdlets

Administrators who need to be able to customize the Start screen on Windows 8.1 and Windows Server 2012 R2 will be glad to learn about the following new cmdlets.

Export-StartLayout

The Export-StartLayout cmdlet exports the layout of the Start screen of the current user. You can export layout as an .xml file to verify the layout, or you can export layout as a .bin file to modify the layout of an existing Windows image. Specify the appropriate file name extension, .bin or .xml, in the name of the file. To modify the layout of a Windows image, export the layout as a .bin file, and then import it into a Windows image by using the Import-StartLayout cmdlet.

Here is an example:

```
PS C:\> Export-StartLayout -Path "C:\Layouts\Marketing.bin" -As BIN
```

This command exports the layout of the Start screen to a file named Marketing.bin in the C:\Layouts folder. The command specifies a value of BIN for the As parameter, so the cmdlet creates a .bin file.

Import-StartLayout

The Import-StartLayout cmdlet imports the layout of the Start screen into a mounted Windows image. When you import a layout, it replaces the existing layout of the Start screen. Before you use this cmdlet, mount the Windows image file to import the layout into.

Use the Export-StartLayout cmdlet to create a .bin file, and then use this cmdlet to import that file. You must have administrator rights to import a layout.

The Export-StartLayout cmdlet also exports layouts as .xml files, but this cmdlet imports only .bin files.

Here is an example:

```
PS C:\> Import-StartLayout -LayoutPath "Layout.bin" -MountPath "E:\MountedImage" -WhatIf
```

This command validates the layout file and the Windows image by using the WhatIf parameter. Besides that parameter, the command is the same as the previous example, but this command makes no changes.

Get-StartApps

The Get-StartApps cmdlet gets the names and AppIDs of apps in the Start screen of the current user. An AppID is an AppUserModelID. You can specify a particular app by using its name, or you can specify a name that includes the wildcard character (*). If you do not specify a name, the cmdlet displays all the apps from the Start screen.

Here is an example:

```
PS C:\> Get-StartApps
Name AppID
---- -----

A. Datum Pro Center Datum.ProCenter
Proseware Studio Proseware.Studio.5
A. Datum 2010 prog..tion_0000000000000000_ebec13db489e8ef9
Fabrikam Initializer Fabrikam.Initializer.1
A. Datum Connector Contoso.Datum.Connector
Proseware Design Pro Proseware.Design.3
```

This command gets all the names and IDs of apps in the Start screen for the current user.

Windows Deployment Services cmdlets

Windows Server 2012 R2 now has cmdlets you can use for managing Windows Deployment Services. This improvement will definitely help administrators who deploy Windows images using Windows Deployment Services. The cmdlets for this functionality are:

- Add-WdsDriverPackage
- Approve-WdsClient
- Copy-WdsInstallImage
- Deny-WdsClient
- Disable-WdsBootImage
- Disable-WdsDriverPackage
- Disable-WdsInstallImage
- Disconnect-WdsMulticastClient
- Enable-WdsBootImage
- Enable-WdsDriverPackage
- Enable-WdsInstallImage
- Export-WdsBootImage
- Export-WdsInstallImage
- Get-WdsBootImage
- Get-WdsClient
- Get-WdsDriverPackage
- Get-WdsInstallImage
- Get-WdsInstallImageGroup
- Get-WdsMulticastClient
- Import-WdsBootImage
- Import-WdsDriverPackage
- Import-WdsInstallImage
- New-WdsClient
- New-WdsInstallImageGroup
- Remove-WdsBootImage
- Remove-WdsClient
- Remove-WdsDriverPackage
- Remove-WdsInstallImage
- Remove-WdsInstallImageGroup
- Set-WdsBootImage
- Set-WdsClient

- Set-WdsInstallImage
- Set-WdsInstallImageGroup

You can use the Get-Help cmdlet on Windows Server 2012 R2 to display additional information about these new cmdlets.

Windows PowerShell Web Access cmdlets

If you use Windows PowerShell Web Access so you can manage the servers in your private cloud from anywhere, at any time, by running Windows PowerShell commands within a web-based console, you'll probably be glad to learn about the following new cmdlets in Windows Server 2012 R2:

- Add-PswaAuthorizationRule
- Get-PswaAuthorizationRule
- Install-PswaWebApplication
- Remove-PswaAuthorizationRule
- Test-PswaAuthorizationRule
- Uninstall-PswaWebApplication

Windows Search cmdlets

Windows Search is a powerful feature you can use for searching for the attributes and contents of documents, email messages, and much more. You can now use the following Windows PowerShell cmdlets to view or modify how Windows Search works.

Get-WindowsSearchSetting

This cmdlet gets the values of settings for Windows Search. Here is an example:

```
PS C:\> Get-WindowsSearchSetting
Setting                                                    Value
-------                                                    -----
EnableWebResultsSetting                                    True
EnableMeteredWebResultsSetting                             True
SearchExperience                                           PersonalizedAndLocation
WindowsSafeSearchSetting                                   Moderate
```

Set-WindowsSearchSetting

This cmdlet modifies values that control Windows Search. Here is an example:

```
Set-WindowsSearchSetting -SearchExperienceSetting "Personalized"
```

This command allows Windows Search to use search history, but not specific location of the user, to personalize results.

Learn more

You can learn more about the new capabilities in Windows PowerShell 4.0 on Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Windows PowerShell" at *http://technet.microsoft.com/library/hh857339.aspx*.
- "Scripting with Windows PowerShell" at *http://technet.microsoft.com/en-us/library/bb978526.aspx*.
- "Windows and Windows Server Automation with Windows PowerShell" at *http://technet.microsoft.com/en-us/library/dn249523.aspx*.

The following Microsoft TechNet and MSDN blog posts also have lots of information about the new Windows PowerShell features and enhancements in Windows Server 2012 R2:

- "DAL in Action: Introducing PCSV Cmdlets for Out-of-Band Management of Server Hardware" at *http://blogs.msdn.com/b/powershell/archive/2013/07/31/dal-in-action-introducing-pcsv-cmdlets-for-out-of-band-management-of-server-hardware.aspx*.
- "DAL in Action: Managing Network Switches Using PowerShell and CIM" at *http://blogs.msdn.com/b/powershell/archive/2013/07/31/dal-in-action-managing-network-switches-using-powershell-and-cim.aspx*.

Be sure also to check out the following videos from TechEd 2013 on Channel 9:

- "Desired State Configuration in Windows Server 2012 R2 PowerShell" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B302*.
- "Advanced Automation Using Windows PowerShell" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B400*.
- "Windows PowerShell Unplugged" at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B340*.

CHAPTER 11

Windows Server Essentials

Microsoft has strived to serve the computing needs of small business users over the years with a variety of offerings. Windows Small Business Server (SBS) was a popular product that went through several versions including 2003, 2008, and 2011. When Windows Server 2012 was released, Microsoft repositioned its small business offering by rebranding it as Windows Server 2012 Essentials and marketing it as an ideal first server for small businesses with up to 25 users. Windows Server 2012 Essentials was a cost-effective and easy-to-use solution to help protect data, organize and access business information from virtually anywhere, support the applications needed to run a business, and quickly connect to online services for email and backup.

The new version of this offering is Windows Server 2012 R2 Essentials and it's designed as a flexible, affordable, and easy-to-use server solution for small businesses and medium-sized businesses. It's also priced affordably in order to help businesses reduce costs and increase their productivity. And it can even be deployed as the primary server in a multiserver environment for small businesses.

Specifically, Windows Server Essentials is now available in two ways:

- As an Edition for Small Businesses that have up to 25 users and 50 devices
- As a server role in Windows Server 2012 R2 Standard edition for medium-sized businesses that have up to 100 users and 200 devices

In addition, both forms of Windows Server Essentials can be deployed in either a physical or virtual environment.

To learn more about this latest version of Windows Server Essentials, let's go to the source now and hear directly from the Windows Server Essentials team at Microsoft.

Introducing Windows Server 2012 R2 Essentials

Less than a year ago we introduced Windows Server 2012 Essentials to the market. Since then, the team has been working really hard to put forward a great release for Windows Server 2012 R2 Essentials that further builds on the value that Windows Server Essentials brings to small businesses. In addition to being a great primary server for small businesses, we've made some major investments in Windows Server 2012 R2 Essentials that allows the experience

that Windows Server Essentials offers to scale to larger, more diverse topologies. We've also made investments to help our small and medium businesses (SMB customers) to more easily virtualize their environments, as well as provide super simple access to the cloud through deep integration with Microsoft Office 365 and Windows Azure. This sidebar describes some of the many improvements introduced in Windows Server 2012 R2 Essentials.

Virtualization made easy

Virtualization continues to be a popular trend in enterprise computing; however, adoption by SMBs is not as aggressive. One of the reasons SMBs are hesitant to move to virtualization has to do with the complexity of properly configuring and managing virtual instances of the operating system.

With Windows Server 2012 R2 Essentials, we have addressed the problem by enabling the virtualization of a Windows Server Essentials guest VM on a Windows Server Essentials host server. This can be set up manually by the administrator or, depending on your OEM configuration, a simple wizard will guide you through the process of setting up the guest VM during the installation process of the server. All of the setup, configuration, and connection to your Essentials server from client PCs is made to the guest virtual machine.

Running Windows Server 2012 R2 Essentials in the cloud

With the availability of Windows Azure Virtual Machines, you can deploy your own customized Windows Server 2012 R2 Essentials image into a **commercially backed** SLA production environment in minutes.

Although this ability has been available previously, with the introduction of Windows Server 2012 R2 Essentials, configuration options are available to deliver an optimized experience in a hosted deployment. Specifically, features such as client backup and storage spaces are turned off by default because moving large amounts of data across the Internet may be slow and costly.

These configuration settings are not only for Windows Azure–hosted deployments, but also for private hosted deployments. Windows Server 2012 R2 Essentials is designed to work with the Windows Azure Pack, enabling service providers to provide hosted solutions that are easy to deploy and maintain.

In addition, when you are running Windows Server Essentials in the cloud, you can use BranchCache to cache files locally to reduce traffic between the cloud and your local office. Enabling this BranchCache functionality in Windows Server Essentials is as easy as flipping a switch.

Integration with cloud services

In Windows Server 2012 Essentials, we did deep integration with cloud services to provide seamless access for daily administrative tasks. Our goal was to keep a consistent user experience for the administrator and avoid the jarring experience of switching from one administration console (the Dashboard) to a completely different one—typically a separate web portal. By keeping the experience within the Dashboard as much as possible, we not only provide ease of use for the administrator, but also save time by surfacing only the key tasks needed for the service as shown here:

In many cases, SMB customers are not even aware of the cloud services that are offered by Microsoft that can help them simplify their businesses. In Windows Server 2012 R2 Essentials, we have added a services integration status page that shows you not only what services are available, but also whether your server is attached to these services.

One of the things you'll notice in the screenshot above is that in addition to services previously available, some new services are integrated as well. The following are some of the new services and key features available with Windows Server 2012 R2 Essentials.

WINDOWS AZURE ACTIVE DIRECTORY

Windows Azure Active Directory is a service that provides identity and access capabilities for on-premises and cloud applications. Integrating Windows Azure Active Directory with Essentials enables SMBs to have single sign-on and password synchronization between the local Active Directory and cloud services such as Office 365.

Additionally, we have enabled user group management directly from the Dashboard, and by using Windows Azure Active Directory integration, these groups are synchronized as well as the user accounts.

MICROSOFT OFFICE 365

Whereas the integration of Office 365 in Windows Server 2012 Essentials was a great step forward, with Windows Server 2012 R2 Essentials we wanted to continue to enhance the experience by providing even deeper integration. As I mentioned earlier, a key goal for the new release was to expand beyond small business to SMB. When you move from an environment of fewer than 25 users to potentially hundreds of users, new challenges surface that need to be addressed.

To help make these management challenges easier, we have integrated the following Office 365 features in the Dashboard:

- **Distribution Groups** The ability to create and manage email distribution groups
- **Mobile Device Management** The ability to manage mobile devices connected to the Office 365 service, enabling remote wipe, policy enforcement, and access management (see the screenshot below)
- **SharePoint Online Library Management** The ability to create and manage SharePoint libraries

WINDOWS INTUNE

Windows Intune is a cloud-based solution for managing your organization's PCs, including device management for multiple operating system platform devices, security management for software patch distribution and endpoint protection, and management of application distribution for bring your own devices (BYOD).

In Windows Server 2012 R2 Essentials, integration with Windows Intune enables the administrator to manage users, security groups, and licenses for Windows Intune services right from within the Dashboard.

WINDOWS AZURE BACKUP

Previously known as Windows Azure Online Backup, the ability to back up your server's key data to Windows Azure cloud storage was made available as an add-in in Windows Server 2012 Essentials. In Windows Server 2012 R2 Essentials, the Windows Azure Backup add-in is now surfaced on the services integration tab of the Dashboard as shown here:

The Windows Server Essentials Experience server role

Consistent feedback we heard from customers and partners was why some of the features unique to Windows Server Essentials were, in fact, unique. Why not make these features available in the Windows Server Standard and Datacenter editions?

It's a great question and one that we took seriously. One of the challenges of doing this, however, was the fact that some of our specific features require dependent roles and services in Windows Server that take additional overhead on the system. Enabling these by default on every server running Windows Server was not the right thing to

do out of the box. We have solved this dilemma in Windows Server 2012 R2 with the addition of the Windows Server Essentials Experience server role shown here:

In the Standard and Datacenter editions of Windows Server 2012 R2, administrators who want the full features and functionality of Windows Server Essentials will be able to add a new server role to the system called the Windows Server Essentials Experience.

The Windows Server Essentials Experience server role enables all the features and dependent services and roles of the Windows Server 2012 R2 Essentials edition, without the locks and limits that are in place for the edition. Enabling or disabling the Windows Server Essentials Experience role is as simple as turning it on or off in Server Manager.

This change enables not only an easy upgrade path for small businesses that want more flexibility, but also offers the following benefits:

- The flexibility to implement a Standard or Datacenter edition server running the Windows Server Essentials Experience role as a domain member rather than as the root domain controller.
- The ability to add the Windows Server Essentials Experience to an existing domain environment that already has multiple servers running Windows Server.
- Running the Standard or Datacenter edition gives you all the features and licensing rights of the operating system (such as expanded virtualization rights and larger hardware configurations).

Empowering remote workers and BYOD

With the continuing trend of mobile PCs outselling desktop PCs, as well as double-digit tablet and smartphone growth, ensuring that multiple devices can easily connect to the Windows Server 2012 R2 Essentials server regardless of location is key.

In addition, touch as a primary input mechanism while on the go is becoming a requirement rather than a luxury. As such, we have made significant new investments in two key areas that are already available today with Windows Server 2012 Essentials: My Server apps for Windows Phone and Windows 8, and Remote Web Access.

MY SERVER APPS FOR WINDOWS PHONE AND WINDOWS

With Windows Small Business Server 2011 Essentials, we introduced the My Server application for Windows Phone 7. With Windows Server 2012 Essentials, we added the My Server app for Windows 8 and Windows RT. We've seen a tremendous number of downloads of these great applications and will continue to update them both for the next release to support key new features such as Microsoft SharePoint Online libraries.

For example, you can access files and folders on your server by using the My Server Windows Phone application:

You can manage users, devices, and alerts by using the My Server Windows Phone application:

You can also manage alerts and access shared folders on the server by using the My Server Windows Store application:

And you can even access files and folders on your server. The recently accessed files are available even when you are offline:

MODERNIZED REMOTE WEB ACCESS

Remote Web Access (RWA) enables users and administrators to access data and connect to computers running in their office network from any Internet browser. The RWA interface that ships with Windows Server 2012 Essentials, although very functional, is not optimized for touch devices. With Windows Server 2012 R2 Essentials, we have completely overhauled the interface to be touch-optimized, as well as leveraging HTML5 rather than Silverlight, enabling a consistent experience across any HTML5-compliant browser.

Improved Connector software

The Connector software connects the client PCs on your network to your Windows Server Essentials server in order to automatically back up the PCs and monitor their health. The Connector also allows you to configure and remotely administer your Windows Server Essentials server. In Windows Server 2012 R2 Essentials, the Connector has been improved in the following ways:

- Its performance has been significantly improved by reducing memory and CPU usage.
- It can be installed and configured on a client PC regardless of where it is located.
- It provides auto-dial virtual private network (VPN) connectivity to domain-joined PCs in order to provide a seamless remote working experience just as if the user is in the office.

Protecting data on the client

In the previous release of Windows Server 2012 Essentials, we centralized the File History management to better protect the important data on the client PCs. In Windows Server 2012 R2 Essentials, we further improved this by providing a quick restore feature to help you more easily replace a PC and restore all the profile data to a new PC.

We also made client full system restore easier. With more and more PCs now selling without a DVD drive, restoring a PC with a DVD is not possible on some models. The new Client Full System Restore capability supported by Windows Deployment Services now allows you to boot a client PC to the network and quickly perform a full system restore on it. This means that you no longer need to maintain hard copies of your restore environment on a DVD or a USB bootable drive.

Conclusion

This sidebar has described a few of the many improvements introduced in Windows Server 2012 R2 Essentials. But there are lots of other enhancements we unfortunately don't have space to describe in detail here, such as the new BranchCache integration functionality, the improved File History feature, support for deploying Windows Server Essentials on a member server in a domain, support for creating user groups (and Office 365 distribution groups if your server is integrated with Office 365), improved client deployment options, and much more. For a full list of new features and enhancements, see the TechNet article "What's New in Windows Server 2012 R2 Essentials" referenced in the Learn More section below.

Jason Anderson
Group Program Manager with the Windows Server Essentials team

Learn more

You can learn more about the new Windows Server Essentials features and enhancements in Windows Server 2012 R2 by checking out the following topics on Microsoft TechNet:

- "What's New in Windows Server 2012 R2 Essentials" at *http://technet.microsoft.com/en-us/library/dn303448.aspx*.
- "Windows Server Essentials" at *http://technet.microsoft.com/en-us/sbs/jj159331.aspx*.

The following Microsoft TechNet and MSDN blog posts also have lots of information about the new Windows Server Essentials features and enhancements in Windows Server 2012 R2:

- "Understanding Licensing for Windows Server 2012 R2 Essentials and the Windows Server Essentials Experience role" at *http://blogs.technet.com/b/sbs/archive/2013/09/03/understanding-licensing-for-windows-server-2012-r2-essentials-and-the-windows-server-essentials-experience-role.aspx*.

APPENDIX

Additional resources

The following additional resources can be used to learn more about Windows Server 2012 R2:

- Download Windows Server 2012 R2 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/bb291020.aspx*
- Windows Server 2012 R2 on the Microsoft Server and Cloud Platform at *http://www.microsoft.com/en-us/server-cloud/windows-server/windows-server-2012-r2.aspx*
- What's New in Windows Server 2012 R2 in the TechNet Library at *http://technet.microsoft.com/en-us/library/dn250019.aspx*
- See also the Windows Server Blog on TechNet at *http://blogs.technet.com/b/windowsserver/*
- You can find videos and slide decks about Windows Server 2012 R2 from Microsoft TechEd North America 2013 on Channel 9 at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013*
- Post your questions about Windows Server 2012 R2 to the Windows Server forums on TechNet at *http://social.technet.microsoft.com/Forums/windowsserver/en-US/home?category=windowsserver*

Index

Symbols and Numbers

.wim files, 186–187

A

access control
multi-factor, 127
role-based, 108–110
activation
dynamic site, 155–156
activation, virtual machine, 11–12
Active Directory
detached clustering, 82
enhancements in Windows Server 2012, 124
Kerberos authentication, 146–148
LDAP search performance, 131–135
multi-factor access control, 127
Web Application Proxy, 127–131
Windows Azure, 206
Work Folders in, 53
Workplace Join, 125–126
Active Directory Administrative Center (ADAC), 124
Active Directory Certificate Services (AD CS), 123
Active Directory Domain Services (AD DS), 112, 123, 131–135
Active Directory Federation Services (AD FS), 123, 127, 130
Active Directory Lightweight Directory Services (AD LDS), 123
Active Directory Rights Management Services (AD RMS), 123
AD CS (Active Directory Certificate Services), 123
AD DS (Active Directory Domain Services), 112, 123, 131–135
AD FS (Active Directory Federation Services), 123, 127, 130
AD LDS (Active Directory Lightweight Directory Services), 123
AD RMS (Active Directory Rights Management Services), 123
ADAC (Active Directory Administrative Center), 124
Add-DhcpServerSecurityGroup cmdlet, 190
address assignment, 114
address filtering, 154
Address Hash, 93, 95–96
address management. *See* IP Address Management (IPAM)
address translation, 196
Add-WindowsImage cmdlet, 186–187
administrators
access to user files, 57
use of Work Folders, 51
aliases, 55
Anderson, Jason, 214
Application Initialization, 154, 156
application pools, 154, 157
apps
group policy settings, 144–145, 150
My Server, 209–212
publishing, 130–131
Start Screen view, 143
Window Store, 150
architecture
extensible switch, 119–120
Hyper-V extensible switch, 115–117
IP Address Management (IPAM), 109
private cloud solution, 30–31
authentication. *See also* preauthentication
compound, 146–147
device, 125, 127
multi-factor, 127

automatic setup, of Work Folders, 145–146
Automatic Virtual Machine Activation (AVMA), 11–12
availability, of virtual machines, 78–80

B

backgrounds, start screen, 143
backups, 20, 24, 207
bandwidth management, 37–38, 86, 96, 120
Benari, Erez, 94
block-based storage, 28–29, 34, 40, 68
booting
    fast, 137
    Generation 2 virtual machines, 7
    secure, 7–8, 10
BranchCache, 87, 204
business needs and cloud computing, 1–3
Butte, Jeff, 186

C

CA (Customer Addresses), 114, 116
cache
    allocation, 73
    write-back, 33, 43
capacity versus performance, 41–42
capturing extensions, 116, 119–120
CAU (Cluster-Aware Updating), 64
Chkdsk, 28
Client Full System Restore, 213
cloud computing
    Microsoft's vision for, 1, 29–31
    platform synchronization, 1–3
    Windows Server Essentials 2012 R2, 204–205
cloud service integration, 205
cluster nodes
    draining, 78–80
    heartbeat thresholds, 75
    transparent failover, 36
    updates, 64
Cluster Shared Volumes (CSV)
    and deduplication, 38
    failover clustering and, 71–73
    for block storage, 68
    overview, 63
    ownership of disks, 71–72
    resiliency enhancements, 72–73
Cluster-Aware Updating (CAU), 64
cold data, 41–44
cold requests, 156–157
color, start screen accent, 143
communication, IP Address Management (IPAM), 110
compression, 16–17
compute layer, in cloud computing solutions, 29
configuration drift, 177–178
Configuration Instance Document script, 178–179
Configuration Manager, 178
configurations
    network, 100–101
    Work Folders, 146
configuring
    ETW logging, 159
    virtual machine health protection, 76–78
    Web Application Proxy, 128–129
connectivity
    testing, 102–105, 191
    virtual machine health protection, 76–78
Connector software, 213
Content protection, 149–150
Copy-VMFile cmdlet, 192
CPU throttling, 154
credentials
    DNS, 189
    restriction of delegation, 148
CSV (Cluster Shared Volumes)
    and deduplication, 38
    failover clustering and, 71–73
    for block storage, 68
    overview, 63
    ownership of disks, 71–72
    resiliency enhancements, 72–73
Customer Addresses (CA), 114, 116

D

Dashboard, 205–207
Data Center Bridging (DCB), 86
data center management, 177–183
data collection, 110–111
data protection, 213
data tiering, 42–44
Datacenter edition, 11–12
Debug-VM cmdlet, 192–195
deduplication, 28, 38–39, 73, 172

delegation, credential, 148
Deployment Image Servicing and Management (DISM) cmdlets, 186–189
Desired State Configuration (DSC), 176–183
Desired State Configuration (DSC) Pull Server, 178–179, 181, 183
Device Manager, 9–10
device policies, 57
devices. *See* mobile device management; personal devices
DHCP (Dynamic Host Configuration Protocol), 86, 105–106, 120, 189–190
disaster recovery, 21–24
disconnection, 75, 78, 175
DISM (Deployment Image Servicing and Management) cmdlets, 186–189
displays
  handling, 169
  multi-monitor, 143–144
distribution groups, 206
distros, 20
DNS credentials management, 189
domain controllers, 124
  search performance, 132–135
Domain Name System (DNS), 87, 105–106, 190
drain on shutdown capability, 78–80
DSC. *See* Desired State Configuration (DSC)
dual parity, 44–49
DX11.1, 168
Dynamic Host Configuration Protocol (DHCP), 86, 105–106, 120, 189–190
Dynamic Memory, 6, 20
Dynamic Site Activation, 155–156
Dynamic Teaming. *See* Link Aggregation Control Protocol (LACP)
Dynamic Witness, 81

E

email distribution groups, 206
Emulex, 115
enabling
  ETW logging, 159–160
  Idle Worker Process Page-Out, 157
  Protected Network on Hyper V host clusters, 75–76
  replication frequencies, 22
Enterprise ID, 149–150
event tracing, 120, 161–162, 197
Event Tracing for Windows, 159–160
Expand-WindowsImage cmdlet, 186–187
Export-StartLayout cmdlet, 198–199
Export-WindowsImage cmdlet, 187
extensible virtual switches, 6, 115–117, 119–120
extensions
  DNS Security, 87
  third-party forwarding extensions, 121
  types of, 115–116, 119–120

F

Failover Clustering
  Active Directory-detached clustering, 82
  cache allocation, 73
  CSV ownership distribution, 71–72
  draining resources off nodes, 78–80
  dynamic witness feature, 81
  enhancements in Windows Server 2012, 63–64
  health monitoring, 73
  heartbeat thresholds, 74–75
  Scale-Out File Servers (SoFS), 70–71
  virtual machine health protection, 76–78
Fast Startup, 137
Federation Proxy Service, 128
Fibre Channel, 7, 32, 35, 40
File and Storage Services, 28, 35, 53
file storage
  group policy settings, 151
  Resilient File System (ReFS), 28, 73
  SoFS, 68
files
  copying to virtual machines, 192
  remote access to, 209–212
filtering
  address, 154
  extensions, 116, 119–120
  network packet, 197
firmware configuration, 191
folders
  remote access to, 209–212
forwarding extensions, 116, 119, 121
FR/CSC, 52

G

gateway solutions, 116–118
Gehazi, Mark, 15
Generation 2 virtual machines, 7–11
  benefits of, 10–11
  booting, 7
  characteristics of, 7–8
  creating, 9–10
  deployment of, 8
  Guest operating system on, 7–8
  hardware device changes, 8
  Security in, 10
GenerationID, virtual machine, 124
Generic Teaming, 95
Get-StartApps cmdlet, 199
Get-WindowsImageContent cmdlet, 187–188
Get-WindowsSearchSetting cmdlet, 201
graphics display
  using DX11.1, 168
Group Policy
  advanced graphics for RDS, 168
  enhancements in Windows Server 2012, 137–138
  infrastructure status, 137
  IPv6, 139–141
  new policy settings for, 142–145
  preferences, 139–141
  starter GPOs, 138
  Windows PowerShell Remoting, 179
  Windows Runtime, 149–150
Group Policy settings
  apps, 144–145, 150
  authentication, 146–148
  automatic sign-in, 150–151
  caching, 138–139
  logon scripts, 148
  start screen, 142–144
  Window Store apps, 150
  Windows SkyDrive, 151–152
  Windows Update, 149
  Work Folders, 145–146
guest clustering, 7, 25, 65–68, 115
guest operating system, 7–8, 12–14

H

hardware certification, 191
HCK (Windows Hardware Certification Kit), 191
heartbeat thresholds, 74–75
help files, 184–186
high availability, 63–65
History Viewer, 124
host clustering, 65
host management, 21, 64–67
hot data, 42–44
hot spares, 30, 44, 49
Hyper-V
  cluster node heartbeat thresholds, 75
  enhancements in Windows Server 2012, 5–7
  extensible switch architecture, 115–116
  improvements to, 25
  live export feature, 18–19
  PowerShell cmdlets, 191–195
  support for Linux, 20–21
  switches, 25, 88, 119–121
  WinDbg in, 193
Hyper-V Manager, 9, 13, 17–18
Hyper-V Network Virtualization
  Hyper-V Virtual Switch, 115–116, 119–121
  in Windows Server 2012 R2, 115–118
  IP addresses on virtual network machines, 115
  overview, 112–114
  performance enhancements, 115
  Windows Server Gateway, 116–118
Hyper-V Port, 93, 96
Hyper-V Recovery Manager, 23–24
Hyper-V Replica, 7, 21–24

I

Idle Worker Process Page-Out, 156–157
IEEE 802.3ad teaming, 95
IEEE 802.lax teaming, 95
IIS 8.0, 153–155
IIS 8.5

cold requests in, 156–157
configuring ETW logging in, 159
Dynamic Site Activation, 155–156
ETW logging, 159–162
logging custom fields, 158–159
IIS logging, 158–160
implementing
guest clustering using shared virtual disks, 69–70
Web Application Proxy, 128–131
Work Folders, 52
Import-StartLayout cmdlet, 199
infrastructure
hoster, 67
key management, 11–12
network, 113–114
separating virtual resources from physical, 65–67
status, 137
Input/Output Operations Per Second. *See* IOPS (Input/Output Operations Per Second)
Intelligent Platform Management Interface (IPMI), 198
Internet Information Services. *See* IIS 8.0; IIS 8.5
Internet Protocol version 6 (IPv6), 139–141
Internet Small Computer System Interface (iSCSI)
Initiator, 35
server storage, 34–36
target cmdlets, 195
Target Server, 28, 35–36
IOPS (Input/Output Operations Per Second), 25, 33, 41, 43–44
IP Address Management (IPAM), 87, 105–112
Active Directory integration, 112
architecture, 109
communication, 110
data collection tasks, 110
in Windows Server 2012, 107
monitoring capabilities, 110–111
role-based access control, 108–110
security groups, 110
storage, 110–111
virtual address management, 107–108
Windows PowerShell and, 112
IPv6 (Internet Protocol version 6), 139–141
iSCSI (Internet Small Computer System Interface)
Initiator, 35
server storage, 34–36
target cmdlets, 195
Target Server, 28, 35–36

J

JBOD storage, 27, 29–33, 40
jobs, scheduled, 176

K

Kerberos authentication, 146–148
key management infrastructure, 11–12

L

LACP (Link Aggregation Control Protocol), 92, 94–95
layouts, start screen, 142
LBFO (load balancing and failover), 86, 91
licensing, virtual machine, 11–12
Lightweight Directory Access Protocol (LDAP), 123, 131–135
Link Aggregation Control Protocol (LACP), 92, 94–95
Linux Integration Services (LIS), 20
Linux support, 20–21, 195
live export feature, 18–19
live migration
cross-version, 14–16
in previous version of Hyper-V, 5
network disconnection during, 78
SMB 3.0 protocol, 37–38
speed of, 16–17
vm availability during, 78–80
load balancing and failover (LBFO), 86, 91
load balancing modes, 92–93, 96, 121
Local Configuration Manager, 178, 180
logging
custom fields, 158–159
ETW, 159–162
software inventory, 198
logical unit numbers. *See* LUNs
logon scripts, 148
LUNs, 36, 40, 66–67, 70–72

M

MAC address spoofing, 120
Managed Object Format (MOF) files, 178, 180–182
Marlin, John, 78
memory allocation, 20, 73
memory management, 6, 153, 168, 192–193
Message Analyzer, 160–162
Microsoft, 1, 29–31
Microsoft Office 365, 206
Microsoft SQL Server databases, 110–111
Microsoft Windows IIS Logging, 160
migration. *See also* live migration
    in previous version of Hyper-V, 5–6
mobile device management, 127–131, 206–207, 209–212
MOF files. *See* Managed Object Format (MOF) files
monitoring
    health, 73
    packet, 120
    using IPAM, 110–111
    virtual machine health, 75–78
multicast scopes, 189
My Server apps, 209–212

N

NAT (Network Address Translation) cmdlets, 196
network adapters
    for guest operating systems, 8
    RDMA-capable, 16–17
    teaming modes, 91
    testing, 97–101, 191–192
Network Address Translation (NAT) cmdlets, 196
network event capture cmdlets, 197
network interruptions, 74–75
network layer, in cloud computing solutions, 30
network packet filtering, 197
network switches, 119–121
network traffic, 116–118, 121
network virtualization, 87, 112–118
networking
    address management, 105–112
    diagnostics, 96–105
    enhancements in Windows Server 2012, 85–88
    Hyper-V Virtual Switch, 121
    load balancing modes, 95–96
    software-defined, 112–120
    virtual RSS (vRSS), 88–90
    Windows NIC Teaming, 90–95
New-WindowsImage cmdlet, 188
NIC Teaming, 90–96
    benefits of, 90–91
    function of, 86
    in Windows Server 2012, 91
    in Windows Server 2012 R2, 92–96
    load-balancing modes, 92–93, 95–96
    network diagnostics, 96
    teaming modes, 91–92, 94–95
NMI. *See* Non-Maskable Interrupt (NMI) method
nodes
    in Configuration Instance Document script, 179
Non-Maskable Interrupt (NMI), 192–193, 195
Non-Uniform Memory Access (NUMA), 86, 153, 168

O

Offloaded Data Transfer (ODX), 28

P

packet filtering, 197
packet monitoring, 120
paged queries, 134–135
page-outs, 156–157
parity space support, 44
PCSV (Physical Computer System View) cmdlets, 198
Performance Monitor, 162
performance versus storage capacity, 41–42
personal devices
    Workplace Join, 125
Physical Computer System View (PCSV) cmdlets, 198
physical storage, in cloud computing solution, 30
policy caching, 138–139
port ACLs, 120–121
port mirroring, 120
Powershell
    cmdlets
        Get-WindowsSearchSetting, 201
        Set-WindowsSearchSetting, 201
PowerShell
    allocating block cache, 73
    changing usage mode of physical disk, 49

cmdlets
Add-DhcpServerSecurityGroup, 190
Add-WindowsImage, 186–187
Copy-VMFile, 192
Debug-VM, 192–195
Deployment Image Servicing and Management (DISM), 186–189
DNS credentials management, 189
DNS server, 190
Dynamic Host Configuration Protocol (DHCP), 189–190
Enable-PSRemoting, 179
Expand-WindowsImage, 186–187
Export-CliXml, 186
Export-StartLayout, 142, 198–199
Export-WindowsImage, 187
Get-Cluster, 73, 81
Get-ClusterGroup, 78
Get-Command, 89
Get-DscLocalConfigurationManager, 180
Get-NetAdapter, 97
Get-NetAdapterRss, 89
Get-NetIPAddress, 98–100
Get-NetIPConfiguration, 100–101
Get-StartApps, 199
Get-VMNetworkAdapter, 77–78, 97
Get-WindowsImageContent, 187–188
hardware certification, 191
Hyper-V, 191–195
Import-StartLayout, 199
Invoke-Command, 185–186
Invoke-GPUpdate, 137
iSCSI target, 195
isolation settings for virtual network adapters, 192
Move-VM, 9
multicast support, 189
Net TCP/IP, 196
Network Address Translation (NAT), 196
network packet filtering, 197
Network Virtualization, 197
New-PSSession, 175
New-VM, 9
New-WindowsImage, 188
Physical Computer System View (PCSV), 198
record repair, 190
Remove-WindowsImage, 188
Repair-DhcpServerv4IPRecord, 190
routing domains and virtual subnets, 192
security groups, 190
Set-DscLocalConfigurationManager, 180
Show-Command, 176
Software Inventory Logging, 198
Split-WindowsImage, 188–189
StartDscConfiguration, 182
Test-NetConnection, 102–105
Test-VMNetworkAdapter, 105, 191
virtual machine firmware, 191
Windows Deployment Services, 200–201
configuring vm health protection, 76–78
Desired State Configuration (DSC), 176–183
domain controllers deployment, 124
enhancements in Windows PowerShell 3.0, 175–176
Group Policy updates, 137
History Viewer, 124
in previous version of Hyper-V, 6
Invoke-Command, 185
IP Address Management (IPAM), 112
IPAM integration with, 112
managing virtual Receive Side Scaling (vRSS), 89–90
network diagnostics, 97–105
Save Help, 184–186
Start Screen layout, 142, 198–199
tiered storage, 43
Web Access, 176, 201
preauthentication, 130
preferences
Group Policy, 139–141
Protected Network setting, 75–78
Provider Addresses, 114, 116
PSRemoting, 179
Pull Server. *See* Desired State Configuration (DSC) Pull Server

Q

Quality of Service (QoS) management, 25, 33–34, 86
queries, paged, 134–135
query optimization, 131–135
Quick Reconnect, 169
quorum functionality, 64, 81

R

RDMA (Remote Direct Memory Access), 16
RDS (Remote Desktop Services)
  data deduplication, 172
  enhancements in Windows Server 2012, 165–167
  Quick Reconnect, 169
  RemoteFX functionality in, 168
  Restricted Admin mode for, 173
  Session Shadowing, 170–172
  thumbnail preview, 167
  video performance, 169
  virtual desktop interface, 172
  VM Connect, 13
Receive Side Scaling (RSS), 86, 88–90
reconnection, session, 169
ReFS (Resilient File System), 28, 73
remote access
  for workers and BYOD, 209–212
  over VMBus, 12–14
Remote Access server role, 127–131
Remote Desktop Services (RDS)
  data deduplication, 172
  enhancements in Windows Server 2012, 165–167
  Quick Reconnect, 169
  RemoteFX functionality in, 168
  Restricted Admin mode for, 173
  Session Shadowing, 170–172
  thumbnail preview, 167
  video performance, 169
  virtual desktop interface, 172
  VM Connect, 13
Remote Direct Memory Access (RDMA), 16
Remote Group Policy updates, 137
Remote Web Access (RWA), 213
RemoteFX, 168
Remove-WindowsImage cmdlet, 188
Repair-DhcpServerv4IPRecord cmdlet, 190
replication
  extended, 23–24
  frequencies, 21–22
  in Windows Server 2012, 7
resiliency
  Cluster Shared Volumes (CSV), 72–73
  in previous version of Hyper-V, 5
Resilient File System (ReFS), 28, 73
resize, virtual hard disk, 17–18, 20
restore, client full system, 213
Restricted Admin mode, 173
Restricted mode policy setting, 148
role services
  Desired State Configuration (DSC), 176–183
  Federation Proxy Service, 128
  File and Storage Services, 28, 35, 53
  Remote Desktop Services (RDS), 165–166
  Web Application Proxy, 127–131
router guards, 120
RSS (Receive Side Scaling), 86, 88–90
RWA (Remote Web Access), 213

S

Save function, group policy setting, 152
Save Help, 184–186
scale out capability, 29–30
  Generation 2 virtual machines, 10
  in Failover Clustering, 63
  NUMA-aware, 153
  SMB, 36
  under Windows Server 2012, 5
Scale-Out File Servers (SoFS), 6, 27, 30, 68, 70–72
SCSI controllers, 7–8
SCSI disks, 7
search cmdlets, 201
Secure Boot, 7–8, 10–11
security
  groups, 190
  in Generation 2 virtual machines, 10
server management, 72–73, 112, 201, 207–209
Server Message Block (SMB), 36–38
  file servers. *See* Scale-Out File Servers (SoFS)
  in Windows Server 2012, 6, 27, 88
  SMB Bandwidth Management, 37–38
  SMB Direct, 16, 36
  SMB Encryption, 36
  SMB Multichannel, 16, 36
  SMB Transparent Failover, 36
Server Name Indication (SNI), 153
Session Shadowing, 170–172
sessions
  disconnected, 175
Set-WindowsSearchSetting cmdlet, 201
shadowing. session, 170–172
Sharepoint online library management, 206
shutdown, virtual machine, 78–80

single-root I/O virtualization (SR-IOV), 6, 88
site
activation, 155–156
SM-API (Storage Management API), 32–33
Smart Paging, 6
SMB (Server Message Block), 36–38
file servers. *See* Scale-Out File Servers (SoFS)
in Windows Server 2012, 6, 27, 88
SMB Bandwidth Management, 37–38
SMB Direct, 16, 36
SMB Encryption, 36
SMB Multichannel, 16, 36
SMB Transparent Failover, 36
SMS-S, 36
SNI (Server Name Indication), 153
SoFS. *See* Scale-Out File Servers (SoFS)
Software Inventory Logging cmdlets, 198
solid-state drives (SSDs), 30
Split-WindowsImage cmdlet, 188–189
SQL Server databases, 110–111
SR-IOV (single-root I/O virtualization), 6, 88
Srivastava, Deepak, 49
SSDs (solid-state drives), 30
SSL certificates, 154
Start Screen
cmdlets, 198–199
group policy settings, 142–144
startup. *See* booting
Static Teaming mode, 91, 94–96
status, Group Policy, 137
storage
block-based, 28–29, 34, 40, 68
capacity versus performance in, 41–42
enhancements in Windows Server 2012, 27–29
file-based, 28, 68, 73, 151
iSCSI-based, 34–36
JBOD, 27, 29–33, 40
layers, 30
management, 28, 32–33
Microsoft's vision for, 29
migration, 6
of SSL certificates, 154
Quality of Service (QoS), 33–34
snapshot, 6
tiered, 33, 43–44
traditional versus WFS cluster, 40
Work Folders, 50–59
Storage Management API (SM-API), 32–33
storage pools, 27, 30, 39, 41
creating, 45–46
storage spaces
in storage pools, 27
rebuilding, 44
Storage Spaces, 39–49
benefits of, 39–40
capacity versus performance in, 41–42
cluster-shared volumes and, 73
compared to SAN-based storage, 40
data tiering, 42–44
dual parity, 44–49
in Windows Server 2012, 27, 40–42
in Windows Server 2012 R2, 42–49
Scale-Out File Servers (SoFS), 30–31, 33
storage resiliency and parity using, 30
write-back cache feature, 33, 43–44
storage tiers, 43–44
storage volumes. *See* LUNs
Switch Dependent teaming mode, 94–95
Switch Independent teaming mode, 91–94
switches, network, 119–121
sync share
device policies for, 57
names, 56
purpose of, 53–55
security groups for access, 56–57
sharing files with, 57–59
user folder structure, 55
Sync Your Settings, 145
synchronization, data, 50–51
System Center, 2–3, 31–32
System Center Virtual Machine Manager (VMM), 31–33, 107–108

T

TCP/IP cmdlets, 196
testing
connectivity, 102–105, 191
network adapters, 97–101
thin provisioning, 40
third-party extensions, 6, 121
third-party solutions
iSCSI-based storage and, 35
touch functionality, 209, 213
traffic, network, 116–118, 121

troubleshooting
network connections, 96–105
network tracing, 121
trunk mode, 120

U

UEFI (Unified Extensible Firmware Interface), 7
Unified Extensible Firmware Interface (UEFI), 7
Unix, 20
updates
failover cluster nodes, 64
Group Policy, 137
usage mode, 49
user aliases, 55
user group management, 206
users, use of Work Folders, 50–51

V

VHDX format, 6, 36
video drivers, 20
video experience, 168
virtual desktop interface, 172
virtual disks
dual parity and parity space support for, 44–49
guest clustering using shared, 65–67, 69–70
shared, 67–68
tiered storage, 44
virtual hard disks
resizing of, 17–18, 20
Virtual Machine Connection (VM Connect), 12–14
Virtual Machine Manager (VMM), 31–33, 107–108
Virtual Machine Queue (VMQ), 85
virtual machines
automatic activation of, 11–12
bandwidth management, 37–38
connectivity, 102–105, 191
debugging, 192–195
draining nodes prior to shutdown, 78–80
file shares, 6
firmware configuration, 191
generation options for, 9–10
health monitoring, 75–78
importation, 6
licensing, 11–12
live export, 18–19
maintaining availability, 78–80
networks, 113–115
remote access to, 12–14
replication, 7, 21–24
virtual Receive Side Scaling (vRSS), 88–90
virtual resources
separating from physical infrastructure, 65–67
virtualization. *See also* Hyper-V
in Windows Server Essentials 2012 R2, 204
network, 87, 113–114
of storage resources, 30
Windows PowerShell 4.0 cmdlets, 197
VLANs, 120
VM Connect, 12–14
vm2dmp.exe tool, 193
VMBus, 12–14
VMM (System Center Virtual Machine Manager), 31–33, 107–108
VMQ (Virtual Machine Queue), 85
vRSS (virtual Receive Side Scaling), 88–90

W

Wait and Verbose switches, 182
Web Application Proxy, 127–131
Web Services Management (WSMAN) devices, 198
WFP (Windows Filtering Platform), 116
WinDbg, 193
Windows 8, 7, 209–212
Windows Activation Service, 155
Windows Azure, 2–3, 20
Windows Azure Active Directory, 206
Windows Azure Backup, 20, 207
Windows Azure Hyper-V Recovery Manager, 23–24
Windows Filtering Platform (WFP), 116
Windows Hardware Certification Kit (HCK), 191
Windows Intune, 207
Windows Management Framework, 175
Windows NIC Teaming. *See* NIC Teaming
Windows Phone, 209–212
Windows PowerShell. *See* PowerShell
Windows PowerShell Workflow, 176
Windows Runtime, 149–150
Windows Search, 201
cmdlets, 201

Windows Server 2012
Active Directory enhancements in, 124
Failover clustering enhancements in, 63–64
Group Policy enhancements in, 137–138
Hyper-V enhancements in, 5–7
Hyper-V Virtual Switch in, 119–121
IIS 8.0 enhancements in, 153–155
IP Address Management (IPAM), 107
network adapters in, 97–101
network diagnostics, 97–101
networking enhancements in, 85–88
NIC Teaming in, 91
PowerShell enhancements in, 175–176
Remote Desktop Services (RDS) enhancements in, 165–167
storage enhancements in, 27–29
Storage Spaces in, 27, 40–42
Windows Server 2012 R2
Hyper-V, 7–25
Hyper-V Network Virtualization enhancements in, 115–118
Hyper-V Virtual Switch, 121
IP Address Management (IPAM), 107–112
network diagnostics, 102–105
policy settings, 142
Windows Server and cloud computing, 2–3
Windows Server Database Edition, 207–209
Windows Server Essentials 2012, 203
Windows Server Essentials 2012 R2, 203–214
Dashboard, 205–207
Experience server role, 207–209
features of, 203–214
in cloud computing, 204–205
versions, 203
virtualization in, 204
Windows Server Gateway (WSG), 116–118
Windows Server Standard Edition, 207–209
Windows SkyDrive, 52, 151–152
Windows Store apps, 150
Windows Update, 149
Work Folders, 50–59
comparison to other data sync solutions, 52
data synchronization, 53–59
functionality, 51
Group Policy settings for, 145–146
implementing, 52
installing, 52–59
Kerberos authentication, 146–148
naming, 55
testing, 59
versus Windows SkyDrive, 52
worker processes, idle, 156–157
workflows, 176
workloads, 64–65, 72
Workplace Join, 125–126
write-back cache, 43–44
WSG (Windows Server Gateway), 116–118
WSMAN (Web Services Management) devices, 198

About the author

MITCH TULLOCH is a well-known expert on Windows Server administration and virtualization. He has published hundreds of articles on a wide variety of technology sites and has written or contributed to over two dozen books, including the *Windows 7 Resource Kit* (Microsoft Press, 2009), for which he was lead author; *Understanding Microsoft Virtualization Solutions: From the Desktop to the Datacenter* (Microsoft Press, 2010); and *Introducing Windows Server 2012* (Microsoft Press, 2012), a free e-book that has been downloaded almost three quarters of a million times.

Mitch has been repeatedly awarded Most Valuable Professional (MVP) status by Microsoft for his outstanding contributions to supporting the global IT community. He is a nine-time MVP in the technology area of Windows Server Software Packaging, Deployment & Servicing. You can find his MVP Profile page at *http://mvp.microsoft.com/en-us/mvp/Mitch%20Tulloch-21182*.

Mitch is also Senior Editor of WServerNews (*http://www.wservernews.com*), a weekly newsletter focused on system admin and security issues for the Windows Servers platform. With more than 100,000 IT Pro subscribers worldwide, WServerNews is the largest Windows Server–focused newsletter in the world.

Mitch runs an IT content development business based in Winnipeg, Canada that produces white papers and other collateral for the business decision maker (BDM) and technical decision maker (TDM) audiences. His published content ranges from white papers about Microsoft cloud technologies to reviews of third-party products designed for the Windows Server platform. Before starting his own business in 1998. Mitch worked as a Microsoft Certified Trainer (MCT) for Productivity Point.

For more information about Mitch, visit his website at *http://www.mtit.com*.

You can also follow Mitch on Twitter at *http://twitter.com/mitchtulloch* or like him on Facebook at *http://www.facebook.com/mitchtulloch*

Now that you've read the book...

Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was there room for improvement?

Let us know at http://aka.ms/tellpress

Your feedback goes directly to the staff at Microsoft Press, and we read every one of your responses. Thanks in advance!

Microsoft

Secrets of PowerShell Remoting

Secrets of PowerShell Remoting

PowerShell.org

This project can be followed at:

https://www.penflip.com/powershellorg/secrets-of-powershell-remoting

©2015 PowerShell.org

Contents

1 Secrets of PowerShell Remoting

Principle author: Don Jones
Contributing author: Dr. Tobias Weltner
With contributions by Dave Wyatt and Aleksandar Nikolik
Cover design by Nathan Vonnahme

Introduced in Windows PowerShell 2.0, Remoting is one of PowerShell's most useful, and most important, core technologies. It enables you to run almost any command that exists on a remote computer, opening up a universe of possibilities for bulk and remote administration. Remoting underpins other technologies, including Workflow, Desired State Configuration, certain types of background jobs, and much more. This guide isn't intended to be a complete document of what Remoting is and does, although it does provide a good introduction. Instead, this guide is designed to document all the little configuration details that don't appear to be documented elsewhere.

Visit *www.penflip.com/powershellorg* to check for newer editions of this e-book.

This guide is released under the Creative Commons Attribution-NoDerivs 3.0 Unported License. The authors encourage you to redistribute this file as widely as possible, but ask that you do not modify the document.

PowerShell.org eBooks are works-in-progress, and many are curated by members of the community. We encourage you to check back for new editions at least twice a year, by visiting *www.penflip.com/powershellorg*.

You can download this book in a number of different formats (including EPUB, PDF, Microsoft Word and Plain Text) by clicking **Download** on the right side of the page.

PDF Users: Penflip's PDF export often doesn't include the entire ebook content. We've reported this problem to them; in the meantime, please consider using a different format, such as EPUB, when you're downloading the book.

You may register to make corrections, contributions, and other changes to the text - we welcome your contributions! However, we recommend you check out our contributor tips and notes before jumping in.

You may also subscribe to our monthly e-mail TechLetter for notifications of updated e-book editions. Visit PowerShell.org for more information on the newsletter.

2 Remoting Basics

Windows PowerShell 2.0 introduced a powerful new technology, Remoting, which was refined and expanded upon for PowerShell 3.0. Based primarily upon standardized protocols and techniques, Remoting is possibly one of the most important aspects of PowerShell: future Microsoft products will rely upon it almost entirely for administrative communications across a network.

Unfortunately, Remoting is also a complex set of components, and while Microsoft has attempted to provide solid guidance for using it in a variety of scenarios, many administrators still struggle with it. This "mini e-book" is designed to help you better understand what Remoting is, how it works, and-most importantly-how to use it in a variety of different situations.

Note This guide isn't meant to replace the myriad of existing books that cover Remoting basics, such as Don's own *Learn Windows PowerShell in a Month of Lunches* (http://MoreLunches.com) or *PowerShell in Depth*. Instead, this guide supplements those by providing step-by-step instructions for many of the "edge" cases in Remoting, and by explaining some of the more unusual Remoting behaviors and requirements.

What is Remoting?

In essence, Remoting enables you to access remote machines across a network and retrieve data from or execute code on one or many remote computers. This is not a new idea, and in the past a number of different remoting technologies have evolved. Some cmdlets have traditionally provided their own limited remoting capabilities while the majority of cmdlets do not support remoting on their own.

With PowerShell remoting there is finally a generic remoting environment that allows remote execution for literally any command that can run in a local PowerShell. So instead of adding remoting capabilities to every single cmdlet and application, you simply leave it to PowerShell to transfer your PowerShell code to the target computer(s), execute it there, and then marshal back the results to you.

Throughout this eBook, we will focus on PowerShell remoting and not cover non-standard private remoting capabilities built into selected cmdlets.

Examining Remoting Architecture

As shown in figure 1.1, PowerShell's generic Remoting architecture consists of numerous different, interrelated components and elements.

Figure 1.1: The elements and components of PowerShell Remoting

Here is the complete list:

At the bottom of the figure is your computer, or more properly your client. This is where you physically sit, and it's where you'll initiate most of your Remoting activities.

Your computer will communicate via the WS-MAN, or Web Services for Management, protocol. This is an HTTP(S)-based protocol that can encapsulate a variety of different communications. We've illustrated this as using HTTP, which is Remoting's default configuration, but it could just as easily be HTTPS.

On the remote computer, in the proper terminology the server (which does not refer to the operating system), the Windows Remote Management (WinRM) service runs. This service is configured to

have one or more listeners. Each listener waits for incoming WS-MAN traffic on a specific port, each bound to a specific protocol (HTTP or HTTPS), and on specific IP addresses (or all local addresses).

When a listener receives traffic, the WinRM service looks to see which endpoint the traffic is meant for. For our purposes, an endpoint will usually be launching an instance of Windows PowerShell. In PowerShell terms, an endpoint is also called a session configuration. This is because, in addition to launching PowerShell, it can auto-load scripts and modules, place restrictions upon what can be done by the connecting user, and apply additional session specific settings not mentioned here.

Note Although we show **PowerShell.exe** in our diagram, that's for illustration purposes. **PowerShell.exe** is the PowerShell console application, and it would not make sense to have this running as a background process on a remote computer. The actual process is called **Wsmprovhost.exe**, which hosts PowerShell in the background for Remoting connections.

As you can see, a single remote computer can easily have dozens or even hundreds of endpoints, each with a different configuration. PowerShell 3.0 sets up three such endpoints by default: One for 32-bit PowerShell (on 64-bit systems), the default PowerShell endpoint (which is 64-bit on x64 systems), and one for PowerShell Workflow. Beginning with Windows Server 2008 R2, there is a fourth default endpoint for Server Manager Workflow tasks.

Enabling Remoting

Most client versions of Windows, beginning Windows Vista, do not enable incoming Remoting connections by default. Newer Windows Server versions do, but older versions may not. So your first step with Remoting will usually be to enable it on those computers which you want to receive incoming connections. There are three ways to enable Remoting, and table 1.1 compares what is achievable with each of them.

Table 1.1 Comparing the ways of enabling remoting

	Enable-PSRemoting	Group Policy
Set WinRM to auto-start and start the service	Yes	Yes
Configure HTTP listener	Yes	You can configure auto-registration of listener
Configure HTTPS listener	No	No
Configure endpoints / session configurations	Yes	No
Configure Windows Firewall exception	Yes*	Yes*

Note Existing client versions of Windows, such as Windows Vista, do not permit firewall exceptions on any network identified as "Public". Networks must either be "Home" or "Work/Domain" in order to permit exceptions. In PowerShell 3.0, you can run **Enable-PSRemoting** with the **-SkipNetworkProfileCheck** switch to avoid this problem.

We'll be enabling Remoting in our test environment by running **Enable-PSRemoting**. It's quick, easy, and comprehensive; you'll also see most of the manual tasks performed in the upcoming sections.

Test Environment

We'll be using a consistent test environment throughout the following sections; this was created on six virtual machines at *CloudShare.com*, and is configured as shown in figure 1.2.

Figure 1.2: Test environment configuration

Some important notes:

.NET Framework v4 and PowerShell 3.0 is installed on all computers. Most of what we'll cover also applies to PowerShell 2.0.

As shown, most computers have a numeric computer name (C2108222963, and so on); the domain controller for each domain (which is also a DNS server) has CNAME records with easier-to-remember names.

Each domain controller has a conditional forwarder set up for the other domain, so that machines in either domain can resolve computer names in the other domain.

We performed all tasks as a member of the Domain Admins group, unless noted otherwise.

We created a sixth, completely standalone server that isn't in any domain at all. This will be useful for covering some of the non-domain situations you can find yourself in with Remoting.

Caution When opening PowerShell on a computer that has User Account Control (UAC) enabled, make sure you right-click the PowerShell icon and select **Run as Administrator**. If the resulting PowerShell window's title bar doesn't begin with **Administrator:** then you do not have administrative privileges. You can check permissions programmatically with this *(whoami /all | select-string S-1-16-12288) -ne $null* from the PowerShell console. In an elevated shell it **True** is returned, otherwise **False** is.

Enabling Remoting

We began by running Enable-PSRemoting on all six computers. We took care to ensure that the command ran without error; any errors at this point are a signal that you must stop and resolve the error before attempting to proceed. Figure 1.3 shows the expected output.

Figure 1.3: Expected output from Enable-PSRemoting

Note: You'll notice profligate use of screen shots throughout this guide. It helps ensure that I don't make any typos or copy/paste errors - you're seeing exactly what we typed and ran.

Running Get-PSSessionConfiguration should reveal the three or four endpoints created by Enable-PSRemoting. Figure 1.4 shows the expected output on a server.

```
Administrator: Windows PowerShell (3)
    1. Starting or restarting (if already started) the WinRM service
    2. Setting the WinRM service startup type to Automatic
    3. Creating a listener to accept requests on any IP address
    4. Enabling Windows Firewall inbound rule exceptions for WS-Management traffic (for http only).

Do you want to continue?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): a
WinRM has been updated to receive requests.
WinRM service started.

WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.


Confirm
Are you sure you want to perform this action?
Performing operation "Set-PSSessionConfiguration" on Target "Name: microsoft.powershell SDDL:
O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD). This will allow selected users to remotely run Windows
PowerShell commands on this computer".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): a
PS C:\Users\Administrator> Get-PSSessionConfiguration


Name          : microsoft.powershell
PSVersion     : 3.0
StartupScript :
RunAsUser     :
Permission    : BUILTIN\Administrators AccessAllowed

Name          : microsoft.powershell.workflow
PSVersion     : 3.0
StartupScript :
RunAsUser     :
Permission    : BUILTIN\Administrators AccessAllowed

Name          : microsoft.powershell32
PSVersion     : 3.0
StartupScript :
RunAsUser     :
Permission    : BUILTIN\Administrators AccessAllowed

Name          : microsoft.ServerManager
PSVersion     : 2.0
StartupScript :
RunAsUser     :
Permission    : BUILTIN\Administrators AccessAllowed


PS C:\Users\Administrator>
```

Figure 1.4: Expected output from Get-PSSessionConfiguration

Note: Figure 1.4 illustrates that you can expect different endpoints to be configured on different machines. This example was from a Windows Server 2008 R2 computer, which has fewer endpoints than a Windows 2012 machine.

It's worth taking a moment to quickly test the Remoting configuration. For computers that are all part of the same domain, when you're logged on as a Domain Admin from that domain, Remoting should "just work." Quickly check it by attempting to remote from one computer to another using Enter-PSSession.

Note: In other environments, a Domain Admin account may not be the only account that can use Remoting. If your home or work environment has additional accounts in the local Administrators group as standard across your domain, you will also be able to use these accounts for Remoting.

Figure 1.5 shows the expected output, in which we also ran a quick Dir command and then exited the remote session.

```
Administrator: Windows PowerShell

PS C:\Users\Administrator.COMPANY> cd \
PS C:\> Enter-PSSession -ComputerName DCA
[DCA]: PS C:\Users\Administrator\Documents> dir
[DCA]: PS C:\Users\Administrator\Documents> cd \
[DCA]: PS C:\> dir


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         7/13/2009   8:20 PM            PerfLogs
d-r--          4/7/2012   8:33 AM            Program Files
d-r--          4/7/2012   8:33 AM            Program Files (x86)
d----         8/25/2010   8:45 AM            Python26
d-r--          4/6/2012   2:43 AM            Users
d----          4/8/2012   8:40 AM            Windows


[DCA]: PS C:\> Exit-PSSession
PS C:\>
```

Figure 1.5: Checking remoting connectivity from COMPANY.loc's CLIENTA to the DCA domain controller.

Caution: If you're following along in your own test environment, don't proceed until you've confirmed Remoting connectivity between two computers in the same domain. No other scenario needs to work right now; we'll get to them in the upcoming sections.

Core Remoting Tasks

PowerShell provides for two principal Remoting use cases. The first, 1-to-1 Remoting, is similar in nature to the SSH secure shell offered on UNIX and Linux systems. With it, you get a command-line prompt on a single remote computer. The second, 1-to-Many Remoting, enables you to send a command (or a list of commands) in parallel to a set of remote computers. There are also a couple of useful secondary techniques we'll look at.

1-to-1 Remoting

The Enter-PSSession command connects to a remote computer and gives you a command-line prompt on that computer. You can run whatever commands are on that computer, provided you have permission to perform that task. Note that you are not creating an interactive logon session; your connection will be audited as a network logon, just as if you were connecting to the computer's C$

administrative share. PowerShell will not load or process profile scripts on the remote computer. Any scripts that you choose to run (and this includes importing script modules) will only work if the remote machine's Execution Policy permits it.

Enter-PSSession -computerName DC01

Note: While connected to a remote machine via Enter-PSSession, your prompt changes and displays the name of the remote system in square brackets. If you have customized your prompt, all customizations will be lost because the prompt is now created on the remote system and transferred back to you. All of your interactive keyboard input is sent to the remote machine, and all results are marshaled back to you. This is important to note because you cannot use Enter-PSSession in a script. If you did, the script would still run on your local machine since no code was entered interactively.

1-to-Many Remoting

With this technique, you specify one or more computer names and a command (or a semicolon-separated list of commands); PowerShell sends the commands, via Remoting, to the specified computers. Those computers execute the commands, serialize the results into XML, and transmit the results back to you. Your computer deserializes the XML back into objects, and places them in the pipeline of your PowerShell session. This is accomplished via the Invoke-Command cmdlet.

```
Invoke-Command -computername DC01,CLIENT1 -scriptBlock { Get-Service }
```

If you have a script of commands to run, you can have Invoke-Command read it, transmit the contents to the remote computers, and have them execute those commands.

```
Invoke-Command -computername DC01,CLIENT1 -filePath c:\Scripts\Task.ps1
```

Note that Invoke-Command will, by default, communicate with only 32 computers at once. If you specify more, the extras will queue up, and Invoke-Command will begin processing them as it finishes the first 32. The -ThrottleLimit parameter can raise this limit; the only cost is to your computer, which must have sufficient resources to maintain a unique PowerShell session for each computer you're contacting simultaneously. If you expect to receive large amounts of data from the remote computers, available network bandwidth can be another limiting factor.

Sessions

When you run Enter-PSSession or Invoke-Command and use their -ComputerName parameter, Remoting creates a connection (or session), does whatever you've asked it to, and then closes the connection (in the case of an interactive session created with Enter-PSSession, PowerShell knows you're done when you run Exit-PSSession). There's some overhead involved in that set-up and tear-down, and so PowerShell also offers the option of creating a persistent connection - called a PSSession. You run New-PSSession to create a new, persistent session. Then, rather than using -ComputerName with Enter-PSSession or Invoke-Command, you use their -Session parameter and pass an existing, open PSSession object. That lets the commands re-use the persistent connection you'd previously created.

When you use the -ComputerName parameter and work with ad-hoc sessions, each time you send a command to a remote machine, there is a significant delay caused by the overhead it takes to create a new session. Since each call to Enter-PSSession or Invoke-Command sets up a new session, you also cannot preserve state. In the example below, the variable $test is lost in the second call:

```
PS> Invoke-Command -computername CLIENT1 -scriptBlock { $test = 1 }
PS> Invoke-Command -computername CLIENT1 -scriptBlock { $test }
PS>
```

When you use persistent sessions, on the other hand, re-connections are much faster, and since you are keeping and reusing sessions, they will preserve state. So here, the second call to Invoke-Command will still be able to access the variable $test that was set up in the first call

```
PS> $Session = New-PSSession -ComputerName CLIENT1
PS> Invoke-Command -Session $Session -scriptBlock { $test = 1 }
PS> Invoke-Command -Session $Session -scriptBlock { $test }
1
PS> Remove-PSSession -Session $Session
```

Various other commands exist to check the session's status and retrieve sessions (Get-PSSession), close them (Remove-PSSession), disconnect and reconnect them (Disconnect-PSSession and Reconnect-PSSession, which are new in PowerShell v3), and so on. In PowerShell v3, you can also pass an open session to Get-Module and Import-Module, enabling you to see the modules listed on a remote computer (via the opened PSSession), or to import a module from a remote computer into your computer for implicit Remoting. Review the help on those commands to learn more.

Note: Once you use New-PSSession and create your own persistent sessions, it is your responsibility to do housekeeping and close and dispose the session when you are done with them. Until you do that, persistent sessions remain active, consume resources and may prevent others from connecting. By default, only 10 simultaneous connections to a remote machine are permitted. If you keep too many active sessions, you will easily run into resource limits. This line demonstrates what happens if you try and set up too many simultaneous sessions:

```
PS> 1..10 | Foreach-Object { New-PSSession -ComputerName CLIENT1 }
```

Remoting Returns Deserialized Data

The results you receive from a remote computer have been serialized into XML, and then deserialized on your computer. In essence, the objects placed into your shell's pipeline are static, detached snapshots of what was on the remote computer at the time your command completed. These deserialized objects lack the methods of the originals objects, and instead only offer static properties.

If you need to access methods or change properties, or in other words if you must work with the live objects, simply make sure you do so on the remote side, before the objects get serialized and travel back to the caller. This example uses object methods on the remote side to determine process owners which works just fine:

```
PS> Invoke-Command -ComputerName CLIENT1 -scriptBlock { Get-WmiObject -Class
    Win32\_Process | Select-Object Name, { $\_.GetOwner().User } }
```

Updated for Server 2012 R2

William Panek

MCSA

Windows Server 2012 R2

COMPLETE STUDY GUIDE

EXAM 70-410
EXAM 70-411
EXAM 70-412
EXAM 70-417

Includes Real-World Scenarios, Hands-On Exercises, and Access to Exam Prep Software Featuring:

+ **Custom Test Engine**
+ **Over 300 Sample Questions**
+ **Electronic Flashcards**

SYBEX
A Wiley Brand

MCSA

Windows Server® 2012 R2

Complete Study Guide

MCSA

Windows Server® 2012 R2

Complete Study Guide

William Panek

SYBEX®
A Wiley Brand

Senior Acquisitions Editor: Jeff Kellum
Development Editor: Gary Schwartz
Technical Editors: Rodney Fournier and Michael Rice
Production Editor: Eric Charbonneau
Copy Editor: Kim Wimpsett
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Professional Technology and Strategy Director: Barry Pruett
Associate Publisher: Jim Minatel
Media Project Manager 1: Laura Moss-Hollister
Media Associate Producer: Marilyn Hummel
Media Quality Assurance: Josh Frank
Book Designer: Judy Fung
Proofreader: Josh Chase, Word One New York
Indexer: Ted Laux
Project Coordinator, Cover: Patrick Redmond
Cover Designer: Wiley

Copyright © 2015 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-118-85991-9

ISBN: 978-1-118-85969-8 (ebk.)

ISBN: 978-1-118-85990-2 (ebk.)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at `www.wiley.com/go/permissions`.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at `http://booksupport.wiley.com`. For more information about Wiley products, visit `www.wiley.com`.

Library of Congress Control Number: 2014948559

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. Windows Server is a registered trademark of Microsoft Corporation. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *MCSA: Windows Server 2012 R2 Complete Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at `contactus@sybex.com`. If you think you've found a technical error in this book, please visit `http://sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,

Chris Webb
Associate Publisher
Sybex, an Imprint of Wiley

This book is dedicated to the three ladies of my life:
—Crystal, Alexandria, and Paige.

Acknowledgments

I would like to thank my wife and best friend, Crystal. She is always the light at the end of my tunnel. I want to thank my two daughters, Alexandria and Paige, for all of their love and support during the writing of all my books. They make it all worthwhile.

I want to thank my family, and especially my brothers, Rick, Gary, and Rob. They have always been there for me. I want to thank my father, Richard, who helped me become the man I am today, and my mother, Maggie, for all of her love and support.

I would like to thank all of my friends and co-workers, especially Vic, Catherine, Jeff, Stephanie, Don, Jason, Doug, Dave, Steve, Pat, Mike (all of them), Tommy, George, Greg, Becca, Deb, Jeri, Lisa, Scotty, and all of the field guys. I want to also thank my team and everyone who works with my group including Moe, Jimmy, Paul, Dana, Dean, Reanna, Todd, and Will F. Because of all of your hard work, you make me look good every day and make it a pleasure to go to work. Thanks to all of you for everything that you do.

I want to thank everyone on my Sybex team, especially my development editor, Gary Schwartz, who helped me make this the best book possible, and Rodney R. Fournier, who is the technical editor of many of my books. It's always good to have the very best technical guy backing you up.

I want to also thank Mike Rice, Winston McMiller, and Jeff Stokes for helping me update some of my chapters from Windows Server 2012 to Windows Server 2012 R2. Their hard work and knowledge helped finish this huge undertaking.

I want to thank Eric Charbonneau, who was my production editor, and my acquisitions editor, Jeff Kellum, who served as lead for the entire book. He has always been there for me, and it is always great to write for him.

Finally, I want to thank everyone else behind the scenes who helped make this book possible. It's truly an amazing thing to have so many people work on my books to help make them the very best. I can't thank you all enough for your hard work.

About the Authors

William Panek holds the following certifications: MCP, MCP+I, MCSA, MCSA+ Security and Messaging, MCSE-NT (3.51 and 4.0), MCSE 2000 and 2003, MCSE+Security and Messaging, MCDBA, MCT, MCTS, MCITP, CCNA, and CHFI. Will is also a two time Microsoft MVP (he won in October 2013 and October 2014).

After many successful years in the computer industry and a degree in computer programming, Will decided that he could better use his talents and his personality as an instructor. He began teaching for schools such as Boston University, Clark University, and the University of Maryland, just to name a few. He has done consulting and training work for some of the biggest government and corporate companies in the world including the U.S. Secret Service, Cisco, the U.S. Air Force, and the U.S. Army.

In 2012, Will became the Director of IT for Green Mountain Communications. He currently lives in New Hampshire with his wife and two daughters. Will was also a Representative in the New Hampshire House of Representatives from 2010 to 2012. In his spare time, he likes to golf, ski, shoot, and go snowmobiling. Will is also a commercially rated helicopter pilot.

Michael Allen Rice holds these certifications: MCP, MCTS, MCSA, MCSE, MCITP, CompTIA Network+, CompTIA Security+, VMware Certified Professional 5 - DCV, and NetApp Certified Data Management Administrator 7-mode.

Michael currently works as a Data Center Administrator for Intelligent Software Solutions, Inc., based in Colorado Springs. He lives there with his wife and two children. He specializes in leading the way for corporate infrastructure in the areas of virtualization, storage, and systems administration. Over the past decade as an IT professional, Michael has received numerous awards for his outstanding performance and dedication to excellence within the IT community.

Winston McMiller holds these certifications: MCP, MCP+I, MCSA, MCSE 2000, 2003, 2012/2012 R2, and ITIL. Winston is a Microsoft Premier Field Engineer.

After 18 years in the computer industry and a degree in information technology, Winston has done consulting and training for some of the largest companies in the world including General Electric, HP Enterprise services, Chrysler, and IBM.

He currently lives in the Seattle area. In his spare time, he likes to ski, do photography, and travel. He is an avid audiophile and songwriter.

Jeff Stokes holds these certifications: MCT, MCSA, MCSE 2003, and MCTS: Windows Internals. Jeff Stokes runs `@WindowsPerf`, a Windows Performance social networking property. He is a frequent guest on RunAsRadio and an avid blogger.

As a previous Premier Field Engineer at Microsoft, Jeff has worked in the Fortune 1000 space for the last eight years. After 21 years in the IT field, Jeff has established himself as a performance SME and a VDI pioneer in Microsoft technologies, including Windows optimization as a VDI guest. His work appears in VDI optimization guidance papers from Microsoft and other parties.

He currently lives in the Atlanta area. In his spare time, he analyzes performance traces, games, and mentors others in the IT field.

Contents at a Glance

Introduction *xxxix*

Assessment Test *lxi*

Part I **Exam 70-410: Installing and Configuring Windows Server 2012 R2** **1**

Chapter 1 Install Windows Server 2012 R2 3

Chapter 2 Configure Network Services 57

Chapter 3 Plan and Install Active Directory 165

Chapter 4 Configure Windows Server 2012 R2 207

Chapter 5 Administer Active Directory 247

Chapter 6 Manage GPOs 297

Chapter 7 Manage Security 357

Chapter 8 Configure TCP/IP 389

Chapter 9 Use Virtualization in Windows Server 2012 439

Part II **Exam 70-411: Administering Windows Server 2012 R2** **473**

Chapter 10 Manage and Maintain Servers 475

Chapter 11 Manage File Services 529

Chapter 12 Configure DNS 555

Chapter 13 Configure Routing and Remote Access 619

Chapter 14 Configure a Network Policy Server Infrastructure 661

Chapter 15 Configure and Manage Active Directory 697

Chapter 16 Configure and Manage Group Policy 751

Part III **Exam 70-412: Configuring Advanced Windows Server 2012 R2 Services** **817**

Chapter 17 Configure and Manage High Availability 819

Chapter 18 Configure File and Storage Solutions 857

Chapter 19 Implement Business Continuity and Disaster Recovery 901

Chapter 20 Configure Advanced Network Services 937
Chapter 21 Configure the Active Directory Infrastructure 977
Chapter 22 Configure Access and Information Protection Solutions 1045

Appendix A Answers to Review Questions 1109
Appendix B About the Additional Study Tools 1133
Index *1137*

Contents

Introduction *xxxix*

Assessment Test *lxi*

Part I **Exam 70-410: Installing and Configuring Windows Server 2012 R2** **1**

Chapter 1 **Install Windows Server 2012 R2** **3**

Features and Advantages of Windows Server 2012 and Server 2012 R2 4
Planning the Windows Server 2012 R2 Installation 7
Server Roles in Windows Server 2012 R2 7
Migrating Roles and Features to Windows Server 2012 R2 10
Roles and Features That Have Been Reduced in Windows Server 2012 R2 12
Deciding Which Windows Server 2012 R2 Versions to Use 16
Deciding on the Type of Installation 17
NIC Teaming 21
Installing Windows Server 2012 R2 22
Using Windows Deployment Services 26
Understanding Features On Demand 30
Storage in Windows Server 2012 R2 31
Initializing Disks 31
Configuring Basic and Dynamic Disks 32
Managing Volumes 34
Storage Spaces in Windows Server 2012 R2 35
Redundant Array of Independent Disks 36
Mount Points 40
Microsoft MPIO 41
iSCSI 43
Internet Storage Name Service 46
Fibre Channel 49
Network Attached Storage 50
Virtual Disk Service 50
Summary 52
Exam Essentials 53
Review Questions 54

Chapter 2 Configure Network Services 57

Introducing DNS 58
The Form of an IP Address 59
Understanding Servers, Clients, and Resolvers 64
Understanding the DNS Process 65
Introducing DNS Database Zones 71
Understanding Primary Zones 72
Understanding Secondary Zones 73
Understanding Active Directory Integrated DNS 74
Understanding Stub Zones 75
Global Name Zones 77
Zone Transfers and Replication 77
Advantages of DNS in Windows Server 2012 R2 80
Background Zone Loading 81
Support for IPv6 Addresses 81
Support for Read-Only Domain Controllers 82
DNS Socket Pools 82
DNS Cache Locking 83
DNS Security Extensions 83
DNS Devolution 84
Zone Level Statistics 84
Record Weighting 85
Netmask Ordering 85
DnsUpdateProxy Group 85
Windows PowerShell Support 85
Introducing DNS Record Types 86
Start of Authority Records 86
Name Server Records 87
Host Record 88
Alias Record 89
Pointer Record 89
Mail Exchanger Record 90
Service (SRV) Record 90
Configuring DNS 91
Installing DNS 91
Load Balancing with Round Robin 94
Configuring a Caching-Only Server 94
Setting Zone Properties 95
Configuring Zones for Dynamic Updates 98
Delegating Zones for DNS 100
DNS Forwarding 101
Manually Creating DNS Records 102
DNS Aging and Scavenging 103
Monitoring and Troubleshooting DNS 104

Monitoring DNS with the DNS Snap-In 105
Troubleshooting DNS 107
Overview of DHCP 116
Introducing the DORA Process 116
Advantages and Disadvantages of DHCP 118
Ipconfig Lease Options 119
Understanding Scope Details 120
Installing and Authorizing DHCP 122
Installing DHCP 122
Introducing the DHCP Snap-In 125
Authorizing DHCP for Active Directory 126
Creating and Managing DHCP Scopes 128
Creating a New Scope in IPv4 129
Creating a New Scope in IPv6 136
Changing Scope Properties (IPv4 and IPv6) 138
Changing Server Properties 140
Managing Reservations and Exclusions 143
Setting Scope Options for IPv4 146
Activating and Deactivating Scopes 149
Creating a Superscope for IPv4 149
Creating IPv4 Multicast Scopes 151
Integrating Dynamic DNS and IPv4 DHCP 153
Using Multiple DHCP Servers 155
Working with the DHCP Database Files 156
Summary 158
Exam Essentials 159
Review Questions 161

Chapter 3 Plan and Install Active Directory 165

Verifying the File system 166
Resilient File System (ReFS) 167
NTFS 168
Verifying Network Connectivity 171
Basic Connectivity Tests 171
Tools and Techniques for Testing Network Configuration 172
Understanding Domain and Forest Functionality 174
About the Domain Functional Level 174
About Forest Functionality 176
Planning the Domain Structure 178
Installing Active Directory 179
Adprep 179
Active Directory Prerequisites 179
The Installation Process 180

Deploying Active Directory IaaS in Windows Azure 189
Verifying Active Directory Installation 190
Using Event Viewer 190
Using Active Directory Administrative Tools 192
Testing from Clients 193
Creating and Configuring Application Data Partitions 195
Creating Application Data Partitions 196
Managing Replicas 198
Removing Replicas 198
Using *ntdsutil* to Manage Application Data Partitions 198
Configuring DNS Integration with Active Directory 201
Summary 203
Exam Essentials 203
Review Questions 204

Chapter 4 Configure Windows Server 2012 R2 207

Understanding File Servers 208
Configuring File Servers 209
Sharing Folders 209
Making Active Directory Objects Available to Users 210
Access-Based Enumeration 212
Configuring Offline Files 212
Volume Shadow Copy Services 215
Configuring Permissions 218
Configuring Disk Quotas 224
Configuring Print Services 226
Creating and Publishing Printers 226
Configuring Printers 228
Migrating Print Servers 232
Printer Pooling 233
Easy Print Driver 233
Configuring Remote Management 233
Windows Remote Management 234
Windows PowerShell 235
Configuring Down-Level Servers 238
Configuring Server Core 239
Summary 241
Exam Essentials 242
Review Questions 244

Chapter 5 Administer Active Directory 247

An Overview of OUs 248
The Purpose of OUs 249
Benefits of OUs 250

Planning the OU Structure 250
Logical Grouping of Resources 250
Understanding OU Inheritance 252
Delegating Administrative Control 253
Applying Group Policies 255
Creating OUs 255
Managing OUs 259
Moving, Deleting, and Renaming OUs 260
Administering Properties of OUs 261
Delegating Control of OUs 263
Troubleshooting OUs 267
Creating and Managing Active Directory Objects 268
Overview of Active Directory Objects 268
Managing Object Properties 275
Understanding Groups 279
Filtering and Advanced Active Directory Features 280
Moving, Renaming, and Deleting Active Directory Objects 282
Resetting an Existing Computer Account 283
Publishing Active Directory Objects 284
Making Active Directory Objects Available to Users 284
Publishing Printers 284
Publishing Shared Folders 286
Querying Active Directory 287
Using the Active Directory Administrative Center 289
Using the Command Prompt for Active Directory Configuration 290
Summary 292
Exam Essentials 292
Review Questions 294

Chapter 6 Manage GPOs 297

Introducing Group Policy 298
Understanding Group Policy Settings 299
The Security Settings Section of the GPO 301
Group Policy Objects 302
Group Policy Inheritance 303
Planning a Group Policy Strategy 304
Implementing Group Policy 305
Creating GPOs 305
Linking Existing GPOs to Active Directory 309
Managing Group Policy 309
Managing GPOs 310
Security Filtering of a Group Policy 311
Delegating Administrative Control of GPOs 313
Controlling Inheritance and Filtering Group Policy 315

Assigning Script Policies 316
Understanding the Loopback Policy 318
Managing Network Configuration 318
Automatically Enrolling User and Computer Certificates in Group Policy 319
Redirecting Folders 322
Managing GPOs with Windows PowerShell Group Policy Cmdlets 324
Deploying Software Through a GPO 324
The Software Management Life Cycle 325
The Windows Installer 326
Deploying Applications 330
Implementing Software Deployment 331
Preparing for Software Deployment 332
Software Restriction Policies 333
Using AppLocker 333
Group Policy Slow Link Detection 333
Publishing and Assigning Applications 334
Applying Software Updates 335
Verifying Software Installation 336
Configuring Automatic Updates in Group Policy 337
Configuring Software Deployment Settings 338
The Software Installation Properties Dialog Box 338
Removing Programs 341
Microsoft Windows Installer Settings 342
Troubleshooting Group Policies 344
RSoP in Logging Mode 345
RSoP in Planning Mode 347
Using the *gpresult.exe* Command 349
Summary 350
Exam Essentials 351
Review Questions 353

Chapter 7 Manage Security 357

Managing Security 358
Understanding Security Principals 358
Managing Security and Permissions 367
Using ACLs and ACEs 369
Configuring User Account Control 370
Delegating Control of Users and Groups 370
Understanding Dynamic Access Control 371
Using Group Policy for Security 372
Implementing an Audit Policy 373
Overview of Auditing 374

Implementing Auditing 374
Using the *Auditpol.exe* Command 376
Features of Windows Server 2012 R2 Auditing 376
Configuring Windows Firewall Options 377
Summary 385
Exam Essentials 385
Review Questions 386

Chapter 8 Configure TCP/IP 389

Understanding TCP/IP 390
Details of the TCP/IP Model 390
How TCP/IP Layers Communicate 391
Understanding Port Numbers 391
Understanding IP Addressing 393
The Hierarchical IP Addressing Scheme 393
Understanding Network Classes 395
Subnetting a Network 398
Implementing Subnetting 400
An Easier Way to Apply Subnetting 406
Applying Subnetting the Traditional Way 410
Working with Classless Inter-Domain Routing 418
Supernetting 421
Understanding IPv6 422
IPv6 History and Need 422
New and Improved IPv6 Concepts 423
IPv6 Addressing Concepts 425
IPv6 Integration/Migration 430
Summary 434
Exam Essentials 435
Review Questions 436

Chapter 9 Use Virtualization in Windows Server 2012 439

Hyper-V Overview 440
What Is Virtualization? 440
Hyper-V Features 441
Hyper-V Architecture 445
Hyper-V Requirements 446
Hyper-V Installation and Configuration 447
Install the Hyper-V Role 447
Hyper-V in Server Manager 450
Using Hyper-V Manager 450
Configure Hyper-V Settings 451
Manage Virtual Switches 453
Managing Virtual Hard Disks 456

Configuring Virtual Machines 461
Creating and Managing Virtual Machines 461
Summary 469
Exam Essentials 469
Review Questions 471

Part II Exam 70-411: Administering Windows Server 2012 R2 473

Chapter 10 Manage and Maintain Servers 475

Using Windows Deployment Services 477
Configuring Windows Server Update Services 484
Windows Update 484
Windows Automatic Updates 485
Using Windows Server Update Services 487
Overview of Windows Server 2012 R2 Performance Monitoring 499
Using Windows Server 2012 R2 Performance Tools 501
Introducing Performance Monitor 501
Using Other Performance-Monitoring Tools 510
Summary 523
Exam Essentials 524
Review Questions 525

Chapter 11 Manage File Services 529

Configuring File Server Resource Manager 530
FSRM Features 530
Installing the FSRM Role Service 531
Configure File and Disk Encryption 532
Using BitLocker Drive Encryption 532
Features of BitLocker 533
Windows 7 and 2008 R2 vs. Windows 8 and 2012 R2 535
Using EFS Drive Encryption 537
Configuring Distributed File System 539
Advantages of DFS 539
Types of DFS 540
What's New in Windows Server 2012 R2 541
Remote Differential Compression 543
Implementing an Audit Policy 543
Overview of Auditing 544
Implementing Auditing 544
Viewing Auditing Information 546
Using the *Auditpol.exe* Command 546
Windows Server 2012 R2 Auditing Features 547

Making Active Directory Objects Available to Users 548
Configuring Offline Folders 549
Summary 551
Exam Essentials 551
Review Questions 552

Chapter 12 Configure DNS 555

Introducing DNS 556
The Form of an IP Address 557
Understanding Servers, Clients, and Resolvers 562
Understanding the DNS Process 563
Introducing DNS Database Zones 569
Understanding Primary Zones 569
Understanding Secondary Zones 571
Understanding Active Directory Integrated DNS 572
Understanding Stub Zones 573
GlobalName Zones 575
Zone Transfers and Replication 575
Advantages of DNS in Windows Server 2012 R2 578
Background Zone Loading 579
Support for IPv6 Addresses 579
Support for Read-Only Domain Controllers 580
DNS Socket Pools 580
DNS Cache Locking 580
DNS Security Extensions 581
DNS Devolution 582
Record Weighting 582
Netmask Ordering 582
DnsUpdateProxy Group 582
Introducing DNS Record Types 583
Start of Authority (SOA) Records 583
Name Server Records 584
Host Record 585
Alias Record 586
Pointer Record 586
Mail Exchanger Record 587
Service Record 587
Configuring DNS 588
Installing DNS 588
Load Balancing with Round Robin 591
Configuring a Caching-Only Server 591
Setting Zone Properties 592
Configuring Zones for Dynamic Updates 595
Delegating Zones for DNS 597
DNS Forwarding 599

Manually Creating DNS Records 599
DNS Aging and Scavenging 600
Monitoring and Troubleshooting DNS 601
Monitoring DNS with the DNS Snap-In 601
Troubleshooting DNS 603
Integrating Dynamic DNS and IPv4 DHCP 612
Summary 614
Exam Essentials 614
Review Questions 616

Chapter 13 Configure Routing and Remote Access 619

Overview of Dial-Up Networking 620
What DUN Does 621
How DUN Works 621
Overview of Virtual Private Networks 625
What VPNs Do 625
VPNs and Windows Server 2012 R2 626
How VPNs Work 626
Configuring Your Remote Access Server 630
Configuring PPP Options 630
Understanding a VPN 634
How VPN Works 634
Enabling RRAS as a VPN 635
Configuring a VPN 636
Configuring VPN Ports 636
Troubleshooting VPNs 637
Managing Your Remote Access Server 638
Managing Remote Users with a RADIUS Server 639
Monitoring Overall Activity 639
Controlling Remote Access Logging 639
Reviewing the Remote Access Event Log 642
Monitoring Ports and Port Activity 643
Network Address Translation 643
Configuring a VPN Client 644
The General Tab 645
The Options Tab 646
The Security Tab 647
The Networking Tab 650
The Sharing Tab 650
Configuring a Web Application Proxy 651
Publishing Applications 651
Configuring Pass-Through Authentication 652
Understanding DirectAccess 653
DirectAccess vs. VPNs 653

Understanding the DirectAccess Process 653
Knowing the DirectAccess Infrastructure Requirements 655
Summary 656
Exam Essentials 656
Review Questions 657

Chapter 14 Configure a Network Policy Server Infrastructure 661

Overview of Wireless Access 662
Configuring Wireless Access 663
Remote Access Security 664
User Authentication 664
Connection Security 666
Access Control 667
Configuring User Access 668
Setting Up User Profiles 668
Using Network Access Policies 670
NPS as a RADIUS Proxy Server 676
Importing and Exporting NPS Policies 678
Using Remote Access Profiles 680
Setting Up a VPN Network Access Policy 685
Configuring Security 687
Controlling Server Security 687
Configuring Network Access Protection 689
Summary 691
Exam Essentials 692
Review Questions 693

Chapter 15 Configure and Manage Active Directory 697

Active Directory Security Overview 699
Understanding Active Directory Features 700
Understanding Security Principals 701
Managing Security and Permissions 711
Using ACLs and ACEs 712
Implementing Active Directory Security 714
Using User Templates 716
Delegating Control of Users and Groups 717
Understanding Dynamic Access Control 719
Using Group Policy for Security 719
Fine-Grained Password Policies 723
Managing Multiple Domains 725
Managing Single-Master Operations 725
Forest Operations Masters 726
Domain Operations Masters 726
Assigning Single-Master Roles 727

Seizing Roles 728
Maintain Active Directory 730
Overview of the Windows Server 2012 R2 Backup Utility 731
Setting Up an Active Directory Backup 736
Restoring Active Directory 739
Active Directory Recycle Bin 741
Restartable Active Directory 742
Offline Maintenance 742
Monitoring Replication 744
Using the ADSI Editor 745
Wbadmin Command Line Utility 745
Summary 746
Exam Essentials 747
Review Questions 748

Chapter 16 Configure and Manage Group Policy 751

Introducing Group Policy Objects 753
Understanding Group Policy Settings 754
The Security Settings Section of the GPO 756
Group Policy Objects 757
Group Policy Inheritance 758
Planning a Group Policy Strategy 759
Implementing Group Policy 760
Creating GPOs 760
Linking Existing GPOs to Active Directory 764
Forcing a GPO to Update 764
Managing Group Policy 766
Managing GPOs 766
Security Filtering of a Group Policy 768
Delegating Administrative Control of GPOs 770
Controlling Inheritance and Filtering Group Policy 771
Assigning Script Policies 773
Understanding the Loopback Policy 774
Managing Network Configuration 775
Automatically Enrolling User and Computer Certificates in Group Policy 776
Redirecting Folders 778
Managing GPOs with Windows PowerShell Group Policy Cmdlets 780
Item-Level Targeting 781
Backup, Restore, Import, Copy, and Migration Tables 782
Deploying Software Through a GPO 785
The Software Management Life Cycle 785

The Windows Installer 787
Deploying Applications 791
Implementing Software Deployment 792
Preparing for Software Deployment 792
Software Restriction Policies 793
Using AppLocker 794
Group Policy Slow Link Detection 794
Publishing and Assigning Applications 794
Applying Software Updates 796
Verifying Software Installation 797
Configuring Automatic Updates in Group Policy 798
Configuring Software Deployment Settings 798
The Software Installation Properties Dialog Box 799
Removing Programs 802
Microsoft Windows Installer Settings 803
Troubleshooting Group Policies 804
RSoP in Logging Mode 805
RSoP in Planning Mode 809
Using the *gpresult.exe* Command 809
Summary 811
Exam Essentials 812
Review Questions 814

Part III Exam 70-412: Configuring Advanced Windows Server 2012 R2 Services 817

Chapter 17 Configure and Manage High Availability 819

Components of High Availability 821
Achieving High Availability 822
High Availability Foundation 822
Configure Network Load Balancing 824
Install NLB Nodes 825
Upgrading an NLB Cluster 830
Achieving High Availability with Failover Clustering 830
Failover Clustering Requirements 831
Cluster Quorum 833
Validating a Cluster Configuration 834
Creating a Cluster 839
Clustered Application Settings 844
Resource Properties 847
Windows Server 2012 R2 Clustering Features 850
Summary 853
Exam Essentials 854
Review Questions 855

Chapter 18 Configure File and Storage Solutions 857

Configure Advanced File Services 858
Configure the NFS Data Store 858
Configure BranchCache 862
Configure File Classification Infrastructure Using File Server Resource Manager 868
Configure File Access Auditing 870
Implement Dynamic Access Control 875
Configure User and Device Claim Types 875
Create and Configure Resource Properties and Lists 879
Create and Configure Central Access Rules and Policies 881
Configure File Classification 884
Implement Policy Changes and Staging 885
Perform Access-Denied Remediation 887
Configure and Optimize Storage 890
Configure iSCSI Target and Initiator 890
Configure Internet Storage Name Server 892
Implement Thin Provisioning and Trim 895
Manage Server Free Space Using Features on Demand 896
Configure Tiered Storage 896
Summary 897
Exam Essentials 897
Review Questions 898

Chapter 19 Implement Business Continuity and Disaster Recovery 901

Protecting the System 902
Backup and Recovery of Active Directory 903
Overview of the Windows Server 2012 R2 Backup Utility 904
Setting Up an Active Directory Backup 909
Restoring Active Directory 913
Active Directory Recycle Bin 914
Restartable Active Directory 915
Offline Maintenance 915
Monitoring Replication 917
Using the ADSI Editor 917
Wbadmin Command-Line Utility 918
Configure Windows Azure Backups 919
Understanding Shadow Copies 921
VssAdmin Command 923
Using Advanced Boot Options 925
Starting in Safe Mode 925
Enabling Boot Logging 926

Using Other Advanced Boot Options Menu Modes 928
Windows Recovery Environment 929
Configure Site-Level Fault Tolerance 929
Using the Startup Repair Tool 932
Summary 933
Exam Essentials 933
Review Questions 934

Chapter 20 Configure Advanced Network Services 937

Working with Advanced DHCP Configuration Options 939
Create and Configure Superscopes 939
Create and Configure Multicast Scopes 940
Implement DHCPv6 943
Configure High Availability for DHCP Including DHCP Failover and Split Scopes 946
Configure DHCP Name Protection 950
Configure DNS Registration 952
The Ins and Outs of DNS 953
DNS Security 953
Configure DNS Logging 956
Configure Delegated Administration 959
Configure Recursion 959
Configure Netmask Ordering 960
Configure a GlobalNames Zone 961
Analyze Zone-Level Statistics 962
IPAM Administration 101 963
Provision IPAM Manually or by Using Group Policy 964
Configure Server Discovery 967
Create and Manage IP Blocks and Ranges 968
Monitor Utilization of IP Address Space 970
Migrate to IPAM 971
Delegate IPAM Administration 971
Manage IPAM Collections 972
Configure IPAM Database Storage 972
Summary 973
Exam Essentials 973
Review Questions 974

Chapter 21 Configure the Active Directory Infrastructure 977

Overview of Network Planning 979
The Three Types of Networks 980
Exploring Network Constraints 980
Overview of Active Directory Replication and Sites 981

Replicating Active Directory 981
Understanding Active Directory Site Concepts 982
Understanding Distributed File System Replication 986
Implementing Sites and Subnets 987
Creating Sites 988
Creating Subnets 991
Configuring Sites 993
Configuring Replication 994
Intrasite Replication 995
Intersite Replication 995
RODCs and Replication 1002
Configuring Server Topology 1003
Using Universal Group Membership Caching 1006
Monitoring and Troubleshooting Active Directory Replication 1007
About System Monitor 1007
Troubleshooting Replication 1007
Reasons for Creating Multiple Domains 1010
Reasons for Using Multiple Domains 1010
Drawbacks of Multiple Domains 1012
Creating Domain Trees and Forests 1013
Planning Trees and Forests 1013
The Promotion Process 1017
Creating a Domain Tree 1017
Joining a New Domain Tree to a Forest 1023
Adding Additional Domain Controllers 1024
Demoting a Domain Controller 1024
Managing Multiple Domains 1026
Managing Single-Master Operations 1026
Forest Operations Masters 1026
Domain Operations Masters 1027
Assigning Single-Master Roles 1028
Managing Trusts 1029
Managing UPN Suffixes 1033
Name Suffix Routing 1034
Managing Global Catalog Servers 1034
Managing Universal Group Membership Caching 1035
Upgrading Existing Domains and Forests 1036
Summary 1037
Exam Essentials 1038
Review Questions 1041

Chapter 22 Configure Access and Information Protection Solutions 1045

What's New in Windows Server 2012 R2 with Active Directory Certificate Services? 1047
Active Directory Certificate Services Roles 1048
Planning the Certificate Authority Hierarchy 1049
Installing AD CS 1055
Configuring Active Directory Certificate Services 1059
Implement Active Directory Federation Services 1070
What Is a Claim? 1070
What's New for AD FS in Windows Server 2012 R2? 1074
Active Directory Federation Services Installation 1076
Workplace Join 1089
Device Registration Service 1090
Workplace Join Your Device 1090
Active Directory Rights Management Services 1091
Considerations and Requirements for AD RMS 1091
Installing AD RMS 1094
Managing AD RMS: AD RMS Service Connection Point 1097
Summary 1104
Exam Essentials 1105
Review Questions 1106

Appendix A Answers to Review Questions 1109

Chapter 1: Install Windows Server 2012 R2 1110
Chapter 2: Configure Network Services 1111
Chapter 3: Plan and Install Active Directory 1112
Chapter 4: Configure Windows Server 2012 R2 1113
Chapter 5: Administer Active Directory 1114
Chapter 6: Manage GPOs 1114
Chapter 7: Manage Security 1115
Chapter 8: Configure TCP/IP 1116
Chapter 9: Use Virtualization in Windows Server 2012 1118
Chapter 10: Manage and Maintain Servers 1119
Chapter 11: Manage File Services 1120
Chapter 12: Configure DNS 1121
Chapter 13: Configure Routing and Remote Access 1122
Chapter 14: Configure a Network Policy Server Infrastructure 1123
Chapter 15: Configure and Manage Active Directory 1124
Chapter 16: Configure and Manage Group Policy 1125
Chapter 17: Configure and Manage High Availability 1126

Chapter 18: Configure File and Storage Solutions 1127
Chapter 19: Implement Business Continuity and Disaster Recovery 1128
Chapter 20: Configure Advanced Network Services 1129
Chapter 21: Configure the Active Directory Infrastructure 1130
Chapter 22: Configure Access and Information Protection Solutions 1131

Appendix B About the Additional Study Tools 1133

Additional Study Tools 1134
Sybex Test Engine 1134
Electronic Flashcards 1134
PDF of Glossary of Terms 1134
Adobe Reader 1135
System Requirements 1135
Using the Study Tools 1135
Troubleshooting 1135
Customer Care 1136

Index 1137

Table of Exercises

Exercise 1.1 Installing Windows Server 2012 R2 with the GUI 22
Exercise 1.2 Installing Windows Server 2012 R2 Using Server Core 25
Exercise 1.3 Initializing Disk Drives 32
Exercise 1.4 Converting a Basic Disk to a Dynamic Disk 33
Exercise 1.5 Creating a Volume Set 34
Exercise 1.6 Creating Mount Points 40
Exercise 1.7 Installing Microsoft MPIO 42
Exercise 1.8 Configuring iSCSI Storage Connection 44
Exercise 1.9 Installing the iSNS Feature on Windows Server 2012 R2 47
Exercise 2.1 Installing and Configuring the DNS Service 92
Exercise 2.2 Configuring a Zone for Dynamic Updates 98
Exercise 2.3 Creating a Delegated DNS Zone 101
Exercise 2.4 Manually Creating DNS RRs 102
Exercise 2.5 Simple DNS Testing 106
Exercise 2.6 Using the `nslookup` Command 111
Exercise 2.7 Installing the DHCP Service 122
Exercise 2.8 Unauthorizing a DHCP Server 127
Exercise 2.9 Authorizing a DHCP Server 128
Exercise 2.10 Creating a New Scope 135
Exercise 2.11 Configuring User Class Options 148
Exercise 2.12 Creating a Superscope 150
Exercise 2.13 Creating a New Multicast Scope 152
Exercise 2.14 Enabling DHCP-DNS Integration 155
Exercise 3.1 Viewing Disk Configuration 170
Exercise 3.2 Promoting a Domain Controller 181
Exercise 3.3 Installing AD DS on Server Core 186
Exercise 3.4 Viewing the Active Directory Event Log 191
Exercise 3.5 Joining a Computer to an Active Directory Domain 195
Exercise 3.6 Configuring DNS Integration with Active Directory 201
Exercise 4.1 Creating and Publishing a Shared Work Folder 210
Exercise 4.2 Configuring Offline Folder Options 214
Exercise 4.3 Configuring a Shared Network Folder for Offline Access 215
Exercise 4.4 Configuring a Shadow Copy on a Volume 216

Exercise 4.5 Configuring Shared and NTFS Settings 223
Exercise 4.6 Configuring Disk Quotas 225
Exercise 4.7 Creating and Publishing a Printer 226
Exercise 4.8 Starting the Windows PowerShell Utility 238
Exercise 5.1 Creating an OU Structure 257
Exercise 5.2 Modifying OU Structure 260
Exercise 5.3 Using the Delegation of Control Wizard 263
Exercise 5.4 Delegating Custom Tasks 264
Exercise 5.5 Creating Active Directory Objects 270
Exercise 5.6 Creating a User Template 273
Exercise 5.7 Managing Object Properties 277
Exercise 5.8 Moving Active Directory Objects 282
Exercise 5.9 Resetting an Existing Computer Account 283
Exercise 5.10 Creating and Publishing a Printer 285
Exercise 5.11 Creating and Publishing a Shared Folder 286
Exercise 5.12 Finding Objects in Active Directory 287
Exercise 6.1 Creating a Group Policy Object Using the GPMC 307
Exercise 6.2 Linking Existing GPOs to Active Directory 309
Exercise 6.3 Filtering Group Policy Using Security Groups 312
Exercise 6.4 Delegating Administrative Control of Group Policy 313
Exercise 6.5 Configuring Automatic Certificate Enrollment in Group Policy 321
Exercise 6.6 Configuring Folder Redirection in Group Policy 322
Exercise 6.7 Creating a Software Deployment Share 332
Exercise 6.8 Publishing and Assigning Applications Using Group Policy 334
Exercise 6.9 Applying Software Updates 336
Exercise 7.1 Delegating Control of Active Directory Objects 370
Exercise 7.2 Enabling Auditing of Active Directory Objects 375
Exercise 7.3 Configuring Windows Firewall 382
Exercise 8.1 Class C, 10 Hosts per Subnet 407
Exercise 8.2 Class C, 20 Hosts per Subnet 408
Exercise 8.3 Class C, Five Subnets 408
Exercise 8.4 Class B, 1,500 Hosts per Subnet 409
Exercise 8.5 Class B, 3,500 Hosts per Subnet 409
Exercise 9.1 Installing Hyper-V in Full Installation Mode 448
Exercise 9.2 Creating an Internal Virtual Network 455

Exercise 9.3 Creating a Differencing Hard Disk 457
Exercise 9.4 Creating a New Virtual Machine 461
Exercise 9.5 Installing Hyper-V Integration Components 468
Exercise 10.1 Installing a WSUS Server. 489
Exercise 10.2 Setting WSUS Server Options 493
Exercise 10.3 Configuring a GPO for WSUS 498
Exercise 10.4 Installing SNMP. 522
Exercise 10.5 Configuring SNMP 522
Exercise 11.1 Enabling BitLocker in Windows Server 2012 R2 536
Exercise 11.2 Installing the DFS Namespace Service 540
Exercise 11.3 Enabling Auditing of Active Directory Objects 545
Exercise 11.4 Generating and Viewing Audit Logs. 546
Exercise 11.5 Creating and Publishing a Shared Network Folder. 549
Exercise 11.6 Configuring Offline Folder Options 550
Exercise 11.7 Configuring a Shared Network Folder for Offline Access 551
Exercise 12.1 Installing and Configuring the DNS Service 589
Exercise 12.2 Configuring a Zone for Dynamic Updates 596
Exercise 12.3 Creating a Delegated DNS Zone 598
Exercise 12.4 Manually Creating DNS RRs 599
Exercise 12.5 Simple DNS Testing 603
Exercise 12.6 Using the `nslookup` Command 607
Exercise 12.7 Enabling DHCP-DNS Integration 613
Exercise 13.1 Installing the Remote Access Role 633
Exercise 13.2 Changing Remote Access Logging Settings 642
Exercise 14.1 Creating a Network Access Policy 674
Exercise 14.2 Restricting a User Profile for Dial-In Access 680
Exercise 14.3 Configuring Encryption 684
Exercise 14.4 Creating a VPN Network Access Policy 685
Exercise 15.1 Creating and Managing Users and Groups 714
Exercise 15.2 Creating and Using User Templates. 717
Exercise 15.3 Delegating Control of Active Directory Objects 718
Exercise 15.4 Applying Security Policies by Using Group Policy 721
Exercise 15.5 Fine-Grained Password Policy 723
Exercise 15.6 Assigning Single-Master Operations 728
Exercise 15.7 Backing Up Active Directory 736

Exercise 16.1 Creating a Group Policy Object Using the GPMC 761
Exercise 16.2 Linking Existing GPOs to Active Directory 764
Exercise 16.3 Filtering Group Policy Using Security Groups 769
Exercise 16.4 Delegating Administrative Control of Group Policy 770
Exercise 16.5 Configuring Automatic Certificate Enrollment in Group Policy 777
Exercise 16.6 Configuring Folder Redirection in Group Policy 779
Exercise 16.7 Creating a Software Deployment Share 793
Exercise 16.8 Publishing and Assigning Applications Using Group Policy 795
Exercise 16.9 Applying Software Updates 796
Exercise 17.1 Installing NLB Nodes 825
Exercise 17.2 Installing the Failover Cluster Feature 835
Exercise 17.3 Running the Validate A Configuration Wizard 837
Exercise 17.4 Creating a Cluster 839
Exercise 17.5 Clustering the Print Services Role 842
Exercise 17.6 Using the Dependency Viewer 846
Exercise 18.1 Configure the NFS Data Store 859
Exercise 18.2 Configuring BranchCache Firewall Exceptions 863
Exercise 18.3 Installing BranchCache on Windows Server 2012 R2 865
Exercise 18.4 Enabling Auditing of Active Directory Objects 872
Exercise 18.5 Generating and Viewing Audit Logs 873
Exercise 18.6 Enable Dynamic Access Control 876
Exercise 18.7 Configure User and Device Claim Types 878
Exercise 18.8 Create and Configure Resource Properties and Lists 880
Exercise 18.9 Create and Configure Central Access Rules and Policies 882
Exercise 18.10 Configure File Classification 884
Exercise 18.11 Implement Policy Stages and Staging 885
Exercise 18.12 Configure Access-Denied Assistance 888
Exercise 18.13 Configuring iSCSI Storage Connection 891
Exercise 18.14 Installing the iSNS Feature on Windows Server 2012 R2 893
Exercise 19.1 Backing Up Active Directory 910
Exercise 19.2 Configuring a Shadow Copy on a Volume 922
Exercise 19.3 Booting Your Computer to Safe Mode 926
Exercise 19.4 Using Boot Logging 927
Exercise 20.1 Creating a Superscope 940
Exercise 20.2 Creating and Activating a New Multicast Scope 941

Exercise 20.3 Creating and Activating a New DHCPv6 Scope. 944
Exercise 20.4 Configuring DHCP Failover 946
Exercise 20.5 Configuring DHCP Filtering 950
Exercise 20.6 Enabling DHCP Name Protection 951
Exercise 20.7 Disabling Dynamic Updates 952
Exercise 20.8 Configuring DNSSEC 954
Exercise 20.9 Enabling DNS Diagnostic Logging 957
Exercise 20.10 Disabling DNS Recursion. 959
Exercise 20.11 Configuring a GlobalNames Zone 961
Exercise 20.12 Installing the IPAM Feature 964
Exercise 20.13 Configuring IPAM Server Discovery. 967
Exercise 20.14 Manually Add IPAM IP Address Space. 968
Exercise 21.1 Creating Sites 988
Exercise 21.2 Creating Subnets 991
Exercise 21.3 Configuring Sites 993
Exercise 21.4 Creating Site Links and Site Link Bridges 998
Exercise 21.5 Moving Server Objects Between Sites. 1001
Exercise 21.6 Creating a New Subdomain. 1018
Exercise 21.7 Assigning Single-Master Operations 1028
Exercise 21.8 Managing Trust Relationships. 1032
Exercise 21.9 Adding a UPN Suffix. 1033
Exercise 21.10 Managing GC Servers 1035
Exercise 21.11 Managing Universal Group Membership Caching 1036
Exercise 22.1 Installing AD CS Through Server Manager 1056
Exercise 22.2 Configuring AD CS Through Server Manager. 1059
Exercise 22.3 Configure an Auto-enrollment Group Policy for a Domain 1062
Exercise 22.4 Creating a Certificate Template. 1065
Exercise 22.5 Publishing a Certificate Template. 1066
Exercise 22.6 Revoking a Certificate 1067
Exercise 22.7 Configuring CA Policy Auditing 1068
Exercise 22.8 Backing Up the Certificate Authority Server. 1069
Exercise 22.9 Installing the AD FS Role on a Computer Using Server Manager. 1076
Exercise 22.10 Configuring the AD FS Role on the Computer Using Server Manager. 1079
Exercise 22.11 Configuring Multifactor Authentication 1088

Exercise 22.12 Workplace Joining a Device 1090
Exercise 22.13 Installing an AD RMS Role on the Local Computer Using Server Manager 1094
Exercise 22.14 Backing Up an AD RMS Database 1100
Exercise 22.15 Adding a Trusted User Domain 1102
Exercise 22.16 Exporting the Trusted User Domain 1103
Exercise 22.17 Exporting the Trusted Publishing Domain 1103
Exercise 22.18 Adding the Trusted Publishing Domain 1104

Introduction

This book is drawn from more than 20 years of IT experience. I have taken that experience and translated it into a Windows Server 2012 R2 book that will help you not only prepare for the MCSA: Windows Server 2012 R2 exams but also develop a clear understanding of how to install and configure Windows Server 2012 R2 while avoiding all of the possible configuration pitfalls.

Many Microsoft books just explain the Windows operating system, but with *MCSA: Windows Server 2012 R2 Complete Study Guide*, I go a step further by providing many in-depth, step-by-step procedures to support my explanations of how the operating system performs at its best.

Microsoft Windows Server 2012 R2 is the newest version of Microsoft's server operating system software. Microsoft has taken the best of Windows Server 2003, Windows Server 2008, and Windows Server 2012 and combined them into the latest creation, Windows Server 2012 R2.

Windows Server 2012 R2 eliminates many of the problems that plagued the previous versions of Windows Server, and it includes a much faster boot time and shutdown. It is also easier to install and configure, and it barely stops to ask the user any questions during installation. In this book, I will show you what features are installed during the automated installation and where you can make changes if you need to be more in charge of your operating system and its features.

This book takes you through all the ins and outs of Windows Server 2012 R2, including installation, configuration, Group Policy Objects, auditing, backups, and so much more.

Windows Server 2012 R2 has improved on Microsoft's desktop environment, made networking easier, enhanced searching capability, and improved performance—and that's only scratching the surface.

When all is said and done, this is a technical book for IT professionals who want to take Windows Server 2012 R2 to the next step and get certified. With this book, not only will you learn Windows Server 2012 R2 and ideally pass the exams, you will also become a Windows Server 2012 R2 expert.

The Microsoft Certification Program

Since the inception of its certification program, Microsoft has certified more than 2 million people. As the computer network industry continues to increase in both size and complexity, this number is sure to grow—and the need for proven ability will also increase. Certifications can help companies verify the skills of prospective employees and contractors.

The Microsoft certification tracks for Windows Server 2012 R2 include the following:

MCSA: Windows Server 2012 R2 The MCSA is now the lowest-level certification you can achieve with Microsoft in relation to Windows Server 2012 R2. It requires passing three exams: 70-410, 70-411, and 70-412. Or, if you qualify, you can take the Upgrading exam: exam 70-417. This book assists in your preparation for all four exams.

MCSE: Server Infrastructure or MCSE: Desktop Infrastructure The MCSE certifications, in relation to Windows Server 2012 R2, require that you become an MCSA first and then pass two additional exams. The additional exams will vary depending on which of the two MCSE tracks you choose. For more information, visit Microsoft's website at `www.microsoft.com/learning`.

MCSM: Directory Services The MCSM certification takes things to an entirely new level. It requires passing a knowledge exam (in addition to having the MCSE in Windows Server 2012 R2) and a lab exam. This is now the elite-level certification in Windows Server 2012 R2.

How Do You Become Certified on Windows Server 2012 R2?

Attaining Microsoft certification has always been a challenge. In the past, students have been able to acquire detailed exam information—even most of the exam questions—from online "brain dumps" and third-party "cram" books or software products. For the new generation of exams, this is simply not the case.

Microsoft has taken strong steps to protect the security and integrity of its new certification tracks. Now prospective candidates must complete a course of study that develops detailed knowledge about a wide range of topics. It supplies them with the true skills needed, derived from working with the technology being tested.

The new generations of Microsoft certification programs are heavily weighted toward hands-on skills and experience. It is recommended that candidates have troubleshooting skills acquired through hands-on experience and working knowledge.

Fortunately, if you are willing to dedicate the time and effort to learn Windows Server 2012 R2, you can prepare yourself well for the exam by using the proper tools. By working through this book, you can successfully meet the requirements to pass the Windows Server 2012 R2 exams.

MCSA Exam Requirements

Candidates for MCSA certification on Windows Server 2012 R2 must pass at least the following three Windows Server 2012 R2 exams:

- 70-410: Installing and Configuring Windows Server 2012 R2
- 70-411: Administering Windows Server 2012 R2
- 70-412: Configuring Advanced Windows Server 2012 R2 Services

MCITP Exam Requirements

Candidates for MCITP certification on Windows Server 2012 R2 must pass one Windows Server 2012 R2 exams. This book will help you get ready for the 70-411: Administering Windows Server 2012 R2 exam.

Microsoft provides exam objectives to give you a general overview of possible areas of coverage on the Microsoft exams. Keep in mind, however, that exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Visit the Microsoft Learning website (`www.microsoft.com/learning`) for the most current listing of exam objectives. The published objectives and how they map to this book are listed later in this Introduction.

For those who have a qualifying certification, they can take the Upgrading Your Skills to MCSA Windows Server 2012 R2 exam (exam 70-417). The objectives for this exam span the three individual exams. This book covers all of the objectives for the Upgrading exam. For details about the exam, visit Microsoft's website at `www.microsoft.com/learning`.

Microsoft provides exam objectives to give you a general overview of possible areas of coverage on the Microsoft exams. Keep in mind, however, that exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Visit the Microsoft Learning website (`www.microsoft.com/learning`) for the most current listing of exam objectives. The published objectives and how they map to this book are listed later in this introduction.

For a more detailed description of the Microsoft certification programs, including a list of all of the exams, visit the Microsoft Learning website at: `www.microsoft.com/learning`.

Tips for Taking the Windows Server 2012 R2 Exams

Here are some general tips for achieving success on your certification exam:

- Arrive early at the exam center so that you can relax and review your study materials. During this final review, you can look over tables and lists of exam-related information.
- Read the questions carefully. Do not be tempted to jump to an early conclusion. Make sure that you know *exactly* what the question is asking.
- Answer all questions. If you are unsure about a question, mark it for review and come back to it at a later time.

- On simulations, do not change settings that are not directly related to the question. Also, assume the default settings if the question does not specify or imply which settings are used.
- For questions about which you're unsure, use a process of elimination to get rid of the obviously incorrect answers first. This improves your odds of selecting the correct answer when you need to make an educated guess.

Exam Registration

At the time this book was released, Microsoft exams are given using Prometric testing centers (800-755-EXAM [800-755-3926]). As of December 31, 2014, Microsoft will be ending its relationship with Prometric and all exams will be delivered through the more than 1,000 Authorized VUE Testing Centers around the world. For the location of a testing center near you, go to VUE's website at `www.vue.com`. If you are outside of the United States and Canada, contact your local VUE registration center.

Find out the number of the exam that you want to take and then register with the Prometric registration center nearest to you. At this point, you will be asked for advance payment for the exam. The exams are $125 each, and you must take them within one year of payment. You can schedule exams up to six weeks in advance, or as late as one working day prior to the date of the exam. You can cancel or reschedule your exam if you contact the center at least two working days prior to the exam. Same-day registration is available in some locations, subject to space availability. Where same-day registration is available, you must register a minimum of two hours before test time.

When you schedule the exam, you will be provided with instructions regarding appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you will receive a registration and payment confirmation letter from Prometric.

Microsoft requires certification candidates to accept the terms of a nondisclosure agreement before taking certification exams.

Who Should Read This Book?

This book is intended for individuals who want to earn their MCSA: Windows Server 2012 R2 certification.

Not only will this book help anyone who is looking to pass the Microsoft exams, it will also help anyone who wants to learn the real ins and outs of the Windows Server 2012 R2 operating system.

What's Inside?

Here is a glance at what's in each chapter:

Chapter 1: Install Windows Server 2012 R2 The first chapter explains the requirements and steps required to install and configure Windows Server 2012 R2.

Chapter 2: Configure Network Services This chapter shows you how to install and configure DNS. It also explains the different types of DNS records and DNS zone types.

Chapter 3: Plan and Install Active Directory This chapter takes you through the advantages and benefits of Windows Server 2012 R2 Active Directory.

Chapter 4: Configure Windows Server 2012 R2 This chapter shows you how to manage file systems, print servers, and file and share access.

Chapter 5: Administer Active Directory This chapter takes you through the different ways to create and manage your users and groups on the Windows Server 2012 R2 operating system.

Chapter 6: Manage GPOs You will see how to configure different types of Group Policy objects (GPOs) in Active Directory.

Chapter 7: Manage Security This chapter shows you how to secure Windows Server 2012 R2.

Chapter 8: Configure TCP/IP This chapter shows you how to configure IPv4 and IPv6. You'll look at IPv4 subnetting and how to manage a TCP/IP network.

Chapter 9: Use Virtualization in Windows Server 2012 This chapter shows you how to implement and configure Windows Server Hyper-V and virtual machines. You will learn about virtual networking, virtual hard disks, migration types, and Integration Services.

Chapter 10: Manage and Maintain Servers This chapter explains the requirements and steps to deploy, manage, and maintain the Windows Server 2012 R2 system.

Chapter 11: Manage File Services This chapter shows you how to configure file and print services. You will learn how to set up a file server for faster response times and about the different ways to set up and configure print services.

Chapter 12: Configure DNS This chapter shows you the advantages and benefits of Windows Server 2012 R2 Network Services.

Chapter 13: Configure Routing and Remote Access This chapter shows you how to configure the different types of remote access and Windows routing protocols.

Chapter 14: Configure a Network Policy Server Infrastructure This chapter takes you through the different ways to create and manage your Windows Server 2012 R2 NPS server.

Chapter 15: Configure and Manage Active Directory You will see how to configure and manage different types of objects in Active Directory.

Chapter 16: Configure and Manage Group Policy This chapter shows you how to manage different parts of Windows policies by using the Group Policy Management Console. This chapter also explains how to install and configure software using GPOs.

Chapter 17: Configure and Manage High Availability This chapter shows how to set up Windows Server 2012 R2 high availability. This includes clustering and failover systems.

Chapter 18: Configure File and Storage Solutions This chapter shows you how to configure file and storage solutions. You will learn how to help your system run faster and give you better response times.

Chapter 19: Implement Business Continuity and Disaster Recovery This chapter shows you how to protect yourself in the event of a system crash or a catastrophic failure.

Chapter 20: Configure Advanced Network Services This chapter shows you how to configure the different types of network services and how to configure them properly.

Chapter 21: Configure the Active Directory Infrastructure This chapter takes you through the different ways to create and manage your Windows Server 2012 R2 Active Directory infrastructure.

Chapter 22: Configure Access and Information Protection Solutions You will see how to set up your Windows Server 2012 R2 system so that your information stays secure.

What's Included with the Book

This book includes many helpful items intended to prepare you for the MCSA: Windows Server 2012 R2 certification. These items include:

Assessment Test There is an Assessment Test at the conclusion of the introduction that can be used to evaluate quickly where you are with Windows Server 2012 R2. This test should be taken prior to beginning your work in this book, and it should help you identify areas in which you are either strong or weak. Note that these questions are purposely simpler than the types of questions you may see on the exams.

Objective Map and Opening List of Objectives Later in this introduction, you will find a detailed exam objective map showing you where each of the exam objectives is covered. Each chapter also includes a list of the exam objectives covered.

Helpful Exercises Throughout the book are step-by-step exercises of some of the more important tasks that you should be able to perform. Some of these exercises have corresponding videos that can be downloaded from the book's website. Also, the following section has a recommended home lab setup that will be helpful in completing these tasks.

Exam Essentials The end of each chapter also includes a listing of exam essentials. These are essentially repeats of the objectives, but remember that any objective on the exam blueprint could show up on the exam.

Chapter Review Questions Each chapter includes review questions. These are used to assess your understanding of the chapter and are taken directly from the chapter. These questions are based on the exam objectives, and they are similar in difficulty to items you might actually receive on the MCSA: Windows Server 2012 R2 exams.

You can obtain the Interactive Online Learning Environment, flashcards, videos, and glossary at `www.sybex.com/go/mcsawin2012r2`.

Interactive Online Learning Environment You can access the Interactive Online Learning Environment, which includes the assessment test and chapter review questions. In addition, there are a total of three practice exams included with the Interactive Online Learning Environment: one each for exams 70-410, 70-411, and 70-412.

Flashcards Flashcards are included for quick reference. They are a great tool for learning important facts quickly. You may even consider these as additional simple practice questions, which is essentially what they are.

Videos Some of the exercises include corresponding videos. These videos show you how we do the exercises. There is also a video that shows you how to set up virtualization so that you can complete the exercises within a virtualized environment. This same video also shows you how to install Windows Server 2012 Datacenter on that virtualized machine.

PDF of Glossary of Terms There is a glossary included that covers the key terms used in this book.

Recommended Home Lab Setup

To get the most out of this book, you will want to make sure you complete the exercises throughout the chapters. To complete the exercises, you will need one of two setups. First, you can set up a machine with Windows Server 2012 R2 and complete the labs using a regular Windows Server 2012 R2 machine.

The second way to set up Windows Server 2012 R2 (the way we set up Server 2012 R2) is by using virtualization. We set up Windows Server 2012 R2 as a virtual hard disk (VHD), and we did all the labs this way. The advantages of using virtualization are that you can always just wipe out the system and start over without losing a real server. Plus, you can set up multiple virtual servers and create a full lab environment on one machine.

We created a video for this book showing you how to set up a virtual machine and how to install Windows Server 2012 R2 onto that virtual machine.

How to Contact the Author/Sybex

Sybex strives to keep you supplied with the latest tools and information that you need for your work. Please check the website at `www.sybex.com/go/mcsawin2012r2`, where we'll post additional content and updates that supplement this book should the need arise.

You can contact Will Panek by going to `www.willpanek.com`.

Certification Objectives Maps

In addition to the book chapters, you will find coverage of exam objectives in the flashcards, practice exams, and videos on the book's companion website.

`http://www.sybex.com/go/mcsawin2012r2`

Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit Microsoft's website (`www.microsoft.com/learning`) for the most current listing of exam objectives.

Objectives

Part I: Exam 70-410: Installing and Configuring Windows Server 2014

Install servers, Chapter 1

- Plan for a server installation
- Plan for server roles
- Plan for a server upgrade
- Install Server Core
- Optimize resource utilization by using Features on Demand
- Migrate roles from previous versions of Windows Server

Configure servers, Chapter 1
- Configure Server Core
- Delegate administration
- Add and remove features in offline images
- Deploy roles on remote servers
- Convert Server Core to/from full GUI
- Configure services
- Configure NIC teaming

Configure local storage, Chapter 1
- Design storage spaces
- Configure basic and dynamic disks
- Configure MBR and GPT disks
- Manage volumes
- Create and mount virtual hard disks
- Configure storage pools and disk pools

Deploy and configure DNS service, Chapter 2
- Configure Active Directory integration of primary zones
- Configure forwarders
- Configure Root Hints
- Manage DNS cache
- Create A and PTR resource records

Deploy and configure Dynamic Host Configuration Protocol (DHCP) service, Chapter 2
- Create and configure scopes
- Configure a DHCP reservation
- Configure DHCP options
- Configure client and server for PXE boot
- Configure DHCP relay agent
- Authorize DHCP server

Install domain controllers, Chapter 3
- Add or remove a domain controller from a domain
- Upgrade a domain controller
- Install Active Directory Domain Services (AD DS) on a Server Core installation
- Install a domain controller from Install from Media (IFM)
- Resolve DNS SRV record registration issues

- Configure a global catalog server
- Deploy Active Directory iaas in Windows Azure

Configure file and share access, Chapter 4

- Create and configure shares
- Configure share permissions
- Configure offline files
- Configure NTFS permissions
- Configure access-based enumeration (ABE)
- Configure Volume Shadow Copy Service (VSS)
- Configure NTFS quotas
- Create and configure Work Folders

Configure print and document services, Chapter 4

- Configure the Easy Print print driver
- Configure Enterprise Print Management
- Configure drivers
- Configure printer pooling
- Configure print priorities
- Configure printer permissions

Configure servers for remote management, Chapter 4

- Configure WinRM
- Configure down-level server management
- Configure servers for day-to-day management tasks
- Configure multi-server management
- Configure Server Core
- Configure Windows Firewall
- Manage non-domain joined servers

Create and manage Active Directory users and computers, Chapter 5

- Automate the creation of Active Directory accounts
- Create, copy, configure, and delete users and computers
- Configure templates
- Perform bulk Active Directory operations
- Configure user rights
- Offline domain join
- Manage inactive and disabled accounts

Create and manage Active Directory groups and organizational units (OUs), Chapter 5

- Configure group nesting
- Convert groups including security, distribution, universal, domain local, and domain global
- Manage group membership using Group Policy
- Enumerate group membership
- Delegate the creation and management of Active Directory objects
- Manage default Active Directory containers
- Create, copy, configure, and delete groups and OUs

Create Group Policy Objects (GPOs), Chapter 6

- Configure a Central Store
- Manage starter GPOs
- Configure GPO links
- Configure multiple local group policies
- Configure security filtering

Configure application restriction policies, Chapter 6

- Configure rule enforcement
- Configure applocker rules
- Configure Software Restriction Policies

Configuring security policies, Chapter 7

- Configure User Rights Assignment
- Configure Security Options settings
- Configure Security templates
- Configure Audit Policy
- Configure Local Users and Groups
- Configure User Account Control (UAC)

Configuring Windows Firewall, Chapter 7

- Configure rules for multiple profiles using Group Policy
- Configure connection security rules
- Configure Windows Firewall to allow or deny applications, scopes, ports, and users
- Configure authenticated firewall exceptions
- Import and export settings

Configure IPv4 and IPv6 addressing, Chapter 8

- Configure IP address options
- Configure IPv4 or IPv6 subnetting

- Configure supernetting
- Configure interoperability between IPv4 and IPv6
- Configure ISATAP
- Configure Teredo

Create and configure virtual machine settings, Chapter 9
Configure dynamic memory , Chapter 9
Configure smart paging, Chapter 9
Configure Resource Metering, Chapter 9
Configure guest integration services, Chapter 9
Create and configure Generation 1 and 2 virtual machines, Chapter 9
Configure and use extended session mode, Chapter 9
Configure remoteFX, Chapter 9
Create and configure virtual machine storage, Chapter 9

- Create VHDs and VHDX
- Configure differencing drives
- Modify VHDs
- Configure pass-through disks
- Manage checkpoints
- Implement a virtual Fibre Channel adapter
- Configure storage Quality of Service

Create and configure virtual networks, Chapter 9

- Configure Hyper-V virtual switches
- Optimize network performance
- Configure MAC addresses
- Configure network isolation
- Configure synthetic and legacy virtual network adapters
- Configure NIC teaming in virtual machines

Part II: Exam 70-411: Administering Windows Server 2012

Deploy and manage server images, Chapter 10

- Install the Windows Deployment Services (WDS) role
- Configure and manage boot, install, and discover images
- Update images with patches, hotfixes, and drivers

Install features for offline images
Configure driver groups and packages

Implement patch management., Chapter 10
Install and configure the Windows Server Update Services (WSUS) role
Configure group policies for updates

Configure client-side targeting, Chapter 10
Configure WSUS synchronization
Configure WSUS groups
Manage patch management in mixed environments Monitor servers
Configure Data Collector Sets (DCS)
Configure alerts
Monitor real-time performance
Monitor virtual machines (VMS)
Monitor events
Configure event subscriptions
Configure network monitoring
Schedule performance monitoring

Configure Distributed File System (DFS), Chapter 11
Install and configure DFS namespaces
Configure DFS Replication Targets
Configure Replication Scheduling
Configure Remote Differential Compression settings
Configure staging
Configure fault tolerance
Clone a DFS database
Recover DFS databases
Optimize DFS replication

Configure File Server Resource Manager (FSRM), Chapter 11
Install the FSRM role service
Configure quotas
Configure file screens
Configure reports
Configure file management tasks

Configure file and disk encryption, Chapter 11

- Configure Bitlocker encryption
- Configure the Network Unlock feature
- Configure Bitlocker policies
- Configure the EFS recovery agent
- Manage EFS and Bitlocker certificates including backup and restore

Configure advanced audit policies, Chapter 11

- Implement auditing using Group Policy and AuditPol.exe
- Create expression-based
- Create removable device audit policies

Configure DNS zones, Chapter 12

- Configure primary and secondary zones
- Configure stub zones
- Configure conditional forwards
- Configure zone and conditional forward storage in Active Directory
- Configure zone delegation
- Configure zone transfer settings
- Configure notify settings

Configure DNS records, Chapter 12

- Create and configure DNS Resource Records (RR) including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records
- Configure zone scavenging
- Configure record options including time to live (TTL) and weight
- Configure round robin
- Configure secure dynamic updates

Configure VPN and routing, Chapter 13

- Install and configure the Remote Access role
- Implement Network Address Translation (NAT)
- Configure VPN settings
- Configure remote dial-in settings for users
- Configure routing
- Configure Web Application proxy in passthrough mode

Configure DirectAccess, Chapter 13

- Implement server requirements

- Implement client configuration
- Configure DNS for DirectAccess
- Configure certificates for DirectAccess

Configure Network Policy Server (NPS), Chapter 14

- Configure a NPS server including RADIUS proxy
- Configure RADIUS clients
- Configure NPS templates
- Configure RADIUS accounting
- Configure certificates

Configure NPS policies, Chapter 14

- Configure connection request policies
- Configure network policies for VPN clients (multilink and bandwidth allocation, IP filters, encryption, IP addressing)
- Import and export NPS policies

Configure Network Access Protection (NAP), Chapter 14

- Configure System Health Validators (SHVs)
- Configure health policies
- Configure NAP enforcement using DHCP and VPN
- Configure isolation and remediation of non-compliant computers using DHCP and VPN
- Configure NAP client settings

Configure service authentication, Chapter 15

- Create and configure Service Accounts
- Create and configure Group Managed Service Accounts
- Configure Kerberos delegation
- Manage Service Principal Names (SPNS)
- Configure virtual accounts

Configure Domain Controllers, Chapter 15

- Transfer and seize operations master roles
- Install and configure a read-only domain controller (RODC)
- Configure domain controller cloning

Maintain Active Directory, Chapter 15

- Back up Active Directory and SYSVOL
- Manage Active Directory offline

- Optimize an Active Directory database
- Clean up metadata
- Configure Active Directory snapshots
- Perform object- and container-level recovery
- Perform Active Directory restore
- Configure and restore objects by using the Active Directory Recycle Bin

Configure account policies, Chapter 15

- Configure domain and local user password policy settings
- Configure and apply Password Settings Objects (PSOs)
- Delegate password settings management
- Configure account lockout policy settings
- Configure Kerberos policy settings

Configure Group Policy processing, Chapter 16

- Configure processing order and precedence
- Configure blocking of inheritance
- Configure enforced policies
- Configure security filtering and WMI filtering
- Configure loopback processing
- Configure and manage slow-link processing and group policy caching
- Configure client-side extension (CSE) behavior
- Force group policy update

Configure Group Policy settings, Chapter 16

- Configure settings including software installation, folder redirection, scripts, and administrative template settings
- Import security templates
- Import custom administrative template file
- Convert administrative templates using admx migrator
- Configure property filters for administrative templates

Manage Group Policy objects (GPOs), Chapter 16

- Back up, import, copy, and restore GPOs
- Create and configure Migration Table
- Reset default GPOs
- Delegate Group Policy management

Configure Group Policy Preferences (GPP), Chapter 16

- Configure GPP settings including printers, network drive mappings, power options, custom registry settings, Control Panel settings, Internet Explorer settings, file and folder deployment, and shortcut deployment
- Configure item-level targeting

Part III: Exam 70-412: Configuring Advanced Windows Server 2012 Services

Configure Network Load Balancing (NLB), Chapter 17

- This objective may include, but is not limited to:
  - Install NLB nodes
  - Configure NLB prerequisites
  - Configure affinity
  - Configure port rules
  - Configure cluster operation mode
  - Upgrade an NLB cluster

Configure failover clustering, Chapter 17

- This objective may include, but is not limited to:
  - Configure Quorum
  - Configure cluster networking
  - Restore single node or cluster configuration
  - Configure cluster storage
  - Implement cluster aware updating
  - Upgrade a cluster

Manage failover-clustering roles, Chapter 17

- This objective may include, but is not limited to:
  - Configure role-specific settings including continuously available shares
  - Configure VM monitoring
  - Configure failover and preference settings

Manage Virtual Machine (VM) Movement, Chapter 17

- This objective may include, but is not limited to:
  - Configure Virtual Machine network health protection
  - Configure drain on shutdown

- Perform quick, live and storage migrations
- Import/export/copy of VMS

Configure advanced file services, Chapter 18

- Configure NFS data store
- Configure BranchCache
- Configure File Classification Infrastructure (FCI) using File Server Resource Manager (FSRM)
- Configure file access auditing

Implement Dynamic Access Control (DAC), Chapter 18

- Configure user and device claim types
- Create and configure resource properties and lists
- Create and configure Central Access Rules and Policies
- Configure file classification
- Implement policy changes and staging
- Perform access-denied remediation

Configure and optimize storage, Chapter 18

- Configure iSCSI Target and Initiator
- Configure Internet Storage Name Server (iSNS)
- Implement thin provisioning and trim
- Manage server free space using Features on Demand
- Configure tiered storage

Configure and manage backups, Chapter 19

- Configure Windows Server backups
- Configure Windows Azure backups
- Configure role-specific backups
- Manage VSS settings using VSSAdmin

Recover Servers, Chapter 19

- Restore from backups
- Perform a Bare Metal Restore (BMR)
- Recover servers using Windows Recovery Environment (Win RE) and safe mode
- Configure the Boot Configuration Data (BCD) store

Configure site-level fault tolerance, Chapter 19

- Configure Hyper-V Replica including Hyper-V Replica Broker and VMs
- Configure multi-site clustering including network settings, Quorum, and failover settings

- Configure Hyper-V Replica extended replication
- Configure Global Update Manager
- Recover a multi-site failover cluster

Implement an advanced Dynamic Host Configuration Protocol (DHCP) solution, Chapter 20

- Create and configure superscopes and multicast scopes
- Implement DHCPv6
- Configure high availability for DHCP including DHCP failover and split scopes
- Configure DHCP Name Protection
- Configure DNS registration

Implement an advanced DNS solution, Chapter 20

- Configure security for DNS including DNSSEC, DNS Socket Pool, and cache locking
- Configure DNS logging
- Configure delegated administration
- Configure recursion
- Configure netmask ordering
- Configure a GlobalNames zone
- Analyze zone level statistics

Deploy and manage IPAM, Chapter 20

- Provision IPAM manually or by using Group Policy
- Configure server discovery
- Create and manage IP blocks and ranges
- Monitor utilization of IP address space
- Migrate to IPAM
- Delegate IPAM administration
- Manage IPAM collections
- Configure IPAM database storage

Configure a forest or a domain, Chapter 21

- Implement multi-domain and multi-forest Active Directory environments including interoperability with previous versions of Active Directory
- Upgrade existing domains and forests including environment preparation and functional levels
- Configure multiple user principal name (UPN) suffixes

Configure Trusts, Chapter 21

- Configure external, forest, shortcut, and realm trusts
- Configure trust authentication

- Configure SID filtering
- Configure name suffix routing

Configure Sites, Chapter 21

- Configure sites and subnets
- Create and configure site links
- Manage site coverage
- Manage registration of SRV records
- Move domain controllers between sites

Manage Active Directory and SYSVOL replication, Chapter 21

- Configure replication to Read-Only Domain Controllers (RODCs)
- Configure Password Replication Policy (PRP) for RODCs
- Monitor and manage replication
- Upgrade SYSVOL replication to Distributed File System Replication (DFSR)

Install and configure Active Directory Certificate Services (AD CS), Chapter 22

- Describe and explain the new features in Windows Server 2012 Active Directory Certificate Services
- Install and configure Active Directory Certificate Services using Server Manager and Windows PowerShell
- Manage Active Directory Certificate Services using management consoles and Windows PowerShell
- Configure CRL distribution points
- Install and configure Online Responder
- Implement administrative role separation
- Configure CA Disaster recovery
- Manage certificates
- Manage certificate templates
- Implement and manage certificate deployment, validation, and revocation
- Manage certificate renewal
- Manage certificate enrollment and renewal to computers and users using Group Policies
- Configure and manage key archival and recovery
- Manage trust between organizations including Certificate Trust List (CTL)
- Managing Cross certifications and bride CAs
- Monitoring CA Health

Install and Configure Active Directory Federation Services (AD FS), Chapter 22

- Implement claims-based authentication including Relying Party Trusts
- Configure authentication policies

Configure Workplace Join
Configure multi-factor authentication

Install and configure Active Directory Rights Management Services (AD RMS), Chapter 22
Install a licensing or certificate AD RMS server
Manage AD RMS Service Connection Point (SCP)
Manage RMS templates
Configure Exclusion Policies
Backup and restore AD RMS

Assessment Test

1. Which of the following is a valid role for a Windows Server 2012 R2 computer?
   - **A.** Stand-alone server
   - **B.** Member server
   - **C.** Domain controller
   - **D.** All of the above

2. Which of the following is a benefit of using Active Directory? (Choose all that apply.)
   - **A.** Hierarchical object structure
   - **B.** Fault-tolerant architecture
   - **C.** Ability to configure centralized and distributed administration
   - **D.** Flexible replication

3. Which of the following features of the Domain Name System (DNS) can be used to improve performance? (Choose all that apply.)
   - **A.** Caching-only servers
   - **B.** DNS forwarding
   - **C.** Secondary servers
   - **D.** Zone delegation

4. Which of the following pieces of information should you have before you begin the Active Directory Installation Wizard? (Choose all that apply.)
   - **A.** Active Directory domain name
   - **B.** Administrator password for the local computer
   - **C.** NetBIOS name for the server
   - **D.** DNS configuration information

5. An Active Directory environment consists of three domains. What is the maximum number of sites that can be created for this environment?
   - **A.** Two
   - **B.** Three
   - **C.** Nine
   - **D.** Unlimited

6. Which of the following is *not* a valid Active Directory object?
   - **A.** User
   - **B.** Group

C. Organizational unit

D. Computer

E. None of the above

7. Which of the following is *not* considered a security principal?

A. Users

B. Security groups

C. Distribution groups

D. Computers

8. Which of the following should play the *least* significant role in planning an OU structure?

A. Network infrastructure

B. Domain organization

C. Delegation of permissions

D. Group Policy settings

9. How can the Windows Server 2012 R2 file and printer resources be made available from within Active Directory?

A. A system administrator can right-click the resource and select Publish.

B. A system administrator can create Printer and Shared Folder objects that point to these resources.

C. The Active Directory Domains and Trusts tool can be used to make resources available.

D. Only resources on a Windows 2000 or newer server can be accessed from within Active Directory.

10. The process by which a higher-level security authority assigns permissions to other administrators is known as which of the following?

A. Inheritance

B. Delegation

C. Assignment

D. Trust

11. What is the minimum amount of information you need to create a Shared Folder Active Directory object?

A. The name of the share

B. The name of the server

C. The name of the server and the name of the share

D. The name of the server, the server's IP address, and the name of the share

12. Which of the following operations is not supported by Active Directory?

A. Assigning applications to users

B. Assigning applications to computers

C. Publishing applications to users

D. Publishing applications to computers

13. Which of the following filename extensions is used primarily for Windows Installer setup programs?

A. `.msi`

B. `.mst`

C. `.zap`

D. `.aas`

14. A system administrator wants to allow a group of users to add computer accounts to a specific organizational unit (OU). What is the easiest way to grant only the required permissions?

A. Delegate control of a user account

B. Delegate control at the domain level

C. Delegate control of an OU

D. Delegate control of a computer account

E. Create a Group Policy object (GPO) at the OU level

15. A Group Policy object (GPO) at the domain level sets a certain option to Disabled, while a GPO at the OU level sets the same option to Enabled. All other settings are left at their default. Which setting will be effective for objects within the OU?

A. Enabled

B. Disabled

C. No effect

D. None of the above

16. Which of the following tools can be used to create Group Policy object (GPO) links to Active Directory?

A. Active Directory Users and Computers

B. Active Directory Domains and Trusts

C. Active Directory Sites and Services

D. Group Policy Management Console

17. To test whether a DNS server is answering queries properly, you can use which of the following tools?

A. The `ping` tool

B. The `nslookup` tool

C. The `tracert` tool

D. The `ipconfig` tool

18. Which of the following is true about the time to live (TTL) attached to a DNS record?

A. A resolver cannot use it; only servers making recursive queries can use it.

B. Only resolvers use it.

C. It is used to determine how long to cache retrieved results.

D. It is refreshed each time the record is modified.

19. Which of the following statements about Windows Server 2012 Dynamic DNS (DDNS) is true?

A. DDNS requires a Microsoft DHCP server to work.

B. The Windows Server 2012 DDNS server can interoperate with recent versions of BIND.

C. DDNS clients may not register their own addresses.

D. DDNS works only with Microsoft clients and servers.

20. You have been given a server that contains three HBAs. Each card can access the storage over a separate path. The application that runs on the server can exceed the usage of a single path. Which of the following MPIO options should be selected to provide the needed bandwidth as well as minimal redundancy?

A. Failover

B. Dynamic Least Queue Depth

C. Weighted path

D. Round robin

21. You need to stop an application from running in Task Manager. Which tab would you use to stop an application from running?

A. Performance

B. Users

C. Options

D. Details

22. As a network administrator, you are responsible for all client computers at the central corporate location. Your company has asked you to make sure that all of the client computers are secure. You need to use MBSA to scan your client computers, based on IP addresses, for possible security violations but you need to use the command-line version. Which of the following command-line commands would you use?

A. `mdsacli.exe /hf -i` *`xxxx.xxxx.xxxx.xxxx`*

B. `mdsacli.exe /ip` *`xxxx.xxxx.xxxx.xxxx`*

C. `mbsa.exe /hf -ip` *xxxx.xxxx.xxxx.xxxx*

D. `mbsa.exe /ip` *xxxx.xxxx.xxxx.xxxx*

23. You are the administrator of a new Windows Server 2012 R2 machine. You need to install DNS and create a primary zone. Which MMC snap-in would you use to install DNS?

A. Add/Remove Programs

B. Programs

C. Server Manager

D. Administrative Tools

24. You are the administrator for a large company that has purchased a new multifunction printer. You want to publish the printer to Active Directory. Where would you click in order to accomplish this task?

A. The Sharing tab

B. The Advanced tab

C. The Device Settings tab

D. The Printing Preferences button

25. Isabel is a system administrator for an Active Directory environment that is running in Native mode. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:

- The accessing of certain sensitive files must be logged.
- Modifications to certain sensitive files must be logged.
- System administrators must be able to provide information about which users accessed sensitive files and when they were accessed.
- All logon attempts for specific shared machines must be recorded.

Which of the following steps should Isabel take to meet these requirements? (Choose all that apply.)

A. Enable auditing with the Computer Management tool.

B. Enable auditing with Group Policy Objects.

C. Enable auditing with the Active Directory Domains and Trusts tool.

D. Enable auditing with the Event Viewer tool.

E. View the audit log using the Event Viewer tool.

F. View auditing information using the Computer Management tool.

G. Enable failure and success auditing settings for specific files stored on NTFS volumes.

H. Enable failure and success auditing settings for logon events on specific computer accounts.

26. You are the network administrator for a large widget distributor. Your company's network has 20 Windows 2012 R2 servers, and all of the clients are running either Windows 8 or Windows 7. All of your end users use laptops to do their work, and many of them work away from the office. What should you configure to help them work on documents when away from the office?

A. Online file access

B. Offline file access

C. Share permissions

D. NTFS permissions

27. Your company has decided to implement an external hard drive. The company IT manager before you always used FAT32 as the system partition. Your company wants to know whether it should move to NTFS. Which of the following are some advantages of NTFS? (Choose all that apply.)

A. Security

B. Quotas

C. Compression

D. Encryption

28. You have been hired by a small company to implement new Windows Server 2012 R2 systems. The company wants you to set up a server for users' home folder locations. What type of server would you be setting up?

A. PDC server

B. Web server

C. Exchange server

D. File server

29. GPOs assigned at which of the following level(s) will override GPO settings at the domain level?

A. OU

B. Site

C. Domain

D. Both OU and site

30. A system administrator wants to ensure that only the GPOs set at the OU level affect the Group Policy settings for objects within the OU. Which option can they use to do this (assuming that all other GPO settings are the defaults)?

A. The Enforced option

B. The Block Policy Inheritance option

C. The Disable option

D. The Deny permission

31. Mateo, a system administrator, is planning to implement Group Policy objects in a new Windows Server 2012 R2 Active Directory environment. To meet the needs of the organization, he decides to implement a hierarchical system of Group Policy settings. At which of the following levels is he able to assign Group Policy settings? (Choose all that apply.)

A. Sites

B. Domains

C. Organizational units

D. Local system

32. Ann is a system administrator for a medium-sized Active Directory environment. She has determined that several new applications that will be deployed throughout the organization use registry-based settings. She would like to do the following:

- Control these registry settings using Group Policy.
- Create a standard set of options for these applications and allow other system administrators to modify them using the standard Active Directory tools.

Which of the following options can she use to meet these requirements? (Choose all that apply.)

A. Implement the inheritance functionality of GPOs.

B. Implement delegation of specific objects within Active Directory.

C. Implement the No Override functionality of GPOs.

D. Create administrative templates.

E. Provide administrative templates to the system administrators who are responsible for creating Group Policy for the applications.

33. You are the network administrator for your organization. A new company policy has been released wherein if a user enters their password incorrectly three times within 5 minutes, they are locked out for 30 minutes. What three actions do you need to set to comply with this policy? (Choose all that apply.)

A. Set Account Lockout Duration to 5 minutes.

B. Set Account Lockout Duration to 30 minutes.

C. Set the Account Lockout Threshold setting to 3 invalid logon attempts.

D. Set the Account Lockout Threshold setting to 30 minutes.

E. Set the Reset Account Lockout Counter setting to 5 minutes.

F. Set the Reset Account Lockout Counter setting to 3 times.

34. You are teaching a Microsoft Active Directory class, and one of your students asks you, "Which of the following containers in the Active Directory Users and Computers tool is used when users from outside the forest are granted access to resources within a domain?" What answer would you give your student?

A. `Users`

B. `Computers`

C. `Domain Controllers`

D. `Foreign Security Principals`

35. Your manager has decided your organization needs to use an Active Directory application data partition. Which command can you use to create and manage application data partitions?

A. `DCPromo.exe`

B. `NTDSUtil.exe`

C. `ADUtil.exe`

D. `ADSI.exe`

36. Your network contains an Active Directory domain named Sybex.com. The domain contains a RADIUS server named Server1 that runs Windows Server 2012 R2. You add a VPN server named Server2 to the network. On Server1, you create several network policies. You need to configure Server1 to accept authentication requests from Server2. Which tool should you use on Server1?

A. Set-RemoteAccessRadius

B. CMAK

C. NPS

D. Routing and Remote Access

37. Your network contains an Active Directory domain named Sybex.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the following role services installed:

- DirectAccess and VPN (RRAS)
- Network Policy Server

Remote users have client computers that run Windows XP, Windows 7, or Windows 8. You need to ensure that only the client computers that run Windows 7 or Windows 8 can establish VPN connections to Server1. What should you configure on Server1?

A. A vendor-specific RADIUS attribute of a Network Policy Server (NPS) connection request policy

B. A condition of a Network Policy Server (NPS) network policy

C. A condition of a Network Policy Server (NPS) connection request policy

D. A constraint of a Network Policy Server (NPS) network policy

38. You are the network administrator for a large organization that contains an Active Directory domain named WillPanek.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed. You plan to deploy 802.1x authentication to secure the wireless network.

You need to identify which Network Policy Server (NPS) authentication method supports certificate-based mutual authentication for the 802.lx deployment. Which authentication method should you identify?

A. PEAP-MS-CHAP v2

B. MS-CHAP v2

C. EAP-TLS

D. MS-CHAP

39. You have an Active Directory domain named WillPanek.com. The domain contains a server named ServerA that runs Windows Server 2012 R2. ServerA has the Network Policy and Access Services server role installed. Your company's security policy requires that certificate-based authentication must be used by some network services. You need to identify which Network Policy Server (NPS) authentication methods comply with the security policy. Which two authentication methods should you identify? Each correct answer presents part of the solution. (Choose two.)

A. MS-CHAP

B. PEAP-MS-CHAP v2

C. CHAP

D. EAP-TLS

E. MS-CHAP v2

40. You are the network administrator, and you have been asked to set up an accounting system so that each department is responsible for the cost of their use of network services. Your network contains a Network Policy Server (NPS) server named ServerA. The network contains a server named Database1 that has Microsoft SQL server installed. All servers run Windows Server 2012 R2. You configure NPS on ServerA to log accounting data to a database on Database1. You need to ensure that the accounting data is captured if Database1 fails. The solution must minimize cost. What should you do?

A. Implement Failover Clustering.

B. Implement database mirroring.

C. Run the Accounting Configuration Wizard.

D. Modify the SQL Server Logging properties.

41. In a secure environment, IPsec encryption should only be disabled for inter-node cluster communication (such as cluster heartbeat) under what circumstances?

A. Certificates use weak encryption methods such as DES

B. LowerQuorumPriorityNodeID is set on a node.

C. DatabaseReadWriteMode is set to 2

D. Group Policy Updates have a high processing latency

42. In Windows Server 2012 R2, Failover Clustering supports how many nodes?

A. 8000

B. 1024

C. 64

D. 1000

43. In Windows Server 2012 R2, what feature dynamically adjusts cluster node votes in order to maintain an odd vote count where no witness is being used?

A. Witness Dynamic Weighting

B. Tie Breaker for a 50% Node Split

C. Lower Quorum Priority Node

D. Force quorum resiliency

44. What authentication mechanism does Active Directory–detached clusters utilize?

A. NTLM

B. MIT Kerberos Realms

C. AD Kerberos

D. SSL

45. Shared virtual hard disks can be utilized by SQL Server and Exchange Server for virtualized workloads.

A. True

B. False

46. What is the default TCP port for iSCSI?

A. 3389

B. 21

C. 1433

D. 3260

47. You are a server administrator, and you are trying to save hard drive space on your Windows Server 2012 R2 machine. Which feature can help you save hard disk space?

A. ADDS

B. `HDSaver.exe`

C. Features On Demand

D. WinRM

48. Your company is headquartered in Colorado Springs and has a remote site location in Tampa. The Colorado Spring office has a file server named FS01. FS01 has the BranchCache for Network Files role service installed. Your Tampa Office has a file server named FS02. FS02 has been configured as a BranchCache-hosted cache server. You need

to preload the data from the file shares on FS01 to the cache on FS02. You have already generated hashes for the file shares on FS01. Which cmdlet should you run next?

A. `Set-BCCache`

B. `Publish-BCFileContent`

C. `Export-BCCachePackage`

D. `Add-BCDataCacheExtension`

49. What command would be used to register an iSCSI initiator manually to an iSNS server?

A. `iscsicli addisnsserver server_name`

B. `iscsicli listisnsservers server_name`

C. `iscsicli removeisnsserver server_name`

D. `iscsicli refreshisnsserver server_name`

50. You have a Windows Server 2012 R2 file server named FS01. FS01 has the File Server Resource Manager role service installed. You attempt to delete a classification property, and you receive the error message "The classification property is in use and cannot be deleted." You need to delete the Contains Personal Information classification property. What should you do?

A. Clear the Contains Personal Information classification property value for all files.

B. Set files that have a Contains Personal Information classification property value of Yes to No.

C. Disable the classification rule that is assigned the Contains Personal Information classification property.

D. Delete the classification rule that is assigned the Contains Personal Information classification property.

51. After you update multiple drivers on your Windows Server 2012 R2 machine, the machine hangs at the logon screen, and you can't log into the machine. You need to get this computer up and running as quickly as possible. Which of the following repair strategies should you try first to correct your problem?

A. Restore your computer's configuration with your last backup.

B. Boot your computer with the Last Known Good Configuration option.

C. Boot your computer with the Safe Mode option.

D. Boot your computer to the Recovery Console and manually copy the old driver back to the computer.

52. You enable the Boot Logging option on the Advanced Boot Options menu. Where can you find the log file that is created?

A. `\Windows\ntbtlog.txt`

B. `\Windows\System32\netlog.txt`

C. `\Windows\netlog.txt`

D. `\Windows\System32\netboot.log`

53. You need to ensure that you can recover your Windows Server 2012 R2 configuration and data if the computer's hard drive fails. What should you do?

A. Create a system restore point.

B. Create a backup of all file categories.

C. Perform an Automated System Recovery (ASR) backup.

D. Create a complete PC Backup and Restore image.

54. You have a file server named FS01 that is running on a server core installation of Windows Server 2012 R2. You need to make sure that your users can access previous versions of files that are shared on FS01 using the Previous Versions tab. Which tool should you use?

A. Wbadmin

B. Vssadmin

C. `Ntsdutil.exe`

D. ADSI Editor

55. You are unable to boot your Windows Server 2012 R2 computer, so you decide to boot the computer to Safe Mode. Which of the following statements regarding Safe Mode is false?

A. When the computer is booted to Safe Mode, there is no network access.

B. Safe Mode loads all of the drivers for the hardware that is installed on the computer.

C. When you run Safe Mode, boot logging is automatically enabled.

D. When you run Safe Mode, the screen resolution is set to 800×600.

56. You are the network administrator for Stellacon Corporation. Stellacon has two trees in its Active Directory forest, `stellacon.com` and `abc.com`. Company policy does not allow DNS zone transfers between the two trees. You need to make sure that when anyone in `abc.com` tries to access the `stellacon.com` domain, all names are resolved from the `stellacon.com` DNS server. What should you do?

A. Create a new secondary zone in `abc.com` for `stellacon.com`.

B. Create a new secondary zone in `stellacon.com` for `abc.com`.

C. Configure conditional forwarding on the `abc.com` DNS server for `stellacon.com`.

D. Configure conditional forwarding on the `stellacon.com` DNS server for `abc.com`.

57. Your IT team has been informed by the compliance team that they need copies of the DNS Active Directory Integrated zones for security reasons. You need to give the Compliance department a copy of the DNS zone. How should you accomplish this goal?

A. Run `dnscmd /zonecopy`.

B. Run `dnscmd /zoneinfo`.

C. Run `dnscmd /zonefile`.

D. Run `dnscmd /zoneexport`.

58. You administer a network that assigns IP addresses via DHCP. You want to make sure that one of the clients always receives the same IP address from the DHCP server. You create an exclusion for that address, but you find that the computer isn't being properly configured at bootup. What's the problem?

A. You excluded the wrong IP address.

B. You must configure the client manually. You cannot assign the address via the DHCP server.

C. You need to create a superscope for the address.

D. You need to make a reservation for the client that ties the IP address to the computer's MAC address. Delete the exclusion.

59. You are the network administrator for a small company with two DNS servers: DNS1 and DNS2. Both DNS servers reside on domain controllers. DNS1 is set up as a standard primary zone, and DNS2 is set up as a secondary zone. A new security policy was written stating that all DNS zone transfers must be encrypted. How can you implement the new security policy?

A. Enable the Secure Only setting on DNS1.

B. Enable the Secure Only setting on DNS2.

C. Configure Secure Only on the Zone Transfers tab for both servers.

D. Delete the secondary zone on DNS2. Convert both DNS servers to use Active Directory Integrated zones.

60. You are the network administrator for a midsize computer company. You have a single Active Directory forest, and your DNS servers are configured as Active Directory Integrated zones. When you look at the DNS records in Active Directory, you notice that there are many records for computers that do not exist on your domain. You want to make sure that only domain computers register with your DNS servers. What should you do to resolve this issue?

A. Set dynamic updates to None.

B. Set dynamic updates to Nonsecure And Secure.

C. Set dynamic updates to Secure Only.

D. Set dynamic updates to Domain Users Only.

61. Which of the following does not need to be created manually when you are setting up a replication scenario involving three domains and three sites?

A. Sites

B. Site links

C. Subnets

D. Connection objects

62. You need to deactivate the UGMC option on some of your domain controllers. At which level in Active Directory would you deactivate UGMC?

A. Server

B. Forest

C. Domain

D. Site

63. Your network contains two Active Directory forests named `contoso.com` and `fabrikam.com`. Both forests contain multiple domains. All domain controllers run Windows Server 2012 R2. `contoso.com` has a one-way forest trust to `fabrikam.com`. A domain named `paris.eu.contoso.com` hosts several legacy Applications that use NTLM authentication. Users in a domain named `london.europe.fabrikam.com` report that it takes a long time to be authenticated when they attempt to access the legacy Applications hosted in `paris.eu.contoso.com`. You need to reduce how long it takes for the `london.europe.fabrikam.com` users to be authenticated in `paris.eu.contoso.com`. What should you do?

A. Create an external trust

B. Create a two-way transitive trust

C. Disable SID filtering on the existing trust

D. Create a shortcut trust

64. A system administrator suspects that there is an error in the replication configuration. How can the system administrator look for specific error messages related to replication?

A. By going to Event Viewer ➢ Directory Service Log

B. By using the Computer Management tool

C. By going to Event Viewer ➢ System Log

D. By using the Active Directory Sites and Services administrative tool

65. Which of the following services of Active Directory is responsible for maintaining the replication topology?

A. File Replication Service

B. Windows Internet Name Service

C. Knowledge Consistency Checker

D. Domain Name System

66. You are the administrator at Adacom. You need to make sure that you have daily backup of the AD CS database, logs, and private key. What command or commands should you run? (Choose all that apply.)

A. Run `certutil -backup`.

B. Run `certutil -backupdb`.

C. Run `Ntbackup /systemstate`.

D. Run `certdb.ps1`.

67. You are the new administrator at MMG Publishing. The previous administrator made a failed attempt to implement Active Directory. You attempt to implement AD RMS and receive an error that states, "The SCP is registered, but the root cluster cannot be contacted." You must remove the SCP. What tool should you use? (Choose all that apply.)

A. Setspn

B. Active Directory Sites and Services

C. ADSI Edit

D. Remove-SCP

68. ABC Company wants to allow external partners to log into a web application and run reports. What AD FS component does Company ABC need to configure for this access?

A. Certificate exchange

B. Transitive trust

C. One-way trust

D. Relying-party trust

69. Which TCP ports does AD RMS use to access the global catalog server?

A. 445

B. 1433

C. 22

D. 3268

Answers to the Assessment Test

1. D. Based on the business needs of an organization, a Windows 2012 R2 Server computer can be configured in any of the roles listed. See Chapter 1 for more information.

2. A, B, C and D. All of the options listed are benefits of using Active Directory. See Chapter 3 for more information.

3. A, B, C and D. One of the major design goals for DNS was support for scalability. All of the features listed can be used to increase the performance of DNS. See Chapter 2 for more information.

4. A, B, C and D. Before beginning the installation of a domain controller, you should have all of the information listed. See Chapter 3 for more information.

5. D. The number of sites in an Active Directory environment is independent of the domain organization. An environment that consists of three domains may have one or more sites, based on the physical network setup. See Chapter 3 for more information.

6. E. All of the choices are valid types of Active Directory objects, and all can be created and managed using the Active Directory Users and Computers tool. See Chapter 5 for more information.

7. C. Permissions and security settings cannot be made on distribution groups. Distribution groups are used only for sending email. See Chapter 4 for more information.

8. A. In general, you can accommodate your network infrastructure through the use of Active Directory sites. All of the other options should play a significant role when you design your OU structure. Permissions and Group Policy can both be applied at the domain or OU level. See Chapter 4 for more information.

9. B. Printer and Shared Folder objects within Active Directory can point to Windows Server 2012 R2 file and printer resources. See Chapter 4 for more information.

10. B. Delegation is the process by which administrators can assign permissions on the objects within an OU. This is useful when administrators want to give other users more control over administrative functions in Active Directory. See Chapter 4 for more information.

11. C. The name of the server and the name of the share make up the Universal Naming Convention (UNC) information required to create a Shared Folder object. See Chapter 4 for more information.

12. D. Applications cannot be published to computers, but they can be published to users and assigned to computers. See Chapter 5 for more information.

13. A. MSI files (`.msi`) are native Windows Installer files used with Windows Installer setup programs. The other file types do not apply to this situation. See Chapter 5 for more information.

14. E. To allow this permission at the OU level, the system administrator must create a GPO with the appropriate settings and link it to the OU. See Chapter 5 for more information.

15. A. Assuming that the default settings are left in place, the Group Policy setting at the OU level will take effect. See Chapter 5 for more information.

16. D. In Windows Server 2012 R2, you can create GPOs only by using the Group Policy Management Console. See Chapter 5 for more information.

17. B. The `nslookup` tool allows you to look up name and address information. See Chapter 2 for more information.

18. C. The TTL indicates how long the record may be safely cached; it may or may not be modified when the record is created. See Chapter 2 for more information on TTL.

19. B. DDNS works with BIND 8.2 and later. See Chapter 2 for more information on DDNS.

20. D. A round-robin configuration uses all of the available active paths and will distribute I/O in a balanced round-robin fashion. Failover uses only the primary and standby paths, allowing for link failure. Weighted path assigns requests to the path with the least weight value. Dynamic Least Queue Depth routes requests to the path with the least number of outstanding requests. See Chapter 2 for more information.

21. D. All of the applications that are running on the Windows Server 2012 R2 machine will show up under the Details tab. Right-click the application and end the process.

22. A. If you use MBSA from the command-line utility `mdsacli.exe`, you can specify several options. You type **`mdsacli.exe/hf`** (from the folder that contains `Mdsacli.exe`) and then customize the command execution with an option such as `/i`*`xxxx.xxxx.xxxx.xxxx`*, which specifies that the computer with the specified IP address should be scanned.

23. C. Server Manager is the one place where you install all roles and features for a Windows Server 2012 R2 system.

24. A. The Sharing tab contains a check box that you can use to list the printer in Active Directory.

25. B, E, G and H. The Active Directory Users and Computers tool allows system administrators to change auditing options and to choose which actions are audited. At the file system level, Isabel can specify exactly which actions are recorded in the audit log. She can then use Event Viewer to view the recorded information and provide it to the appropriate managers.

26. B. Offline files give you the opportunity to set up files and folders so that users can work on the data while outside the office.

27. A, B, C and D. Improved security, quotas, compression, and encryption are all advantages of using NTFS over FAT32. These features are not available in FAT32. The only security you have in FAT32 is shared folder permissions.

28. D. File servers are used for storage of data, especially for users' home folders. Home folders are folder locations for your users to store data that is important and that needs to be backed up.

29. A. GPOs at the OU level take precedence over GPOs at the domain level. GPOs at the domain level, in turn, take precedence over GPOs at the site level.

30. B. The Block Policy Inheritance option prevents group policies of higher-level Active Directory objects from applying to lower-level objects as long as the Enforced option is not set.

31. A, B, C and D. GPOs can be set at all of the levels listed. You cannot set GPOs on security principals such as users or groups.

32. D and E. Administrative templates are used to specify the options available for setting Group Policy. By creating new administrative templates, Ann can specify which options are available for the new applications. She can then distribute these templates to other system administrators in the environment.

33. B, C and E. The Account Lockout Duration setting states how long an account will be locked out if the password is entered incorrectly. The Account Lockout Threshold setting is the number of bad password attempts, and the Account Lockout Counter setting is the time in which the bad password attempts are made. Once the Account Lockout Counter setting reaches 0, the number of bad password attempts returns to 0.

34. D. When resources are made available to users who reside in domains outside the forest, Foreign Security Principal objects are automatically created. These new objects are stored within the `Foreign Security Principals` container.

35. B. The primary method by which systems administrators create and manage application data partitions is through the `ntdsutil` tool.

36. C. The NPS snap-in allows you to set up RADIUS servers and designate which RADIUS server will accept authentication from other RADIUS servers. You can do your entire RADIUS configuration through the NPS snap-in.

37. C. NPS allows you to set up policies on how your users could log into the network. NPS allows you to set up policies that systems need to follow, and if they don't follow these policies or rules, they will not have access to the full network.

38. C. Windows Server 2012 R2 comes with *EAP-Transport Level Security (TLS)*. This EAP type allows you to use public key certificates as an authenticator. TLS is similar to the familiar Secure Sockets Layer (SSL) protocol used for web browsers and 802.1x authentication. When EAP-TLS is turned on, the client and server send TLS-encrypted messages back and forth. EAP-TLS is the strongest authentication method you can use; as a bonus, it supports smart cards. However, EAP-TLS requires your NPS server to be part of the Windows Server 2012 R2 domain.

39. B and D. PEAP-MS-CHAP v2 is an EAP type protocol that is easier to deploy than Extensible Authentication Protocol with Transport Level Security (EAP-TLS). It is easier because user authentication is accomplished by using password-based credentials (user name and password) instead of digital certificates or smart cards. Both PEAP and EAP use certificates with their protocols.

40. C. One advantage of NPS is that you can use the accounting part of NPS so that you can keep track of what each department does on your NPS server. This way, departments pay for the amount of time they use the SQL server database.

41. D. Group Policy Updates have a high processing latency, because IPsec encryption is interrupted until updates to the Group Policies are complete. If the updates to Group Policy do not occur quickly, cluster heartbeat can be impacted (eg if the processing delay exceeds the heartbeat threshold).

42. C. In Windows Server 2012, the number of cluster nodes increased to 64. 8000 is the number of VMs/Clustered Roles. 1024 is the maximum amount of VMs or Clustered Roles per cluster node, and 1000 is the maximum amount of VMs or Clustered Roles per cluster node in Windows Server 2008 R2.

43. B. Witness Dynamic Weighting and Lower Quorum Priority Node are options in PowerShell to modify Dynamic Quorum, but they are not a good answer. Force quorum resiliency is completely incorrect.

44. A. NTLM is the only supported authentication mechanism that will utilize local security authorities (non-active directory integrated Windows Servers).

45. A. Prior to Windows Server 2012 R2, shared virtual hard disks did not exist. At release of Windows Server 2012 R2, shared virtual disks were supported for file server roles as well as Exchange Server and SQL Server workloads.

46. D. The iSCSI default port is TCP 3260. Port 3389 is used for RDP, port 1433 is used for MS SQL, and port 21 is used for FTP.

47. C. Windows Server 2012 R2 Features On Demand allows an administrator not only to disable a role or feature but also to remove the role or feature's files completely from the hard drive.

48. C. After generating hashes on the Colorado Springs file server that will be preloading Tampa's file server cache with file share data, the next logical step is to run the `Export-BCCachePackage` to get the data to FS02 from FS01.

49. A. The `iscsicli addisnsserver server_name` command manually registers the host server to an iSNS server. `refreshisnsserver` refreshes the list of available servers. `removeisnsserver` removes the host from the iSNS server. `listisnsservers` lists the available iSNS servers.

50. D. Since there is a classification rule that is currently configured and applied to company resources, you will be unable to delete the Contains Personal Information classification property manually because the classification rule controls the property. In this case, you have to delete the classification rule in order to be able to delete the classification property.

51. B. If you need to get a stalled computer up and running as quickly as possible, you should start with the Last Known Good Configuration option. This option is used when you've made changes to your computer's hardware configuration and are having problems restarting but have not logged into the machine. The Last Known Good Configuration option will revert to the configuration used the last time the computer was successfully booted.

52. A. When you enable boot logging, the file created is `\Windows\ntbtlog.txt`. This log file is used to troubleshoot the boot process.

53. D. Using images allows you to back up and restore your entire Windows Server 2012 R2 machine instead of just certain parts of data.

54. B. Out of the tools listed, remember that Vssadmin gives you the ability to use Shadow Copies, which in turn provides backups and previous versions of shared data. Wbadmin is used for Windows Server Backups, `Ntsdutil.exe` is used for Active Directory maintenance, and the ADSI Editor is used for extended Active Directory attribute management.

55. B. When you run your computer in Safe Mode, you simplify your Windows Server 2012 R2 configuration. Only the drivers that are needed to get the computer up and running are loaded.

56. C. Conditional forwarding allows you to send a DNS query to different DNS servers based on the request. Conditional forwarding lets a DNS server on a network forward DNS queries according to the DNS domain name in the query.

57. D. The `dnscmd /zoneexport` command creates a file using the zone resource records. This file can then be given to the Compliance department as a copy.

58. D. An exclusion just marks addresses as excluded; the DHCP server doesn't maintain any information about them. A reservation marks an address as reserved for a particular client.

59. D. Active Directory Integrated zones give you many benefits over using primary and secondary zones including less network traffic, secure dynamic updates, encryption, and reliability in the event of a DNS server going down. The Secure Only option is for dynamic updates to a DNS database.

60. C. The Secure Only option is for DNS servers that have an Active Directory Integrated zone. When a computer tries to register with DNS dynamically, the DNS server checks Active Directory to verify that the computer has an Active Directory account. If the computer that is trying to register has an account, DNS adds the host record. If the computer trying to register does not have an account, the record gets tossed away and the database is not updated.

61. D. By default, Connection objects are automatically created by the Active Directory replication engine. You can choose to override the default behavior of Active Directory replication topology by manually creating Connection objects, but this step is not required.

62. D. The NTDS settings for the site level are where you would activate and deactivate UGMC.

63. D. Remember that a shortcut trust is used to eliminate multiple hops to and from certain domains within a multiforest, multidomain infrastructure. By configuring a shortcut trust between the two domains, you will reduce the slowness and authentication latency between them.

64. A. The Directory Service event log contains error messages and information related to replication. These details can be useful when you are troubleshooting replication problems.

65. C. The Knowledge Consistency Checker (KCC) is responsible for establishing the replication topology and ensuring that all domain controllers are kept up-to-date.

66. A and B. `Certutil -backup` backs up the CA certificate including private key in the backup. `Certutil -backupdb` backs up only the certificate database and logs.

67. B and C. Under AD Sites and Services, navigate to Services ➢ RightsManagementServices and remove the SCP object. This operation can also be done by using ADSI Edit.

68. D. The relying party is the organization that receives and processes claims from a resource partner. The resource partner issues claims-based security tokens that contains published web-based applications that users in the account partner can access. This is accomplished through a relying-party trust. See Chapter 22 for more details.

69. D. AD RMS contacts the global catalog through port 3268. See Chapter 22 for more details.

MCSA

Windows Server® 2012 R2

Complete Study Guide

Exam 70-410: Installing and Configuring Windows Server 2012 R2

CHAPTER 1 ■ Install Windows Server 2012 R2

CHAPTER 2 ■ Configure Network Services

CHAPTER 3 ■ Plan and Install Active Directory

CHAPTER 4 ■ Configure Windows Server 2012 R2

CHAPTER 5 ■ Administer Active Directory

CHAPTER 6 ■ Manage GPOs

CHAPTER 7 ■ Manage Security

CHAPTER 8 ■ Configure TCP/IP

CHAPTER 9 ■ Use Virtualization in Windows Server 2012

Chapter 1

Install Windows Server 2012 R2

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Install servers**

- Plan for a server installation
- Plan for server roles
- Plan for a server upgrade
- Install Server Core
- Optimize resource utilization by using Features on Demand
- Migrate roles from previous versions of Windows Server
- Configure Server Core
- Add and remove features in offline images
- Deploy roles on remote servers
- Convert Server Core to/from full GUI
- Configure NIC teaming

✓ **Configure local storage**

- Design storage spaces
- Configure basic and dynamic disks
- Configure MBR and GPT disks
- Manage volumes
- Create and mount virtual hard disks
- Configure storage pools and disk pools

This chapter covers the installation of Windows Server 2012 R2. It shows how to install both the full version of Windows Server 2012 R2 and the Server Core version. It also shows you how to use some PowerShell commands in Windows Server 2012 R2 Server Core.

Let's dive right into the server by talking about some of the new features and advantages of Windows Server 2012 R2.

Features and Advantages of Windows Server 2012 and Server 2012 R2

Before I show how to install and configure Windows Server 2012 R2, let's take a look at some of the new features and the advantages it offers.

Since many of you will be upgrading from Windows Server 2003 and Windows Server 2008/2008 R2, these are the new features introduced by Microsoft since then. I will specifically identify any new features or advantages that are new to Windows Server 2012 R2 only.

I will talk about all of these features in greater detail throughout this book. What follows are merely brief descriptions.

Active Directory Certificate Services *Active Directory Certificate Services (AD CS)* provides a customizable set of services that allow you to issue and manage *public key infrastructure (PKI) certificates*. These certificates can be used in software security systems that employ public key technologies.

Active Directory Domain Services *Active Directory Domain Services (AD DS)* includes new features that make deploying domain controllers simpler and that let you implement them faster. AD DS also makes the domain controllers more flexible, both to audit and to authorize for access to files. Moreover, AD DS has been designed to make performing administrative tasks easier through consistent graphical and scripted management experiences.

Active Directory Rights Management Services *Active Directory Rights Management Services (AD RMS)* provides management and development tools that let you work with

industry security technologies, including encryption, certificates, and authentication. Using these technologies allows organizations to create reliable information protection solutions.

BitLocker *BitLocker* is a tool that allows you to encrypt the hard drives of your computer. By encrypting the hard drives, you can provide enhanced protection against data theft or unauthorized exposure of your computers or removable drives that are lost or stolen.

BranchCache *BranchCache* allows data from files and web servers on a wide area network (WAN) to be cached on computers at a local branch office. By using BranchCache, you can improve application response times while also reducing WAN traffic. Cached data can be either distributed across peer client computers (distributed cache mode) or centrally hosted on a server (hosted cache mode). BranchCache is included with Windows Server 2012 R2 and Windows 8.

In this book, I will refer to *Windows 8*, which includes both Windows 8 and Windows 8.1. This is also true for *Windows Server 2008*. It will be used for both Windows Server 2008 and Windows Server 2008 R2. If, for some reason, both versions of Server 2008 did not cover an item, I will actually say 2008 R2.

DHCP *Dynamic Host Configuration Protocol (DHCP)* is an Internet standard that allows organizations to reduce the administrative overhead of configuring hosts on a TCP/IP-based network. Some of the new features are DHCP failover, policy-based assignment, and the ability to use Windows PowerShell for DHCP Server.

DNS *Domain Name System (DNS)* services are used in TCP/IP networks. DNS will convert a computer name or fully qualified domain name (FQDN) to an IP address. DNS also has the ability to do a reverse lookup and convert an IP address to a computer name. DNS allows you to locate computers and services through user-friendly names.

Failover Clustering *Failover Clustering* gives an organization the ability to provide high availability and scalability to networked servers. Failover clusters can include file share storage for server applications, such as Hyper-V and Microsoft SQL Server, and those that run on physical servers or virtual machines.

File Server Resource Manager *File Server Resource Manager* is a set of tools that allows administrators to manage and control the amount and type of data stored on the organization's servers. By using File Server Resource Manager, administrators have the ability to set up file management tasks, use quota management, get detailed reports, set up a file classification infrastructure, and configure file-screening management.

Hyper-V *Hyper-V* is one of the most changed features in Windows Server 2012 R2. Microsoft's new slogan is "Windows Server 2012 R2, built from the cloud up," and this has a lot to do with Hyper-V. It allows an organization to consolidate servers by creating and managing a virtualized computing environment. It does this by using virtualization technology that is built into Windows Server 2012 R2.

Hyper-V allows you to run multiple operating systems simultaneously on one physical computer. Each virtual operating system runs in its own virtual machine environment. I cover Hyper-V in detail in Chapter 9: "Use Virtualization in Windows Server 2012."

IPAM *IP Address Management (IPAM)* is one of the features introduced with Windows Server 2012 R2. IPAM allows an administrator to customize and monitor the IP address infrastructure on a corporate network.

Kerberos Authentication Windows Server 2012 R2 uses the *Kerberos authentication* (version 5) protocol and extensions for password-based and public key authentication. The Kerberos client is installed as a *security support provider (SSP)*, and it can be accessed through the *Security Support Provider Interface (SSPI)*.

Managed Service Accounts (gMSAs) Stand-alone *managed service accounts*, originally created for Windows Server 2008 R2 and Windows 7, are configured domain accounts that allow automatic password management and *service principal names* (SPNs) management, including the ability to delegate management to other administrators.

Networking There are many networking technologies and features in Windows Server 2012 R2, including BranchCache, Data Center Bridging (DCB), NIC Teaming, and many more.

Remote Desktop Services Before Windows Server 2008, we used to refer to this as Terminal Services. *Remote Desktop Services* allows users to connect to virtual desktops, RemoteApp programs, and session-based desktops. Using Remote Desktop Services allows users to access remote connections from within a corporate network or from the Internet.

Security Auditing *Security auditing* gives an organization the ability to help maintain the security of an enterprise. By using security audits, you can verify authorized or unauthorized access to machines, resources, applications, and services. One of the best advantages of security audits is to verify regulatory compliance.

Smart Cards Using *smart cards* (referred to as *two-factor authentication*) and their associated *personal identification numbers (PINs)* is a popular, reliable, and cost-effective way to provide authentication. When using smart cards, the user not only must have the physical card but also must know the PIN to be able to gain access to network resources. This is effective because even if the smart card is stolen, thieves can't access the network unless they know the PIN.

TLS/SSL (Schannel SSP) *Schannel* is a security support provider (SSP) that uses the *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)* Internet standard authentication protocols together. The Security Support Provider Interface is an API used by Windows systems to allow security-related functionality, including authentication.

Windows Deployment Services *Windows Deployment Services* allows an administrator to install Windows operating systems remotely. Administrators can use Windows Deployment Services to set up new computers by using a network-based installation.

Planning the Windows Server 2012 R2 Installation

Before you install Windows Server 2012 R2, you must first ask yourself these important questions: What type of server do I need? Will the server be a domain controller? What roles do I need to install on this server?

Once you have figured out what you need the server to do, you can make a game plan for the installation. So, let's start by looking at some of the server roles and technologies that can be installed on a Windows Server 2012 R2 computer.

Server Roles in Windows Server 2012 R2

When you install Windows Server 2012 R2, you have to decide which roles and features are going to be installed onto that server. This is an important decision in the computer world. Many administrators not only overuse a server but also underutilize servers in their organization.

For example, many administrators refuse to put any other roles or features on a domain controller. This may not be a good use of a server. Domain controllers help authenticate users onto the network, but after that the domain controllers are really not very busy all day long. Domain controllers have tasks that they must perform all day, but the server on which they reside is not heavily used when compared to a SQL Server machine or an Exchange mail server. This is where monitoring your server can be useful.

Now let's take a look at some of the roles and features you can install onto a Windows Server 2012 R2 machine. Knowing the different roles and features you can install will help you to design, deploy, manage, and troubleshoot technologies in Windows Server 2012 R2. Figure 1.1 shows the Add Roles And Features Wizard in Server Manager. It shows you just some of the roles that can be installed on a Windows Server 2012 R2 machine.

Roles and Features

Many of these features were discussed in the section "Features and Advantages of Windows Server 2012 and Server 2012 R2." I include them here again because they are also *roles* that can also be installed on Windows Server 2012 R2.

The following roles are available in Windows Server 2012 R2:

Active Directory Certificate Services The AD CS server role in Windows Server 2012 R2 allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

FIGURE 1.1 Available roles in Windows Server 2012 R2

Feature AD CS provides a customizable set of services that allows you to issue and manage PKI certificates. These certificates can be used in software security systems that employ public key technologies.

Role AD CS in Windows Server 2012 R2 is the server role that allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

Active Directory Domain Services The AD DS server role allows you to create a scalable, secure, and manageable infrastructure for user and resource management and to provide support for directory-enabled applications, such as Microsoft Exchange Server.

Active Directory Federation Services *Active Directory Federation Services (AD FS)* provides Internet-based clients with a secure identity access solution that works on both Windows and non-Windows operating systems. AD FS gives users the ability to do a *single sign-on (SSO)* and access applications on other networks without needing a secondary password.

Active Directory Lightweight Directory Services *Active Directory Lightweight Directory Services (AD LDS)* is a *Lightweight Directory Access Protocol (LDAP)* directory service that provides flexible support for directory-enabled applications, without the dependencies and domain-related restrictions of AD DS.

Active Directory Rights Management Services Active Directory Rights Management Services (AD RMS) in Windows Server 2012 R2 is the server role that provides you with management and development tools that work with industry security technologies including encryption, certificates, and authentication to help organizations create reliable information protection solutions.

Application Server *Application Server* provides an integrated environment for deploying and running custom, server-based business applications.

Failover Clustering The Failover Clustering feature provides a way to create, configure, and manage failover clusters for up to 4,000 virtual machines or up to 64 physical nodes.

File and Storage Services *File and Storage Services* allows an administrator to set up and manage one or more file servers. These servers can provide a central location on your network where you can store files and then share those files with network users. If users require access to the same files and applications or if centralized backup and file management are important issues for your organization, administrators should set up network servers as a file server.

Group Policy *Group policies* are a set of rules and management configuration options that you can control through the Group Policy settings. These policy settings can be placed on users' computers throughout the organization.

Hyper-V The Hyper-V role allows administrators to create and manage a virtualized environment by taking advantage of the technology built into the Windows Server 2012 R2 operating system. When an administrator installs the Hyper-V role, all required virtualization components are installed.

Some of the required components include the Windows hypervisor, Virtual Machine Management Service, the virtualization WMI provider, the virtual machine bus (VMbus), the virtualization service provider (VSP), and the virtual infrastructure driver (VID).

Networking This feature allows administrators to design, deploy, and maintain a Windows Server 2012 R2 network. The networking features include 802.1X authenticated wired and wireless access, BranchCache, Data Center Bridging, low-latency workload technologies, and many more.

Network Load Balancing The *Network Load Balancing (NLB)* feature dispenses traffic across multiple servers by using the TCP/IP networking protocol. By combining two or more computers that are running applications in Windows Server 2012 R2 into a single virtual cluster, NLB provides reliability and performance for mission-critical servers.

Network Policy and Access Services Use the *Network Policy and Access Services* server role to install and configure *Network Access Protection (NAP)*, secure wired and wireless access points, and RADIUS servers and proxies.

Print and Document Services *Print and Document Services* allows an administrator to centralize print server and network printer tasks. This role also allows you to receive scanned documents from network scanners and route the documents to a shared network resource, Windows SharePoint Services site, or email addresses. Print and Document

Services also provides fax servers with the ability to send and receive faxes while also giving the administrator the ability to manage fax resources such as jobs, settings, reports, and fax devices on the fax server.

Remote Desktop Services Remote Desktop Services allows for faster desktop and application deployments to any device, improving remote user effectiveness while helping to keep critical data secure. Remote Desktop Services allows for both a *virtual desktop infrastructure (VDI)* and session-based desktops, allowing users to connect from anywhere.

Security and Protection Windows Server 2012 R2 has many new and improved security features for your organization. These security features include Access Control, AppLocker, BitLocker, Credential Locker, Kerberos, NTLM, passwords, security auditing, smart cards, and Windows Biometric Framework (WBF).

Telemetry The *Telemetry* service allows the Windows Feedback Forwarder to send feedback to Microsoft automatically by deploying a Group Policy setting to one or more organizational units. Windows Feedback Forwarder is available on all editions of Windows Server 2012 R2, including Server Core.

Volume Activation Windows Server 2012 R2 *Volume Activation* will help your organization benefit from using this service to deploy and manage volume licenses for a medium to large number of computers.

Web Server (IIS) The *Web Server (IIS)* role in Windows Server 2012 R2 allows an administrator to set up a secure, easy-to-manage, modular, and extensible platform for reliably hosting websites, services, and applications.

Windows Deployment Services Windows Deployment Services allows an administrator to install a Windows operating system over the network. Administrators do not have to install each operating system directly from a CD or DVD.

Windows Server Backup Feature The *Windows Server Backup* feature gives an organization a way to back up and restore Windows servers. You can use Windows Server Backup to back up the entire server (all volumes), selected volumes, the system state, or specific files or folders.

Windows Server Update Services *Windows Server Update Services (WSUS)* allows administrators to deploy application and operating system updates. By deploying WSUS, administrators have the ability to manage updates that are released through Microsoft Update to computers in their network. This feature is integrated with the operating system as a server role on a Windows Server 2012 R2 system.

Migrating Roles and Features to Windows Server 2012 R2

Once you decide on which roles and features you are going to install onto your Windows Server 2012 R2 system, then you either have to install those roles and features from scratch or migrate them from a previous version of Windows server.

Windows Server 2012 R2 includes a set of migration tools that administrators can use to help ease the process of migrating server roles, features, operating system settings, and data. Administrators can migrate this data from an existing server that is running Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2 to a computer that is running Windows Server 2012 R2.

Using Windows Server Migration Tools to migrate roles, role services, and features can simplify the deployment of new servers. You can migrate roles and features on servers running the Server Core installation option of Windows Server 2012 R2 and virtual servers. By using Windows Server Migration Tools, an administrator can reduce migration downtime, increase the accuracy of the migration process, and help eliminate conflicts that could otherwise occur during the migration process.

One advantage of using the migration tools is that most of them support cross-architecture migrations (x86-based to x64-based computing platforms), migrations between physical and virtual environments, and migrations between both the full and Server Core installation options of the Windows Server operating system. In Windows Server 2012 R2, Windows Server Migration Tools also supports cross-subnet migrations.

To use Windows Server Migration Tools, the feature must be installed on both the source and destination computers. Windows Server Migration Tools installation and preparation can be divided into the following stages:

1. Installing Windows Server Migration Tools on destination servers that run Windows Server 2012 R2
2. Creating deployment folders on destination servers that run Windows Server 2012 R2 for copying to source servers
3. Copying deployment folders from destination servers to source servers
4. Registering Windows Server Migration Tools on source servers

If you plan to use Windows Server Migration Tools, you must be a member of the Administrators group on both the source and destination servers to install, remove, or set up the tools.

Administrators can install Windows Server Migration Tools by using either the Add Roles Or Features Wizard in Server Manager or Windows PowerShell deployment cmdlets for Server Manager.

To install Windows Server Migration Tools on a Server Core installation of Windows Server 2012 R2, you would complete the following steps:

1. Open a Windows PowerShell session by typing **`powershell.exe`** in the current command prompt session and then pressing Enter.
2. In the Windows PowerShell session, install Windows Server Migration Tools by using the Windows PowerShell `Install-WindowsFeature` cmdlet for Server Manager. In the Windows PowerShell session, type the following, and then press Enter. (Omit the `ComputerName` parameter if you are installing the Windows Server Migration Tools on the local server.)

   ```
   Install-WindowsFeature Migration -ComputerName computer_name
   ```

Roles and Features That Have Been Reduced in Windows Server 2012 R2

One thing that we want to look at is which Roles and Features are being deprecated or removed from Windows Server 2012 and Windows Server 2012 R2. Table 1.1 was taken directly from Microsoft's website (`http://technet.microsoft.com/en-us/library/dn303411.aspx`), and this table may change at any time. Thus I would recommend that you go out to Microsoft's website to see the current list of Roles and Features.

Table 1.1 lists the features and functionalities in Windows Server 2012 and Windows Server 2012 R2 that either have been removed from the product in the current release or are planned for potential removal in subsequent releases (shown as *deprecated*).

TABLE 1.1 Roles and Features Updates

	Windows Server 2012		Windows Server 2012 R2	
	Removed	**Deprecated**	**Removed**	**Deprecated**
AD FS v1 Web Agent			X	
AD FS in-place upgrade from AD FS 1.0 or "out-of-the-box" AD FS 2.0	X			
AD FS support for "Resource Group"	X			
AD FS support for NT Token mode	X			
AD FS support for using AD LDS as an authentication store	X			
AD RMS license revocation				X
AD RMS SDK				X
Application Server role				X
Built-in drivers for tape drives				X
Cluster Automation Server COM API	X (Optional)		X (Optional)	
Cluster.exe command-line interface	X (Optional)		X (Optional)	

CertObj COM and InetInfo interfaces of the Web Server role				X
Dcpromo.exe		X		
Dfscmd.exe				X
Drivers for Jet Red RDBMS and ODBC		X		X
File Replication Service				X
Internet Information Service (IIS) 6.0 Manager				X
Layered Service Providers		X		X
LPR/LPD protocol		X		X
Namespace for version 1.0 of WMI; WMIC (in WMI)		X	X	
NDIS version 5.0, 5.1, and 5.2 APIs		X	X	
Net DMA	X			
Network Access Protection (NAP)				X
Network Information Service (NIS) and Tools (in RSAT)				X
Nfsshare.exe				X
NFSv2 support				X
Oclist.exe	X			
ODBC support for 16- and 32-bit applications and drivers		X		X
ODBC/OLEDB support for Microsoft Oracle		X		
ODBC/OLEDB support for SQL beyond SQL Server 7 and SQL 2000		X		X

TABLE 1.1 Roles and Features Updates *(continued)*

	Windows Server 2012		Windows Server 2012 R2	
	Removed	**Deprecated**	**Removed**	**Deprecated**
Providers for SNMP, Win32_ ServerFeature API, Active Directory, MSClus WMI1.0 (in WMI)		X		X
Recovery disk creation			X	
Remote Data Service		X		
Role Collector (Ceiprole.exe) and associated API	X			
SCSIport host-bus adapter	X			
Servermanagercmd.exe		X	X	
SIS Limited API				X
Slmgr.vbs options			X	
SMB 1.0				X
SMB.sys	X			
SMTP and associated management tools		X		X
SQLXMLX		X		X
Storage Explorer snap-in for MMC	X			
Storage Manager for SANs snap-in for MMC	X			
Subsystem for UNIX-based applications		X	X	
Support for 32-bit cluster resource DLLs	X			
Support for hardware drivers for XDDM	X			

Support for Microsoft SQL Server prior to 7.0	X			
Support for native VGA via the PC/AT BIOS or UEFI CSM	X			
Support for Static VMQ	X			
Support for Token Rings	X			
Support for Visual Studio Analyzer 2003 over ODBC, OLEDB, and ADO	X			
System Image Backup (“Windows 7 File Recovery”)			X	
Telnet server				X
VM Chimney (also called TCP Offload) in Hyper-V	X			
Windows Server 2003 domain and functional levels of Active Directory				X
Windows Authorization Manager (AzMan)		X	X	
Windows Help executable (WinHlp32.exe)	X			
Windows Identity Foundation 3.5				X
Windows Server Resource Manager		X	X	
Winsock Direct		X	X	
WMI root/virtualization namespace v1 (in Hyper-V)		X	X	
XDR schema elements, XSI pattern feature of MSXML3 (in XML)		X		X

Deciding Which Windows Server 2012 R2 Versions to Use

You may be wondering which version of Windows Server 2012 R2 is best for your organization. After all, Microsoft offers the following four versions of Windows Server 2012 R2.

Windows Server 2012 R2 Datacenter This version is designed for organizations that are looking to migrate to a highly virtualized, private cloud environment. Windows Server 2012 R2 Datacenter has full Windows Server functionality with unlimited virtual instances.

Windows Server 2012 R2 Standard This version is designed for organizations with physical or minimally virtualized environments. Windows Server 2012 R2 Standard has full Windows Server functionality with two virtual instances.

Windows Server 2012 R2 Essentials This version is ideal for small businesses that have as many as 25 users and 50 devices. Windows Server 2012 R2 Essentials has a simpler interface and preconfigured connectivity to cloud-based services but no virtualization rights.

Windows Server 2012 R2 Foundation This version is designed for smaller companies that need a Windows Server experience for as few as 15 users. Windows Server 2012 R2 Foundation is a general-purpose server with basic functionality but no virtualization rights.

Once you choose what roles are going on your server, you must then decide how you're going to install Windows Server 2012 R2. There are two ways to install Windows Server 2012 R2. You can upgrade a Windows Server 2008 R2 with SP1 or Windows Server 2012 machine to Windows Server 2012 R2, or you can do a clean install of Windows Server 2012 R2. If you decide that you are going to upgrade, there are specific upgrade paths you must follow.

Your choice of Windows Server 2012 R2 version is dictated by how your current network is designed. If you are building a network from scratch, then it's pretty straightforward. Just choose the Windows Server 2012 R2 version based on your server's tasks. However, if you already have a version of Windows Server 2008 installed, you should follow the recommendations in Table 1.2, which briefly summarize the supported upgrade paths to Windows Server 2012 R2.

If your version of Microsoft Windows Server is not listed in the left column, upgrading to Windows Server 2012 R2 is not supported. If there is more than one edition listed in the right column, you can then choose either edition.

TABLE 1.2 Supported Windows Server 2012 R2 upgrade path recommendations

Current System	Upgraded System
Windows Server 2008 R2 Datacenter with SP1	Windows Server 2012 R2 Datacenter
Windows Server 2008 R2 Enterprise with SP1	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter

Windows Server 2008 R2 Standard with SP1	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter
Windows Web Server 2008 R2 with SP1	Windows Server 2012 R2 Standard
Windows Server 2012 Datacenter	Windows Server 2012 R2 Datacenter
Windows Server 2012 Standard	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter
Hyper-V Server 2012	Hyper-V Server 2012 R2
Windows Storage Server 2012 Standard	Windows Storage Server 2012 R2 Standard
Windows Storage Server 2012 Workgroup	Windows Storage Server 2012 R2 Workgroup

Deciding on the Type of Installation

One of the final choices you must make before installing Windows Server 2012 R2 is what type of installation you want. There are three ways to install Windows Server 2012 R2.

Windows Server 2012 R2 with the Graphical User Interface (GUI) This is the version with which most administrators are familiar. This is the version that uses *Microsoft Management Console (MMC)* windows, and it is the version that allows the use of a mouse to navigate through the installation.

Windows Server 2012 R2 Server Core This is a bare-bones installation of Windows Server 2012 R2. You can think of it this way: If Windows Server 2012 R2 is a top-of-the-line luxury car, then Windows Server 2012 R2 Server Core is the stripped-down model with no air-conditioning, manual windows, and cloth seats. It might not be pretty to look at, but it gets the job done.

Windows Server 2012 R2 MinShell This is the best of both installation types mentioned previously. Minimum Shell (MinShell) gives you the advantage of using the GUI management tools, but MinShell does not actually install the GUI. It gives administrators the ability to use tools with which they are familiar but still provides a small attack surface and the advantages of Server Core.

In Windows Server 2012 R2, an administrator has the ability to remove the GUI shell after a GUI shell install has been completed. This removes Internet Explorer 10, Windows Explorer, the desktop, and the Start screen. Microsoft Management Console (MMC), Server Manager, and a subset of Control Panel are still present, giving you a MinShell installation plus PowerShell.

Real World Scenario

Server Core

Here is an explanation of Server Core that I have used ever since it was introduced in Windows Server 2008.

I am a *huge* sports fan. I love watching sports on TV, and I enjoy going to games. If you have ever been to a hockey game, you know what a hockey goal looks like. Between hockey periods, the stadium workers often bring out a huge piece of Plexiglas onto the ice. There is a tiny square cut out of the bottom of the glass. The square is just a bit bigger than a hockey puck itself.

Now they pick some lucky fan out of the stands, give them a puck at center ice, and then ask them to shoot the puck into the net with the Plexiglas in front of it. If they get it through that tiny little square at the bottom of the Plexiglas, they win a car or some such great prize.

Well, Windows Server 2012 R2 with the GUI is like regular hockey with a net, and Windows Server 2012 R2 Server Core is the Plexiglas version.

Server Core supports a limited number of roles.

- Active Directory Certificate Services (AD CS)
- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS)
- Application Server
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services
- BITS Server
- BranchCache
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services

- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services
- .NET Framework 3.5 Features
- .NET Framework 4.5 Features
- Streaming Media Services
- Failover Clustering
- iSCSI
- Network Load Balancing
- MPIO
- qWave
- Telnet Server/Client
- Windows Server Migration Tools
- Windows PowerShell 4.0

Server Core does not have the normal Windows interface or GUI. Almost everything has to be configured via the command line or, in some cases, using the Remote Server Administration Tools from a full version of Windows Server 2012 R2. While this might scare off some administrators, it has the following benefits:

Reduced Management Because Server Core has a minimum number of applications installed, it reduces management effort.

Minimal Maintenance Only basic systems can be installed on Server Core, so it reduces the upkeep you would need to perform in a normal server installation.

Smaller Footprint Server Core requires only 1GB of disk space to install and 2GB of free space for operations.

Tighter Security With only a few applications running on a server, it is less vulnerable to attacks.

The prerequisites for Server Core are basic. It requires the Windows Server 2012 R2 installation media, a product key, and the hardware on which to install it.

After you install the base operating system, you use PowerShell or the remote administrative tools to configure the network settings, add the machine to the domain, create and format disks, and install roles and features. It takes only a few minutes to install Server Core, depending on the hardware.

One of the new things to keep in mind is that you can upgrade or downgrade to Server Core or MinShell. In Windows Server 2008 R2 and Windows Server 2008, if you wanted to switch your Windows Server GUI to Server Core, or vice versa, there was no way to convert to a full Windows Server installation or a Server Core installation without reinstalling the operating system. In Windows Server 2012 R2, the Server Core or GUI installation options are no longer an irreversible selection made during setup. An administrator now has the ability to convert between a Server Core installation and a full installation as needed.

Real World Scenario

Better Security

When I started in this industry more than 20 years ago, I was a programmer. I used to program computer hospital systems. When I switched to the networking world, I continued to work under contract with hospitals and with doctors' offices.

One problem I ran into is that many doctors are affiliated with hospitals, but they don't actually have offices within the hospital. Generally, they have offices either near the hospital or, in some cases, right across the street.

Here is the issue: Do we put servers in the doctors' offices, or do we make the doctor log into the hospital network through a remote connection? Doctors' offices normally don't have computer rooms, and we don't want to place a domain controller or server on someone's desk. It's just unsafe!

This is where Windows Server 2012 R2 Server Core can come into play. Since it is a slimmed-down version of Windows and there is no GUI, it makes it harder for anyone in the office to hack into the system. Also, Microsoft introduced a new domain controller in Windows Server 2008 called a *read-only domain controller (RODC)*. As its name suggests, it is a read-only version of a domain controller (explained in detail later in this book).

With Server Core and an RODC, you can feel safer placing a server on someone's desk or in any office. Server Core systems allow you to place servers in areas that you would never have placed them before. This can be a great advantage to businesses that have small, remote locations without full server rooms.

If you have a server that is running Server Core, there may be a situation in which you need to use the graphical user interfaces available only in Windows Server 2012 R2 with a GUI mode. Windows Server 2012 and Windows Server 2012 R2 allow you to switch the Server Core system to a Server with a GUI mode, or vice versa.

To convert from a Windows 2012 or Windows Server 2012 R2 Server Core system to Server with a GUI mode, run this code snippet (a restart is required):

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
```

To convert from Server Core mode to Server with a GUI mode, follow these steps when the server is initially installed in Server Core mode:

1. Determine the index number for a server with a GUI image (for example, `SERVERDATACENTER`, not `SERVERDATACENTERCORE`) using this cmdlet:

   ```
   Get-WindowsImage -ImagePath path to wim\install.wim
   ```

2. Run this line of code:

   ```
   Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
   -Source wim: path to wim\install.wim: Index # from step 1
   ```

3. Alternatively, if you want to use Windows Update as the source instead of a WIM file, use this Windows PowerShell cmdlet:

   ```
   Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
   ```

After you have completed the management tasks, you can switch the server back to Server Core mode whenever it is convenient (a restart is required) with this Windows PowerShell cmdlet:

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra -restart
```

NIC Teaming

NIC Teaming, also known as *load balancing and failover (LBFO)*, gives an administrator the ability to allow multiple network adapters on a system to be placed into a team. Independent hardware vendors (IHVs) have required NIC Teaming, but until Windows Server 2012, NIC Teaming was *not* part of the Windows Server Operating System.

To be able to use NIC Teaming, the computer system must have at least one Ethernet adapter. If you want to provide fault protection, an administrator must have a minimum of two Ethernet adapters. One advantage of Windows Server 2012 R2 is that an administrator can setup 32 network adapters in a NIC Team.

NIC Teaming is a very common practice when setting up virtualization. It is one way that you can have load balancing with Hyper-V.

NIC Teaming gives an administrator the ability to allow a virtual machine to use virtual network adapters in Hyper-V. The advantage of using NIC Teaming in Hyper-V is that the administrator can use it to connect to more than one Hyper-V switch. This allows Hyper-V to maintain connectivity even if the network adapter under the Hyper-V switch gets disconnected.

An administrator can configure NIC Teaming in either Server Manager or PowerShell.

Installing Windows Server 2012 R2

In the following sections, I am going to walk you through two different types of installs. I will show you how to do a full install of Windows 2012 Server with the GUI, and then I will show you how to install the Server Core version of the same software.

For these labs, I am using the full release of Windows Server 2012 R2 Datacenter, but you can use Windows Server 2012 R2 Standard.

Installing with the GUI

In Exercise 1.1, I will show you how to install Windows Server 2012 R2 Datacenter with the GUI. The GUI represents the Windows applications on the Desktop and the operating system functions that you can control and navigate with a mouse. The Server Core version is a command-line version only—you cannot use a mouse with Server Core unless you are going to use the mouse wheel for scrolling.

Windows Installation

At the time of this writing, I used the first full release of Windows Server 2012 R2 Datacenter. For this reason, there may be screens that have changed somewhat since this book was published.

EXERCISE 1.1

Installing Windows Server 2012 R2 with the GUI

1. Insert the Windows Server 2012 R2 installation DVD, and restart the machine from the installation media.
2. At the first screen, Windows Server 2012 R2 will ask you to configure your language, time and currency, and keyboard. Make your selections, and click Next.
3. At the next screen, click Install Now.
4. Depending on what version of Windows Server 2012 R2 you have (MSDN, TechNet, and so on), you may be asked to enter a product key. If this screen appears, enter your product key and click Next. If this screen does not appear, just go to step 5.
5. The Select The Operating System That You Want To Install screen then appears. Choose the Windows Server 2012 R2 Datacenter (Server With A GUI) selection and click Next.

6. The license terms screen appears. After reading the Windows Server 2012 R2 license agreement, check the I Accept The License Terms check box and click Next.
7. On the Which Type Of Installation Do You Want? screen, choose Custom: Install Windows Only (Advanced).

EXERCISE 1.1 *(continued)*

8. The next screen will ask you where you want to install Windows. If your hard disk is already formatted as NTFS, click the drive and then click Next. If the hard disk is not yet set up or formatted, choose the New link and create a partition. After creating the partition, click the Format link. Once the format is done, make sure you choose the new partition and click Next.
9. The Installing Windows screen will appear next. This is where the files from your media will be installed onto the system. The machine will reboot during this installation.
10. After the machine is finished rebooting, a screen requesting the administrator password will appear. Type in your password. (**P@ssword** is used in this exercise.) Your password must meet the password complexity requirements (one capitalized letter, one number, and/or one special character). Click Finish.
11. Next, log into the system. Press Ctrl+Alt+Del, and type in the administrator password. The machine will set up the properties of the administrator account.
12. Notice that the Server Manager dashboard automatically appears. Your Windows Server 2012 R2 installation is now complete.
13. Close Server Manager.

After you have logged into the Windows Server 2012 R2 Datacenter system, you will notice some big changes. The first is that the Start button in the lower-left corner of the screen has changed its look. Also, you can get to a Start button by clicking the Windows key (see Figure 1.2).

FIGURE 1.2 Windows key on a standard keyboard

Installing Windows Server 2012 R2 Server Core

In Exercise 1.2, you will learn how to install Windows Server 2012 R2 Server Core. You'll notice that the steps are similar to the ones in Exercise 1.1, with a couple of exceptions. As mentioned earlier, Server Core is a command-line configuration of Windows Server 2012 R2.

EXERCISE 1.2

Installing Windows Server 2012 R2 Using Server Core

1. Insert the Windows Server 2012 R2 installation DVD, and restart the machine from the installation media.
2. At the first screen, Windows Server 2012 R2 will prompt you to configure your language, time and currency, and keyboard. Make your selections, and click Next.
3. At the next screen, click Install Now.
4. Depending on what version of Windows Server 2012 R2 you have (MSDN, TechNet, and so on), you may be asked to enter a product key. If this screen appears, enter your product key and click Next. If this screen does not appear, just go to step 5.
5. The Select The Operating System That You Want To Install screen then appears. Choose the Windows Server 2012 R2 Datacenter (Server Core Installation) selection and click Next.
6. The license terms screen appears. After reading the Windows Server 2012 R2 license agreement, check the I Accept The License Terms check box and click Next.
7. At the Which Type Of Installation Do You Want? screen, choose Custom: Install Windows Only (Advanced).
8. The next screen will ask you where you want to install Windows. If your hard disk is already formatted as NTFS, click the drive and then click Next. If the hard disk is not set up or formatted, choose the New link and create a partition. After creating the partition, click the Format link. Once the format is done, make sure you choose the new partition and click Next.
9. The Installing Windows screen will appear next. This is where the files from your media will be installed onto the system. The machine will reboot during this installation.
10. After the machine is finished rebooting, a screen requesting the administrator password will appear. Type in your password. (**P@ssword** is used in this exercise.) Your password must meet the password complexity requirements (one capitalized letter, one number, and/or one special character).
11. Log into the system. Press Ctrl+Alt+Del, and type in the administrator password. The machine will set up the properties of the administrator account.
12. You will notice that the command prompt will automatically appear. Your Windows Server 2012 R2 Server Core installation is now complete.
13. To log out or turn off the machine, press Ctrl+Alt+Del and then click Sign Out.

After Windows Server 2012 R2 server is installed, you need to look at how to manage and configure the server. In the next section, you will learn how to manage a server remotely and with Windows PowerShell.

Using Windows Deployment Services

Another way that many IT departments deploy operating systems has been through the use of Windows Deployment Services (WDS). WDS allows an IT administrator to install a Windows operating system without using an installation disc. Using WDS allows you to deploy the operating system through a network installation. WDS can deploy Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows Server 2008/2008 R2, Microsoft Windows 2012, and Microsoft Windows Server 2012 R2.

The following are some of the advantages of using WDS for automated installation:

- You can remotely install Windows 7/Windows 8.
- The procedure simplifies management of the server image by allowing you to access Windows 7/8 distribution files from a distribution server.
- You can quickly recover the operating system in the event of a computer failure.

Here are the basic steps of the WDS process from a PXE-enabled WDS client:

1. The WDS client initiates a special boot process through the PXE network adapter (and the computer's BIOS configured for a network boot). On a PXE client, the user presses F12 to start the PXE boot process and to indicate that they want to perform a WDS installation.
2. A list of available Windows PE boot images is displayed. The user should select the appropriate Windows PE boot image from the boot menu.
3. The Windows Welcome screen is displayed. The user should click the Next button.
4. The WDS user is prompted to enter credentials for accessing and installing images from the WDS server.
5. A list of available operating system images is displayed. The user should select the appropriate image file to install.
6. The WDS user is prompted to enter the product key for the selected image.
7. The Partition And Configure The Disk screen is displayed. This screen provides the ability to install a mass storage device driver, if needed, by pressing F6.
8. The image copy process is initiated, and the selected image is copied to the WDS client computer.

The following sections describe how to set up the WDS server and the WDS clients and how to install Windows 7/8 through WDS.

Preparing the WDS Server

With the WDS server, you can manage and distribute Windows 7/8 operating system images to WDS client computers. The WDS server contains any files necessary for PXE booting, Windows PE boot images, and the Windows 7/8 images to be deployed.

The following steps for preparing the WDS server are discussed in the upcoming sections:

1. Make sure that the server meets the requirements for running WDS.
2. Install WDS.
3. Configure and start WDS.
4. Configure the WDS server to respond to client computers (if this was not configured when WDS was installed).

For WDS to work, the server on which you will install WDS must meet the requirements for WDS and be able to access the required network services.

WDS Server Requirements

The WDS server must meet these requirements:

- The computer must be a domain controller or a member of an Active Directory domain.
- At least one partition on the server must be formatted as NTFS.
- WDS must be installed on the server.
- The operating system must be Windows Server 2003, Windows Server 2008/2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- A network adapter must be installed.

Network Services

The following network services must be running on the WDS server or be accessible to the WDS server from another network server:

- TCP/IP installed and configured.
- A DHCP server, which is used to assign DHCP addresses to WDS clients. (Ensure that your DHCP scope has enough addresses to accommodate all of the WDS clients that will need IP addresses.)
- A DNS server, which is used to locate the Active Directory controller.
- Active Directory, which is used to locate WDS servers and WDS clients as well as authorize WDS clients and manage WDS configuration settings and client installation options.

Installing the WDS Server Components

You can configure WDS on a Windows Server 2003/2008/2008 R2, Windows Server 2012, or Windows Server 2012 R2 computer by using the Windows Deployment Services Configuration Wizard or by using the WDSUTIL command-line utility. Table 1.3 describes the `WDSUTIL` command-line options.

TABLE 1.3 `WDSUTIL` command-line options

WDSUTIL Option	Description
`/initialize-server`	Initializes the configuration of the WDS server
`/uninitialized-server`	Undoes any changes made during the initialization of the WDS server
`/add`	Adds images and devices to the WDS server
`/convert-ripimage`	Converts Remote Installation Preparation (RIPrep) images to WIM images
`/remove`	Removes images from the server
`/set`	Sets information in images, image groups, WDS servers, and WDS devices
`/get`	Gets information from images, image groups, WDS servers, and WDS devices
`/new`	Creates new capture images or discover images
`/copy- image`	Copies images from the image store
`/export-image`	Exports to WIM files images contained within the image store
`/start`	Starts WDS services
`/stop`	Stops WDS services
`/disable`	Disables WDS services
`/enable`	Enables WDS services
`/approve-autoadddevices`	Approves Auto-Add devices
`/reject-autoadddevices`	Rejects Auto-Add devices
`/delete-autoadddevices`	Deletes records from the Auto-Add database
`/update`	Uses a known good resource to update a server resource

The first step in setting up WDS to deploy operating systems to the clients is to install the WDS role. You do this by using Server Manager.

One of the advantages of using the Windows deployment server is that WDS can work with Windows image (`.wim`) files. Windows image files can be created through the use of the Windows Sysprep utility.

One component to which you need to pay attention when using the Windows deployment server is *Preboot Execution Environment (PXE)* network devices. PXE boot devices are network interface cards (NICs) that can talk to a network without the need for an operating system. PXE boot NIC adapters are network adapters that have a set of preboot commands within the boot firmware.

This is important when using WDS because PXE boot adapters connect to a WDS server and request the data needed to load the operating system remotely. Remember, most of the machines for which you are using WDS do not have an operating system on the computer. You need NIC adapters that can connect to a network without the need for an operating system for WDS to work properly.

For the same reason, you must set up DHCP to accept PXE machines. Those machines need a valid TCP/IP address so that they can connect to the WDS server.

Preparing the WDS Client

The WDS client is the computer on which Windows 7/8 will be installed. WDS clients rely on a technology called PXE, which allows the client computer to boot remotely and connect to a WDS server.

To act as a WDS client, the computer must meet all of the hardware requirements for Windows 7/Windows 8 and have a PXE-capable network adapter installed, and a WDS server must be present on the network. Additionally, the user account used to install the image must be a member of the Domain Users group in Active Directory.

After the WDS server has been installed and configured, you can install Windows 7/Windows 8 on a WDS client that uses a PXE-compliant network card.

To install Windows 7/Windows 8 on the WDS client, follow these steps:

1. Start the computer. When prompted, press F12 for a network service boot. The Windows PE appears.
2. The Windows Welcome screen appears. Click the Next button to start the installation process.
3. Enter the username and password of an account that has permissions to access and install images from the WDS server.
4. A list of available operating system images stored on the WDS server appears. Select the image to install and click Next.
5. Enter the product key for the selected Windows 7/8 image and click Next.
6. The Partition And Configure The Disk screen appears. Select the desired disk-partitioning options, or click OK to use the default options.
7. Click Next to initiate the image-copying process. The Windows Setup process will begin after the image is copied to the WDS client computer.

Understanding Features On Demand

One of the problems in previous versions of Windows Server was how roles and features were stored on the hard disk. Before the introduction of Windows Server 2012, even if a server role or feature was disabled on a server, the binary files for that role or feature were still present on the disk. The problem with this approach is that, even if you disable the role, it still consumes space on your hard drive.

Features On Demand in Windows Server 2012 R2 solves this issue because not only can administrators disable a role or feature, they can also completely remove the role or feature's files.

Once this is done, a state of Removed is shown in Server Manager, or the state of Disabled With Payload Removed is shown in the `Dism.exe` utility. To reinstall a role or feature that has been completely removed, you must have access to the installation files.

If you want to remove a role or feature completely from the system, use `-Remove` with the `Uninstall-WindowsFeature` cmdlet of Windows PowerShell. For example, if you want to remove Windows Explorer, Internet Explorer, and all dependent components completely, run the following Windows PowerShell command:

```
Uninstall-WindowsFeature Server-Gui-Shell -Remove
```

If you want to reinstall a role or feature that has been removed completely, use the Windows PowerShell `-Source` option of the `Install-WindowsFeature Server Manager` cmdlet. Using the `-Source` option states the path where the WIM image files and the index number of the image will be located. If an administrator decides not to use the `-Source` option, Windows will use Windows Update by default.

When you're using the Features On Demand configuration, if feature files are not available on the server computer and the installation requires those feature files, Windows Server 2012 R2 can be directed to get those files from a side-by-side feature store, which is a shared folder that contains feature files. It is available to the server on the network, from Windows Update, or from installation media. This can be overwritten using the `-Source` option in the Windows PowerShell utility.

Source Files for Roles or Features

Offline virtual hard disks (VHDs) cannot be used as a source for installing roles or features that have been completely removed. Only sources for the same version of Windows Server 2012 R2 are supported.

To install a removed role or feature using a WIM image, follow these steps:

1. Run the following command:

   `Get-windowsimage -`*`imagepath`* `\install.wim`

In step 1, *imagepath* is the path where the WIM files are located.

2. Run the following command:

   `Install-WindowsFeature` *`featurename`* `-Source wim:` *`path`*`:`*`index`*

   In step 2, *featurename* is the name of the role or feature from `Get-WindowsFeature`. *path* is the path to the WIM mount point, and *index* is the index of the server image from step 1.

To add or remove a role or feature, you must have administrative rights to the Windows Server 2012 R2 machine.

Storage in Windows Server 2012 R2

As an IT administrator, you'll need to ask many questions before you start setting up a server. What type of disks should be used? What type of RAID sets should be made? What type of hardware platform should be purchased? These are all questions you must ask when planning for storage in a Windows Server 2012 R2 server. In the following sections, I will answer these questions so that you can make the best decisions for storage in your network's environment.

Initializing Disks

To begin, I must first discuss how to add disk drives to a server. Once a disk drive has been physically installed, it must be initialized by selecting the type of partition. Different types of partition styles are used to initialize disks: *Master Boot Record (MBR)* and *GUID Partition Table (GPT)*.

MBR has a partition table that indicates where the partitions are located on the disk drive, and with this particular partition style, only volumes up to 2TB (2,048GB) are supported. An MBR drive can have up to four primary partitions or can have three primary partitions and one extended partition that can be divided into unlimited logical drives.

Windows Server 2012 R2 can only boot off an MBR disk unless it is based on the Extensible Firmware Interface (EFI); then it can boot from GPT. An Itanium server is an example of an EFI-based system. GPT is not constrained by the same limitations as MBR. In fact, a GPT disk drive can support volumes of up to 18EB (18,874,368 million terabytes) and 128 partitions. As a result, GPT is recommended for disks larger than 2TB or disks used on Itanium-based computers. Exercise 1.3 demonstrates the process of initializing additional disk drives to an active computer running Windows Server 2012 R2. If you're not adding a new drive, then stop after step 4. I am completing this exercise using Computer Management, but you also can do this exercise using Server Manager.

EXERCISE 1.3

Initializing Disk Drives

1. Open Computer Management under Administrative Tools.
2. Select Disk Management.
3. After disk drives have been installed, right-click Disk Management and select Rescan Disks.
4. A pop-up box appears indicating that the server is scanning for new disks. If you did not add a new disk, go to step 9.
5. After the server has completed the scan, the new disk appears as Unknown.
6. Right-click the Unknown disk, and select Initialize Disk.
7. A pop-up box appears asking for the partition style. For this exercise, choose MBR.
8. Click OK.
9. Close Computer Management.

The disk will now appear online as a basic disk with unallocated space.

Configuring Basic and Dynamic Disks

Windows Server 2012 R2 supports two types of disk configurations: basic and dynamic. Basic disks are divided into partitions and can be used with previous versions of Windows. Dynamic disks are divided into volumes and can be used with Windows 2000 Server and newer releases.

When a disk is initialized, it is automatically created as a basic disk, but when a new fault-tolerant (RAID) volume set is created, the disks in the set are converted to dynamic disks. Fault-tolerance features and the ability to modify disks without having to reboot the server are what distinguish dynamic disks from basic disks.

Fault tolerance (RAID) is discussed in detail later in this chapter in the "Redundant Array of Independent Disks" section.

A basic disk can simply be converted to a dynamic disk without loss of data. When a basic disk is converted, the partitions are automatically changed to the appropriate volumes. However, converting a dynamic disk back to a basic disk is not as simple. First, all the data on the dynamic disk must be backed up or moved. Then, all the volumes on the dynamic disk have to be deleted. The dynamic disk can then be converted to a basic disk. Partitions and logical drives can be created, and the data can be restored.

The following are actions that can be performed on basic disks:

- Formatting partitions
- Marking partitions as active
- Creating and deleting primary and extended partitions
- Creating and deleting logical drives
- Converting from a basic disk to a dynamic disk

The following are actions that can be performed on dynamic disks:

- Creating and deleting simple, striped, spanned, mirrored, or RAID-5 volumes
- Removing or breaking a mirrored volume
- Extending simple or spanned volumes
- Repairing mirrored or RAID-5 volumes
- Converting from a dynamic disk to a basic disk after deleting all volumes

In Exercise 1.4, you'll convert a basic disk to a dynamic disk.

EXERCISE 1.4

Converting a Basic Disk to a Dynamic Disk

1. Open Computer Management under Administrative Tools.
2. Select Disk Management.
3. Right-click a basic disk that you want to convert and select Convert To Dynamic Disk.

EXERCISE 1.4 *(continued)*

4. The Convert To Dynamic Disk dialog box appears. From here, select all of the disks that you want to convert to dynamic disks. In this exercise, only one disk will be converted.
5. Click OK.
6. The Convert To Dynamic Disk dialog box changes to the Disks To Convert dialog box and shows the disk/disks that will be converted to dynamic disks.
7. Click Convert.
8. Disk Management will warn that if you convert the disk to dynamic, you will not be able to start the installed operating system from any volume on the disk (except the current boot volume). Click Yes.
9. Close Computer Management.

The converted disk will now show as Dynamic in Disk Management.

Managing Volumes

A *volume set* is created from volumes that span multiple drives by using the free space from those drives to construct what will appear to be a single drive. The following list includes the various types of volume sets and their definitions:

- *Simple volume* uses only one disk or a portion of a disk.
- *Spanned volume* is a simple volume that spans multiple disks, with a maximum of 32. Use a spanned volume if the volume needs are too great for a single disk.
- *Striped volume* stores data in stripes across two or more disks. A striped volume gives you fast access to data but is not fault tolerant, nor can it be extended or mirrored. If one disk in the striped set fails, the entire volume fails.
- *Mirrored volume* duplicates data across two disks. This type of volume is fault tolerant because if one drive fails, the data on the other disk is unaffected.
- *RAID-5 volume* stores data in stripes across three or more disks. This type of volume is fault tolerant because if a drive fails, the data can be re-created from the parity off of the remaining disk drives. Operating system files and boot files cannot reside on the RAID-5 disks.

Exercise 1.5 illustrates the procedure for creating a volume set.

EXERCISE 1.5

Creating a Volume Set

1. Open Computer Management under Administrative Tools.
2. Select Disk Management.

3. Select and right-click a disk that has unallocated space. If there are no disk drives available for a particular volume set, that volume set will be grayed out as a selectable option. In this exercise, you'll choose a spanned volume set, but the process after the volume set selection is the same regardless of which kind you choose. The only thing that differs is the number of disk drives chosen.
4. The Welcome page of the New Spanned Volume Wizard appears and explains the type of volume set chosen. Click Next.
5. The Select Disks page appears. Select the disk that will be included with the volume set and click Add. Repeat this process until all of the desired disks have been added. Click Next.
6. The Assign Drive Letter Or Path page appears. From here you can select the desired drive letter for the volume, mount the volume in an empty NTFS folder, or choose not to assign a drive letter. The new volume is labeled as E. Click Next.
7. The Format Volume page appears. Choose to format the new volume. Click Next.
8. Click Finish.
9. If the disks have not been converted to dynamic, you will be asked to convert the disks. Click Yes.

The new volume will appear as a healthy spanned dynamic volume with the new available disk space of the new volume set.

Storage Spaces in Windows Server 2012 R2

Windows Server 2012 R2 includes a technology called *Storage Spaces*. Windows Server 2012 R2 allows an administrator to virtualize storage by grouping disks into storage pools. These storage pools can then be turned into virtual disks called *storage spaces*.

The Storage Spaces technology allows an administrator to have a highly available, scalable, low-cost, and flexible solution for both physical and virtual installations. Storage Spaces allows you to set up this advantage on either a single server or in scalable multinode mode. So, before going any further, let's look at these two terms that you must understand.

Storage Pools *Storage pools* are a group of physical disks that allows an administrator to delegate administration, expand disk sizes, and group disks together.

Storage Spaces *Storage spaces* allow an administrator to take free space from storage pools and create virtual disks called storage spaces. Storage spaces give administrators the ability to have precise control, resiliency, and storage tiers.

Storage spaces and storage pools can be managed by an administrator through the use of the Windows Storage Management API, Server Manager, or Windows PowerShell.

One of the advantages of using the Storage Spaces technology is the ability to set up resiliency. There are three types of Storage Space resiliency: mirror, parity, and simple (no resiliency).

Fault tolerance (RAID) is discussed in detail in the "Redundant Array of Independent Disks" section.

Now that you understand what storage spaces and storage pools do, let's take a look at some of the other advantages of using these features in Windows Server 2012 R2.

Availability One advantage to the Storage Spaces technology is the ability to fully integrate the storage space with failover clustering. This advantage allows administrators to achieve service deployments that are continuously available. Administrators have the ability to set up storage pools to be clustered across multiple nodes within a single cluster.

Tiered Storage The Storage Spaces technology allows virtual disks to be created with a two-tier storage setup. For data that is used often, you have an SSD tier; for data that is not used often, you use an HDD tier. The Storage Spaces technology will automatically transfer data at a subfile level between the two different tiers based on how often the data is used. Because of tiered storage, performance is greatly increased for data that is used most often, and data that is not used often still gets the advantage of being stored on a low-cost storage option.

Delegation One advantage of using storage pools is that administrators have the ability to control access by using access control lists (ACLs). What is nice about this advantage is that each storage pool can have its own unique access control lists. Storage pools are fully integrated with Active Directory Domain Services.

Redundant Array of Independent Disks

The ability to support drive sets and arrays using *Redundant Array of Independent Disks (RAID)* technology is built into Windows Server 2012 R2. RAID can be used to enhance data performance, or it can be used to provide fault tolerance to maintain data integrity in case of a hard disk failure. Windows Server 2012 R2 supports three types of RAID technologies: RAID-0, RAID-1, and RAID-5.

RAID-0 (Disk Striping) *Disk striping* is using two or more volumes on independent disks created as a single striped set. There can be a maximum of 32 disks. In a striped set, data is divided into blocks that are distributed sequentially across all of the drives in the set. With RAID-0 disk striping, you get very fast read and write performance because multiple blocks of data can be accessed from multiple drives simultaneously. However, RAID-0 does not offer the ability to maintain data integrity during a single disk failure. In other words, RAID-0 is not fault tolerant; a single disk event will cause the entire striped set to be lost, and it will have to be re-created through some type of recovery process, such as a tape backup.

RAID-1 (Disk Mirroring) *Disk mirroring* is two logical volumes on two separate identical disks created as a duplicate disk set. Data is written on two disks at the same time; that way, in the event of a disk failure, data integrity is maintained and available. Although this fault tolerance gives administrators data redundancy, it comes with a price because it

diminishes the amount of available storage space by half. For example, if an administrator wants to create a 300GB mirrored set, they would have to install two 300GB hard drives into the server, thus doubling the cost for the same available space.

RAID-5 Volume (Disk Striping with Parity) With a RAID-5 volume, you have the ability to use a minimum of three disks and a maximum of 32 disks. RAID-5 volumes allow data to be striped across all of the disks with an additional block of error-correction called parity. *Parity* is used to reconstruct the data in the event of a disk failure. RAID-5 has slower write performance than the other RAID types because the OS must calculate the parity information for each stripe that is written, but the read performance is equivalent to a stripe set, RAID-0, because the parity information is not read. Like RAID-1, RAID-5 comes with additional cost considerations. For every RAID-5 set, roughly an entire hard disk is consumed for storing the parity information. For example, a minimum RAID-5 set requires three hard disks, and if those disks are 300GB each, approximately 600GB of disk space is available to the OS and 300GB is consumed by parity information, which equates to 33.3 percent of the available space. Similarly, in a five-disk RAID-5 set of 300GB disks, approximately 1,200GB of disk space is available to the OS, which means that 20 percent of the total available space is consumed by the parity information. The words *roughly* and *approximately* are used when calculating disk space because a 300GB disk will really be only about 279GB of space. This is because vendors define a gigabyte as 1 billion bytes, but the OS defines it as 2^{30} (1,073,741,824) bytes. Also, remember that file systems and volume managers have overhead as well.

NOTE

Software RAID is a nice option for a small company, but hardware RAID is definitely a better option if the money is available.

Table 1.4 breaks down the various aspects of the supported RAID types in Window Server 2012 R2.

TABLE 1.4 Supported RAID-level properties in Windows Server 2012 R2

RAID Level	RAID Type	Fault Tolerant	Advantages	Minimum Number of Disks	Maximum Number of Disks
0	Disk striping	No	Fast reads and writes	2	32
1	Disk mirroring	Yes	Data redundancy and faster writes than RAID-5	2	2
5	Disk striping with parity	Yes	Data redundancy with less overhead and faster reads than RAID-1	3	32

Creating RAID Sets

Now that you understand the concepts of RAID and how to use it, you can look at the creation of RAID sets in Windows Server 2012 R2. The process of creating a RAID set is the same as the process for creating a simple or spanned volume set, except for the minimum disk requirements associated with each RAID type.

Creating a mirrored volume set is basically the same as creating a volume set, as shown in Exercise 1.6, except that you will select New Mirrored Volume. It is after the disk select wizard appears that you'll begin to see the difference. Since a new mirrored volume is being created, the volume requires two disks.

During the disk select process, if only one disk is selected, the Next button will be unavailable because the disk minimum has not been met. Refer to Figure 1.3 to view the Select Disks page of the New Mirrored Volume Wizard during the creation of a new mirrored volume, and notice that the Next button is not available.

FIGURE 1.3 Select Disks page of the New Mirrored Volume Wizard

To complete the process, you must select a second disk by highlighting the appropriate disk and adding it to the volume set. Once the second disk has been added, the Add button becomes unavailable, and the Next button is available to complete the mirrored volume set creation (see Figure 1.4).

FIGURE 1.4 Adding the second disk to complete a mirrored volume set

After you click Next, the creation of the mirrored volume set is again just like the rest of the steps in Exercise 1.5. A drive letter will have to be assigned, and the volume will need to be formatted. The new mirrored volume set will appear in Disk Management. In Figure 1.5, notice that the capacity of the volume equals one disk even though two disks have been selected.

FIGURE 1.5 Newly created mirrored volume set

To create a RAID-5 volume set, you use the same process that you use to create a mirrored volume set. The only difference is that a RAID-5 volume set requires that a minimum of three disks be selected to complete the volume creation. The process is simple: Select New RAID-5 Volume, select the three disks that will be used in the volume set, assign a drive letter, and format the volume. Figure 1.6 shows a newly created RAID-5 volume set in Disk Management.

FIGURE 1.6 Newly created RAID-5 volume set

Mount Points

With the ever-increasing demands of storage, mount points are used to surpass the limitation of 26 drive letters and to join two volumes into a folder on a separate physical disk drive. A *mount point* allows you to configure a volume to be accessed from a folder on another existing disk.

Through Disk Management, a mount point folder can be assigned to a drive instead of using a drive letter, and it can be used on basic or dynamic volumes that are formatted with NTFS. However, mount point folders can be created only on empty folders within a volume. Additionally, mount point folder paths cannot be modified; they can be removed only once they have been created. Exercise 1.6 shows the steps to create a mount point.

EXERCISE 1.6

Creating Mount Points

1. Open Server Manager.
2. Click and then expand Storage.
3. Select Disk Management.

4. Right-click the volume where the mount point folder will be assigned, and select Change Drive Letter And Paths.
5. Click Add.
6. Either type the path to an empty folder on an NTFS volume or click Browse to select or make a new folder for the mount point.

When you explore the drive, you'll see the new folder created. Notice that the icon indicates that it is a mount point.

Microsoft MPIO

Multipath I/O (MPIO) is associated with high availability because a computer will be able to use a solution with redundant physical paths connected to a storage device. Thus, if one path fails, an application will continue to run because it can access the data across the other path.

The MPIO software provides the functionality needed for the computer to take advantage of the redundant storage paths. MPIO solutions can also load-balance data traffic across both paths to the storage device, virtually eliminating bandwidth bottlenecks to the computer. What allows MPIO to provide this functionality is the new native *Microsoft Device Specific Module (Microsoft DSM)*. The Microsoft DSM is a driver that communicates with storage devices—iSCSI, Fibre Channel, or SAS—and it provides the chosen load-balancing policies. Windows Server 2012 R2 supports the following load-balancing policies:

Failover In a failover configuration, there is no load balancing. There is a primary path that is established for all requests and subsequent standby paths. If the primary path fails, one of the standby paths will be used.

Failback This is similar to failover in that it has primary and standby paths. However, with failback you designate a preferred path that will handle all process requests until it fails, after which the standby path will become active until the primary reestablishes a connection and automatically regains control.

Round Robin In a round-robin configuration, all available paths will be active and will be used to distribute I/O in a balanced round-robin fashion.

Round Robin with a Subset of Paths In this configuration, a specific set of paths will be designated as a primary set and another as standby paths. All I/O will use the primary set of paths in a round-robin fashion until all of the sets fail. Only at this time will the standby paths become active.

Dynamic Least Queue Depth In a dynamic least queue depth configuration, I/O will route to the path with the least number of outstanding requests.

Weighted Path In a weighted path configuration, paths are assigned a numbered weight. I/O requests will use the path with the least weight—the higher the number, the lower the priority.

Exercise 1.7 demonstrates the process of installing the Microsoft MPIO feature for Windows Server 2012 R2.

EXERCISE 1.7

Installing Microsoft MPIO

1. Choose Server Manager by clicking the Server Manager icon on the Taskbar.
2. Click number 2, Add Roles And Features.
3. Choose role-based or feature-based installation and click Next.
4. Choose your server and click Next.
5. Click Next on the Roles screen.
6. On the Select Features screen, choose the Multipath I/O check box. Click Next.

7. On the Confirm Installation Selections page, verify that Multipath I/O is the feature that will be installed. Click Install.
8. After the installation completes, the Installation Results page appears stating that the server must be rebooted to finish the installation process.
9. Click Close.
10. Restart the system.

Typically, most storage arrays work with the Microsoft DSM. However, some hardware vendors require DSM software that is specific to their products. Third-party DSM software is installed through the MPIO utility as follows:

1. Open Administrative Tools ➢ MPIO.
2. Select the DSM Install tab (see Figure 1.7).

FIGURE 1.7 The DSM Install tab in the MPIO Properties dialog box

3. Add the path of the INF file and click Install.

iSCSI

Internet Small Computer System Interface (iSCSI) is an interconnect protocol used to establish and manage a connection between a computer (initiator) and a storage device (target). It does this by using a connection through TCP port 3260, which allows it to be used over a LAN, a WAN, or the Internet. Each initiator is identified by its iSCSI Qualified Name (iqn), and it is used to establish its connection to an iSCSI target.

iSCSI was developed to allow block-level access to a storage device over a network. This is different from using a network attached storage (NAS) device that connects through the use of Common Internet File System (CIFS) or Network File System (NFS).

Block-level access is important to many applications that require direct access to storage. Microsoft Exchange and Microsoft SQL are examples of applications that require direct access to storage.

By being able to leverage the existing network infrastructure, iSCSI was also developed as an alternative to Fibre Channel storage by alleviating the additional hardware costs associated with a Fibre Channel storage solution.

iSCSI also has another advantage over Fibre Channel in that it can provide security for the storage devices. iSCSI can use Challenge Handshake Authentication Protocol (CHAP or MS-CHAP) for authentication and Internet Protocol Security (IPsec) for encryption. Windows Server 2012 R2 is able to connect an iSCSI storage device out of the box with no additional software needing to be installed. This is because the Microsoft iSCSI initiator is built into the operating system.

Windows Server 2012 R2 supports two different ways to initiate an iSCSI session.

- Through the native Microsoft iSCSI software initiator that resides on Windows Server 2012 R2
- Using a hardware iSCSI host bus adapter (HBA) that is installed in the computer

Both the Microsoft iSCSI software initiator and iSCSI HBA present an iSCSI qualified name that identifies the host initiator. When the Microsoft iSCSI software initiator is used, the CPU utilization may be as much as 30 percent higher than on a computer with a hardware iSCSI HBA. This is because all of the iSCSI process requests are handled within the operating system. Using a hardware iSCSI HBA, process requests can be offloaded to the adapter, thus freeing the CPU overhead associated with the Microsoft iSCSI software initiator. However, iSCSI HBAs can be expensive, whereas the Microsoft iSCSI software initiator is free.

It is worthwhile to install the Microsoft iSCSI software initiator and perform load testing to see how much overhead the computer will have prior to purchasing an iSCSI HBA or HBAs, depending on the redundancy level. Exercise 1.8 explains how to install and configure an iSCSI connection.

EXERCISE 1.8

Configuring iSCSI Storage Connection

1. Click the Windows key or Start button in the left-hand corner ➢ Administrative Tools ➢ iSCSI Initiator.
2. If a dialog box appears, click Yes to start the service.
3. Click the Discovery tab.

4. In the Target Portals portion of the page, click Discover Portal.
5. Enter the IP address of the target portal and click OK.
6. The IP address of the target portal appears in the Target Portals box.

EXERCISE 1.8 *(continued)*

7. Click OK.

To use the storage that has now been presented to the server, you must create a volume on it and format the space. Refer to Exercise 1.3 to review this process.

Internet Storage Name Service

Internet Storage Name Service (iSNS) allows for central registration of an iSCSI environment because it automatically discovers available targets on the network. The purpose of iSNS is to help find available targets on a large iSCSI network.

The Microsoft iSCSI initiator includes an iSNS client that is used to register with the iSNS. The iSNS feature maintains a database of clients that it has registered either through DCHP discovery or through manual registration. iSNS DHCP is available after the

installation of the service, and it is used to allow iSNS clients to discover the location of the iSNS. However, if iSNS DHCP is not configured, iSNS clients must be registered manually with the `iscsicli` command.

To execute the command, launch a command prompt on a computer hosting the Microsoft iSCSI and type **`iscsicli addisnsserver`** ***`server_name`***, where ***`server_name`*** is the name of the computer hosting iSNS. Exercise 1.9 walks you through the steps required to install the iSNS feature on Windows Server 2012 R2, and then it explains the different tabs in iSNS.

EXERCISE 1.9

Installing the iSNS Feature on Windows Server 2012 R2

1. Choose Server Manager by clicking the Server Manager icon on the Taskbar.
2. Click number 2 ➢ Add Roles And Features.
3. Choose role-based or featured-based installation and click Next.
4. Choose your server and click Next.
5. Click Next on the Roles screen.

6. On the Select Features screen, choose the iSNS Server Service check box. Click Next.
7. On the Confirmation screen, click the Install button.
8. Click the Close button. Close Server Manager and reboot.
9. Log in and open the iSNS server under Administrative Tools.

EXERCISE 1.9 *(continued)*

10. Click the General tab. This tab displays the list of registered initiators and targets. In addition to their iSCSI qualified name, it lists storage node type (Target or Initiator), alias string, and entity identifier (the Fully Qualified Domain Name [FQDN] of the machine hosting the iSNS client).

11. Click the Discovery Domains tab. The purpose of Discovery Domains is to provide a way to separate and group nodes. This is similar to zoning in Fibre Channel. The following options are available on the Discovery Domains tab:

    - *Create* is used to create a new discovery domain.
    - *Refresh* is used to repopulate the Discovery Domain drop-down list.
    - *Delete* is used to delete the currently selected discovery domain.
    - *Add* is used to add nodes that are already registered in iSNS to the currently selected discovery domain.
    - *Add New* is used to add nodes by entering the iSCSI Qualified Name (iQN) of the node. These nodes do not have to be currently registered.
    - *Remove Used* is used to remove selected nodes from the discovery domain.

12. Click the Discovery Domain Sets tab. The purpose of discovery domain sets is to separate further discovery domains. Discovery domains can be enabled or disabled, giving administrators the ability to restrict further the visibility of all initiators and targets. The options on the Discovery Domain Sets tab are as follows:

- The *Enable* check box is used to indicate the status of the discovery domain sets and to turn them off and on.
- *Create* is used to create new discovery domain sets.
- *Refresh* is used to repopulate the Discovery Domain Sets drop-down list.
- *Delete* is used to delete the currently selected discovery domain set.
- *Add* is used to add discovery domains to the currently selected discovery domain set.
- *Remove* is used to remove selected nodes from the discovery domain sets.

13. Close the iSNS server.

Fibre Channel

Fibre Channel storage devices are similar to iSCSI storage devices in that they both allow block-level access to their data sets and can provide MPIO policies with the proper hardware configurations. However, Fibre Channel requires a Fibre Channel HBA, fiber-optic cables, and Fibre Channel switches to connect to a storage device.

A *World Wide Name (WWN)* from the Fibre Channel HBA is used from the host and device so that they can communicate directly with each other, similar to using a NIC's MAC address. In other words, a logical unit number (LUN) is presented from a Fibre

Channel storage device to the WWN of the host's HBA. Fibre Channel has been the preferred method of storage because of the available connection bandwidth between the storage and the host.

Fibre Channel devices support 1Gb/s, 2Gb/s, and 4Gb/s connections, and they soon will support 8Gb/s connections, but now that 10Gb/s Ethernet networks are becoming more prevalent in many datacenters, iSCSI can be a suitable alternative. It is important to consider that 10Gb/s network switches can be more expensive than comparable Fibre Channel switches.

N-Port Identification Virtualization (NPIV) is a Fibre Channel facility allowing multiple n-port IDs to share a single physical N-Port. This allows multiple Fibre Channel initiators to occupy a single physical port. By using a single port, this eases hardware requirements in storage area network (SAN) design.

Network Attached Storage

The concept of a *network attached storage (NAS)* solution is that it is a low-cost device for storing data and serving files through the use of an Ethernet LAN connection. A NAS device accesses data at the file level via a communication protocol such as NFS, CIFS, or even HTTP, which is different from iSCSI or FC Fibre Channel storage devices that access the data at the block level. NAS devices are best used in file-storing applications, and they do not require a storage expert to install and maintain the device. In most cases, the only setup that is required is an IP address and an Ethernet connection.

Virtual Disk Service

Virtual Disk Service (VDS) was created to ease the administrative efforts involved in managing all of the various types of storage devices. Many storage hardware providers used their own applications for installation and management, and this made administering all of these various devices very cumbersome.

VDS is a set of application programming interfaces (APIs) that provides a centralized interface for managing all of the various storage devices. The native VDS API enables the management of disks and volumes at an OS level, and hardware vendor-supplied APIs manage the storage devices at a RAID level. These are known as software and hardware providers.

A *software provider* is host based, and it interacts with Plug and Play Manager because each disk is discovered and operates on volumes, disks, and disk partitions. VDS includes two software providers: basic and dynamic. The basic software provider manages basic disks with no fault tolerance, whereas the dynamic software providers manage dynamic disks with fault management. A hardware provider translates the VDS APIs into instructions specific to the storage hardware. This is how storage management applications are able to communicate with the storage hardware to create LUNs or Fibre Channel HBAs to view the WWN. The following are Windows Server 2012 R2 storage management applications that use VDS:

- The *Disk Management snap-in* is an application that allows you to configure and manage the disk drives on the host computer. You have already seen this application in use when you initialized disks and created volume sets.
- `DiskPart` is a command-line utility that configures and manages disks, volumes, and partitions on the host computer. It can also be used to script many of the storage management commands. `DiskPart` is a robust tool that you should study on your own because it is beyond the scope of this book. Figure 1.8 shows the various commands and their function in the `DiskPart` utility.

FIGURE 1.8 `DiskPart` commands

- `DiskRAID` is also a scriptable command-line utility that configures and manages hardware RAID storage systems. However, at least one VDS hardware provider must be installed for `DiskRAID` to be functional. `DiskRAID` is another useful utility that you should study on your own because it's beyond the scope of this book.

Booting from a VHD

Once you have installed each operating system, you can choose the operating system that you will boot to during the boot process. You will see a boot selection screen that asks you to choose which operating system you want to boot.

The Boot Configuration Data (BCD) store contains boot information parameters that were previously found in `boot.ini` in older versions of Windows. To edit the boot options in the BCD store, use the `bcdedit` utility, which can be launched only from a command prompt. To open a command prompt window, do the following:

1. Launch `\Windows\system32\cmd.exe`.
2. Open the Run command by pressing the Windows key plus the R key and then entering **`cmd`**.
3. Type **`cmd.exe`** in the Search Programs And Files box and press Enter.

After the command prompt window is open, type **`bcdedit`** to launch the `bcdedit` utility. You can also type **`bcdedit /?`** to see all of the different `bcdedit` commands.

Virtualization is covered in greater detail in Chapter 9: "Use Virtualization in Windows Server 2012."

Summary

In this chapter, you studied the latest advantages of using Windows Server 2012 R2. You also learned about the different roles and features you can install on a Windows Server 2012 R2 machine. You also explored how to migrate those roles and features from a Windows Server 2008, 2008 R2, and Windows Server 2012 machine to a Windows Server 2012 R2 machine.

I discussed the different upgrade paths that are available and which upgrades are best for your current network setup. You learned that another important issue to decide when installing Windows Server 2012 R2 is whether to use Server Core or the GUI installation.

You learned how to install Windows Server 2012 R2 Datacenter with GUI, and you installed the Windows Server 2012 R2 Server Core. Remember, Server Core is a slimmed-down version of Windows Server. With no GUI desktop available, it's a safer alternative to a normal Windows install. As discussed, a nice advantage of Windows Server 2012 R2 is that you can change from Server Core to the GUI version and back again.

I discussed a feature called Features On Demand. This feature allows you to remove roles and features from the operating system and remove the associated files completely from the hard drive, thus saving disk space.

You examined the various aspects of Windows Server 2012 R2 storage services as well as the various types of storage technologies and native Windows Server 2012 R2 storage

management tools. I started the chapter by discussing initializing disks and choosing a partition type: MBR or GPT. I then discussed the types of disk configurations, dynamic and basic, that are supported in Windows Server 2012 R2. You learned that various properties are associated with each type of configuration. Then I discussed the different types of RAID and the properties of each.

The next section explored storage technologies, namely, iSCSI, Fibre Channel, and NAS. I primarily focused on iSCSI because of the native support in Window Server 2012 R2. You learned how to configure an iSCSI initiator and a connection to an iSCSI target. After that, you looked at its iSNS server and how to configure it.

The chapter concluded by looking at Storage Manager for SANs and Storage Explorer, which are built-in management tools in Windows Server 2012 R2 for storage devices and firewall settings.

Exam Essentials

Understand the upgrade paths. It's important to make sure you understand the different upgrade paths from Windows Server 2008 R2 with SP1 and Windows Server 2012 to Windows Server 2012 R2.

Understand Windows Server 2012 R2 server roles. Understand what the Windows Server 2012 R2 server roles do for an organization and its users.

Understand Windows Server 2012 R2 GUI vs. Server Core. Understand the difference between the Windows Server 2012 R2 GUI version and the Windows Server 2012 R2 Server Core version. Know the benefits of using Server Core, and know that you can convert between the two different versions.

Understand Features On Demand. Understand the new feature called Features On Demand. Microsoft loves to ask exam questions about its new features, and this will be no exception. Understand how features and roles stay on the system until you physically remove them from the hard drive.

Know disk types. Know how to initialize disks and the type of partitioning to choose. Also know the difference between dynamic and basic disks and when to use them.

Understand RAID. Know the various RAID types, the requirements for each, and when it is appropriate to use each type.

Know storage technologies. Understand how to use the storage technologies Fibre Channel, iSCSI, and NAS. Know how to configure an iSCSI initiator and how to establish a connection to a target. Know the various MPIO policies.

Understand how to manage storage. Know what type of administrative features are available for Storage Manager for SANs and Storage Explorer.

Review Questions

1. You are the administrator for the ABC Company. You are looking to install Windows Server 2012 R2, and you need to decide which version to install. You need to install a version of Windows that is just for logon authentication and nothing else. You want the most secure option and cost is not an issue. What should you install?
   - **A.** Windows Server 2012 R2 Datacenter with GUI
   - **B.** Windows Server 2012 R2 Datacenter Server Core
   - **C.** Windows Server 2012 R2 Standard with GUI
   - **D.** Windows Server 2012 R2 Web Server Core

2. You are the IT manager for a large organization. One of your co-workers installed a new Windows Server 2012 R2 Datacenter Server Core machine, but now the IT team has decided that it should be a Windows Server 2012 R2 Datacenter with GUI. What should you do?
   - **A.** Reinstall Windows Server 2012 R2 Datacenter Server Core on the same machine.
   - **B.** Install a new machine with Windows Server 2012 R2 Datacenter Server Core.
   - **C.** Convert the current Windows Server 2012 R2 Datacenter Server Core to the Windows Server 2012 R2 Datacenter with GUI version.
   - **D.** Dual-boot the machine with both Windows Server 2012 R2 Datacenter Server Core and Windows Server 2012 R2 Datacenter with GUI.

3. You are the administrator for your company, and you are looking at upgrading your Windows Server 2008 web server to Windows Server 2012 R2. Which version of Windows Server 2012 R2 does Microsoft recommend you use?
   - **A.** Windows Server 2012 R2 Datacenter
   - **B.** Windows Server 2012 R2 Standard
   - **C.** Windows Server 2012 R2 Essentials
   - **D.** Windows Server 2012 R2 Foundation

4. You are looking at upgrading your Windows Server 2008 R2 Enterprise with SP2 machine to Windows Server 2012 R2. Your organization is considering virtualizing its entire server room, which has 25 servers. To which version of Windows Server 2012 R2 would you upgrade?
   - **A.** Windows Server 2012 R2 Datacenter
   - **B.** Windows Server 2012 R2 Standard
   - **C.** Windows Server 2012 R2 Essentials
   - **D.** Windows Server 2012 R2 Foundation

5. You have been hired to help a small company set up its first Windows network. It has had the same 13 users for the entire two years it has been open, and the company has no plans to expand. What version of Windows Server 2012 R2 would you recommend?
   - **A.** Windows Server 2012 R2 Datacenter
   - **B.** Windows Server 2012 R2 Standard
   - **C.** Windows Server 2012 R2 Essentials
   - **D.** Windows Server 2012 R2 Foundation

6. You have been hired to help a small company set up its Windows network. It has 20 users, and it has no plans to expand. What version of Windows Server 2012 R2 would you recommend?
   - **A.** Windows Server 2012 R2 Datacenter
   - **B.** Windows Server 2012 R2 Standard
   - **C.** Windows Server 2012 R2 Essentials
   - **D.** Windows Server 2012 R2 Foundation

7. Which of the following are benefits of using Windows Server 2012 R2 Server Core? (Choose all that apply.)
   - **A.** Reduced management
   - **B.** Minimal maintenance
   - **C.** Smaller footprint
   - **D.** Tighter security

8. You are a server administrator, and you are trying to save hard drive space on your Windows Server 2012 R2 Datacenter machine. Which feature can help you save hard disk space?
   - **A.** `HDSaver.exe`
   - **B.** Features On Demand
   - **C.** ADDS
   - **D.** WinRM

9. You have a server named SRV1 that runs Windows Server 2012 R2. You want to remove Windows Explorer, Windows Internet Explorer, and all components and files from this machine. Which command should you run?
   - **A.** `msiexec.exe /uninstall iexplore.exe /x`
   - **B.** `msiexec.exe /uninstall explorer.exe /x`
   - **C.** `Uninstall-WindowsFeature Server-Gui-Mgmt-Infra Remove`
   - **D.** `Uninstall-WindowsFeature Server-Gui-Shell Remove`

10. What type of domain controller would you install into an area where physical security is a concern?

A. Primary domain controller

B. Backup domain controller

C. Read-only domain controller

D. Locked-down domain controller

Chapter 2

Configure Network Services

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Deploy and configure DNS service**

- Configure Active Directory integration of primary zones
- Configure forwarders
- Configure Root Hints
- Manage DNS cache
- Create A and PTR resource records

✓ **Deploy and configure Dynamic Host Configuration Protocol (DHCP) service**

- Create and configure scopes
- Configure a DHCP reservation
- Configure DHCP options
- Configure client and server for PXE boot
- Configure DHCP relay agent
- Authorize DHCP server

The Domain Name System (DNS) is one of the key topics that you'll need to understand if you plan to take any of the Microsoft Windows Server 2012 R2 administration exams (70-410, 70-411, 70-412, and so forth).

It's also imperative that you understand DNS to work with Active Directory because it requires DNS to function properly, and many important system functions (including Kerberos authentication and finding domain controllers) are handled through DNS lookups. Windows 2000, Windows XP, Windows Vista, Windows 7, and Windows 8 clients use DNS for name resolution and to find Kerberos key distribution centers (KDCs), global catalog servers, and other services that may be registered in DNS.

By the time you complete this chapter, you will have a deeper understanding of how DNS works and how to set up, configure, manage, and troubleshoot DNS in Microsoft Windows Server 2012 R2.

In this chapter, you'll also learn how to install and manage DHCP, including how to set up plain DHCP scopes, superscopes, and multicast scopes. You'll also learn how to set up integration between Dynamic DNS and DHCP and how to authorize a DHCP server to integrate with Active Directory.

NOTE

There are two versions of DHCP: DHCP v4 and DHCP v6. In this chapter, I will just say "DHCP server" when referring to the physical DHCP server. If I am referring to a specific version of DHCP, I will specify the version.

Introducing DNS

The *Domain Name System (DNS)* is a service that allows you to resolve a hostname to an Internet Protocol (IP) address. One of the inherent complexities of operating in networked environments is working with multiple protocols and network addresses. Owing largely to the tremendous rise in the popularity of the Internet, however, most environments have transitioned to use *Transmission Control Protocol/Internet Protocol (TCP/IP)* as their primary networking protocol. Microsoft is no exception when it comes to supporting TCP/IP in its workstation and server products. All current versions of Microsoft's operating systems support TCP/IP, as do most other modern operating systems.

An easy way to understand DNS is to think about making a telephone call. If you wanted to call Microsoft and did not know the phone number, you could call information, tell

them the name (Microsoft), and get the telephone number. You would then make the call. Now think about trying to connect to Server1. You don't know the TCP/IP number (the computer's telephone number), so your computer asks DNS (information) for the number of Server1. DNS returns the number, and your system makes the connection (call). DNS is your network's 411, or information, and it returns the TCP/IP data for your network.

TCP/IP is actually a collection of different technologies (protocols and services) that allow computers to function together on a single, large, and heterogeneous network. Some of the major advantages of this protocol include widespread support for hardware, software, and network devices; reliance on a system of standards; and scalability. TCP handles tasks such as sequenced acknowledgments. IP involves many jobs, such as logical subnet assignment and routing.

The Form of an IP Address

To understand DNS, you must first understand how TCP/IP addresses are formed. Because DNS is strictly on a network to support TCP/IP, understanding the basics of TCP/IP is extremely important.

Microsoft exams cover TCP/IP. The TCP/IP material will be covered in Chapter 8, "Configure TCP/IP."

An *IP address* is a logical number that uniquely identifies a computer on a TCP/IP network. TCP/IP allows a computer packet to reach the correct host. Windows Server 2012 R2 works with two versions of TCP/IP: IPv4 and IPv6. An IPv4 address takes the form of four octets (eight binary bits), each of which is represented by a decimal number between 0 and 255. The four numbers are separated by decimal points. For example, all of the following are valid IP addresses:

- 128.45.23.17
- 230.212.43.100
- 10.1.1.1

The dotted decimal notation was created to make it easier for users to deal with IP addresses, but this idea did not go far enough. As a result, another abstraction layer was developed, which used names to represent the dotted decimal notation—the domain name. For example, the IP address 11000000 10101000 00000001 00010101 maps to 192.168.1.21, which in turn might map to `server1.company.org`, which is how the computer's address is usually presented to the user or application.

As stated earlier, IPv4 addresses are made up of octets, or the decimal (base 10) representation of 8 bits. It takes four octets to add up to the 32 bits required. IPv6 expands the address space to 128 bits. The address is usually represented in hexadecimal notation as follows:

```
2001:0DB8:0000:0000:1234:0000:A9FE:133E
```

You can tell that the implementation of DNS would make life a lot easier for everyone, even those of us who like to use alphanumeric values. (For example, some of us enjoy pinging the address in lieu of the name.) Fortunately, DNS already has the ability to handle IPv6 addresses using an AAAA record. An A record in IPv4's addressing space is 32 bits, and an AAAA record (4 *A*s) in IPv6's is 128 bits.

Nowadays, most computer users are quite familiar with navigating to DNS-based resources, such as `www.microsoft.com`. To resolve these "friendly" names to TCP/IP addresses that the network stack can use, you need a method for mapping them. Originally, ASCII flat files (often called HOSTS files, as shown in Figure 2.1) were used for this purpose. In some cases, they are still used today in small networks, and they can be useful in helping to troubleshoot name resolution problems.

FIGURE 2.1 HOSTS file

As the number of machines and network devices grew, it became unwieldy for administrators to manage all of the manual updates required to enter new mappings to a master HOSTS file and distribute it. Clearly, a better system was needed.

As you can see from the sample HOSTS file in Figure 2.1, you can conduct a quick test of the email server's name resolution as follows:

1. Open the HOSTS file: `C:\Windows\Systems32\drivers\etc`.
2. Add the IP-address-to-hostname mapping.
3. Try to ping the server using the hostname to verify that you can reach it using an easy-to-remember name.

Following these steps should drive home the concept of DNS for you because you can see it working to make your life easier. Now you don't have to remember 10.0.0.10; you only need to remember exchange03. However, you can also see how this method can become unwieldy if you have many hosts that want to use easy-to-remember names instead of IP addresses to locate resources on your network.

When dealing with large networks, users and network administrators must be able to locate the resources they require with minimal searching. Users don't care about the actual physical or logical network address of the machine; they just want to be able to connect to it using a simple name that they can remember.

From a network administrator's standpoint, however, each machine must have its own logical address that makes it part of the network on which it resides. Therefore, some scalable and easy-to-manage method for resolving a machine's logical name to an IP address and then to a domain name is required. DNS was created just for this purpose.

DNS is a hierarchically distributed database. In other words, its layers are arranged in a definite order, and its data is distributed across a wide range of machines, each of which can exert control over a portion of the database. DNS is a standard set of protocols that defines the following:

- A mechanism for querying and updating address information in the database
- A mechanism for replicating the information in the database among servers
- A schema of the database

DNS is defined by a number of requests for comments (RFCs), though primarily by RFC 1034 and RFC 1035.

DNS was originally developed in the early days of the Internet (called ARPAnet at the time) when it was a small network created by the Department of Defense for research purposes. Before DNS, computer names, or hostnames, were manually entered into a HOSTS file located on a centrally administered server. Each site that needed to resolve hostnames outside of its organization had to download this file. As the number of computers on the Internet grew, so did the size of this HOSTS file—and along with it the problems of its management. The need for a new system that would offer features such as scalability, decentralized administration, and support for various data types became more and more obvious. DNS, introduced in 1984, became this new system.

With DNS, the hostnames reside in a database that can be distributed among multiple servers, decreasing the load on any one server and providing the ability to administer this naming system on a per-partition basis. DNS supports hierarchical names and allows for the registration of various data types in addition to the hostname-to-IP-address mapping used in HOSTS files. Database performance is ensured through its distributed nature as well as through caching.

The DNS distributed database establishes an inverted logical tree structure called the *domain namespace*. Each node, or domain, in that space has a unique name. At the top of the tree is the root. This may not sound quite right, which is why the DNS hierarchical

model is described as being an inverted tree, with the root at the top. The root is represented by the null set "". When written, the root node is represented by a single dot (.).

Each node in the DNS can branch out to any number of nodes below it. For example, below the root node are a number of other nodes, commonly referred to as *top-level domains (TLDs)*. These are the familiar .com, .net, .org, .gov, .edu, and other such names. Table 2.1 lists some of these TLDs.

TABLE 2.1 Common top-level DNS domains

Common top-level domain names	Type of organization
com	Commercial (for example, stellacon.com for Stellacon Training Corporation).
edu	Educational (for example, gatech.edu for the Georgia Institute of Technology)
gov	Government (for example, whitehouse.gov for the White House in Washington, D.C.)
int	International organizations (for example, nato.int for NATO); this top-level domain is fairly rare
mil	Military organizations (for example, usmc.mil for the Marine Corps); there is a separate set of root name servers for this domain
net	Networking organizations and Internet providers (for example, hiwaay.net for HiWAAY Information Systems); many commercial organizations have registered names under this domain too
org	Noncommercial organizations (for example, fidonet.org for FidoNet)
au	Australia
uk	United Kingdom
ca	Canada
us	United States
jp	Japan

Each of these nodes then branches out into another set of domains, and they combine to form what we refer to as domain names, such as microsoft.com. A *domain name* identifies the domain's position in the logical DNS hierarchy in relation to its parent domain by separating each branch of the tree with a dot. Figure 2.2 shows a few of the top-level

domains, where the Microsoft domain fits, and a host called Tigger within the `microsoft.com` domain. If someone wanted to contact that host, they would use the *fully qualified domain name (FQDN)*, `tigger.microsoft.com`.

An FQDN includes the trailing dot (`.`) to indicate the root node, but it's commonly left off in practice.

FIGURE 2.2 The DNS hierarchy

As previously stated, one of the strengths of DNS is the ability to delegate control over portions of the DNS namespace to multiple organizations. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) assigns the control over TLDs to one or more organizations. In turn, those organizations delegate portions of the DNS namespace to other organizations. For example, when you register a domain name, let's call it `example.com`, you control the DNS for the portion of the DNS namespace within `example.com`. The registrar controlling the `.com` TLD has delegated control over the `example.com` node in the DNS tree. No other node can be named `example` directly below the `.com` within the DNS database.

Within the portion of the domain namespace that you control (`example.com`), you could create host and other records (more on these later). You could also further subdivide `example.com` and delegate control over those divisions to other organizations or departments. These divisions are called *subdomains*. For example, you might create subdomains named for the cities in which the company has branch offices and then delegate control over those subdomains to the branch offices. The subdomains might be named `losangeles.example.com`, `chicago.example.com`, `portsmouth.example.com`, and so on.

Each domain (or delegated subdomain) is associated with DNS name servers. In other words, for every node in the DNS, one or more servers can give an authoritative answer to

queries about that domain. At the root of the domain namespace are the root servers. More on these later.

Domain names and hostnames must contain only characters `a` to `z`, `A` to `Z`, `0` to `9`, and `-` (hyphen). Other common and useful characters, such as the `&` (ampersand), `/` (slash), `.` (period), and `_` (underscore), are not allowed. This is in conflict with NetBIOS's naming restrictions. However, you'll find that Windows Server 2012 R2 is smart enough to take a NetBIOS name, like `Server_1`, and turn it into a legal DNS name, like `server1.example.com`.

DNS servers work together to resolve hierarchical names. If a server already has information about a name, it simply fulfills the query for the client. Otherwise, it queries other DNS servers for the appropriate information. The system works well because it distributes the authority over separate parts of the DNS structure to specific servers. A *DNS zone* is a portion of the DNS namespace over which a specific DNS server has authority (DNS zone types are discussed in detail later in this chapter).

There is an important distinction to make between DNS zones and Active Directory (AD) domains. Although both use hierarchical names and require name resolution, DNS zones do not map directly to AD domains.

Within a given DNS zone, resource records (RRs) contain the hosts and other database information that make up the data for the zone. For example, an RR might contain the host entry for `www.example.com`, pointing it to the IP address 192.168.1.10.

Understanding Servers, Clients, and Resolvers

You will need to know a few terms and concepts in order to manage a DNS server. Understanding these terms will make it easier to understand how the Windows Server 2012 R2 DNS server works.

DNS Server Any computer providing domain name services is a *DNS name server*. No matter where the server resides in the DNS namespace, it's still a DNS name server. For example, 13 root name servers at the top of the DNS tree are responsible for delegating the TLDs. The *root servers* provide referrals to name servers for the TLDs, which in turn provide referrals to an authoritative name server for a given domain.

The Berkeley Internet Name Domain (BIND) was originally the only software available for running the root servers on the Internet. However, a few years ago the organizations responsible for the root servers undertook an effort to diversify the software running on these important machines. Today, root servers run multiple types of name server software. BIND is still primarily on Unix-based machines, and it is also the most popular for Internet providers. No root servers run Windows DNS.

Any DNS server implementation supporting Service Location Resource Records (see RFC 2782) and Dynamic Updates (RFC 2136) is sufficient to provide the name service for any operating system running Windows 2003 software and newer.

DNS Client A *DNS client* is any machine that issues queries to a DNS server. The client hostname may or may not be registered in a DNS database. Clients issue DNS requests through processes called *resolvers*. You'll sometimes see the terms *client* and *resolver* used synonymously.

Resolver *Resolvers* are software processes, sometimes implemented in software libraries that handle the actual process of finding the answers to queries for DNS data. The resolver is also built into many larger pieces of software so that external libraries don't have to be called to make and process DNS queries. Resolvers can be what you'd consider client computers or other DNS servers attempting to resolve an answer on behalf of a client (for example, Internet Explorer).

Query A *query* is a request for information sent to a DNS server. Three types of queries can be made to a DNS server: recursive, inverse, and iterative. I'll discuss the differences between these query types in the section "DNS Queries," a bit later in the chapter.

Understanding the DNS Process

To help you understand the DNS process, I will start by covering the differences between Dynamic DNS and Non-Dynamic DNS. During this discussion, you will learn how Dynamic DNS populates the DNS database. You'll also see how to implement security for Dynamic DNS. I will then talk about the workings of different types of DNS queries. Finally, I will discuss caching and time to live (TTL). You'll learn how to determine the best setting for your organization.

Dynamic DNS and Non-Dynamic DNS

To understand Dynamic DNS and Non-Dynamic DNS, you must go back in time. (Here is where the TV screen always used to get wavy.) Many years ago when many of us worked on Windows NT 3.51 and Windows NT 4.0, almost all Microsoft networks used Windows Internet Name Service (WINS) to do their TCP/IP name resolution. Windows versions 95/98 and NT 4.0 Professional were all built on the idea of using WINS. This worked out well for administrators because WINS was dynamic (which meant that once it was installed, it automatically built its own database). Back then, there was no such thing as Dynamic DNS; administrators had to enter DNS records into the server manually. This is important to know even today. If you have clients still running any of these older operating systems (95/98 or NT 4), these clients cannot use Dynamic DNS.

Now let's move forward in time to the release of Windows Server 2000. Microsoft announced that DNS was going to be the name resolution method of choice. Many administrators (myself included) did not look forward to the switch. Because there was no such thing as Dynamic DNS, most administrators had nightmares about manually entering

records. However, luckily for us, when Microsoft released Windows Server 2000, DNS had the ability to operate dynamically. Now when you're setting up Windows Server 2012 R2 DNS, you can choose what type of dynamic update you would like to use, if any. Let's talk about why you would want to choose one over the other.

The *Dynamic DNS (DDNS) standard*, described in RFC 2136, allows DNS clients to update information in the DNS database files. For example, a Windows Server 2012 R2 DHCP server can automatically tell a DDNS server which IP addresses it has assigned to what machines. Windows 2000, 2003, 2008, XP Pro, Vista, Windows 7, and Windows 8 DHCP clients can do this too. For security reasons, however, it's better to let the DHCP server do it. The result: IP addresses and DNS records stay in sync so that you can use DNS and DHCP together seamlessly. Because DDNS is a proposed Internet standard, you can even use the Windows Server 2012 R2 DDNS-aware parts with Unix/Linux-based DNS servers.

Non-Dynamic DNS (NDDNS) does not automatically populate the DNS database. The client systems do not have the ability to update to DNS. If you decide to use Non-Dynamic DNS, an administrator will need to populate the DNS database manually. Non-Dynamic DNS is a reasonable choice if your organization is small to midsized and you do not want extra network traffic (clients updating to the DNS server) or if you need to enter the computer's TCP/IP information manually because of strict security measures.

Dynamic DNS has the ability to be secure, and the chances are slim that a rogue system (a computer that does not belong in your DNS database) could update to a secure DNS server. Nevertheless, some organizations have to follow stricter security measures and are not allowed to have dynamic updates.

The major downside to entering records into DNS manually occurs when the organization is using the *Dynamic Host Configuration Protocol (DHCP)*. When using DHCP, it is possible for users to end up with different TCP/IP addresses every day. This means an administrator has to update DNS manually each day to keep it accurate.

If you choose to allow Dynamic DNS, you need to decide how you want to set it up. When setting up dynamic updates on your DNS server, you have three choices (see Figure 2.3).

None This means your DNS server is Non-Dynamic.

Nonsecure and Secure This means that any machine (even if it does not have a domain account) can register with DNS. Using this setting could allow rogue systems to enter records into your DNS server.

Secure Only This means that only machines with accounts in Active Directory can register with DNS. Before DNS registers any account in its database, it checks Active Directory to make sure that account is an authorized domain computer.

FIGURE 2.3 Setting the Dynamic Updates option

How Dynamic DNS Populates the DNS Database

TCP/IP is the protocol used for network communications on a Microsoft Windows Server 2012 R2 network. Users have two ways to receive a TCP/IP number:

- Static (administrators manually enter the TCP/IP information)
- Dynamic (using DHCP)

When an administrator sets up TCP/IP, DNS can also be configured.

Once a client gets the address of the DNS server, if that client is allowed to update with DNS, the client sends a registration to DNS or requests DHCP to send the registration. DNS then does one of two things, depending on which Dynamic Updates option is specified:

- Check with Active Directory to see whether that computer has an account (Secure Only updates), and if it does, enter the record into the database.
- Enter the record into its database (Nonsecure and Secure updates).

What if you have clients that cannot update DNS? Well, there is a solution—DHCP. In the DNS tab of the IPv4 Properties window, check the option labeled "Dynamically update DNS A and PTR records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)," which is shown in Figure 2.4.

DHCP, along with Dynamic DNS clients, allows an organization to update its DNS database dynamically without the time and effort of having an administrator manually enter DNS records.

FIGURE 2.4 DHCP settings for DNS

DNS Queries

As stated earlier, a client can make three types of queries to a DNS server: recursive, inverse, and iterative. Remember that the client of a DNS server can be a resolver (what you'd normally call a client) or another DNS server.

Iterative Queries

Iterative queries are the easiest to understand: A client asks the DNS server for an answer, and the server returns the best answer. This information likely comes from the server's cache. The server never sends out an additional query in response to an iterative query. If the server doesn't know the answer, it may direct the client to another server through a referral.

Recursive Queries

In a *recursive query*, the client sends a query to a name server, asking it to respond either with the requested answer or with an error message. The error states one of two things:

- The server can't come up with the right answer.
- The domain name doesn't exist.

In a recursive query, the name server isn't allowed just to refer the client to some other name server. Most resolvers use recursive queries. In addition, if your DNS server uses a forwarder, the requests sent by your server to the forwarder will be recursive queries.

Figure 2.5 shows an example of both recursive and iterative queries. In this example, a client within the Microsoft Corporation is querying its DNS server for the IP address for `www.whitehouse.gov`.

FIGURE 2.5 A sample DNS query

Here's what happens to resolve the request:

1. The resolver sends a recursive DNS query to its local DNS server asking for the IP address of `www.whitehouse.gov`. The local name server is responsible for resolving the name, and it cannot refer the resolver to another name server.
2. The local name server checks its zones, and it finds no zones corresponding to the requested domain name.
3. The root name server has authority for the root domain, and it will reply with the IP address of a name server for the `.gov` top-level domain.
4. The local name server sends an iterative query for `www.whitehouse.gov` to the Gov name server.
5. The Gov name server replies with the IP address of the name server servicing the `whitehouse.gov` domain.
6. The local name server sends an iterative query for `www.whitehouse.gov` to the `whitehouse.gov` name server.
7. The `whitehouse.gov` name server replies with the IP address corresponding to `www.whitehouse.gov`.
8. The local name server sends the IP address of `www.whitehouse.gov` back to the original resolver.

Inverse Queries

Inverse queries use pointer (PTR) records. Instead of supplying a name and then asking for an IP address, the client first provides the IP address and then asks for the name. Because there's no direct correlation in the DNS namespace between a domain name and its associated IP address, this search would be fruitless without the use of the `in-addr.arpa` domain. Nodes in the `in-addr.arpa` domain are named after the numbers in the dotted-octet representation of IP addresses. However, because IP addresses get more specific from left to right and domain names get less specific from left to right, the order of IP address octets must be reversed when building the `in-addr.arpa` tree. With this arrangement, administration of the lower limbs of the DNS `in-addr.arpa` tree can be given to companies as they are assigned their Class A, B, or C subnet address or delegated even further down thanks to Variable Length Subnet Masking (VLSM).

Once the domain tree is built into the DNS database, a special PTR record is added to associate the IP addresses with the corresponding hostnames. In other words, to find a hostname for the IP address 206.131.234.1, the resolver would query the DNS server for a PTR record for `1.234.131.206.in-addr.arpa`. If this IP address is outside of the local domain, the DNS server will start at the root and sequentially resolve the domain nodes until arriving at `234.131.206.in-addr.arpa`, which would contain the PTR record for the desired host.

Caching and Time to Live

When a name server is processing a recursive query, it may be required to send out several queries to find the definitive answer. Name servers, acting as resolvers, are allowed to cache all of the received information during this process; each record contains information called *time to live (TTL)*. The TTL specifies how long the record will be held in the local cache until it must be resolved again. If a query comes in that can be satisfied by this cached data, the TTL that's returned with it equals the current amount of time left before the data is flushed.

There is also a negative cache TTL. The *negative cache TTL* is used when an authoritative server responds to a query indicating that the record queried doesn't exist, and it indicates the amount of time that this negative answer may be held. Negative caching is quite helpful in preventing repeated queries for names that don't exist.

The administrator for the DNS zone sets TTL values for the entire zone. The value can be the same across the zone, or the administrator can set a separate TTL for each RR within the zone. Client resolvers also have data caches and honor the TTL value so that they know when to flush.

Choosing Appropriate TTL Values

For zones that you administer, you can choose the TTL values for the entire zone, for negative caching, and for individual records. Choosing an appropriate TTL depends on a number of factors, including the following:

- Amount of change you anticipate for the records within the zone
- Amount of time you can withstand an outage that might require changing an IP address
- Amount of traffic you believe the DNS server can handle

Resolvers query the name server every time the TTL expires for a given record. A low TTL, say 60 seconds, can burden the name server, especially for popular DNS records. (DNS queries aren't particularly intensive for a server to handle, but they can add up quickly if you mistakenly use 60 seconds instead of 600 seconds for the TTL on a popular record.) Set a low TTL only when you need to respond quickly to a changing environment.

A high TTL, say 604,800 seconds (that's one week), means that if you need to make a change to the DNS record, clients might not see the change for up to a week. This consideration is especially important when making changes to the network, and it's one that's all too frequently overlooked. I can't count the number of times I've worked with clients who had recently made a DNS change to a new IP for their email or website only to ask why it's not working for some clients. The answer can be found in the TTL value. If the record is being cached, then the only thing that can solve their problem is time.

You should choose a TTL that's appropriate for your environment. Take the following factors into account:

- The amount of time that you can afford to be offline if you need to make a change to a DNS record that's being cached
- The amount of load that a low TTL will cause on the DNS server

In addition, you should plan well ahead of any major infrastructure changes and change the TTL to a lower value to lessen the effect of the downtime by reducing the amount of time that the record(s) can be cached.

Introducing DNS Database Zones

As mentioned earlier in this chapter, a DNS zone is a portion of the DNS namespace over which a specific DNS server has authority. Within a given DNS zone, there are resource records (RRs) that define the hosts and other types of information that make up the database for the zone. You can choose from several different zone types. Understanding the characteristics of each will help you choose which is right for your organization.

NOTE

The DNS zones discussed in this book are all Microsoft Windows Server 2012 / 2012 R2 zones. Non-Windows (for example, Unix) systems set up their DNS zones differently.

In the following sections, I will discuss the different zone types and their characteristics.

Understanding Primary Zones

When you're learning about zone types, things can get a bit confusing. But it's really not difficult to understand how they work and why you would want to choose one type of zone over the other. Zones are databases that store records. By choosing one zone type over another, you are basically just choosing how the database works and how it will be stored on the server.

The primary zone is responsible for maintaining all of the records for the DNS zone. It contains the primary copy of the DNS database. All record updates occur on the primary zone. You will want to create and add primary zones whenever you create a new DNS domain.

There are two types of primary zones:

- Primary zone
- Primary zone with Active Directory Integration (Active Directory DNS)

From this point forward, I refer to a primary zone with Active Directory Integration as an *Active Directory DNS*. When I use only the term *primary zone*, Active Directory is not included.

To install DNS as a primary zone, you must first install DNS using the Server Manager MMC. Once DNS is installed and running, you create a new zone and specify it as a primary zone.

The process of installing DNS and its zones will be discussed later in this chapter. In addition, there will be step-by-step exercises to walk you through how to install these components.

Primary zones have advantages and disadvantages. Knowing the characteristics of a primary zone will help you decide when you need the zone and when it fits into your organization.

Local Database

Primary DNS zones get stored locally in a file (with the suffix `.dns`) on the server. This allows you to store a primary zone on a domain controller or a member server. In addition, by loading DNS onto a member server, you can help a small organization conserve resources. Such an organization may not have the resources to load DNS on an Active Directory domain controller.

Unfortunately, the local database has many disadvantages:

Lack of Fault Tolerance Think of a primary zone as a contact list on your smartphone. All of the contacts in the list are the records in your database. The problem is that, if you lose your phone or the phone breaks, you lose your contact list. Until your phone gets fixed or you swap out your phone card, the contacts are unavailable.

It works the same way with a primary zone. If the server goes down or you lose the hard drive, DNS records on that machine are unreachable. An administrator can install a secondary zone (explained later in the next section), and that provides temporary fault tolerance. Unfortunately, if the primary zone is down for an extended period of time, the secondary server's information will no longer be valid.

Additional Network Traffic Let's imagine that you are looking for a contact number for John Smith. John Smith is not listed in your smartphone directory, but he is listed in your partner's smartphone. You have to contact your partner to get the listing. You cannot directly access your partner's phone's contacts.

When a resolver sends a request to DNS to get the TCP/IP address for Jsmith (in this case Jsmith is a computer name) and the DNS server does not have an answer, it does not have the ability to check the other server's database directly to get an answer. Thus it forwards the request to another DNS. When DNS servers are replicating zone databases with other DNS servers, this causes additional network traffic.

No Security Staying with the smartphone example, let's say that you call your partner looking for John Smith's phone number. When your partner gives you the phone number over your wireless phone, someone with a scanner can pick up your conversation. Unfortunately, wireless telephone calls are not very secure.

Now a resolver asks a primary zone for the Jsmith TCP/IP address. If someone on the network has a packet sniffer, they can steal the information in the DNS packets being sent over the network. The packets are not secure unless you implement some form of secondary security. Also, the DNS server has the ability to be dynamic. A primary zone accepts all updates from DNS servers. You cannot set it to accept secure updates only.

Understanding Secondary Zones

In Windows Server 2012 R2 DNS, you have the ability to use secondary DNS zones. Secondary zones are noneditable copies of the DNS database. You use them for *load balancing* (also referred to as *load sharing*), which is a way of managing network overloads on a single server. A secondary zone gets its database from a primary zone.

A *secondary zone* contains a database with all of the same information as the primary zone, and it can be used to resolve DNS requests. Secondary zones have the following advantages:

- A secondary zone provides fault tolerance, so if the primary zone server becomes unavailable, name resolution can still occur using the secondary zone server.
- Secondary DNS servers can also increase network performance by offloading some of the traffic that would otherwise go to the primary server.

Secondary servers are often placed within the parts of an organization that have high-speed network access. This prevents DNS queries from having to run across slow wide area network (WAN) connections. For example, if there are two remote offices within the `stellacon.com` organization, you may want to place a secondary DNS server in each remote office. This way, when clients require name resolution, they will contact the nearest server for this IP address information, thus preventing unnecessary WAN traffic.

WARNING Having too many secondary zone servers can actually cause an increase in network traffic because of replication (especially if DNS changes are fairly frequent). Therefore, you should always weigh the benefits and drawbacks and properly plan for secondary zone servers.

Understanding Active Directory Integrated DNS

Windows Server 2000 introduced *Active Directory Integrated DNS* to the world. This zone type was unique and was a separate choice during setup. In Windows Server 2003, this zone type became an add-on to a primary zone. In Windows Server 2012 R2, it works the same way. After choosing to set up a primary zone, you check the box labeled Store The Zone In Active Directory (see Figure 2.6).

FIGURE 2.6 Setting up an Active Directory Integrated zone

Disadvantages of Active Directory Integrated DNS

The main disadvantage of Active Directory Integrated DNS is that it has to reside on a domain controller because the DNS database is stored in Active Directory. As a result, you cannot load this zone type on a member server, and small organizations might not have the resources to set up a dedicated domain controller.

Advantages of Active Directory Integrated DNS

The advantages of using an Active Directory Integrated DNS zone well outweigh the disadvantage just discussed. The following are some of the major advantages to an Active Directory Integrated zone:

Full Fault Tolerance Think of an Active Directory Integrated zone as a database on your server that stores contact information for all your clients. If you need to retrieve John Smith's phone number, as long as it was entered, you can look it up on the software.

If John Smith's phone number was stored only on your computer and your computer stopped working, no one could access John Smith's phone number. But since John Smith's phone number is stored in a database to which everyone has access, if your computer stops working, other users can still retrieve John Smith's phone number.

An Active Directory Integrated zone works the same way. Since the DNS database is stored in Active Directory, all Active Directory DNS servers can have access to the same data. If one server goes down or you lose a hard drive, all other Active Directory DNS servers can still retrieve DNS records.

No Additional Network Traffic As previously discussed, an Active Directory Integrated zone is stored in Active Directory. Since all records are now stored in Active Directory, when a resolver needs a TCP/IP address for Jsmith, any Active Directory DNS server can access Jsmith's address and respond to the resolver.

When you choose an Active Directory Integrated zone, DNS zone data can be replicated automatically to other DNS servers during the normal Active Directory replication process.

DNS Security An Active Directory Integrated zone has a few security advantages over a primary zone:

- An Active Directory Integrated zone can use secure dynamic updates.
- As explained earlier, the Dynamic DNS standard allows secure-only updates or dynamic updates, not both.
- If you choose secure updates, then only machines with accounts in Active Directory can register with DNS. Before DNS registers any account in its database, it checks Active Directory to make sure that it is an authorized domain computer.
- An Active Directory Integrated zone stores and replicates its database through Active Directory replication. Because of this, the data gets encrypted as it is sent from one DNS server to another.

Background Zone Loading Background zone loading (discussed in more detail later in this chapter) allows an Active Directory Integrated DNS zone to load in the background. As a result, a DNS server can service client requests while the zone is still loading into memory.

Understanding Stub Zones

Stub zones work a lot like secondary zones—the database is a noneditable copy of a primary zone. The difference is that the stub zone's database contains only the information

necessary (three record types) to identify the authoritative DNS servers for a zone (see Figure 2.7). You should not use stub zones to replace secondary zones, nor should you use them for redundancy and load balancing.

FIGURE 2.7 DNS stub zone type

Stub zone databases contain only three record types: name server (NS), start of authority (SOA), and glue host (A) records. Understanding these records will help you on the Microsoft certification exams. Microsoft asks many questions about stub zones on all DNS-related exams.

When to Use Stub Zones

Stub zones become particularly useful in a couple of different scenarios. Consider what happens when two large companies merge: `example.com` and `example.net`. In most cases, the DNS zone information from both companies must be available to every employee. You could set up a new zone on each side that acts as a secondary for the other side's primary zone, but administrators tend to be very protective of their DNS databases, and they probably wouldn't agree to this plan.

A better solution is to add to each side a stub zone that points to the primary server on the other side. When a client in `example.com` (which you help administer) makes a request for a name in `example.net`, the stub zone on the `example.com` DNS server would send the client to the primary DNS server for `example.net` without actually resolving the name. At this point, it would be up to `example.net`'s primary server to resolve the name.

An added benefit is that, even if the administrators over at `example.net` change their configuration, you won't have to do anything because the changes will automatically replicate to the stub zone, just as they would for a secondary server.

Stub zones can also be useful when you administer two domains across a slow connection. Let's change the previous example a bit and assume that you have full control over `example.com` and `example.net` but that they connect through a 56Kbps line. In this case, you wouldn't necessarily mind using secondary zones because you personally administer the entire network. However, it could get messy to replicate an entire zone file across that slow line. Instead, stub zones would refer clients to the appropriate primary server at the other site.

GlobalName Zones

Earlier in this chapter, I talked about organizations using WINS to resolve NetBIOS names (also referred to as *computer names*) to TCP/IP addresses. Even today, many organizations still use WINS along with DNS for name resolution. Unfortunately, WINS is slowly becoming obsolete.

To help organizations move forward with an all-DNS network, Microsoft Windows Server 2012 R2 DNS supports *GlobalName zones*. These use single-label names (DNS names that do not contain a suffix such as `.com`, `.net`, and so on). GlobalName zones are not intended to support peer-to-peer networks and workstation name resolution, and they don't support dynamic DNS updates.

GlobalName zones are designed to be used with servers. Because GlobalName zones are not dynamic, an administrator has to enter the records into the zone database manually. In most organizations, the servers have static TCP/IP addresses, and this works well with the GlobalName zone design. GlobalName zones are usually used to map single-label CNAME (alias) resource records to an FQDN.

Zone Transfers and Replication

DNS is such an important part of the network that you should not just use a single DNS server. With a single DNS server, you also have a single point of failure, and in fact, many domain registrars encourage the use of more than two name servers for a domain. Secondary servers or multiple primary Active Directory Integrated servers play an integral role in providing DNS information for an entire domain.

As previously stated, secondary DNS servers receive their zone databases through zone transfers. When you configure a secondary server for the first time, you must specify the primary server that is authoritative for the zone and that will send the zone transfer. The primary server must also permit the secondary server to request the zone transfer.

Zone transfers occur in one of two ways: *full zone transfers (AXFR)* and *incremental zone transfers (IXFR)*.

When a new secondary server is configured for the first time, it receives a full zone transfer from the primary DNS server. The full zone transfer contains all of the information in the DNS database. Some DNS implementations always receive full zone transfers.

After the secondary server receives its first full zone transfer, subsequent zone transfers are incremental. The primary name server compares its zone version number with that of the secondary server, and it sends only the changes that have been made in the interim. This significantly reduces network traffic generated by zone transfers.

The secondary server typically initiates zone transfers when the refresh interval time for the zone expires or when the secondary or stub server boots. Alternatively, you can configure notify lists on the primary server that send a message to the secondary or stub servers whenever any changes to the zone database occur.

When you consider your DNS strategy, you must carefully consider the layout of your network. If you have a single domain with offices in separate cities, you want to reduce the number of zone transfers across the potentially slow or expensive WAN links, although this is becoming less of a concern because of continuous increases in bandwidth.

Active Directory Integrated zones do away with traditional zone transfers altogether. Instead, they replicate across Active Directory with all of the other AD information. This replication is secure and encrypted because it uses the Active Directory security.

How DNS Notify Works

Windows Server 2012 R2 supports DNS Notify. *DNS Notify* is a mechanism that allows the process of initiating notifications to secondary servers when zone changes occur (RFC 1996). DNS Notify uses a push mechanism for communicating to a select set of secondary zone servers when their zone information is updated. (DNS Notify does not allow you to configure a notify list for a stub zone.)

After being notified of the changes, secondary servers can then start a pull zone transfer and update their local copies of the database.

Many different mechanisms use the push/pull relationship. Normally, one object pushes information to another, and the second object pulls the information from the first. Most applications push replication on a change value and pull it on a time value. For example, a system can push replication after 10 updates, or it can be pulled every 30 minutes.

To configure the DNS Notify process, you create a list of secondary servers to notify. List the IP address of the server in the primary master's Notify dialog box (see Figure 2.8). The Notify dialog box is located under the Zone Transfers tab, which is located in the zone Properties dialog box (see Figure 2.9).

FIGURE 2.8 DNS Notify dialog box

FIGURE 2.9 DNS Zone Transfers tab

Configuring Stub Zone Transfers with Zone Replication

In the preceding section, I talked about how to configure secondary server zone transfers. What if you wanted to configure settings for stub zone transfers? This is where zone replication scope comes in.

Only Active Directory–Integrated primary and stub zones can configure their replication scope. Secondary servers do not have this ability.

You can configure zone replication scope configurations in two ways. An administrator can set configuration options through the DNS snap-in or through a command-line tool called `DNSCmd`.

To configure zone replication scope through the DNS snap-in, follow these steps:

1. Click Start ➢ Administrative Tools ➢ DNS.
2. Right-click the zone you want to set up.
3. Choose Properties.
4. In the Properties dialog box, click the Change button next to Replication (see Figure 2.10).

FIGURE 2.10 DNS zone replication scope

5. Choose the replication scope that fits your organization.

Advantages of DNS in Windows Server 2012 R2

DNS in Microsoft Windows Server 2012 R2 has some great advantages over many other versions of Microsoft DNS. Here are some of the improvements of DNS in Windows Server 2012 R2 (some of these became available in Windows Server 2008, but they have been improved upon):

- Background zone loading
- Support for TCP/IP version 6 (IPv6)
- Read-only domain controllers
- GlobalName zone
- DNS Socket Pool
- DNS Cache Locking
- DNS Security Extensions (DNSSEC)
- DNS Devolution
- Zone Level Statistics
- Record Weighting
- Netmask Ordering
- DnsUpdateProxy Group
- Windows PowerShell Support

Background Zone Loading

If an organization had to restart a DNS server with an extremely large Active Directory Integrated DNS zones database in the past, DNS had a common problem with an Active Directory Integrated DNS zone. After the DNS restart, it could take hours for DNS data to be retrieved from Active Directory. During this time, the DNS server was unable to service any client requests.

Microsoft Windows Server 2008 DNS addressed this problem by implementing background zone loading, and Windows Server 2012 R2 has taken it a step further. As the DNS restarts, the Active Directory zone data populates the database in the background. This allows the DNS server to service client requests for data from other zones almost immediately after a restart.

Background zone loading accomplishes this task by loading the DNS zone using separate threads. This allows a DNS server to service requests while still loading the rest of the zone. If a client sends a request to the DNS server for a computer that has not yet loaded into memory, the DNS server retrieves the data from Active Directory and updates the record.

Support for IPv6 Addresses

Over the past few years, the Internet has starting running into a problem that was not foreseen when it was first created—it started running out of TCP/IP addresses. As you probably know, when the Internet was created, it was used for government and academic purposes only. Then, seemingly overnight, it grew to be the information superhighway. Nowadays, asking someone for his or her email address is almost as common as asking for their phone number.

Version 4 (IPv4) was the common version of TCP/IP. The release of TCP/IP version 6 (IPv6) has solved the lack-of-IP-addresses problem. IPv4 addresses are 32 bits long, but IPv6 addresses are 128 bits in length. The longer lengths allow for a much greater number of globally unique TCP/IP addresses.

Microsoft Windows Server 2012 R2 DNS has built-in support to accommodate both IPv4 and IPv6 address records. (DNS records are explained later in this chapter.) DHCP can also issue IPv6 addresses, which lets administrators allow DHCP to register the client with DNS, or the IPv6 client can register their address with the DNS server.

Support for Read-Only Domain Controllers

Windows Server 2008 introduced a new type of domain controller called the *read-only domain controller (RODC)*. This is a full copy of the Active Directory database without the ability to write to Active Directory. The RODC gives an organization the ability to install a domain controller in a location (onsite or offsite) where security is a concern.

Microsoft Windows Server 2012 R2 DNS has implemented a type of zone to help support an RODC. A primary read-only zone allows a DNS server to receive a copy of the application partition (including ForestDNSZones and DomainDNSZones) that DNS uses. This allows DNS to support an RODC because DNS now has a full copy of all DNS zones stored in Active Directory.

A primary, read-only zone is just what it says—a read-only zone; so to make any changes to it, you have to change the primary zones located on the Active Directory Integrated DNS server.

DNS Socket Pools

If your server is running Windows Server 2012 R2, you will be able to take advantage of DNS socket pools. *DNS socket pools* allow source port randomization to protect against DNS cache-poisoning attacks.

If you choose to use source port randomization, when the DNS service starts, the DNS server will randomly pick a source port from a pool of available sockets. This is an advantage because, instead of DNS using a well-known source port when issuing queries, the DNS server uses a random port selected from the socket pool. This helps guard against attacks because a hacker must correctly access the source port of the DNS query. The socket pool is automatically enabled in DNS with the default settings.

When using the DNS Socket Pool, the default size of the DNS socket pool is 2,500. When configuring the socket pool, you have the ability to choose a size value from 0 to 10,000. The larger the value, the greater the protection you will have against DNS spoofing attacks. If you decide to configure your socket pool size with a zero value, only a single socket for remote DNS queries will be used.

DNS Cache Locking

Windows Server 2012 R2 *DNS cache locking* allows cached DNS records to remain safe for the duration of the record's time to live (TTL) value. This means that the cached DNS records cannot be overwritten or changed. Because of this new DNS feature, it's tougher for hackers to perform cache-poisoning attacks against your DNS server.

DNS administrators can set how long a record will remain safe in cache. The configuration is based on a percent value. For example, if you set your cache locking value to 50 percent, then the cached records cannot be overwritten until half of the TTL has been reached. DNS cache locking is set to 100 percent by default. This means that the cached records never get overwritten.

DNS Security Extensions

One major issue that you must always look at is keeping your DNS safe. Think about it—DNS is a database of computer names and IP addresses. As a hacker, if I control DNS, I can control your company. In organizations that do not support extra security like IPsec, DNS security is even more important. This is where DNSSEC can help.

Windows Server 2012 R2 can use a suite of extensions that will help add security to DNS, and that suite is called *Domain Name System Security Extensions (DNSSEC)*, which was introduced in Windows Server 2008 R2. The DNSSEC protocol allows your DNS servers to be secure by validating DNS responses. DNSSEC secures your DNS resource records by accompanying the records with a digital signature.

To allow your DNS resource records to receive digital signatures, DNSSEC is applied to your DNS server by a procedure called *zone signing*. This process begins when a DNS resolver initiates a DNS query for a resource record in a signed DNS zone. When a response is returned, a digital signature (RRSIG) accompanies the response, and this allows the response to be verified. If the verification is successful, then the DNS resolver knows that the data has not been modified or tampered with in any way.

Once you implement a zone with DNSSEC, all of the records that are contained within that zone get individually signed. Since all of the records in the zone get individually signed, this gives administrators the ability to add, modify, or delete records without resigning the entire zone. The only requirement is to resign any updated records.

Trust Anchors

Trust anchors are an important part of the DNSSEC process because trust anchors allow the DNS servers to validate the DNSKEY resource records. *Trust anchors* are preconfigured public keys that are linked to a DNS zone. For a DNS server to perform validation, one or more trust anchors must be configured. If you are running an Active Directory Integrated zone, trust anchors can be stored in the Active Directory Domain Services directory partition of the forest. If you decide to store the trust anchors in the directory partition, then all DNS servers that reside on a domain controller get a copy of this trust anchor. On DNS servers that reside on stand-alone servers, trust anchors are stored in a file called `TrustAnchors.dns`.

If your servers are running Windows Server 2012 R2, then you can view trust anchors in the DNS Manager Console tree in the Trust Points container. You can also use Windows PowerShell or `Dnscmd.exe` to view trust anchors. Windows PowerShell is the recommended command-line method for viewing trust anchors. The following line is a PowerShell command to view the trust anchors for `Contoso.com`:

```
get-dnsservertrustanchor sec.contoso.com
```

DNSSEC Clients

Windows 7, Windows 8, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2 are all DNS clients that receive a response to a DNS query, examine the response, and then evaluate whether the response has been validated by a DNS server. The DNS client itself is nonvalidating, and the DNS client relies on the local DNS server to indicate that validation was successful. If the server doesn't perform validation, then the DNS client service can be configured to return no results.

If you are interested in learning how to set up DNSSEC in a lab environment, Microsoft has a website that explains all about DNSSEC and how to set up the lab environment. Visit `http://technet.microsoft.com/en-us/library/hh831411.aspx`.

DNS Devolution

Using *DNS devolution*, if a client computer is a member of a child namespace, the client computer will be able to access resources in the parent namespace without the need to provide explicitly the fully qualified domain name (FQDN) of the resource. DNS devolution removes the leftmost label of the namespace to get to the parent suffix. DNS devolution allows the DNS resolver to create the new FQDNs. DNS devolution works by appending the single-label, unqualified domain name with the parent suffix of the primary DNS suffix name.

Zone Level Statistics

DNS zone level server statistics are available in Windows Server 2012 R2 by using the Windows PowerShell cmdlet `Get-DnsServerStatistics`. This powerful Windows PowerShell cmdlet retrieves statistics and data for the DNS server. The following is an example of the `Get-DnsServerStatistics` cmdlet:

```
Get-DnsServerStatistics -ZoneName <String[]> [-AsJob][-CimSession
<CimSession[]> ][-Clear][-ComputerName <String> ][-ThrottleLimit <Int32> ]
[ <CommonParameters>]
```

The ZoneName parameter allows an administrator to get specific statistics for the DNS zone that you have specified. If the ZoneName parameter is not specified during the

PowerShell cmdlet, the server-level statistics are retrieved and shown. If an administrator uses the Clear parameter in the PowerShell cmdlet along with the ZoneName parameter, the statistics for the specified zone will be cleared. So, use this cmdlet carefully.

Record Weighting

Weighting DNS records will allow an administrator to place a value on DNS SRV records. Clients will then randomly choose SRV records proportional to the weight value assigned.

Netmask Ordering

If round robin is enabled, when a client requests name resolution, the first address entered in the database is returned to the resolver, and it is then sent to the end of the list. The next time a client attempts to resolve the name, the DNS server returns the second name in the database (which is now the first name) and then sends it to the end of the list, and so on. Round robin is enabled by default.

Netmask ordering is part of the round-robin process. When an administrator configures netmask ordering, the DNS server will detect the subnet of the querying client. The DNS server will then return a host address available for the same subnet. Netmask ordering is enabled through the DNS Manager console on the Advanced tab of the server Properties dialog box.

DnsUpdateProxy Group

As mentioned previously, the DHCP server can be configured to register host (A) and pointer (PTR) resource records dynamically on behalf of DHCP clients. Because of this, the DNS server can end up with stale resources. To help solve this issue, an administrator can use the built-in security group called *DnsUpdateProxy*.

To use the DnsUpdateProxy group, an administrator must first create a dedicated user account and configure the DHCP servers with its credentials. This will protect against the creation of unsecured records. Also, when you create the dedicated user account, members of the DnsUpdateProxy group will be able to register records in zones that allow only secured dynamic updates. Multiple DHCP servers can use the same credentials of one dedicated user account.

Now that you have looked at some of the new features of Windows Server 2012 R2 DNS, let's take a look at some of the DNS record types.

Windows PowerShell Support

Microsoft has more than 100 PowerShell cmdlets specifically for DNS. While in Windows PowerShell, you can list all of the DNS cmdlets that are available. To see the entire list, use the following PowerShell command:

```
Get-Command -Module DnsServer cmdlet.
```

For an entire list of all of the Windows PowerShell DNS cmdlets, go to `http://technet.microsoft.com/en-us/library/jj649850.aspx`.

Introducing DNS Record Types

No matter where your zone information is stored, you can rest assured that it contains a variety of DNS information. Although the DNS snap-in makes it unlikely that you'll ever need to edit these files by hand, it's good to know exactly what data is contained there.

As stated previously, zone files consist of a number of resource records. You need to know about several types of resource records to manage your DNS servers effectively. They are discussed in the following sections.

Part of the resource record is its class. *Classes* define the type of network for the resource record. There are three classes: Internet, Chaosnet, and Hesoid. By far, the Internet class is the most popular. In fact, it's doubtful that you'll see either Chaosnet or Hesoid classes in the wild.

The following are some of the more important resource records in a DNS database. For a listing of records in a Microsoft DNS database, visit Microsoft's website at `http://technet.microsoft.com/en-us/library/cc958958.aspx`.

Start of Authority Records

The first record in a database file is the *start of authority (SOA) record*. The SOA defines the general parameters for the DNS zone, including the identity of the authoritative server for the zone.

The SOA appears in the following format:

```
@ IN SOA primary_mastercontact_e-mailserial_number
refresh_timeretry_timeexpiration_timetime_to_live
```

Here is a sample SOA from the domain `example.com`:

```
@ IN SOA win2k3r2.example.com. hostmaster.example.com. (
                        5            ; serial number
                        900          ; refresh
                        600          ; retry
                        86400        ; expire
                        3600       ) ; default TTL
```

Table 2.2 lists the attributes stored in the SOA record.

TABLE 2.2 The SOA record structure

Field	Meaning
Current zone	The current zone for the SOA. This can be represented by an `@` symbol to indicate the current zone or by naming the zone itself. In the example, the current zone is `example.com`. The trailing dot (`.com.`) indicates the zone's place relative to the root of the DNS.
Class	This will almost always be the letters *IN* for the Internet class.
Type of record	The type of record follows. In this case, it's SOA.
Primary master	The primary master for the zone on which this file is maintained.
Contact email	The Internet email address for the person responsible for this domain's database file. There is no `@` symbol in this contact email address because `@` is a special character in zone files. The contact email address is separated by a single dot (`.`). So the email address of `root@example.com` would be represented by `root.example.com` in a zone file.
Serial number	This is the "version number" of this database file. It increases each time the database file is changed.
Refresh time	The amount of time (in seconds) that a secondary server will wait between checks to its master server to see if the database file has changed and a zone transfer should be requested.
Retry time	The amount of time (in seconds) that a secondary server will wait before retrying a failed zone transfer.
Expiration time	The amount of time (in seconds) that a secondary server will spend trying to download a zone. Once this time limit expires, the old zone information will be discarded.
Time to live	The amount of time (in seconds) that another DNS server is allowed to cache any resource records from this database file. This is the value that is sent out with all query responses from this zone file when the individual resource record doesn't contain an overriding value.

Name Server Records

Name server (NS) records list the name servers for a domain. This record allows other name servers to look up names in your domain. A zone file may contain more than one name server record. The format of these records is simple:

```
example.com.    IN      NS      Hostname.example.com
```

Table 2.3 explains the attributes stored in the NS record.

TABLE 2.3 The NS record structure

Field	Meaning
Name	The domain that will be serviced by this name server. In this case, I used `example.com`.
AddressClass	Internet (IN)
RecordType	Name server (NS)
Name Server Name	The FQDN of the server responsible for the domain

Any domain name in the database file that is not terminated with a period will have the root domain appended to the end. For example, an entry that just has the name *sales* will be expanded by adding the root domain to the end, whereas the entry `sales.example.com.` won't be expanded.

Host Record

A *host record* (also called an *A record* for IPv4 and *AAAA record* for IPv6) is used to associate statically a host's name to its IP addresses. The format is pretty simple:

```
host_nameoptional_TTL IN  A  IP_Address
```

Here's an example from my DNS database:

```
www  IN  A  192.168.0.204
SMTP IN  A  192.168.3.144
```

The A or AAAA record ties a hostname (which is part of an FQDN) to a specific IP address. This makes these records suitable for use when you have devices with statically assigned IP addresses. In this case, you create these records manually using the DNS snap-in. As it turns out, if you enable DDNS, your DHCP server can create these for you. This automatic creation is what enables DDNS to work.

Notice that an optional TTL field is available for each resource record in the DNS. This value is used to set a TTL that is different from the default TTL for the domain. For example, if you wanted a 60-second TTL for the www A or AAAA record, it would look like this:

```
www 60 IN  A  192.168.0.204
```

Alias Record

Closely related to the host record is the *alias record*, or *canonical name (CNAME) record*. The syntax of an alias record is as follows:

```
aliasoptional_TTL  IN  CNAME  hostname
```

Aliases are used to point more than one DNS record toward a host for which an A record already exists. For example, if the hostname of your web server was actually `chaos`, you would likely have an A record such as this:

```
chaos IN A 192.168.1.10
```

Then you could make an alias or CNAME for the record so that `www.example.com` would point to `chaos`:

```
www IN CNAME chaos.example.com.
```

Note the trailing dot (`.`) on the end of the CNAME record. This means the root domain is not appended to the entry.

Pointer Record

A or AAAA records are probably the most visible component of the DNS database because Internet users depend on them to turn FQDNs like `www.microsoft.com` into the IP addresses that browsers and other components require to find Internet resources. However, the host record has a lesser-known but still important twin: the *pointer (PTR) record*. The format of a PTR record appears as follows:

```
reversed_address.in-addr.arpa. optional_TTL IN PTR targeted_domain_name
```

The A or AAAA record maps a hostname to an IP address, and the PTR record does just the opposite—mapping an IP address to a hostname through the use of the `in-addr.arpa` zone.

The PTR record is necessary because IP addresses begin with the least-specific portion first (the network) and end with the most-specific portion (the host), whereas hostnames begin with the most-specific portion at the beginning and the least-specific portion at the end.

Consider the example 192.168.1.10 with a subnet mask 255.255.255.0. The portion 192.168.1 defines the network and the final .10 defines the host, or the most-specific portion of the address. DNS is just the opposite: The hostname `www.example.com.` defines the most-specific portion, `www`, at the beginning and then traverses the DNS tree to the least-specific part, the dot (`.`), at the root of the tree.

Reverse DNS records, therefore, need to be represented in this most-specific-to-least-specific manner. The PTR record for mapping 192.168.1.10 to `www.example.com` would look like this:

```
10.1.168.192.in-addr.arpa. IN PTR www.example.com.
```

Now a DNS query for that record can follow the logical DNS hierarchy from the root of the DNS tree all the way to the most-specific portion.

Mail Exchanger Record

The *mail exchanger (MX) record* is used to specify which servers accept mail for this domain. Each MX record contains two parameters—a preference and a mail server, as shown in the following example:

```
domain IN MX preference mailserver_host
```

The MX record uses the preference value to specify which server should be used if more than one MX record is present. The preference value is a number. The lower the number, the more preferred the server. Here's an example:

```
example.com.    IN  MX  0  mail.example.com.
example.com.    IN  MX  10 backupmail.example.com.
```

In the example, `mail.example.com` is the default mail server for the domain. If that server goes down for any reason, emailers then use the `backupmail.example.com` mail server.

Service (SRV) Record

Windows Server 2012 R2 depends on some other services, like the Lightweight Directory Access Protocol (LDAP) and Kerberos. Using a service record, which is another type of DNS record, a Windows 2000, XP, Vista, Windows 7, Windows 8, and all Windows Server products can query DNS servers for the location of a domain controller. This makes it much easier (for both the client and the administrator) to manage and distribute logon traffic in large-scale networks. For this approach to work, Microsoft has to have some way to register the presence of a service in DNS. Enter the service (SRV) record.

Service (SRV) records tie together the location of a service (like a domain controller) with information about how to contact the service. SRV records provide seven items of information. Let's review an example to help clarify this powerful concept. (Table 2.4 explains the fields in the following example.)

```
ldap.tcp.example.com.  86400 IN SRV  10  100  389  hsv.example.com
ldap.tcp.example.com.  86400 IN SRV  20  100  389  msy.example.com
```

TABLE 2.4 The SRV record structure

Field	Meaning
Domain name	Domain for which this record is valid (`ldap.tcp.example.com.`).
TTL	Time to live (86,400 seconds).
Class	This field is always `IN`, which stands for Internet.

Record type	Type of record (`SRV`).
Priority	Specifies a preference, similar to the Preference field in an MX record. The SRV record with the lowest priority is used first (`10`).
Weight	Service records with equal priority are chosen according to their weight (`100`).
Port number	The port where the server is listening for this service (`389`).
Target	The FQDN of the host computer (`hsv.example.com` and `msy.example.com`).

You can define other types of service records. If your applications support them, they can query DNS to find the services they need.

Configuring DNS

In the following sections, you'll begin to learn about the actual DNS server. You will start by installing DNS. Then I will talk about different zone configuration options and what they mean. Finally, you'll complete an exercise that covers configuring Dynamic DNS, delegating zones, and manually entering records.

DNS requires that you use a static IP address on the server. The reason for this is that clients access the DNS server by using its TCP/IP address, and that's why DNS servers need to install a static IP address.

If you are currently using DHCP on your server, change your DNS server to have a static IP address before completing this exercise. I know that most of you already know how to change your IP address, but for anyone new to Microsoft Server 2012 R2, click the Start button and go into Control Panel. Make sure that the VIEW BY in the upper-right corner is set to large icons, and then choose Network and Sharing Center. On the right side of the windows under Access Type, click the access type link you have (Ethernet, Wireless, and so forth). Choose Properties, and then click Internet Protocol Version 4 (TCP/IPv4) and choose Properties. Choose the radio button for Use The Following IP Address and enter your local TCP/IP settings. Click OK to change it from DHCP to a static TCP/IP address.

Installing DNS

Let's start by installing DNS. Installing DNS is an important part of running a network. Exercise 2.1 walks you through the installation of a DNS server.

EXERCISE 2.1

Installing and Configuring the DNS Service

1. Open Server Manager.
2. On the Server Manager dashboard, click the Add Roles And Features link.

3. If a Before You Begin screen appears, click Next.
4. On the Selection type page, choose Role-Based Or Feature-Based Installation and click Next.
5. Click the Select A Server From The Server Pool radio button and choose the server under the Server Pool section. Click Next.
6. Click the DNS Server Item in the Server Role list. If a pop-up window appears telling you that you need to add additional features, click the Add Features button. If you did not give your system a static TCP/IP address, a window appears stating that you need a static TCP/IP address; just click the Continue button to bypass the error. Click Next to continue.
7. On the Add Features page, just click Next.
8. Click Next on the DNS Server information screen.
9. On the Confirm Installation screen, choose the Restart The Destination Server Automatically If Required check box and then click the Install button.

10. At the Installation progress screen, click Close after the DNS server is installed.
11. Close Server Manager.

Load Balancing with Round Robin

Like other DNS implementations, the Windows Server 2012 R2 implementation of DNS supports load balancing through the use of round robin. Load balancing distributes the network load among multiple network hosts if they are available. You set up round-robin load balancing by creating multiple resource records with the same hostname but different IP addresses for multiple computers. Depending on the options you select, the DNS server responds with the addresses of one of the host computers.

If round robin is enabled, when a client requests name resolution, the first address entered in the database is returned to the resolver and is then sent to the end of the list. The next time a client attempts to resolve the name, the DNS server returns the second name in the database (which is now the first name) and then sends it to the end of the list, and so on. Round robin is enabled by default.

Configuring a Caching-Only Server

Although all DNS name servers cache queries that they have resolved, caching-only servers are DNS name servers that only perform queries, cache the answers, and return the results. They are not authoritative for any domains, and the information that they contain is limited to what has been cached while resolving queries. Accordingly, they don't have any zone files, and they don't participate in zone transfers. When a caching-only server is first started, it has no information in its cache; the cache is gradually built over time.

Caching-only servers are easy to configure. After installing the DNS service, simply make sure the root hints are configured properly:

1. Right-click your DNS server and choose the Properties command.
2. When the Properties dialog box appears, switch to the Root Hints tab (see Figure 2.11).

FIGURE 2.11 The Root Hints tab of the DNS server's Properties dialog box

3. If your server is connected to the Internet, you should see a list of root hints for the root servers maintained by ICANN and the Internet Assigned Numbers Authority (IANA). If not, click the Add button to add root hints as defined in the `cache.dns` file.

   You can obtain current `cache.dns` files on the Internet by using a search engine. Just search for *cache.dns* and download one. (I always try to get `cache.dns` files from a university or a company that manages domain names.)

Setting Zone Properties

There are six tabs on the Properties dialog box for a forward or reverse lookup zone. You only use the Security tab to control who can change properties and to make dynamic updates to records on that zone. The other tabs are discussed in the following sections.

Secondary zones don't have a Security tab, and their SOA tab shows you the contents of the master SOA record, which you can't change.

General Tab

The General tab includes the following:

- The Status indicator and the associated Pause button let you see and control whether this zone can be used to answer queries. When the zone is running, the server can use it to answer client queries; when it's paused, the server won't answer any queries it gets for that particular zone.
- The Type indicator and its Change button allow you to select the zone type. The options are Standard Primary, Standard Secondary, and AD-Integrated. (See "Introducing DNS Database Zones" earlier in this chapter.) As you change the type, the controls you see below the horizontal dividing line change too. For primary zones, you'll see a field that lets you select the zone filename; for secondary zones, you'll get controls that allow you to specify the IP addresses of the primary servers. But the most interesting controls are the ones you see for AD Integrated zones. When you change to the AD Integrated zones, you have the ability to make the dynamic zones Secure Only.
- The Replication indicator and its Change button allow you to change the replication scope if the zone is stored in Active Directory. You can choose to replicate the zone data to any of the following:
  - All DNS servers in the Active Directory forest
  - All DNS servers in a specified domain
  - All domain controllers in the Active Directory domain (required if you use Windows 2000 domain controllers in your domain)
  - All domain controllers specified in the replication scope of the application directory partition

- The Dynamic Updates field gives you a way to specify whether you want to support Dynamic DNS updates from compatible DHCP servers. As you learned earlier in the section "Dynamic DNS and Non-Dynamic DNS," the DHCP server or DHCP client must know about and support Dynamic DNS in order to use it, but the DNS server has to participate too. You can turn dynamic updates on or off, or you can require that updates be secured.

Start Of Authority (SOA) Tab

The options on the Start Of Authority (SOA) tab, shown in Figure 2.12, control the contents of the SOA record for this zone.

FIGURE 2.12 The Start Of Authority (SOA) tab of the zone Properties dialog box

- The Serial Number field indicates which version of the SOA record the server currently holds. Every time you change another field, you should increment the serial number so that other servers will notice the change and get a copy of the updated record.
- The Primary Server and Responsible Person fields indicate the location of the primary name server (NS) for this zone and the email address of the administrator responsible for the maintenance of this zone, respectively. The standard username for this is hostmaster.
- The Refresh Interval field controls how often any secondary zones of this zone must contact the primary zone server and get any changes that have been posted since the last update.
- The Retry Interval field controls how long secondary servers will wait after a zone transfer fails before they try again. They'll keep trying at the interval you specify (which should be shorter than the refresh interval) until they eventually succeed in transferring zone data.

- The Expires After field tells the secondary servers when to throw away zone data. The default of 1 day (24 hours) means that a secondary server that hasn't gotten an update in 24 hours will delete its local copy of the zone data.
- The Minimum (Default) TTL field sets the default TTL for all RRs created in the zone. You can assign specific TTLs to individual records if you want.
- The TTL For This Record field controls the TTL for the SOA record itself.

Name Servers Tab

The *name server (NS) record* for a zone indicates which name servers are authoritative for the zone. That normally means the zone primary server and any secondary servers you've configured for the zone. (Remember, secondary servers are authoritative read-only copies of the zone.) You edit the NS record for a zone using the Name Servers tab (see Figure 2.13). The tab shows you which servers are currently listed, and you use the Add, Edit, and Remove buttons to specify which name servers you want included in the zone's NS record.

FIGURE 2.13 The Name Servers tab of the zone Properties dialog box

WINS Tab

The WINS tab allows you to control whether this zone uses WINS forward lookups. These lookups pass on queries that DNS can't resolve to WINS for action. This is a useful setup if you're still using WINS on your network. You must explicitly turn this option on with the Use WINS Forward Lookup check box on the WINS tab for a particular zone.

Zone Transfers Tab

Zone transfers are necessary and useful because they're the mechanism used to propagate zone data between primary and secondary servers. For primary servers (whether AD Integrated or not), you can specify whether your servers will allow zone transfers and, if so, to whom.

You can use the following controls on the Zone Transfers tab to configure these settings per zone:

- The Allow Zone Transfers check box controls whether the server answers zone transfer requests for this zone at all; when it's not checked, no zone data is transferred. The Allow Zone Transfers selections are as follows:
  - To Any Server allows any server anywhere on the Internet to request a copy of your zone data.
  - Only To Servers Listed On The Name Servers Tab (the default) limits transfers to servers you specify. This is a more secure setting than To Any Server because it limits transfers to other servers for the same zone.
  - Only To The Following Servers allows you to specify exactly which servers are allowed to request zone transfers. This list can be larger or smaller than the list specified on the Name Servers tab.
- The Notify button is for setting up automatic notification triggers that are sent to secondary servers for this zone. Those triggers signal the secondary servers that changes have occurred on the primary server so that the secondary servers can request updates sooner than their normally scheduled interval. The options in the Notify dialog box are similar to those in the Zone Transfers tab. You can enable automatic notification and then choose either Servers Listed On The Name Servers Tab or The Following Servers.

Configuring Zones for Dynamic Updates

In Exercise 2.2, you will create and then modify the properties of a forward lookup zone. In addition, you'll configure the zone to allow dynamic updates. You are installing this DNS zone as a primary zone *without* AD integration. Even if you installed this DNS server onto a domain controller, do not choose the check box for AD integration.

EXERCISE 2.2

Configuring a Zone for Dynamic Updates

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Click the DNS server to expand it and then click the Forward Lookup Zones folder. Right-click the Forward Lookup Zones folder and choose New Zone.
3. At the New Zone Welcome screen, click Next.
4. At the Zone Type screen, choose the Primary Zone option. Again, if your DNS server is also a domain controller, do not check the box to store the zone in Active Directory. Click Next when you are ready.

5. Enter a new zone name in the Zone Name field and click Next. (I used my last name—`Panek.com`.)
6. Leave the default zone filename and click Next.
7. Select the Do Not Allow Dynamic Updates radio button and click Next.
8. Click Finish to end the wizard.
9. Right-click the zone you just created and choose the Properties command.

EXERCISE 2.2 *(continued)*

10. Click the down arrow next to Dynamic Updates. Notice that there are only two options (None and Nonsecure And Secure). The Secure Only option is not available because you are not using Active Directory Integrated. Make sure Nonsecure And Secure is chosen.

11. Click OK to close the Properties box.
12. Close the DNS management snap-in.
13. Close the Server Manager snap-in.

Delegating Zones for DNS

DNS provides the ability to divide the namespace into one or more zones, which can then be stored, distributed, and replicated to other DNS servers. When deciding whether to divide your DNS namespace to make additional zones, consider the following reasons to use additional zones:

- A need to delegate management of part of your DNS namespace to another location or department within your organization.
- A need to divide one large zone into smaller zones for distributing traffic loads among multiple servers, for improving DNS name-resolution performance, or for creating a more fault-tolerant DNS environment.
- A need to extend the namespace by adding numerous subdomains at once, such as to accommodate the opening of a new branch or site.

Each newly delegated zone requires a primary DNS server just as a regular DNS zone does. When delegating zones within your namespace, be aware that for each new zone you create, you need to place delegation records in other zones that point to the authoritative DNS servers for the new zone. This is necessary both to transfer authority and to provide correct referral to other DNS servers and clients of the new servers being made authoritative for the new zone.

In Exercise 2.3, you'll create a delegated subdomain of the domain you created back in Exercise 2.2. Note that the name of the server to which you want to delegate the subdomain must be stored in an A or CNAME record in the parent domain.

EXERCISE 2.3

Creating a Delegated DNS Zone

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Expand the DNS server and locate the zone you created in Exercise 2.2.
3. Right-click the zone and choose the New Delegation command.
4. The New Delegation Wizard appears. Click Next to dismiss the initial wizard page.
5. Enter **`ns1`** (or whatever other name you like) in the Delegated Domain field of the Delegated Domain Name page. This is the name of the domain for which you want to delegate authority to another DNS server. It should be a subdomain of the primary domain (for example, to delegate authority for `farmington.example.net`, you'd enter **`farmington`** in the Delegated Domain field). Click Next to complete this step.
6. When the Name Servers page appears, click the Add button to add the name(s) and IP address(es) of the servers that will be hosting the newly delegated zone. For the purpose of this exercise, enter the server name you used in Exercise 2.2. Click the Resolve button to resolve this domain name's IP address automatically into the IP address field. Click OK when you are finished. Click Next to continue with the wizard.
7. Click the Finish button. The New Delegation Wizard disappears, and you'll see the new zone you just created appear beneath the zone you selected in step 3. The newly delegated zone's folder icon is drawn in gray to indicate that control of the zone is delegated.

DNS Forwarding

If a DNS server does not have an answer to a DNS request, it may be necessary to send that request to another DNS server. This is called *DNS forwarding*. You need to understand the two main types of forwarding:

External Forwarding When a DNS server forwards an external DNS request to a DNS server outside of your organization, this is considered *external forwarding*. For example, a

resolver requests the host `www.microsoft.com`. Most likely, your internal DNS server is not going to have Microsoft's web address in its DNS database. So, your DNS server is going to send the request to an external DNS (most likely your ISP).

Conditional Forwarding *Conditional forwarding* is a lot like external forwarding except that you are going to forward requests to specific DNS servers based on a condition. Usually, this is an excellent setup for internal DNS resolution. For example, let's say you have two companies, `stellacon.com` and `stellatest.com`. If a request comes in for `Stellacon.com`, it gets forwarded to the Stellacon DNS server, and any requests for `Stellatest.com` will get forwarded to the Stellatest DNS server. Requests are forwarded to a specific DNS server depending on the condition that an administrator sets up.

Manually Creating DNS Records

From time to time, you may find it necessary to add resource records manually to your Windows Server 2012 R2 DNS servers. Although Dynamic DNS frees you from the need to fiddle with A and PTR records for clients and other such entries, you still have to create other resource types (including MX records, required for the proper flow of SMTP email) manually. You can manually create A, PTR, MX, SRV, and many other record types.

There are only two important things to remember for manually creating DNS records:

- You must right-click the zone and choose either the New Record command or the Other New Records command.
- You must know how to fill in the fields of whatever record type you're using.

  For example, to create an MX record, you need three pieces of information (the domain, the mail server, and the priority). To create an SRV record, however, you need several more pieces of information.

In Exercise 2.4, you will manually create an MX record for a mailtest server in the zone you created in Exercise 2.2.

EXERCISE 2.4

Manually Creating DNS RRs

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Expand your DNS server, right-click its zone and choose New Host (A record).
3. Enter **`mailtest`** in the Name field. Enter a TCP/IP number in the IP Address field. (You can use any number for this exercise, for example, 192.168.1.254.) Click the Add Host button.
4. A dialog box appears stating that the host record was created successfully. Click OK. Click Done.

5. Right-click your zone name and choose New Mail Exchanger (MX).
6. Enter **`mailtest`** in the Host Or Child Domain field and enter **`mailtest.yourDomain.com`** (or whatever domain name you used in Exercise 2.2) in the Fully-Qualified Domain Name (FQDN) Of Mail Server field; then click OK. Notice that the new record is already visible.
7. Next create an alias (or CNAME) record to point to the mail server. (It is assumed that you already have an A record for `mailtest` in your zone.) Right-click your zone, and choose New Alias (CNAME).
8. Type **`mail`** into the Alias Name field.
9. Type **`mailtest.yourDomain.com`** into the Fully-Qualified Domain Name (FQDN) For Target Host field.
10. Click the OK button.
11. Close the DNS management snap-in.

DNS Aging and Scavenging

When using dynamic updates, computers (or DHCP) will register a resource record with DNS. These records get removed when a computer is shut down properly. A major problem in the industry is that laptops are frequently removed from the network without a proper shutdown. Therefore, their resource records continue to live in the DNS database.

Windows Server 2012 R2 DNS supports two features called *DNS aging* and *DNS scavenging*. These features are used to clean up and remove stale resource records of a primary DNS zone. DNS aging and DNS scavenging flags old resource records that have

not been updated in a certain amount of time (determined by the scavenging interval). These stale records will be scavenged at the next cleanup interval. DNS uses time stamps on the resource records to determine how long they have been listed in the DNS database.

DNS allows an administrator to set up and configure aging and scavenging through the use of the DNS snap-in. DNS aging and scavenging allows an administrator to perform some of the following related tasks for your DNS servers and any of the Active Directory–Integrated zones that they load:

- Administrators can enable or disable the use of scavenging at a DNS server and/or for selected zones at the DNS server.
- You can modify the no-refresh/refresh interval, either as a server default or by specifying an overriding value at selected zones.
- Administrators can specify when periodic scavenging occurs automatically at the DNS server for any of its eligible zones and how often these operations are repeated.
- Manually initiate a single scavenging operation for all eligible zones at the DNS server.

Enabling Scavenging of Stale Records

When you install Windows Server 2012 R2 DNS aging and scavenging features on all DNS servers and any of their zones, administrators should consider the following settings before using these features:

Determine whether you should use aging and scavenging for server-wide settings. When using these settings, you are choosing to affect every one of the zone-level properties for all Active Directory–Integrated zones that are loaded at the server.

Determine whether you should use aging and scavenging for zone settings. When using these settings, you are choosing to use them for zone-specific properties for just the selected zones and not the entire server. These settings apply only to the applicable zone and its resource records, and they do not apply to any other zone on the DNS server. Unless these zone-level properties are otherwise configured, they inherit their defaults from comparable settings that are maintained in server aging and scavenging properties.

Enabling aging and scavenging for use with standard primary zones modifies the format of zone files. This change does not affect zone replication to secondary servers, but the modified zone files cannot be loaded by other versions of DNS servers.

Monitoring and Troubleshooting DNS

Now that you have set up and configured your DNS name server and created some resource records, you will want to confirm that it is resolving and replying to client DNS requests. A couple of tools allow you to do some basic monitoring and managing. Once you are able to monitor DNS, you'll want to start troubleshooting.

The simplest test is to use the `ping` command to make sure that the server is alive. A more thorough test would be to use `nslookup` to verify that you can actually resolve addresses for items on your DNS server.

In the following sections, you'll look at some of these monitoring and management tools and how to troubleshoot DNS.

Monitoring DNS with the DNS Snap-In

You can use the DNS snap-in to do some basic server testing and monitoring. More important, you use the snap-in to monitor and set logging options. On the Event Logging tab of the server's Properties dialog box (see Figure 2.14), you can pick which events you want logged. The more events you select, the more logging information you'll get. This is useful when you're trying to track what's happening with your servers, but it can result in a very large log file if you're not careful.

FIGURE 2.14 The Event Logging tab of the server's Properties dialog box

The Monitoring tab (see Figure 2.15) gives you some testing tools. When the check box labeled A Simple Query Against This DNS Server is checked, a test is performed that asks for a single record from the local DNS server. It's useful for verifying that the service is running and listening to queries, but not much else. When the check box labeled A Recursive Query To Other DNS Servers is checked, the test is more sophisticated—a recursive query checks whether forwarding is working okay. The Test Now button and the Perform Automatic Testing At The Following Interval check box allow you to run these tests now or later as you require.

FIGURE 2.15 The Monitoring tab of the server's Properties dialog box

Another tab in the server's properties that allows you to monitor the activity of the DNS server is the Debug Logging tab. The Debug Logging tab allows you to monitor all outbound and inbound DNS traffic, packet content, packet type, and which transport protocol (TCP or UDP) that you want to monitor on the DNS server.

If the simple query fails, check that the local server contains the zone `1.0.0.127.in-addr.arpa`. If the recursive query fails, check that your root hints are correct and that your root servers are running.

In Exercise 2.5, you will enable logging, use the DNS MMC to test the DNS server, and view the contents of the DNS log.

EXERCISE 2.5

Simple DNS Testing

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Right-click the DNS server name on the top left and select Properties.
3. Switch to the Debug Logging tab, check all of the debug logging options except Filter Packets By IP Address, and enter a full path and filename in the File Path And Name field. Click the Apply button.

4. Switch to the Monitoring tab and check both A Simple Query Against This DNS Server and A Recursive Query To Other DNS Servers.
5. Click the Test Now button several times and then click OK.
6. Press the Windows key on the keyboard (left side between the Ctrl and Alt keys) and then choose Computer. Navigate to the folder that you specified in step 3 and use WordPad or Notepad to view the contents of the log file.

Troubleshooting DNS

When troubleshooting DNS problems, ask yourself the following basic questions:

- What application is failing? What works? What doesn't work?
- Is the problem basic IP connectivity, or is it name resolution? If the problem is name resolution, does the failing application use NetBIOS names, DNS names, or hostnames?
- How are the things that do and don't work related?
- Have the things that don't work ever worked on this computer or network? If so, what has changed since they last worked?

Windows Server 2012 R2 provides several useful tools, discussed in the following sections, which can help you answer these questions:

- `Nslookup` is used to perform DNS queries and to examine the contents of zone files on local and remote servers.
- `DNSLint` is a command-line utility used for troubleshooting many common DNS issues.

- `Ipconfig` allows you to perform the following tasks:
  - View DNS client settings
  - Display and flush the resolver cache
  - Force a dynamic update client to register its DNS records
- The DNS log file monitors certain DNS server events and logs them for your edification.

Using *Nslookup*

`Nslookup` is a standard command-line tool provided in most DNS server implementations, including Windows Server 2012 R2. Windows Server 2012 R2 gives you the ability to launch `nslookup` from the DNS snap-in.

When `nslookup` is launched from the DNS snap-in, a command prompt window opens automatically. You enter `nslookup` commands in this window.

`Nslookup` offers you the ability to perform query testing of DNS servers and to obtain detailed responses at the command prompt. This information can be useful for diagnosing and solving name resolution problems, for verifying that resource records are added or updated correctly in a zone, and for debugging other server-related problems. You can do a number of useful things with `nslookup`:

- Use it in noninteractive mode to look up a single piece of data
- Enter interactive mode and use the debug feature
- Perform the following from within interactive mode:
  - Set options for your query
  - Look up a name
  - Look up records in a zone
  - Perform zone transfers
  - Exit `nslookup`

When you are entering queries, it is generally a good idea to enter FQDNs so that you can control what name is submitted to the server. However, if you want to know which suffixes are added to unqualified names before they are submitted to the server, you can enter `nslookup` in debug mode and then enter an unqualified name.

Using Nslookup on the Command Line

To use `nslookup` in plain-old command-line mode, enter the following in the command prompt window:

```
nslookup DNS_name_or_IP_address server_IP_address
```

This command will look up a DNS name or address using a server at the IP address you specify.

Using *Nslookup* in Interactive Mode

`Nslookup` is a lot more useful in interactive mode because you can enter several commands in sequence. Entering **`nslookup`** by itself (without specifying a query or server) puts it in interactive mode, where it will stay until you type **`exit`** and press Enter. Before that point, you can look up lots of useful stuff. The following are some of the tasks you can perform with `nslookup` in interactive mode:

Setting Options with the `set` Command While in interactive mode, you can use the `set` command to configure how the resolver will carry out queries. Table 2.5 shows a few of the options available with `set`.

TABLE 2.5 Command-line options available with the `set` command

Option	Purpose
`set all`	Shows all the options available.
`set d2`	Puts `nslookup` in debug mode so that you can examine the query and response packets between the resolver and the server.
`set domain=`*`domain name`*	Tells the resolver what domain name to append for unqualified queries.
`set timeout=`*`timeout`*	Tells the resolver how long to keep trying to contact the server. This option is useful for slow links where queries frequently time out and the wait time must be lengthened.
`set type=`*`record type`*	Tells the resolver which type of resource records to search for (for example, A, PTR, or SRV). If you want the resolver to query for all types of resource records, type **`settype=all`**.

Looking Up a Name While in interactive mode, you can look up a name just by typing it: **`stellacon.com`**. In this example, `stellacon` is the owner name for the record for which you are searching, and `.com` is the server you want to query.

You can use the wildcard character (`*`) in your query. For example, if you want to look for all resource records that have *k* as the first letter, just type **`k*`** as your query.

Looking Up a Record Type If you want to query a particular type of record (for instance, an MX record), use the `set type` command. The command `set type=mx` tells `nslookup` you're interested only in seeing MX records that meet your search criteria.

Listing the Contents of a Domain To get a list of the contents of an entire domain, use the `ls` command. To find all of the hosts in your domain, you'd type **`set type=a`** and then type **`ls -t yourdomain.com`**.

Troubleshooting Zone Transfers You can simulate zone transfers by using the `ls` command with the `-d` switch. This can help you determine whether the server you are querying allows zone transfers to your computer. To do this, type **`ls -d domain__name`**.

Nslookup Responses and Error Messages

A successful `nslookup` response looks like this:

```
Server: Name_of_DNS_server
Address: IP_address_of_DNS_server
Response_data
```

`Nslookup` might also return an error message. Some common messages are listed in Table 2.6.

TABLE 2.6 Common `nslookup` error messages

Error message	Meaning

`DNS request timed out.`
`Timeout was` *x* `seconds.`
`*** Can't find server name for address` *IP_Address*`: Timed out`
`*** Default servers are not available`
`Default Server: Unknown`
`Address:` *IP_address_of_DNS_server*
	The resolver did not locate a PTR resource record (containing the hostname) for the server IP address you specified. `Nslookup` can still query the DNS server, and the DNS server can still answer queries.

`*** Request to Server timed-out`	A request was not fulfilled in the allotted time. This might happen, for example, if the DNS service was not running on the DNS server that is authoritative for the name.
`*** Server can't find` *Name_or_IP_address_queried_for*`: No response from server`	The server is not receiving requests on User Datagram Protocol (UDP) port 53.
`*** Server can't find` *Name_or_IP_address_queried_for:* `Non-existent domain`	The DNS server was unable to find the name or IP address in the authoritative domain. The authoritative domain might be on the remote DNS server or on another DNS server that this DNS server is unable to reach.

`*** Server can't find` *`Name_or_IP_address_queried_for`*`: Server failed`	The DNS server is running, but it is not working properly. For example, it might include a corrupted packet, or the zone in which you are querying for a record might be paused. However, this message can also be returned if the client queries for a host in a domain for which the DNS server is not authoritative. You will also receive the error if the DNS server cannot contact its root servers, it is not connected to the Internet, or it has no root hints.

In Exercise 2.6, you'll get some hands-on practice with the `nslookup` tool. You can run this exercise from Windows 7, Windows 8, and Windows Server 2012 R2.

EXERCISE 2.6

Using the `nslookup` Command

1. Click the Start button and in the Search Programs And Files box (above the Start button), type **CMD**. Then hit Enter.
2. Type **`nslookup`** and press the Enter key. (For the rest of the exercise, use the Enter key to terminate each command.)
3. Try looking up a well-known address: Type **`www.microsoft.com`**.
4. Try looking up a nonexistent host: Type **`www.example.ccccc`**. Notice that your server indicates that it can't find the address and times out. This is normal behavior.
5. Type **`exit`** at the prompt. Type **`exit`** again to leave the command prompt.

Using *DNSLint*

Microsoft Windows Server 2012 R2 DNS can use the `DNSLint` command-line utility to help diagnose some common DNS name-resolution issues and to help diagnose potential problems of incorrect delegation. You need to download `DNSLint` from the Microsoft Download Center.

`DNSLint` uses three main functions to verify DNS records and to generate a report in HTML:

`dnslint/d` This function helps diagnose the reasons for "lame delegation" and other related DNS problems.

`dnslint/ql` This function helps verify a user-defined set of DNS records on multiple DNS servers.

`dnslint/ad` This function helps verify DNS records pertaining to Active Directory replication.

Here is the syntax for DNSLint:

```
dnslint /d domain_name | /ad [LDAP_IP_address] | /ql input_file
[/c [smtp,pop,imap]] [/no_open] [/r report_name]
[/t] [/test_tcp] [/s DNS_IP_address] [/v] [/y]
```

The following are some sample queries:

```
dnslint /d stellacon.com
dnslint /ad /s 192.168.36.201
dnslint /ql dns_server.txt
dnslint /ql autocreate
dnslint /v /d stellacon.com
dnslint /r newfile /d stellacon.com
dnslint /y /d stellacon.com
dnslint /no_open /d stellacon.com
```

Table 2.7 explains the command options.

TABLE 2.7 DNSLint command options

Command option	Meaning
/d	Domain name that is being tested.
/ad	Resolves DNS records that are used for Active Directory forest replication.
/s	TCP/IP address of host.
/ql	Requests DNS query tests from a list. This switch sends DNS queries specified in an input file.
/v	Turns on verbose mode.
/r *filename*	Allows you to create a report file.
/y	Overwrites an existing report file without being prompted.
/no_open	Prevents a report from opening automatically.

Using *Ipconfig*

You can use the command-line tool ipconfig to view your DNS client settings, to view and reset cached information used locally for resolving DNS name queries, and to register the resource records for a dynamic update client. If you use the ipconfig command with no parameters, it displays DNS information for each adapter, including the domain name and

DNS servers used for that adapter. Table 2.8 shows some command-line options available with `ipconfig`.

TABLE 2.8 Command-line options available for the `ipconfig` command

Command	What It Does
`ipconfig /all`	Displays additional information about DNS, including the FQDN and the DNS suffix search list.
`ipconfig /flushdns`	Flushes and resets the DNS resolver cache. For more information about this option, see the section "Configuring DNS" earlier in this chapter.
`ipconfig /displaydns`	Displays the contents of the DNS resolver cache. For more information about this option, see the section "Configuring DNS" earlier in this chapter.
`ipconfig /registerdns`	Refreshes all DHCP leases and registers any related DNS names. This option is available only on Windows 2000 and newer computers that run the DHCP client service.

You should know and be comfortable with the `ipconfig` commands related to DNS for the exam.

Using *DNSCmd*

`DNSCmd` allows you to display and change the properties of DNS servers, zones, and resource records through the use of command-line commands. The `DNSCmd` utility allows you to modify, create, and delete resource records and/or zones manually, and it allows you to force replication between two DNS servers.

Table 2.9 lists some of the `DNSCmd` commands and their explanations.

TABLE 2.9 `DNSCmd` command-line options

Command	Explanation
`dnscmd /clearcache`	Clears the DNS server cache
`dnscmd /config`	Resets DNS server or zone configuration
`dnscmd /createdirectorypartition`	Creates a DNS application directory partition
`dnscmd /deletedirectorypartition`	Deletes a DNS application directory partition
`dnscmd /enumrecords`	Shows the resource records in a zone

TABLE 2.9 DNSCmd command-line options *(continued)*

Command	Explanation
`dnscmd /exportsettings`	Creates a text file of all server configuration information
`dnscmd /info`	Displays server information
`dnscmd /recordadd`	Adds a resource record to a zone
`dnscmd /recorddelete`	Deletes a resource record from a zone
`dnscmd /zoneadd`	Creates a new DNS zone
`dnscmd /zonedelete`	Deletes a DNS zone
`dnscmd /zoneexport`	Creates a text file of all resource records in the zone
`dnscmd /zoneinfo`	Displays zone information
`dnscmd /zonerefresh`	Forces replication of the master zone to the secondary zone

Using the DNS Log File

You can configure the DNS server to create a log file that records the following information:

- Queries
- Notification messages from other servers
- Dynamic updates
- Content of the question section for DNS query messages
- Content of the answer section for DNS query messages
- Number of queries this server sends
- Number of queries this server has received
- Number of DNS requests received over a UDP port
- Number of DNS requests received over a TCP port
- Number of full packets sent by the server
- Number of packets written through by the server and back to the zone

The DNS log appears in `systemroot\System32\dns\Dns.log`. Because the log is in RTF format, you must use WordPad or Word to view it.

Once the log file reaches the maximum size, Windows Server 2012 R2 writes over the beginning of the file. You can change the maximum size of the log. If you increase the size value, data persists for a longer time period, but the log file consumes more disk space. If

you decrease the value, the log file uses less disk space, but the data persists for a shorter time period.

Do not leave DNS logging turned on during normal operation because it sucks up both processing and hard disk resources. Enable it only when diagnosing and solving DNS problems.

Troubleshooting the *.(root)* Zone

The *DNS root zone* is the top-level DNS zone in the DNS hierarchy. Windows Server 2012 R2-based DNS servers will build a `.(root)` zone when a connection to the Internet can't be found.

Because of this, the `.(root)` zone may prevent access to the Internet. The DNS forwarding option and DNS root hints will not be configurable. If you want your DNS to work as a DNS forwarder or you want to use root hints, you must remove the `.(root)` zone.

Issues with Non-Microsoft DNS Servers

Another troubleshooting problem that you may run into is working with both Microsoft DNS servers and non-Microsoft DNS servers. One of the most common non-Microsoft DNS servers is the Unix-based BIND DNS server.

If you need to complete a zone transfer from Microsoft DNS to a BIND DNS server, you need to enable BIND Secondaries on the Microsoft DNS server (see Figure 2.16).

FIGURE 2.16 Enabling BIND secondaries

If you need to enable Bind Secondaries, complete the following steps:

1. Open DNS management.
2. Right-click the server name and choose Properties.
3. Click the Advanced tab.
4. Check the Enable BIND Secondaries box.
5. Click OK.

Overview of DHCP

As you will see in Chapter 7, TCP/IP is the priority protocol for Windows Server 2012 R2. There are two ways to have clients and servers get TCP/IP addresses:

- You can manually assign the addresses.
- The addresses can be assigned automatically.

Manually assigning addresses is a fairly simple process. An administrator goes to each of the machines on the network and assigns TCP/IP addresses. The problem with this method arises when the network becomes midsized or larger. Think of an administrator trying to individually assign 4,000 TCP/IP addresses, subnet masks, default gateways, and all other configuration options needed to run the network.

DHCP's job is to centralize the process of IP address and option assignment. You can configure a DHCP server with a range of addresses (called a *pool*) and other configuration information and let it assign all of the IP parameters—addresses, default gateways, DNS server addresses, and so on.

DHCP is defined by a series of request for comments documents, notably 2131 and 2132.

Introducing the DORA Process

An easy way to remember how DHCP works is to learn the acronym DORA. *DORA* stands for Discover, Offer, Request, and Acknowledge. In brief, here is DHCP's DORA process:

1. *Discover*: When IP networking starts up on a DHCP-enabled client, a special message called a DHCPDISCOVER is broadcast within the local physical subnet.
2. *Offer*: Any DHCP server that hears the request checks its internal database and replies with a message called a DHCPOFFER, which contains an available IP address.

The contents of this message depend on how the DHCP server is configured—there are numerous options aside from an IP address that you can specify to pass to the client on a Windows Server DHCP server.

3. *Request*: The client receives one or more DHCPOFFERs (depending on how many DHCP servers exist on the local subnet), chooses an address from one of the offers, and sends a DHCPREQUEST message to the server to signal acceptance of the DHCPOFFER.

   This message might also request additional configuration parameters.

   Other DHCP servers that sent offers take the request message as an acknowledgment that the client didn't accept their offer.

4. *Acknowledge*: When the DHCP server receives the DHCPREQUEST, it marks the IP address as being in use (that is, usually, though it's not required). Then it sends a DHCPACK to the client.

   The acknowledgment message might contain requested configuration parameters.

   If the server is unable to accept the DHCPREQUEST for any reason, it sends a DHCPNAK message. If a client receives a DHCPNAK, it begins the configuration process over again.

5. When the client accepts the IP offer, the address is assigned to the client for a specified period of time, called a *lease*. After receiving the DHCPACK message, the client performs a final check on the parameters (sometimes it sends an ARP request for the offered IP address) and makes note of the duration of the lease. The client is now configured. If the client detects that the address is already in use, it sends a DHCPDECLINE.

If the DHCP server has given out all of the IP addresses in its pool, it won't make an offer. If no other servers make an offer, the client's IP network initialization will fail, and the client will use Automatic Private IP Addressing (APIPA).

DHCP Lease Renewal

No matter how long the lease period, the client sends a new lease request message directly to the DHCP server when the lease period is half over (give or take some randomness required by RFC 2131). This period goes by the name *T1* (not to be confused with the T1 type of network connection). If the server hears the request message and there's no reason to reject it, it sends a DHCPACK to the client. This resets the lease period.

If the DHCP server isn't available, the client realizes that the lease can't be renewed. The client continues to use the address, and once 87.5 percent of the lease period has elapsed (again, give or take some randomness), the client sends out another renewal request. This interval is known as *T2*. At that point, any DHCP server that hears the renewal can respond to this *DHCP request message* (which is a request for a lease renewal) with a DHCPACK and renew the lease. If at any time during this process the client gets a negative DHCPNACK message, it must stop using its IP address immediately and start the leasing process over from the beginning by requesting a new lease.

When a client initializes its IP networking, it always attempts to renew its old address. If the client has time left on the lease, it continues to use the lease until its end. If the client is unable to get a new lease by that time, all IP functions stop until a new, valid address can be obtained.

DHCP Lease Release

Although leases can be renewed repeatedly, at some point they might run out. Furthermore, the lease process is "at will." That is, the client or server can cancel the lease before it ends. In addition, if the client doesn't succeed in renewing the lease before it expires, the client loses its lease and reverts to APIPA. This release process is important for reclaiming extinct IP addresses used by systems that have moved or switched to a non-DHCP address.

Advantages and Disadvantages of DHCP

DHCP was designed from the start to simplify network management. It has some significant advantages, but it also has some drawbacks.

Advantages of DHCP

The following are advantages of DHCP:

- Configuration of large and even midsized networks is much simpler. If a DNS server address or some other change is necessary to the client, the administrator doesn't have to touch each device in the network physically to reconfigure it with the new settings.
- Once you enter the IP configuration information in one place—the server—it's automatically propagated to clients, eliminating the risk that a user will misconfigure some parameters and require you to fix them.
- IP addresses are conserved because DHCP assigns them only when requested.
- IP configuration becomes almost completely automatic. In most cases, you can plug in a new system (or move one) and then watch as it receives a configuration from the server. For example, when you install new network changes, such as a gateway or DNS server, the client configuration is done at only one location—the DHCP server.
- It allows a preboot execution environment (PXE) client to get a TCP/IP address from DHCP. PXE clients (also called Microsoft Windows Deployment Services [WDS] clients) can get an IP address without needing to have an operating system installed. This allows WDS clients to connect to a WDS server through the TCP/IP protocol and download an operating system remotely.

Disadvantages of DHCP

Unfortunately, there are a few drawbacks with DHCP:

- DHCP can become a single point of failure for your network. If you have only one DHCP server and it's not available, clients can't request or renew leases.

- If the DHCP server contains incorrect information, the misinformation will automatically be delivered to all of your DHCP clients.
- If you want to use DHCP on a multisegment network, you must put either a DHCP server or a relay agent on each segment, or you must ensure that your router can forward Bootstrap Protocol (BOOTP) broadcasts.

Ipconfig Lease Options

The `ipconfig` command-line tool is useful for working with network settings. Its `/renew` and `/release` switches make it particularly handy for DHCP clients. These switches allow you to request renewal of, or give up, your machine's existing address lease. You can do the same thing by toggling the Obtain An IP Address Automatically button in the Internet Protocol (TCP/IP) Properties dialog box, but the command-line option is useful especially when you're setting up a new network.

For example, I spend about a third of my time teaching MCSA or MCSE classes, usually in temporary classrooms set up at conferences, hotels, and so on. Laptops are used in these classes, with one brawny one set up as a DNS/DHCP/DC server. Occasionally, a client will lose its DHCP lease (or not get one, perhaps because a cable has come loose). The quickest way to fix it is to pop open a command-line window and type **`ipconfig/renew`**.

You can configure DHCP to assign options only to certain classes. *Classes*, defined by an administrator, are groups of computers that require identical DHCP options. The `/setclassid`*`classID`* switch of `ipconfig` is the only way to assign a machine to a class.

More specifically, the switches do the following:

`ipconfig /renew` Instructs the DHCP client to request a lease renewal. If the client already has a lease, it requests a renewal from the server that issued the current lease. This is equivalent to what happens when the client reaches the half-life of its lease. Alternatively, if the client doesn't currently have a lease, it is equivalent to what happens when you boot a DHCP client for the first time. It initiates the DHCP mating dance, listens for lease offers, and chooses one it likes.

`ipconfig /release` Forces the client to give up its lease immediately by sending the server a DHCP release notification. The server updates its status information and marks the client's old IP address as "available," leaving the client with no address bound to its network interface. When you use this command, most of the time it will be immediately followed by `ipconfig/renew`. The combination releases the existing lease and gets a new one, probably with a different address. (It's also a handy way to force your client to get a new set of settings from the server before the lease expiration time.)

`ipconfig /setclassid`*`classID`* Sets a new class ID for the client. You will see how to configure class options later in the section "Setting Scope Options for IPv4." For now, you should know that the only way to add a client machine to a class is to use this command. Note that you need to renew the client lease for the class assignment to take effect.

If you have multiple network adapters in a single machine, you can provide the name of the adapter (or adapters) upon which you want the command to work, including an

asterisk (*) as a wildcard. For example, one of my servers has two network cards: an Intel EtherExpress (ELNK1) and a generic 100Mbps card. If you want to renew DHCP settings for both adapters, you can type **`ipconfig /renew *`**. If you just want to renew the Intel EtherExpress card, you can type **`ipconfig /renew ELNK¹`**.

Understanding Scope Details

By now you should have a good grasp of what a lease is and how it works. To learn how to configure your servers to hand out those leases, however, you need to have a complete understanding of some additional topics: scopes, superscopes, exclusions, reservations, address pool, and relay agents.

Scope

Let's start with the concept of a *scope*, which is a contiguous range of addresses. There's usually one scope per physical subnet, and a scope can cover a Class A, Class B, or Class C network address or a TCP/IP v6 address. DHCP uses scopes as the basis for managing and assigning IP addressing information.

Each scope has a set of parameters, or scope options, that you can configure. *Scope options* control what data is delivered to DHCP clients when they're completing the DHCP negotiation process with a particular server. For example, the DNS server name, default gateway, and default network time server are all separate options that can be assigned. These settings are called *option types*. You can use any of the types provided with Windows Server 2012 R2, or you can specify your own.

Superscope

A *superscope* enables the DHCP server to provide addresses from more than one scope to clients on the same physical subnet. This is helpful when clients within the same subnet have more than one IP network and thus need IPs from more than one address pool. Microsoft's DHCP snap-in allows you to manage IP address assignment in the superscope, though you must still configure other scope options individually for each child scope.

Exclusions and Reservations

The scope defines what IP addresses could potentially be assigned, but you can influence the assignment process in two additional ways by specifying exclusions and reservations:

Exclusions These are IP addresses within the range that you never want automatically assigned. These excluded addresses are off-limits to DHCP. You'll typically use exclusions to tag any addresses that you never want the DHCP server to assign at all. You might use exclusions to set aside addresses that you want to assign permanently to servers that play a vital role in your organization.

Reservations These are IP addresses within the range for which you want a permanent DHCP lease. They essentially reserve a particular IP address for a particular device. The device still goes through the DHCP process (that is, its lease expires and it asks for a new one), but it always obtains the same addressing information from the DHCP server.

Exclusions are useful for addresses that you don't want to participate in DHCP at all. *Reservations* are helpful for situations in which you want a client to get the same settings each time they obtain an address.

An address cannot be simultaneously reserved and excluded. Be aware of this fact for the exam, possibly relating to a troubleshooting question.

Real World Scenario

Using Reservations and Exclusions

Deciding when to assign a reservation or exclusion can sometimes be confusing. In practice, you'll find that certain computers in the network greatly benefit by having static IP network information. Servers such as DNS servers, the DHCP server itself, SMTP servers, and other low-level infrastructure servers are good candidates for static assignment. There are usually so few of these servers that the administrator is not overburdened if a change in network settings requires going out to reconfigure each individually. Chances are that the administrator would still need to reconfigure these servers manually (by using `ipconfig /release` and then `ipconfig /renew`), even if they did not have IP addresses reserved. Even in large installations, I find it preferable to manage these vital servers by hand rather than to rely on DHCP.

Reservations are also appropriate for application servers and other special but nonvital infrastructure servers. With a reservation in DHCP, the client device will still go through the DHCP process but will always obtain the same addressing information from the DHCP server. The premise behind this strategy is that these nonvital servers can withstand a short outage if DHCP settings change or if the DHCP server fails.

Address Pool

The range of IP addresses that the DHCP server can assign is called its *address pool*. For example, let's say you set up a new DHCP scope covering the 192.168.1 subnet. That gives you 255 IP addresses in the pool. After adding an exclusion from 192.168.1.240 to 192.168.1.254, you're left with 241 (255 – 14) IP addresses in the pool. That means (in theory, at least) that you can service 241 unique clients at a time before you run out of IP addresses.

DHCP Relay Agent

By design, DHCP is intended to work only with clients and servers on a single IP network to communicate. But RFC 1542 sets out how BOOTP (on which DHCP is based) should work in circumstances in which the client and server are on different IP networks. If no DHCP server is available on the client's network, you can use a DHCP relay agent to forward DHCP broadcasts from the client's network to the DHCP server. The relay agent acts like a radio repeater, listening for DHCP client requests and retransmitting them through the router to the server.

Installing and Authorizing DHCP

Installing DHCP is easy using the Windows Server 2012/2012 R2 installation mechanism. Unlike some other services discussed in this book, the installation process installs just the service and its associated snap-in, starting it when the installation is complete. At that point, it's not delivering any DHCP service, but you don't have to reboot.

Installing DHCP

Exercise 2.7 shows you how to install DHCP Server using Server Manager. This exercise was completed on a Windows Server 2012 R2 Member Server since Active Directory is not installed yet.

EXERCISE 2.7

Installing the DHCP Service

1. Choose Server Manager by clicking the Server Manager icon on the taskbar.
2. Click Add Roles And Features.
3. Choose role-based or feature-based installation and click Next.
4. Choose your server and click Next.
5. Choose DHCP and click Next.
6. At the Features screen, click Next.
7. Click Next at the DHCP screen.
8. At the DHCP confirmation screen, click the Install button.

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-8TQ5IEL9OHR
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
< Previous
Next >
Install
Cancel

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-8TQ5IEL9OHR
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
View installation progress
Feature installation
Installation started on WIN-8TQ5IEL9OHR
DHCP Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

EXERCISE 2.7 *(continued)*

9. When the installation is complete, click the Close button.
10. On the left side, click the DHCP link.
11. Click the More link next to Configuration Required For DHCP Server.
12. Under Action, click Complete DHCP Configuration.

13. At the DHCP Description page, click Commit.
14. Click Close at the Summary screen.

15. Close Server Manager.

Introducing the DHCP Snap-In

When you install the DHCP server, the DHCP snap-in is also installed. You can open it by selecting Administrative Tools ➢ DHCP. Figure 2.17 shows the snap-in.

As you can see, the snap-in follows the standard MMC model. The left pane displays IPv4 and IPv6 sections and which servers are available; you can connect to servers other than the one to which you're already connected. A `Server Options` folder contains options that are specific to a particular DHCP server. Each server contains subordinate items grouped into folders. Each scope has a folder named after the scope's IP address range. Within each scope, four subordinate views show you interesting things about the scope, such as the following:

- The Address Pool view shows what the address pool looks like.
- The Address Leases view shows one entry for each current lease. Each lease shows the computer name to which the lease was issued, the corresponding IP address, and the current lease expiration time.

FIGURE 2.17 DHCP snap-in

- The Reservations view shows the IP addresses that are reserved and which devices hold them.
- The Scope Options view lists the set of options you've defined for this scope.

Authorizing DHCP for Active Directory

Authorization creates an Active Directory object representing the new server. It helps keep unauthorized servers off your network. Unauthorized servers can cause two kinds of problems. They may hand out bogus leases, or they may fraudulently deny renewal requests from legitimate clients.

When you install a DHCP server using Windows Server 2012/2012 R2 and Active Directory is present on your network, the server won't be allowed to provide DHCP services to clients until it has been authorized. If you install DHCP on a member server in an Active Directory domain or on a stand-alone server, you'll have to authorize the server manually. When you authorize a server, you're adding its IP address to the Active Directory object that contains the IP addresses of all authorized DHCP servers.

NOTE

You also have the ability to authorize a DHCP server during the installation of DHCP if you are installing DHCP onto an Active Directory machine.

At start time, each DHCP server queries the directory, looking for its IP address on the "authorized" list. If it can't find the list or if it can't find its IP address on the list, the DHCP service fails to start. Instead, it adds a message to the event log, indicating that it couldn't service client requests because the server wasn't authorized.

Exercise 2.8 and Exercise 2.9 show you how to authorize and unauthorize a DHCP server onto a network with Active Directory. If you installed DHCP onto a network with a domain, you can complete the following two exercises, but if you are still on a member server, you *cannot* do these exercises. These are here to show you how to do it after you have Active Directory on your network.

EXERCISE 2.8

Unauthorizing a DHCP Server

1. From Administrative Tools, choose DHCP to open the DHCP snap-in.
2. Right-click the server you want to unauthorize and choose the Unauthorize command.

3. Click Yes on the dialog box asking if you are sure you want to complete this action.

EXERCISE 2.9

Authorizing a DHCP Server

1. From Administrative Tools, choose DHCP to open the DHCP snap-in.
2. Right-click the server you want to authorize and choose the Authorize command.

3. Wait a short time (30 to 45 seconds) to allow the authorization to take place.
4. Right-click the server again. Verify that the Unauthorize command appears in the pop-up menu. This indicates that the server is now authorized.

Creating and Managing DHCP Scopes

You can use any number of DHCP servers on a single physical network if you divide the range of addresses that you want assigned into multiple scopes. Each scope contains a number of useful pieces of data, but before you can understand them, you need to know some additional terminology.

You can perform the following management tasks on DHCP scopes:

- Create a scope
- Configure scope properties
- Configure reservations and exclusions
- Set scope options

- Activate and deactivate scopes
- Create a superscope
- Create a multicast scope
- Integrate Dynamic DNS and DHCP

I will cover each task in the following sections.

Creating a New Scope in IPv4

Like many other things in Windows Server 2012 R2, a wizard drives the process of creating a new scope. You will most likely create a scope while installing DHCP, but you may need to create more than one. The overall process is simple, as long as you know beforehand what the wizard is going to ask. If you think about what defines a scope, you'll be well prepared. You need to know the following:

- The IP address range for the scope you want to create.
- Which IP addresses, if any, you want to exclude from the address pool.
- Which IP addresses, if any, you want to reserve.
- Values for the DHCP options you want to set, if any. This item isn't strictly necessary for creating a scope. However, to create a useful scope, you'll need to have some options to specify for the clients.

To create a scope, under the server name, right-click the IPv4 option in the DHCP snap-in, and use the Action ➢ New Scope command. This starts the New Scope Wizard (see Figure 2.18). You will look at each page of the wizard in the following sections.

FIGURE 2.18 Welcome page of the New Scope Wizard

Setting the Screen Name

The Scope Name page allows you to enter a name and description for your scope. These will be displayed by the DHCP snap-in.

> It's a good idea to pick sensible names for your scopes so that other administrators will be able to figure out the purpose of the scope. For example, the name DHCP is likely not very helpful, whereas a name like 1st Floor Subnet is more descriptive and can help in troubleshooting.

Defining the IP Address Range

The IP Address Range page (see Figure 2.19) is where you enter the start and end IP addresses for your range. The wizard does minimal checking on the addresses you enter, and it automatically calculates the appropriate subnet mask for the range. You can modify the subnet mask if you know what you're doing.

FIGURE 2.19 IP Address Range page of the New Scope Wizard

Adding Exclusions and Delay

The Add Exclusions And Delay page (see Figure 2.20) allows you to create exclusion ranges. Exclusions are TCP/IP numbers that are in the pool, but they do not get issued to clients. To exclude one address, put it in the Start IP Address field. To exclude a range, also fill in the End IP Address field. The delay setting is a time duration by which the server will delay the transmission of a DHCPOFFER message.

> Although you can always add exclusions later, it's best to include them when you create the scope so that no excluded addresses are ever passed out to clients.

FIGURE 2.20 Add Exclusions And Delay page of the New Scope Wizard

Setting a Lease Duration

The Lease Duration page (see Figure 2.21) allows you to set how long a device gets to use an assigned IP address before it has to renew its lease. The default lease duration is eight days. You may find that a shorter or longer duration makes sense for your network. If your network is highly dynamic, with lots of arrivals, departures, and moving computers, set a shorter lease duration; if it's less active, make it longer.

FIGURE 2.21 Lease Duration page of the New Scope Wizard

Remember that renewal attempts begin when approximately half of the lease period is over (give or take a random interval), so don't set them too short.

Configuring Basic DHCP Options

The Configure DHCP Options page (see Figure 2.22) allows you to choose whether you want to set up basic DHCP options such as default gateway and DNS settings. The options are described in the following sections. If you choose not to configure options, you can always do so later. However, you should not activate the scope until you've configured the options you want assigned.

FIGURE 2.22 Configure DHCP Options page of the New Scope Wizard

Configuring a Router

The first option configuration page is the Router (Default Gateway) page (see Figure 2.23), in which you enter the IP addresses of one or more routers (more commonly referred to as *default gateways*) that you want to use for outbound traffic. After entering the IP addresses of the routers, use the Up and Down buttons to order the addresses. Clients will use the routers in the order specified when attempting to send outgoing packets.

Providing DNS Settings

On the Domain Name And DNS Servers page (see Figure 2.24), you specify the set of DNS servers and the parent domain you want passed down to DHCP clients. Normally, you'll want to specify at least one DNS server by filling in its DNS name or IP address. You can also specify the domain suffix that you want clients to use as the base domain for all connections that aren't fully qualified. For example, if your clients are used to navigating based on server name alone rather than the fully qualified domain name (FQDN) of `server.willpanek.com`, then you'll want to place your domain here.

FIGURE 2.23 Router (Default Gateway) page of the New Scope Wizard

FIGURE 2.24 Domain Name And DNS Servers page of the New Scope Wizard

Providing WINS Settings

If you're still using Windows Internet Name Service (WINS) on your network, you can configure DHCP so that it passes WINS server addresses to your Windows clients. (If you want the Windows clients to honor it, you'll also need to define the WINS/NBT Node Type option for the scope.) As on the DNS server page, on the WINS Servers page (see Figure 2.25) you can enter the addresses of several servers and move them into the order in which you want clients to try them. You can enter the DNS or NetBIOS name of each server, or you can enter an IP address.

FIGURE 2.25 WINS Servers page of the New Scope Wizard

Here are some of the more common options you can set on a DHCP server:

003 Router Used to provide a list of available routers or default gateways on the same subnet.

006 DNS Servers Used to provide a list of DNS servers.

015 DNS Domain Name Used to provide the DNS suffix.

028 Broadcast Address Used to configure the broadcast address, if different than the default, based on the subnet mask.

44 WINS/NBNS Servers Used to configure the IP addresses of WINS servers.

46 WINS/NBT Node Type Used to configure the preferred NetBIOS name resolution method. There are four settings for node type:

B node (0x1) Broadcast for NetBIOS resolution

P node (0x2) Peer-to-peer (WINS) server for NetBIOS resolution

M node (0x4) Mixed node (does a B node and then a P node)

H node (0x8) Hybrid node (does a P node and then a B node)

051 Lease Used to configure a special lease duration.

Activating the Scope

The Activate Scope page (see Figure 2.26) gives you the option to activate the scope immediately after creating it. By default, the wizard assumes that you want the scope activated unless you select the No, I Will Activate This Scope Later radio button, in which case the scope will remain dormant until you activate it manually.

FIGURE 2.26 Activate Scope page of the New Scope Wizard

Be sure to verify that there are no other DHCP servers assigned to the address range you choose!

In Exercise 2.10, you will create a new scope for the 192.168.0.xprivate Class C network. First you need to complete Exercise 2.7 before beginning this exercise.

EXERCISE 2.10

Creating a New Scope

1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Right-click the IPv4 folder and choose New Scope. The New Scope Wizard appears.
3. Click the Next button on the welcome page.
4. Enter a name and a description for your new scope and click the Next button.
5. On the IP Address Range page, enter **192.168.0.2** as the start IP address for the scope and **192.168.0.250** as the end IP address. Leave the subnet mask controls alone (though when creating a scope on a production network, you might need to change them). Click the Next button.
6. On the Add Exclusions And Delay page, click Next without adding any excluded addresses or delays.
7. On the Lease Duration page, set the lease duration to 3 days and click the Next button.
8. On the Configure DHCP Options page, click the Next button to indicate you want to configure default options for this scope.

EXERCISE 2.10 *(continued)*

9. On the Router (Default Gateway) page, enter **192.168.0.1** for the router IP address and then click the Add button. Once the address is added, click the Next button.
10. On the Domain Name And DNS Servers page, enter the IP address of a DNS server on your network in the IP Address field (for example, you might enter **192.168.0.251**) and click the Add button. Click the Next button.
11. On the WINS Servers page, click the Next button to leave the WINS options unset.
12. On the Activate Scope page, if your network is currently using the 192.168.0.*x* range, select Yes, I Want To Activate This Scope Now. Click the Next button.
13. When the wizard's summary page appears, click the Finish button to create the scope.

Creating a New Scope in IPv6

Now that you have seen how to create a new scope in IPv4, I'll go through the steps to create a new scope in IPv6.

To create a scope, right-click the IPv6 option in the DHCP snap-in under the server name and select the Action ➢ New Scope command. This starts the New Scope Wizard. Just as with creating a scope in IPv4, the welcome page of the wizard tells you that you've launched the New Scope Wizard. You will look at each page of the wizard in the following sections.

Setting the Screen Name

The Scope Name page (see Figure 2.27) allows you to enter a name and description for your scope. These will be displayed by the DHCP snap-in.

FIGURE 2.27 IPv6 Scope Name page of the New Scope Wizard

It's a good idea to pick a sensible name for your scopes so that other administrators will be able to figure out what the scope is used for.

Scope Prefix

The Scope Prefix page (see Figure 2.28) gets you started creating the IPv6 scope. IPv6 has three types of addresses, which can be categorized by type and scope.

FIGURE 2.28 Scope Prefix page of the New Scope Wizard

Unicast Addresses *One-to-one*. A packet from one host is delivered to another host. The following are some examples of IPv6 unicast:

- The unicast prefix for site-local addresses is FEC0::/48.
- The unicast prefix for link-local addresses is FE80::/64.

The 6to4 address allows communication between two hosts running both IPv4 and IPv6. The way to calculate the 6to4 address is by combining the global prefix 2002::/16 with the 32 bits of a public IPv4 address of the host. This gives you a 48-bit prefix. 6to4 is described in RFC 3056.

Multicast addresses *One-to-many*. A packet from one host is delivered to multiple hosts (but not everyone). The prefix for multicast addresses is FF00::/8.

Anycast addresses A packet from one host is delivered to the nearest of multiple hosts (in terms of routing distance).

Adding Exclusions

As with the IPv4 New Scope Wizard, the Add Exclusions page (see Figure 2.29) allows you to create exclusion ranges. *Exclusions* are TCP/IP numbers that are in the pool but do not get issued to clients. To exclude one address, put it in the Start IPv6 Address field. To exclude a range, also fill in the End IPv6 Address field.

FIGURE 2.29 Add Exclusions page of the New Scope Wizard

Setting a Lease Duration

The Scope Lease page (see Figure 2.30) allows you to set how long a device gets to use an assigned IP address before it has to renew its lease. You can set two different lease durations. The section labeled Non Temporary Address (IANA) is the lease time for your more permanent hosts (such as printers and server towers). The one labeled Temporary Address (IATA) is for hosts that might disconnect at any time, such as laptops.

Activating the Scope

The Completing The New Scope Wizard page (see Figure 2.31) gives you the option to activate the scope immediately after creating it. By default, the wizard will assume you want the scope activated. If you want to wait to activate the scope, choose No in the Activate Scope Now box.

Changing Scope Properties (IPv4 and IPv6)

Each scope has a set of properties associated with it. Except for the set of options assigned by the scope, you can find these properties on the General tab of the scope's Properties

FIGURE 2.30 Scope Lease page of the New Scope Wizard

FIGURE 2.31 Completing The New Scope Wizard page of the New Scope Wizard

dialog box (see Figure 2.32). Some of these properties, such as the scope name and description, are self-explanatory. Others require a little more explanation.

FIGURE 2.32 General tab of the scope's Properties dialog box for an IPv4 scope

- The Start IP Address and End IP Address fields allow you to set the range of the scope.
- For IPv4 scopes, the settings in the section Lease Duration For DHCP Clients control how long leases in this scope are valid.

  The IPv6 scope dialog box includes a Lease tab where you set the lease properties.

When you make changes to these properties, they have no effect on existing leases. For example, say you create a scope from 172.30.1.1 to 172.30.1.199. You use that scope for a while and then edit its properties to reduce the range from 172.30.1.1 to 172.30.1.150. If a client has been assigned the address 172.30.1.180, which was part of the scope before you changed it, the client will retain that address until the lease expires but will not be able to renew it.

Changing Server Properties

Just as each scope has its own set of properties, so too does the server itself. You access the server properties by right-clicking the IPv4 or IPv6 object within the DHCP management console and selecting Properties.

IPv4 Server Properties

Figure 2.33 shows the IPv4 Properties dialog box.

FIGURE 2.33 General tab of the IPv4 Properties dialog box for the server

The IPv4 Properties dialog box has four tabs: General, DNS, Network Access Protection, and Advanced.

The Advanced tab, shown in Figure 2.34, contains the following configuration parameters:

- Audit Log File Path is where you enter the location for log files.
- Conflict Detection Attempts specifies how many ICMP echo requests (pings) the server sends for an address it is about to offer. The default is 0. Conflict detection is a way to verify that the DHCP server is not issuing IP addresses that are already being used on the network.

The Network Access Protection tab (see Figure 2.35) allows you to set up *Network Access Protection (NAP)*. With NAP, which is a Windows Server 2012 R2 service, an administrator can perform the following tasks:

- Carry out computer health policy validation
- Ensure ongoing compliance with health policies
- Optionally restrict the access of computers that do not meet the computer health requirements

FIGURE 2.34 The Advanced tab of the IPv4 Properties dialog box for the server

FIGURE 2.35 The Network Access Protection tab of the IPv4 Properties dialog box for the server

IPv6 Server Properties

The IPv6 Properties dialog box for the server has two tabs: General and Advanced. On the General tab (see Figure 2.36), you can configure the following settings:

- Frequency with which statistics are updated
- DHCP auditing

FIGURE 2.36 Server's IPv6 Properties, General tab

The Advanced tab (see Figure 2.37) allows you to configure the following settings:

- Database path for the audit log file path.
- Connection bindings.
- Registration credentials for dynamic DNS. The registration credential is the user account that DHCP will use to register clients with Active Directory.

Managing Reservations and Exclusions

After defining the address pool for your scope, the next step is to create reservations and exclusions, which reduce the size of the pool. In the following sections, you will learn how to add and remove exclusions and reservations.

FIGURE 2.37 Server's IPv6 Properties, Advanced tab

Adding and Removing Exclusions

When you want to exclude an entire range of IP addresses, you need to add that range as an exclusion. Ordinarily, you'll want to do this before you enable a scope because that prevents any of the IP addresses you want excluded from being leased before you have a chance to exclude them. In fact, you can't create an exclusion that includes a leased address—you have to get rid of the lease first.

Adding an Exclusion Range

Here's how to add an exclusion range:

1. Open the DHCP snap-in and find the scope to which you want to add an exclusion (either IPv4 or IPv6).
2. Expand the scope so that you can see its Address Pool item for IPv4 or the Exclusion section for IPv6.
3. Right-click the Address Pool or Exclusion section and choose the New Exclusion Range command.
4. When the Add Exclusion dialog box appears (see Figure 2.38), enter the IP addresses you want to exclude. To exclude a single address, type it in the Start IP Address field. To exclude a range of addresses, also fill in the End IP Address field.
5. Click the Add button to add the exclusion.

When you add exclusions, they appear in the Address Pool node, which is under the Scope section for IPv4 and under the Exclusion section of IPv6.

FIGURE 2.38 Add Exclusion dialog boxes for IPv4 and IPv6

IPv4 Add Exclusion dialog box

IPv6 Add Exclusion dialog box

Removing an Exclusion Range

To remove an exclusion, just right-click it and choose the Delete command. After confirming your command, the snap-in removes the excluded range and the addresses become immediately available for issuance.

Adding and Removing Reservations

Adding a reservation is simple as long as you have the MAC address of the device for which you want to create a reservation. Because reservations belong to a single scope, you create and remove them within the Reservations node beneath each scope.

Adding a Reservation

To add a reservation, perform the following tasks:

1. Right-click the scope and select New Reservation.

   This displays the New Reservation dialog box, shown in Figure 2.39.

FIGURE 2.39 New Reservation dialog boxes for IPv4 and IPv6

IPv4 New Reservation dialog box

IPv6 New Reservation dialog box

2. Enter the IP address and MAC address or ID for the reservation.

To find the MAC address of the local computer, use the `ipconfig` command. To find the MAC address of a remote machine, use the `nbtstat-a`*`computername`* command.

3. If you want, you can also enter a name and description.
4. For IPv4, in the Supported Types section, choose whether the reservation will be made by DHCP only, BOOTP only (useful for remote-access devices), or both.

Removing a Reservation

To remove a reservation, right-click it and select Delete. This removes the reservation but does nothing to the client device.

There's no way to change a reservation once it has been created. If you want to change any of the associated settings, you'll have to delete and re-create the reservation.

Setting Scope Options for IPv4

Once you've installed a server, authorized it in Active Directory, and fixed up the address pool, the next step is to set scope options that you want sent out to clients, such as router (that is, default gateway) and DNS server addresses. You must configure the options you want sent out before you activate a scope. If you don't, clients may register in the scope without getting any options, rendering them virtually useless. Thus, configure the scope options, along with the IP address and subnet mask that you configured earlier in this chapter.

In the following sections, you will learn how to configure and assign scope options on the DHCP server.

Understanding Option Assignment

You can control which DHCP options are doled out to clients in five (slightly overlapping) ways:

Predefined Options *Predefined options* are templates that are available in the Server, Scope, or Client Options dialog box.

Server Options *Server options* are assigned to all scopes and clients of a particular server. That means if there's some setting you want all clients of a DHCP server to have, no matter what scope they're in, this is where you assign it. Specific options (those that are set at the class, scope, or client level) will override server-level options. That gives you an escape

valve; it's a better idea, though, to be careful about which options you assign if your server manages multiple scopes.

Scope Options If you want a particular option value assigned only to those clients in a certain subnet, you should assign it as a *scope option*. For example, it's common to specify different routers for different physical subnets; if you have two scopes corresponding to different subnets, each scope would probably have a separate value for the router option.

Class Options You can assign different options to clients of different types, that is, *class options*. For example, Windows 2000, XP, Vista, Windows 7, Windows 8, Server 2003, Server 2003 R2, Server 2008, Server 2008 R2, and Server 2012/2012 R2 machines recognize a number of DHCP options that Windows 98, Windows NT, and Mac OS machines ignore, and vice versa. By defining a Windows 2000 or newer class (using the `ipconfig /setclassid` command you saw earlier), you could assign those options only to machines that report themselves as being in that class.

Client Options If a client is using DHCP reservations, you can assign certain options to that specific client. You attach *client options* to a particular reservation. Client options override scope, server, and class options. The only way to override a client option is to configure the client manually. The DHCP server manages client options.

Client options override class options, class options override scope options, and scope options override server options.

Assigning Options

You can use the DHCP snap-in to assign options at the scope, server, reserved address, or class level. The mechanism you use to assign these options is the same for each; the only difference is where you set the options.

When you create an option assignment, remember that it applies to all of the clients in the server or the scope from that point forward. Option assignments aren't retroactive, and they don't migrate from one scope to another.

Creating and Assigning a New Option

To create a new option and have it assigned, follow these steps:

1. Select the scope or server where you want the option assigned.
2. Select the corresponding Options node and choose Action ➢ Configure Options.

   To set options for a reserved client, right-click its entry in the Reservations node and select Configure Options.

   Then you'll see the Scope Options dialog box (see Figure 2.40), which lists all of the options that you might want to configure.
3. To select an individual option, check the box next to it and then use the controls in the Data Entry control group to enter the value you want associated with the option.

FIGURE 2.40 The Scope Options dialog box

4. Continue to add options until you've specified all of the ones you want attached to the server or scope. Then click OK.

Configuring the DHCP Server for Classes

You saw how to assign classes to individual machines earlier in the chapter. Now you will learn how to configure the DHCP server to recognize your customized classes and configure options for them. In Exercise 2.11, you will create a new user class and configure options for the new class. Before you begin, make sure that the computers you want to use in the class have been configured with the `ipconfig /setclassid` command, as described in the section "`Ipconfig` Lease Options" earlier in this chapter.

EXERCISE 2.11

Configuring User Class Options

1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Right-click the IPv4 item and select Define User Classes.
3. Click the Add button in the DHCP User Classes dialog box.
4. In the New Class dialog box, enter a descriptive name for the class in the Display Name field. Enter a class ID in the ID field. (Typically, you will enter the class ID in the ASCII portion of the ID field.) When you have finished, click OK.
5. The new class appears in the DHCP User Classes dialog box. Click the Close button to return to the DHCP snap-in.

6. Right-click the Scope Options node and select Configure Options.
7. Click the Advanced tab. Select the class you defined in step 4 from the User Class pop-up menu.
8. Configure the options you want to set for the class. Click OK when you have finished. Notice that the options you configured (and the class with which they are associated) appear in the right pane of the DHCP window.

About the Default Routing and Remote Access Predefined User Class

Windows Server 2012/2012 R2 includes a predefined user class called the *Default Routing and Remote Access class*. This class includes options important to clients connecting to Routing and Remote Access, notably the 051 Lease option.

Be sure to know that the 051 Lease option is included within this class and that it can be used to assign a shorter lease duration for clients connecting to Routing and Remote Access.

Activating and Deactivating Scopes

When you've completed the steps in Exercise 2.5 and you're ready to unleash your new scope so that it can be used to make client assignments, the final required step is activating the scope. When you activate a scope, you're just telling the server that it's OK to start handing out addresses from that scope's address pool. As soon as you activate a scope, addresses from its pool may be assigned to clients. Of course, this is a necessary precondition to getting any use out of your scope.

If you later want to stop using a scope, you can, but be aware that it's a permanent change. When you deactivate a scope, DHCP tells all clients registered with the scope that they need to release their leases immediately and renew them someplace else—the equivalent of a landlord who evicts tenants when the building is condemned!

Don't deactivate a scope unless you want clients to stop using it immediately.

Creating a Superscope for IPv4

A *superscope* allows the DHCP server to provide multiple logical subnet addresses to DHCP clients on a single physical network. You create superscopes with the New Superscope command, which triggers the New Superscope Wizard.

You can have only one superscope per server.

The steps in Exercise 2.12 take you through the process of creating a superscope.

EXERCISE 2.12

Creating a Superscope

1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Follow the instructions in Exercise 2.10 to create two scopes: one for 192.168.0.2 through 192.168.0.127 and one for 192.168.1.12 through 192.168.1.127.
3. Right-click IPv4 and choose the New Superscope command. The New Superscope Wizard appears. Click the Next button.
4. On the Superscope Name page, name your superscope and click the Next button.
5. The Select Scopes page appears, listing all scopes on the current server. Select the two scopes you created in step 2 and then click the Next button.
6. The wizard's summary page appears. Click the Finish button to create your scope.
7. Verify that your new superscope appears in the DHCP snap-in.

Deleting a Superscope

You can delete a superscope by right-clicking it and choosing the Delete command. A superscope is just an administrative convenience, so you can safely delete one at any time—it doesn't affect the "real" scopes that make up the superscope.

Adding a Scope to a Superscope

To add a scope to an existing superscope, find the scope you want to add, right-click it, and choose Action ➢ Add To Superscope. A dialog box appears, listing all of the superscopes known to this server. Pick the one to which you want the current scope appended and click the OK button.

Removing a Scope from a Superscope

To remove a scope from a superscope, open the superscope and right-click the target scope. The pop-up menu provides a Remove From Superscope command that will do the deed.

Activating and Deactivating Superscopes

Just as with regular scopes, you can activate and deactivate superscopes. The same restrictions and guidelines apply. You must activate a superscope before it can be used, and

you must not deactivate it until you want all of your clients to lose their existing leases and be forced to request new ones.

To activate or deactivate a superscope, right-click the superscope name, and select Activate or Deactivate, respectively, from the pop-up menu.

Creating IPv4 Multicast Scopes

Multicasting occurs when one machine communicates to a network of subscribed computers rather than specifically addressing each computer on the destination network. It's much more efficient to multicast a video or audio stream to multiple destinations than it is to unicast it to the same number of clients, and the increased demand for multicast-friendly network hardware has resulted in some head scratching about how to automate the multicast configuration.

In the following sections, you will learn about MADCAP, the protocol that controls multicasting, and about how to build and configure a multicast scope.

Understanding the Multicast Address Dynamic Client Allocation Protocol

DHCP is usually used to assign IP configuration information for *unicast* (or one-to-one) network communications. With multicast, there's a separate type of address space assigned from 224.0.0.0 through 239.255.255.255. Addresses in this space are known as *Class D addresses*, or simply *multicast addresses*. Clients can participate in a multicast just by knowing (and using) the multicast address for the content they want to receive. However, multicast clients also need to have an ordinary IP address.

How do clients know what address to use? Ordinary DHCP won't help because it's designed to assign IP addresses and option information to one client at a time. Realizing this, the Internet Engineering Task Force (IETF) defined a new protocol: *Multicast Address Dynamic Client Allocation Protocol (MADCAP)*. MADCAP provides an analog to DHCP but for multicast use. A MADCAP server issues leases for multicast addresses only. MADCAP clients can request a multicast lease when they want to participate in a multicast.

DHCP and MADCAP have some important differences. First you have to realize that the two are totally separate. A single server can be a DHCP server, a MADCAP server, or both; no implied or actual relation exists between the two. Likewise, clients can use DHCP and/or MADCAP at the same time—the only requirement is that every MADCAP client has to get a unicast IP address from somewhere.

Remember that DHCP can assign options as part of the lease process but MADCAP cannot. The only thing MADCAP does is dynamically assign multicast addresses.

Building Multicast Scopes

Most of the steps you go through when creating a multicast scope are identical to those required for an ordinary unicast scope. Exercise 2.13 highlights the differences.

EXERCISE 2.13

Creating a New Multicast Scope

1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Right-click IPv4 and choose New Multicast Scope. The New Multicast Scope Wizard appears. Click the Next button on the welcome page.
3. In the Multicast Scope Name page, name your multicast scope (and add a description if you'd like). Click the Next button.
4. The IP Address Range page appears. Enter a start IP address of **224.0.0.0** and an end IP address of **224.255.0.0**. Adjust the TTL to 1 to make sure that no multicast packets escape your local network segment. Click the Next button when you're finished.
5. The Add Exclusions page appears; click its Next button.
6. The Lease Duration page appears. Since multicast addresses are used for video and audio, you'd ordinarily leave multicast scope assignments in place somewhat longer than you would with a regular unicast scope, so the default lease length is 30 days (instead of 8 days for a unicast scope). Click the Next button.
7. The wizard asks you if you want to activate the scope now. Click the No radio button and then the Next button.
8. The wizard's summary page appears; click the Finish button to create your scope.
9. Verify that your new multicast scope appears in the DHCP snap-in.

Setting Multicast Scope Properties

Once you create a multicast scope, you can adjust its properties by right-clicking the scope name and selecting Properties.

The Multicast Scope Properties dialog box has two tabs. The General tab (see Figure 2.41) allows you to change the scope's name, its start and end addresses, its Time To Live (TTL) value, its lease duration, and its description—in essence, all of the settings you provided when you created it in the first place.

The Lifetime tab (see Figure 2.42) allows you to limit how long your multicast scope will be active. By default, a newly created multicast scope will live forever, but if you're creating a scope to provide MADCAP assignments for a single event (or a set of events of limited duration), you can specify an expiration time for the scope. When that time is reached, the scope disappears from the server but not before making all of its clients give up their multicast address leases. This is a nice way to make sure that the lease cleans up after itself when you're finished with it.

FIGURE 2.41 General tab of the Multicast Scope Properties dialog box

FIGURE 2.42 Lifetime tab of the Multicast Scope Properties dialog box

Integrating Dynamic DNS and IPv4 DHCP

DHCP integration with Dynamic DNS is a simple concept but powerful in action. By setting up this integration, you can pass addresses to DHCP clients while still maintaining the integrity of your DNS services.

The DNS server can be updated in two ways. One way is for the DHCP client to tell the DNS server its address. Another way is for the DHCP server to tell the DNS server when it registers a new client.

Neither of these updates will take place, however, unless you configure the DNS server to use Dynamic DNS. You can make this change in two ways:

- If you change it at the scope level, it will apply only to the scope.
- If you change it at the server level, it will apply to all scopes and superscopes served by the server.

Which of these options you choose depends on how widely you want to support Dynamic DNS; most of the sites I visit have enabled DNS updates at the server level.

To update the settings at either the server or scope level, you need to open the scope or server properties by right-clicking the appropriate object and choosing Properties. The DNS tab of the Properties dialog box (see Figure 2.43) includes the following options:

Enable DNS Dynamic Updates According To The Settings Below This check box controls whether this DHCP server will attempt to register lease information with a DNS server. It must be checked to enable Dynamic DNS.

Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients This radio button (which is on by default) tells the DHCP server to register the update only if the DHCP client asks for DNS registration. When this button is active, DHCP clients that aren't hip to DDNS won't have their DNS records updated. However, Windows 2000, XP, Vista, Windows 7, Windows 8, Server 2003/2003 R2, Server 2008/2008 R2, and Server 2012/2012 R2 DHCP clients are smart enough to ask for the updates.

Always Dynamically Update DNS A And PTR Records This radio button forces the DHCP server to register any client to which it issues a lease. This setting may add DNS registrations for DHCP-enabled devices that don't really need them, such as print servers. However, it allows other clients (such as Mac OS, Windows NT, and Linux machines) to have their DNS information automatically updated.

Discard A And PTR Records When Lease Is Deleted This check box has a long name but a simple function. When a DHCP lease expires, what should happen to the DNS registration? Obviously, it would be nice if the DNS record associated with a lease vanished when the lease expired. When this check box is checked (as it is by default), that's exactly what happens. If you uncheck this box, your DNS will contain entries for expired leases that are no longer valid. When a particular IP address is reissued on a new lease, the DNS will be updated, but in between leases you'll have incorrect data in your DNS—something that's always best to avoid.

Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates This check box lets you handle these older clients graciously by making the updates using a separate mechanism.

In Exercise 2.14, you will enable a scope to participate in Dynamic DNS updates.

FIGURE 2.43 DNS tab of the scope's IPv4 Properties dialog box

EXERCISE 2.14

Enabling DHCP-DNS Integration

1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Right-click the IPv4 item and select Properties.
3. The Server Properties dialog box appears. Click the DNS tab.
4. Verify that the check box labeled Enable DNS Dynamic Updates According To The Settings Below is checked and verify that the radio button labeled Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients is selected.
5. Verify that the check box labeled Discard A And PTR Records When Lease Is Deleted is checked. If not, then check it.
6. Click the OK button to apply your changes and close the Server Properties dialog box.

Using Multiple DHCP Servers

DHCP can become a single point of failure within a network if there is only one DHCP server. If that server becomes unavailable, clients will not be able to obtain new leases or renew existing leases. For this reason, it is recommended that you have more than one DHCP server in the network. However, more than one DHCP server can create problems if they both are configured to use the same scope or set of addresses. Microsoft recommends the 80/20 rule for redundancy of DHCP services in a network.

Implementing the 80/20 rule calls for one DHCP server to make approximately 80 percent of the addresses for a given subnet available through DHCP while another server makes the remaining 20 percent of the addresses available. For example, with a /24 network of 254 addresses, say 192.168.1.1 to 192.168.1.254, you might have Server 1 offer 192.168.1.10 to 192.168.1.210 while Server 2 offers 192.168.1.211 to 192.168.254.

DHCP Load Sharing

Load sharing is the normal default way that you use multiple DHCP servers (as explained earlier). Both servers cover the same subnets (remember that a DHCP server can handle multiple subnets at the same time) simultaneously, and both servers assign IP addresses and options to clients on the assigned subnets. The client requests are load balanced and shared between the two servers.

This is a good option for a company that has multiple DHCP servers in the same physical location. The DHCP servers are set up in a failover relationship at the same site, and both servers respond to all DHCP client requests from the subnets to which they are associated. The DHCP server administrator can set the load distribution ratio between the multiple DHCP servers.

DHCP Hot Standby

When thinking of a DHCP hot standby setup, think of the old server failover cluster. You have two servers where one server does all of the work and the other server is a standby server in the event that the first server crashes or goes down.

In a DHCP hot standby situation, the two DHCP servers operate in a failover relationship where one server acts as an active server and is responsible for leasing IP addresses to all clients in a scope or subnet. The secondary DHCP server assumes the standby role, and it is ready to go in the event that the primary DHCP server becomes unavailable. If the primary server becomes unavailable, the secondary DHCP server is given the role of the primary DHCP server and takes over all the responsibilities of the primary DHCP server.

This failover situation is best suited to DHCP deployments where a company has DHCP servers in multiple locations.

To learn more about DHCP failover situations, please visit Microsoft at `http://technet.microsoft.com/en-us/library/hh831385.aspx`. Microsoft has been known for taking questions right off its websites, and this website is the perfect solution for doing this.

Working with the DHCP Database Files

DHCP uses a set of database files to maintain its knowledge of scopes, superscopes, and client leases. These files, which live in the *systemroot*`\System32\DHCP` folder, are always

open when the DHCP service is running. DHCP servers use Joint Engine Technology (JET) databases to maintain their records.

You shouldn't modify or alter the DHCP database files when the service is running.

The primary database file is `dhcp.mdb`—it has all of the scope data in it.

The following files are also part of the DHCP database:

`Dhcp.tmp` This is a backup copy of the database file created during reindexing of the database. You normally won't see this file, but if the service fails during reindexing, it may not remove the file when it should.

`J50.log` This file (plus a number of files named `J50`*xxxxx*`.log`, where *xxxxx* stands for 00001, 00002, 00003, and so on) is a log file that stores changes before they're written to the database. The DHCP database engine can recover some changes from these files when it restarts.

`J50.chk` This is a checkpoint file that tells the DHCP engine which log files it still needs to recover.

In the following sections, you will see how to manipulate the DHCP database files.

Removing the Database Files

If you're convinced that your database is corrupt because the lease information that you see doesn't match what's on the network, the easiest repair mechanism is to remove the database files and start over with an empty database.

If you think the database is corrupt because the DHCP service fails at startup, you should check the event log.

To start over, follow these steps:

1. Stop the DHCP service by typing **`net stop dhcpserver`** at the command prompt.
2. Remove all of the files from the *`systemroot`*`\system32\DHCP` folder.
3. Restart the service (at command prompt type **`net start dhcpserver`**).
4. Reconcile the scope.

Changing the Database Backup Interval

By default, the DHCP service backs up its databases every 60 minutes. You can adjust this setting by editing the Backup Interval value under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters`. This allows you to make backups either more frequently (if your database changes a lot or if you seem to have ongoing corruption problems) or less often (if everything seems to be on an even keel).

Moving the DHCP Database Files

You may find that you need to dismantle or change the role of your DHCP server and offload the DHCP functions to another computer. Rather than spend the time re-creating the DHCP database on the new machine by hand, you can copy the database files and use them directly. This is especially helpful if you have a complicated DHCP database with lots of reservations and option assignments.

By copying the files, you also minimize the amount of human error that could be introduced by reentering the information by hand.

Compacting the DHCP Database Files

There may be a time when you need to compact the DHCP database. Microsoft has a utility called `jetpack.exe` that allows you to compact the JET database. Microsoft JET databases are used for WINS and DHCP databases. If you wanted to use the `jetpack` command, the proper syntax is

```
JETPACK.EXE <database name><temp database name>
```

After you compact the database, you rename the temp database to `dhcp.mdb`.

Summary

DNS was designed to be a robust, scalable, and high-performance system for resolving friendly names to TCP/IP host addresses. This chapter presented an overview of the basics of DNS and how DNS names are generated. We then looked at the many new features available in the Microsoft Windows Server 2012 R2 version of DNS, and we focused on how to install, configure, and manage the necessary services. Microsoft's DNS is based on a widely accepted set of industry standards. Because of this, Microsoft's DNS can work with both Windows- and non-Windows-based networks.

This chapter also covered the DHCP lease process as it relates to TCP/IP configuration information for clients. The following stages were covered: IP discovery, IP lease offer, IP lease selection, and IP lease acknowledgment. You learned how to install and configure the DHCP server on Windows Server 2012 R2 and how to create and manage DHCP scopes and scope options. I also discussed the authorization of DHCP servers within Active Directory and scopes for IPv4 and IPv6 and showed how to create them. Finally, I covered superscopes as well as managing client leases with the options therein.

Exam Essentials

Understand the purpose of DNS. DNS is a standard set of protocols that defines a mechanism for querying and updating address information in the database, a mechanism for replicating the information in the database among servers, and a schema of the database.

Understand the different parts of the DNS database. The SOA record defines the general parameters for the DNS zone, including who is the authoritative server. NS records list the name servers for a domain; they allow other name servers to look up names in your domain. A host record (also called an address record or an A record) statically associates a host's name with its IP addresses. Pointer records (PTRs) map an IP address to a hostname, making it possible to do reverse lookups. Alias records allow you to use more than one name to point to a single host. The MX record tells you which servers can accept mail bound for a domain. SRV records tie together the location of a service (like a domain controller) with information about how to contact the service.

Know how DNS resolves names. With iterative queries, a client asks the DNS server for an answer, and the client, or resolver, returns the best kind of answer it has available. In a recursive query, the client sends a query to one name server, asking it to respond either with the requested answer or with an error. The error states either that the server can't come up with the right answer or that the domain name doesn't exist. With inverse queries, instead of supplying a name and then asking for an IP address, the client first provides the IP address and then asks for the name.

Understand the differences among DNS servers, clients, and resolvers. Any computer providing domain name services is a DNS server. A DNS client is any machine issuing queries to a DNS server. A resolver handles the process of mapping a symbolic name to an actual network address.

Know how to install and configure DNS. DNS can be installed before, during, or after installing the Active Directory service. When you install the DNS server, the DNS snap-in is installed too. Configuring a DNS server ranges from easy to difficult, depending on what you're trying to make it do. In the simplest configuration, for a caching-only server, you don't have to do anything except to make sure the server's root hints are set correctly. You can also configure a root server, a normal forward lookup server, and a reverse lookup server.

Know how to create new forward and reverse lookup zones. You can use the New Zone Wizard to create a new forward or reverse lookup zone. The process is basically the same for both types, but the specific steps and wizard pages differ somewhat. The wizard walks you through the steps, such as specifying a name for the zone (in the case of forward lookup zones) or the network ID portion of the network that the zone covers (in the case of reverse lookup zones).

Know how to configure zones for dynamic updates. The DNS service allows dynamic updates to be enabled or disabled on a per-zone basis at each server. This is easily done in the DNS snap-in.

Know how to delegate zones for DNS. DNS provides the ability to divide the namespace into one or more zones; these can then be stored, distributed, and replicated to other DNS servers. When delegating zones within your namespace, be aware that for each new zone you create, you need delegation records in other zones that point to the authoritative DNS servers for the new zone.

Understand the tools that are available for monitoring and troubleshooting DNS. You can use the DNS snap-in to do some basic server testing and monitoring. More important, you use the snap-in to monitor and set logging options. Windows Server 2012 R2 automatically logs DNS events in the event log under a distinct DNS server heading. `Nslookup` offers the ability to perform query testing of DNS servers and to obtain detailed responses at the command prompt. You can use the command-line tool `ipconfig` to view your DNS client settings, to view and reset cached information used locally for resolving DNS name queries, and to register the resource records for a dynamic update client. Finally, you can configure the DNS server to create a log file that records queries, notification messages, dynamic updates, and various other bits of DNS information.

Know how to install and authorize a DHCP server. You install the DHCP service using the Add/Remove Windows Components Wizard. You authorize the DHCP server using the DHCP snap-in. When you authorize a server, you're actually adding its IP address to the Active Directory object that contains a list of the IP addresses of all authorized DHCP servers.

Know how to create a DHCP scope. You use the New Scope Wizard to create a new scope for both IPv4 and IPv6. Before you start, you'll need to know the IP address range for the scope you want to create; which IP addresses, if any, you want to exclude from the address pool; which IP addresses, if any, you want to reserve; and the values for the DHCP options you want to set, if any.

Understand how relay agents help with multiple physical network segments. A question about relay agents on the exam may appear to be a DHCP-related question. Relay agents assist DHCP message propagation across network or router boundaries where such messages ordinarily wouldn't pass.

Understand the difference between exclusions and reservations. When you want to exclude an entire range of IP addresses, you need to add that range as an exclusion. Any IP addresses within the range for which you want a permanent DHCP lease are known as reservations. Remember that exclusions are TCP/IP numbers in a pool that do not get issued and reservations are numbers in a TCP/IP pool that get issued only to the same client each time.

Review Questions

1. You are the network administrator for the ABC Company. Your network consists of two DNS servers named *DNS1* and *DNS2*. The users who are configured to use DNS2 complain because they are unable to connect to Internet websites. The following table shows the configuration of both servers:

DNS1	DNS2
`_msdcs.abc.comabc.com`	`.(root)_msdcs.abc.comabc.com`

   The users connected to DNS2 need to be able to access the Internet. What needs to be done?

   A. Build a new Active Directory Integrated zone on DNS2.

   B. Delete the `.(root)` zone from DNS2 and configure conditional forwarding on DNS2.

   C. Delete the current `cache.dns` file.

   D. Update your `cache.dns` file and root hints.

2. You are the network administrator for a large company that has one main site and one branch office. Your company has a single Active Directory forest, `ABC.com`. You have a single domain controller (ServerA) in the main site that has the DNS role installed. ServerA is configured as a primary DNS zone. You have decided to place a domain controller (ServerB) in the remote site and implement the DNS role on that server. You want to configure DNS so that, if the WAN link fails, users in both sites can still update records and resolve any DNS queries. How should you configure the DNS servers?

   A. Configure ServerB as a secondary DNS server. Set replication to occur every five minutes.

   B. Configure ServerB as a stub zone.

   C. Configure ServerB as an Active Directory Integrated zone and convert ServerA to an Active Directory Integrated zone.

   D. Convert ServerA to an Active Directory Integrated zone and configure ServerB as a secondary zone.

3. You are the network administrator for a midsize computer company. You have a single Active Directory forest, and your DNS servers are configured as Active Directory Integrated zones. When you look at the DNS records in Active Directory, you notice that there are many records for computers that do not exist on your domain. You want to make sure that only domain computers register with your DNS servers. What should you do to resolve this issue?

   A. Set dynamic updates to None.

   B. Set dynamic updates to Nonsecure And Secure.

   C. Set dynamic updates to Domain Users Only.

   D. Set dynamic updates to Secure Only.

4. Your company consists of a single Active Directory forest. You have a Windows Server 2012 R2 domain controller that also has the DNS role installed. You also have a Unix-based DNS server at the same location. You need to configure your Windows DNS server to allow zone transfers to the Unix-based DNS server. What should you do?
   - **A.** Enable BIND secondaries.
   - **B.** Configure the Unix machine as a stub zone.
   - **C.** Convert the DNS server to Active Directory Integrated.
   - **D.** Configure the Microsoft DNS server to forward all requests to the Unix DNS server.

5. You are the network administrator for Stellacon Corporation. Stellacon has two trees in its Active Directory forest, `stellacon.com` and `abc.com`. Company policy does not allow DNS zone transfers between the two trees. You need to make sure that when anyone in `abc.com` tries to access the `stellacon.com` domain, all names are resolved from the `stellacon.com` DNS server. What should you do?
   - **A.** Create a new secondary zone in `abc.com` for `stellacon.com`.
   - **B.** Configure conditional forwarding on the `abc.com` DNS server for `stellacon.com`.
   - **C.** Create a new secondary zone in `stellacon.com` for `abc.com`.
   - **D.** Configure conditional forwarding on the `stellacon.com` DNS server for `abc.com`.

6. You are the network administrator for your organization. A new company policy states that all inbound DNS queries need to be recorded. What can you do to verify that the IT department is compliant with this new policy?
   - **A.** Enable Server Auditing – Object Access.
   - **B.** Enable DNS debug logging.
   - **C.** Enable server database query logging.
   - **D.** Enable DNS Auditing – Object Access.

7. You are the network administrator for a small company with two DNS servers: DNS1 and DNS2. Both DNS servers reside on domain controllers. DNS1 is set up as a standard primary zone, and DNS2 is set up as a secondary zone. A new security policy was written stating that all DNS zone transfers must be encrypted. How can you implement the new security policy?
   - **A.** Enable the Secure Only setting on DNS1.
   - **B.** Enable the Secure Only setting on DNS2.
   - **C.** Configure Secure Only on the Zone Transfers tab for both servers.
   - **D.** Delete the secondary zone on DNS2. Convert both DNS servers to use Active Directory Integrated zones.

8. You are responsible for DNS in your organization. You look at the DNS database and see a large number of older records on the server. These records are no longer valid. What should you do?
   - **A.** In the zone properties, enable Zone Aging and Scavenging.
   - **B.** In the server properties, enable Zone Aging and Scavenging.
   - **C.** Manually delete all of the old records.
   - **D.** Set Dynamic Updates to None.

9. Your IT team has been informed by the compliance team that it needs copies of the DNS Active Directory Integrated zones for security reasons. You need to give the Compliance department a copy of the DNS zone. How should you accomplish this goal?
   - **A.** Run `dnscmd /zonecopy`.
   - **B.** Run `dnscmd /zoneinfo`.
   - **C.** Run `dnscmd /zoneexport`.
   - **D.** Run `dnscmd /zonefile`.

10. You are the network administrator for a Windows Server 2012 R2 network. You have multiple remote locations connected to your main office by slow satellite links. You want to install DNS into these offices so that clients can locate authoritative DNS servers in the main location. What type of DNS servers should be installed in the remote locations?
    - **A.** Primary DNS zones
    - **B.** Secondary DNS zones
    - **C.** Active Directory Integrated zones
    - **D.** Stub zones

Chapter 3

Plan and Install Active Directory

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Install domain controllers**

- Add or remove a domain controller from a domain
- Upgrade a domain controller
- Install Active Directory Domain Services (AD DS) on a Server Core installation
- Install a domain controller from Install from Media (IFM)
- Resolve DNS SRV record registration issues
- Configure a global catalog server
- Deploy Active Directory iaas in Windows Azure

Now that you are familiar with Domain Name System (DNS), you need to verify that the computer you upgrade to a domain controller (DC) meets the basic file system and network connectivity requirements so that Active Directory runs smoothly and efficiently in your organization.

Next, you'll explore the concept of *domain functional levels*, which essentially determine what sorts of domain controllers you can use in your environment. For instance, in the Windows Server 2003 domain functional level, you can include Server 2012/2012 R2, Server 2008 R2, Server 2008, and Server 2003 domain controllers, but the functionality of the domain is severely limited.

Once you understand how to plan properly for your domain environment, you will learn how to install Active Directory, which you will accomplish by promoting a Windows Server 2012 R2 computer to a domain controller. I will also discuss a feature in Windows Server 2012 R2 called a *read-only domain controller (RODC)*.

After you become familiar with the initial Active Directory installation, you will learn how to install and configure Application Directory partitions. These partitions provide replicable data repositories using the Active Directory paradigm, but they don't actually store any security principals, such as users or groups. As the name implies, you use Application Directory partitions primarily to store data generated by applications that need to be replicated throughout your network environments independent of the rest of Active Directory.

The final section of this chapter deals with integrating DNS with Active Directory. You learned about DNS in Chapter 2, "Configure Network Services," but in this chapter I will review how DNS implements with Active Directory.

For these exercises, I assume you are creating a Windows Server 2012 R2 machine in a test environment and not on a live network. If this Windows Server 2012 R2 machine is being added into a Windows Server 2012 or 2008 R2 domain, you will need to prep the domain (explained in the section "Adprep" later in this chapter).

Verifying the File system

When you're planning your Active Directory deployment, the file system that the operating system uses is an important concern for two reasons. First, the file system can provide the ultimate level of security for all the information stored on the server itself. Second, it is

responsible for managing and tracking all of this data. The Windows Server 2012 R2 platform supports two file systems:

- Windows NT File System (NTFS)
- Resilient File System (ReFS)

Although ReFS was new to Windows Server 2012, NTFS has been around for many years, and NTFS in Windows Server 2012 R2 has been improved for better performance.

If you have been working with servers for many years, you may have noticed a few changes to the server file system choices. For example, in Windows Server 2003, you could choose between FAT, FAT32, and NTFS. In Windows Server 2008 R2, you could choose between FAT32 and NTFS. In Windows Server 2012 R2, you will notice that all versions of FAT have been removed (see Figure 3.1).

FIGURE 3.1 Format options on Windows Server 2012 R2

Resilient File System (ReFS)

Windows Server 2012 R2 now includes a new file system called *Resilient File System (ReFS)*. ReFS was created to help Windows Server 2012 R2 maximize the availability of data and online operation. ReFS allows the Windows Server 2012 R2 system to continue to function despite some errors that would normally cause data to be lost or the system to go down. ReFS uses data integrity to protect your data from errors and also to make sure that all of your important data is online when that data is needed.

One of the issues that IT members have had to face over the years is the problem of rapidly growing data sizes. As we continue to rely more and more on computers, our data continues to get larger and larger. This is where ReFS can help an IT department. ReFS was designed specifically with the issues of scalability and performance in mind, which resulted in some of the following ReFS features:

Availability If your hard disk becomes corrupt, ReFS has the ability to implement a salvage strategy that removes the data that has been corrupted. This feature allows the healthy data to continue to be available while the unhealthy data is removed. All of this can be done without taking the hard disk offline.

Scalability One of the main advantages of ReFS is the ability to support volume sizes up to 2^78 bytes using 16KB cluster sizes, while Windows stack addressing allows 2^64 bytes. ReFS also supports file sizes of 2^64-1 bytes, 2^64 files in a directory, and the same number of directories in a volume.

Robust Disk Updating ReFS uses a disk updating system referred to as an *allocate-on-write transactional model* (also known as *copy on write*). This model helps to avoid many hard disk issues while data is written to the disk because ReFS updates data using disk writes to multiple locations in an atomic manner instead of updating data in place.

Data Integrity ReFS uses a check-summed system to verify that all data that is being written and stored is accurate and reliable. ReFS always uses allocate-on-write for updates to the data, and it uses checksums to detect disk corruption.

Application Compatibility ReFS allows for most NTFS features and also supports the Win32 API. Because of this, ReFS is compatible with most Windows applications.

NTFS

Let's start with some of the features of NTFS. There are many benefits to using NTFS, including support for the following:

Disk Quotas To restrict the amount of disk space used by users on the network, system administrators can establish *disk quotas*. By default, Windows Server 2012 R2 supports disk quota restrictions at the volume level. That is, you can restrict the amount of storage space that a specific user uses on a single disk volume. Third-party solutions that allow more granular quota settings are also available.

File System Encryption One of the fundamental problems with network operating systems (NOSs) is that system administrators are often given full permission to view all files and data stored on hard disks, which can be a security and privacy concern. In some cases, this is necessary. For example, to perform backup, recovery, and disk management functions, at least one user must have all permissions. Windows Server 2012 R2 and NTFS address these issues by allowing for *file system encryption*. Encryption essentially scrambles all of the data stored within files before they are written to the disk. When an authorized user requests the files, they are transparently decrypted and provided. By using encryption, you

can prevent the data from being used in case it is stolen or intercepted by an unauthorized user—even a system administrator.

Dynamic Volumes Protecting against disk failures is an important concern for production servers. Although earlier versions of Windows NT supported various levels of Redundant Array of Independent Disks (RAID) technology, software-based solutions had some shortcomings. Perhaps the most significant was that administrators needed to perform server reboots to change RAID configurations. Also, you could not make some configuration changes without completely reinstalling the operating system. With Windows Server 2012 R2 support for *dynamic volumes*, system administrators can change RAID and other disk configuration settings without needing to reboot or reinstall the server. The result is greater data protection, increased scalability, and increased uptime. Dynamic volumes are also included with ReFS.

Mounted Drives By using *mounted drives*, system administrators can map a local disk drive to an NTFS directory name. This helps them organize disk space on servers and increase manageability. By using mounted drives, you can mount the `C:\Users` directory to an actual physical disk. If that disk becomes full, you can copy all of the files to another, larger drive without changing the directory path name or reconfiguring applications.

Remote Storage System administrators often notice that as soon as they add more space, they must plan the next upgrade. One way to recover disk space is to move infrequently used files to external hard drives. However, backing up and restoring these files can be quite difficult and time-consuming. System administrators can use the *remote storage* features supported by NTFS to off-load seldom-used data automatically to a backup system or other devices. The files, however, remain available to users. If a user requests an archived file, Windows Server 2012 R2 can automatically restore the file from a remote storage device and make it available. Using remote storage like this frees up system administrators' time and allows them to focus on tasks other than micromanaging disk space.

Self-healing NTFS In previous versions of the Windows Server operating system, if you had to fix a corrupted NTFS volume, you used a tool called `Chkdsk.exe`. The disadvantage of this tool is that the Windows Server's availability was disrupted. If this server was your domain controller, that could stop domain logon authentication.

To help protect the Windows Server 2012 R2 NTFS file system, Microsoft now uses a feature called self-healing NTFS. *Self-healing NTFS* attempts to fix corrupted NTFS file systems without taking them offline. Self-healing NTFS allows an NTFS file system to be corrected without running the `Chkdsk.exe` utility. New features added to the NTFS kernel code allow disk inconsistencies to be corrected without system downtime.

Security NTFS allows you to configure not only folder-level security but also file-level security. NTFS security is one of the biggest reasons most companies use NTFS. ReFS also allows folder- and file-level security.

Setting Up the NTFS Partition

Although the features mentioned in the previous section likely compel most system administrators to use NTFS, additional reasons make using it mandatory. The most important reason is that the Active Directory data store must reside on an NTFS partition. Therefore, before you begin installing Active Directory, make sure you have at least one NTFS partition available. Also, be sure you have a reasonable amount of disk space available (at least 4GB). Because the size of the Active Directory data store will grow as you add objects to it, also be sure that you have adequate space for the future.

Exercise 3.1 shows you how to use the administrative tools to view and modify disk configuration.

WARNING

Before you make any disk configuration changes, be sure you completely understand their potential effects; then perform the test in a lab environment and make sure you have good, verifiable backups handy. Changing partition sizes and adding and removing partitions can result in a total loss of all information on one or more partitions.

If you want to convert an existing partition from FAT or FAT32 to NTFS, you need to use the `CONVERT` command-line utility. For example, the following command converts the `C:` partition from FAT to NTFS:

```
CONVERT c: /fs:ntfs
```

EXERCISE 3.1

Viewing Disk Configuration

1. Press the Windows key on the keyboard (left side between the Ctrl and Alt keys) and then choose Administrative Tools.

2. Double-click Computer Management.
3. Under Storage, click Disk Management.

The Disk Management program shows you the logical and physical disks that are currently configured on your system. Note that information about the size of each partition is also displayed (in the Capacity column).

4. Use the View menu to choose various depictions of the physical and logical drives in your system.
5. To see the available options for modifying partition settings, right-click any of the disks or partitions. This step is optional.
6. Close Computer Management.

Verifying Network Connectivity

Although a Windows Server 2012 R2 computer can be used by itself without connecting to a network, you will not harness much of the potential of the operating system without network connectivity. Because the fundamental purpose of a network operating system is to provide resources to users, you must verify network connectivity.

Basic Connectivity Tests

Before you begin to install Active Directory, you should perform several checks of your current configuration to ensure that the server is configured properly on the network. You should test the following:

Network Adapter At least one network adapter should be installed and properly configured on your server. A quick way to verify that a network adapter is properly installed is to use the Computer Management administrative tool. Under Device Manager, Network Adapters branch, you should have at least one network adapter listed. If you do not, use the Add Hardware icon in Control Panel to configure hardware.

TCP/IP Make sure that TCP/IP is installed, configured, and enabled on any necessary network adapters. The server should also be given a valid IP address and subnet mask. Optionally, you may need to configure a default gateway, DNS servers, WINS servers, and other network settings. If you are using DHCP, be sure that the assigned information is correct. It is always a good idea to use a static IP address for servers because IP address changes can cause network connectivity problems if they are not handled properly.

You must understand TCP/IP to use Windows Server 2012 R2 and Active Directory. TCP/IP will be covered in greater detail in Chapter 8, "Configure TCP/IP."

Internet Access If the server should have access to the Internet, verify that it is able to connect to external web servers and other machines outside of the local area network (LAN). If the server is unable to connect, you might have a problem with the TCP/IP configuration.

LAN Access The server should be able to view other servers and workstations on the network. If other machines are not visible, make sure that the network and TCP/IP configurations are correct for your environment.

Client Access Network client computers should be able to connect to your server and view any shared resources. A simple way to test connectivity is to create a share and test whether other machines are able to see files and folders within it. If clients cannot access the machine, make sure that both the client and the server are configured properly.

Wide Area Network Access If you're working in a distributed environment, you should ensure that you have access to any remote sites or users who will need to connect to this machine. Usually, this is a simple test that can be performed by a network administrator.

Tools and Techniques for Testing Network Configuration

In some cases, verifying network access can be quite simple. You might have some internal and external network resources with which to test. In other cases, it might be more complicated. You can use several tools and techniques to verify that your network configuration is correct.

Using the `Ipconfig` Utility By typing **`ipconfig/all`** at the command prompt, you can view information about the TCP/IP settings of a computer. Figure 3.2 shows the types of information you'll receive.

FIGURE 3.2 Viewing TCP/IP information with the **ipconfig** utility

Using the `Ping` Command The `ping` command was designed to test connectivity to other computers. You can use the command simply by typing **`ping`** and then an IP address or hostname at the command line. The following are some steps for testing connectivity using the `ping` command.

Ping Other Computers on the Same Subnet You should start by pinging a known active IP address on the network to check for a response. If you receive one, then you have connectivity to the network.

Next check to see whether you can ping another machine using its hostname. If this works, then local name resolution works properly.

Ping Computers on Different Subnets To ensure that routing is set up properly, you should attempt to ping computers that are on other subnets (if any exist) on your network. If this test fails, try pinging the default gateway. Any errors may indicate a problem in the network configuration or a problem with a router.

When You Don't Receive a Response

Some firewalls, routers, or servers on your network or on the Internet might prevent you from receiving a successful response from a `ping` command. This is usually for security reasons (malicious users might attempt to disrupt network traffic using excessive pings as well as redirects and smurf attacks). If you do not receive a response, do not assume that the service is not available. Instead, try to verify connectivity in other ways. For example, you can use the `TRACERT` command to demonstrate connectivity beyond your subnet, even if other routers ignore Internet Control Message Protocol (ICMP) responses. Because the display of a second router implies connectivity, the path to an ultimate destination shows success even if it does not display the actual names and addresses.

Browsing the Network To ensure that you have access to other computers on the network, be sure that they can be viewed by clicking Network. This verifies that your name resolution parameters are set up correctly and that other computers are accessible. Also, try connecting to resources (such as file shares or printers) on other machines.

By default, Network Discovery is turned off. To browse the network, you must first enable Network Discovery from the Control Panel in the Network and Sharing Center ➢ Advanced Sharing settings.

Browsing the Internet You can quickly verify whether your server has access to the Internet by visiting a known website, such as `www.microsoft.com`. Success ensures that you have access outside of your network. If you do not have access to the Web, you might need to verify your proxy server settings (if applicable) and your DNS server settings.

By performing these simple tests, you can ensure that you have a properly configured network connection and that other network resources are available.

Understanding Domain and Forest Functionality

Windows Server 2012 R2 Active Directory uses a concept called *domain and forest functionality*. The functional level that you choose during the Active Directory installation determines which features your domain can use.

Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 include additional forest functionality compared to Windows Server 2003. Forest functionality applies to all of the domains within a forest.

About the Domain Functional Level

Windows Server 2012 R2 will support the following domain functional levels:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Which function level you use depends on the domain controllers you have installed on your network. This is an important fact to remember. You can use Windows Server 2003, Windows Server 2008/2008 R2, and Windows 2012 member servers in the Windows

Server 2012 R2 function level as long as all domain controllers are running Windows Server 2012 R2.

When you are deciding which function level you will use in your organization, you must choose the function level of your lowest domain controller. For example, if you have a Windows Server 2003 domain controller, your function levels should be Windows Server 2003. If you choose a higher level, the Windows Server 2003 domain controller will not function. Be careful—once a forest function level is upgraded, it cannot be downgraded lower than Windows Server 2008.

Table 3.1 shows the features available in Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 domain function levels.

TABLE 3.1 Comparing domain functional levels

Domain functional feature	Windows Server 2003	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012	Windows Server 2012 R2
Authentication assurance	Disabled	Disabled	Enabled	Enabled	Enabled
Fine-grained password policies	Disabled	Enabled	Enabled	Enabled	Enabled
Last interactive logon information	Disabled	Enabled	Enabled	Enabled	Enabled
Advanced Encryption Services (AES 128 and 256) support for the Kerberos protocol	Disabled	Enabled	Enabled	Enabled	Enabled
Distributed File System replication support for Sysvol	Disabled	Enabled	Enabled	Enabled	Enabled
Read-only domain controller (RODC)	Enabled	Enabled	Enabled	Enabled	Enabled
Ability to redirect the Users and Computers containers	Enabled	Enabled	Enabled	Enabled	Enabled
Ability to rename domain controllers	Enabled	Enabled	Enabled	Enabled	Enabled

TABLE 3.1 Comparing domain functional levels *(continued)*

Domain functional feature	Windows Server 2003	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012	Windows Server 2012 R2
Logon time stamp updates	Enabled	Enabled	Enabled	Enabled	Enabled
Kerberos KDC key version numbers	Enabled	Enabled	Enabled	Enabled	Enabled
Passwords for `InetOrgPerson` objects	Enabled	Enabled	Enabled	Enabled	Enabled
Converts NT groups to domain local and global groups	Enabled	Enabled	Enabled	Enabled	Enabled
SID history	Enabled	Enabled	Enabled	Enabled	Enabled
Group nesting	Enabled	Enabled	Enabled	Enabled	Enabled
Universal groups	Enabled	Enabled	Enabled	Enabled	Enabled

About Forest Functionality

Windows Server 2012 R2 forest functionality applies to all of the domains in a forest. All domains have to be upgraded to Windows Server 2012 R2 before the forest can be upgraded to Windows Server 2012 R2.

There are five levels of forest functionality:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 have many of the same forest features. Some of these features are described in the following list:

Global Catalog Replication Enhancements When an administrator adds a new attribute to the global catalog, only those changes are replicated to other global catalogs in the forest. This can significantly reduce the amount of network traffic generated by replication.

Defunct Schema Classes and Attributes You can never permanently remove classes and attributes from the Active Directory schema. However, you can mark them as defunct so that they cannot be used. With Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 forest functionality, you can redefine the defunct schema attribute so that it occupies a new role in the schema.

Forest Trusts Previously, system administrators had no easy way of granting permission on resources in different forests. Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 resolve some of these difficulties by allowing trust relationships between separate Active Directory forests. Forest trusts act much like domain trusts, except that they extend to every domain in two forests. Note that all forest trusts are intransitive.

Linked Value Replication Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 use a concept called *linked value replication*. With linked value replication, only the user record that has been changed is replicated (not the entire group). This can significantly reduce network traffic associated with replication.

Renaming Domains Although the Active Directory domain structure was originally designed to be flexible, there were several limitations. Because of mergers, acquisitions, corporate reorganizations, and other business changes, you may need to rename domains. In Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 you can change the DNS and NetBIOS names for any domain. Note that this operation is not as simple as just issuing a `rename` command. Instead, there's a specific process that you must follow to make sure the operation is successful. Fortunately, when you properly follow the procedure, Microsoft supports domain renaming even though not all applications support it.

Other Features Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 also support the following features:

- Improved replication algorithms and dynamic auxiliary classes are designed to increase performance, scalability, and reliability.
- *Active Directory Federation Services (AD FS)*, also known as *Trustbridge*, handles federated identity management. *Federated identity management* is a standards-based information technology process that enables distributed identification, authentication, and authorization across organizational and platform boundaries. The ADFS solution in Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 helps administrators address these challenges by enabling organizations to share a user's identity information securely.

- *Active Directory Lightweight Directory Services (AD LDS)* was developed for organizations that require flexible support for directory-enabled applications. AD LDS, which uses the Lightweight Directory Access Protocol (LDAP), is a directory service that adds flexibility and helps organizations avoid increased infrastructure costs.
- Active Directory Recycle Bin (Windows Server 2008 R2 Forest level or higher) provides administrators with the ability to restore deleted objects in their entirety while AD DS is running. Before this, if you deleted an Active Directory object, you needed to recover it from a backup. Now you can recover the object from the AD recycle bin.

Many of the concepts related to domain and forest functional features are covered in greater detail later in this book.

Planning the Domain Structure

Once you have verified the technical configuration of your server for Active Directory, it's time to verify the Active Directory configuration for your organization. Since the content of this chapter focuses on installing the first domain in your environment, you really need to know only the following information prior to beginning setup:

- The DNS name of the domain
- The computer name or the NetBIOS name of the server (which will be used by previous versions of Windows to access server resources)
- In which domain function level the domain will operate
- Whether other DNS servers are available on the network
- What type of and how many DNS servers are available on the network

However, if you will be installing additional domain controllers in your environment or will be attaching to an existing Active Directory structure, you should also have the following information:

- If this domain controller will join an existing domain, you should know the name of that domain. You will also either require a password for a member of the Enterprise Administrators group for that domain or have someone with those permissions create a domain account before promotion.
- You should know whether the new domain will join an existing tree and, if so, the name of the tree it will join.
- You should know the name of a forest to which this domain will connect (if applicable).

Installing Active Directory

Installing Active Directory is an easy and straightforward process as long as you plan adequately and make the necessary decisions beforehand. There are many ways that you can install Active Directory. You can install Active Directory by using the Windows Server 2012 R2 installation disk (Install from Media (IFM)), using Server Manager, or using Windows PowerShell. But before you can do the actual installation, you must first make sure that your network is ready for the install.

In the following sections, you'll look at the required steps to install the first domain controller in a given environment.

Adprep

When you are adding a new user to Active Directory, you fill in fields such as First Name, Last Name, and so on. These fields are called *attributes*. The problem is that when you go to install Windows Server 2012 R2, its version of Active Directory has newer attributes than the previous versions of Active Directory. Thus, you need to set up your current version of Active Directory so that it can accept the installation of Windows Server 2012 R2 Active Directory. This is why you use Adprep. Adprep is required to run in order to add the first Windows Server 2012 R2 domain controller to an existing domain or forest.

You would need to run `Adprep /forestprep` to add the first Windows Server 2012 R2 domain controller to an existing forest. `Adprep /forestprep` must be run by an administrator who is a member of the Enterprise Admins group, the Schema Admins group, and the Domain Admins group of the domain that hosts the schema master.

You would need to run `Adprep /domainprep` to add the first Windows Server 2012 R2 domain controller to an existing domain. Again, to achieve this command, you must be a member of the Domain Admins group of the domain where you are installing the Windows Server 2012 R2 domain controller.

`Adprep /rodcprep` must be run to add the first Windows Server 2012 R2 RODC to an existing forest. The administrator who runs this command must be a member of the Enterprise Admins group.

One feature that is new to the Windows Server 2012 R2 Active Directory installation process is that, if needed, Adprep will automatically be executed during the normal Active Directory Domain Services installation.

Active Directory Prerequisites

Before you install Active Directory into your network, you must first make sure that your network and the server meet some minimum requirements. Table 3.2 will show you the requirements needed for Active Directory.

TABLE 3.2 Active Directory requirements

Requirement	Description
Adprep	When adding the first Windows Server 20012 R2 domain controller to an existing Active Directory domain, Adprep commands run automatically as needed.
Credentials	When installing a new AD DS forest, the administrator must be set to local Administrator on the first server. To install an additional domain controller in an existing domain, you need to be a member of the Domain Admins group.
DNS	Domain Name System needs to be installed for Active Directory to function properly. You can install DNS during the Active Directory installation.
NTFS	The Windows Server 2012 R2 drives that store the database, log files, and SYSVOL folder must be placed on a volume that is formatted with the NTFS file system.
RODCs	Read Only Domain Controllers can be installed as long as another domain controller (Windows Server 2008 or newer) already exists on the domain. Also the Forest functional level must be at least Windows Server 2003.
TCP/IP	You must configure the appropriate TCP/IP settings on your domain, and you must configure the DNS server addresses.

The Installation Process

Windows Server 2012 R2 computers are configured as either member servers (if they are joined to a domain) or stand-alone servers (if they are part of a workgroup). The process of converting a server to a domain controller is known as *promotion*. Through the use of a simple and intuitive wizard in Server Manager, system administrators can quickly configure servers to be domain controllers after installation. Administrators also have the ability to promote domain controllers using Windows PowerShell.

The first step in installing Active Directory is promoting a Windows Server 2012 R2 computer to a domain controller. The first domain controller in an environment serves as the starting point for the forest, trees, domains, and the operations master roles.

Exercise 3.2 shows the steps you need to follow to promote an existing Windows Server 2012 R2 computer to a domain controller. To complete the steps in this exercise, you must have already installed and configured a Windows Server 2012 R2 computer. You also need a DNS server that supports SRV records. If you do not have a DNS server available, the Active Directory Installation Wizard automatically configures one for you.

EXERCISE 3.2

Promoting a Domain Controller

1. Install the Active Directory Domain Services by clicking the Add Roles And Features link in Server Manager's Dashboard view.
2. At the Before You Begin screen, click Next.
3. The Select installation Type screen will be next. Make sure that the Role-Based radio button is selected and click Next.
4. At the Select Destination Server screen, choose the local machine. Click Next.
5. At the Select Server Roles screen, click the check box for Active Directory Domain Services.

6. After you check the Active Directory Domain Services box, a pop-up menu will appear asking you to install additional features. Click the Add Features button.
7. Click Next.
8. At the Select Features screen, accept the defaults and click Next.

EXERCISE 3.2 *(continued)*

9. Click Next at the information screen.
10. Click the Install button at the Confirmation Installation screen.
11. The Installation Progress screen will show you how the installation is progressing.

12. After the installation is complete, click the Close button.
13. On the left side window, click the AD DS link.
14. Click the More link next to Configuration Required for Active Directory Domain Services.

15. Under the Post-Deployment Configuration section, click the Promote This Server To A Domain Controller link.

16. At this point, you will configure this domain controller. You are going to install a new domain controller in a new domain in a new forest. At the Deployment Configuration screen, choose the Add A New Forest radio button. You then need to add a root domain name. In this exercise, I will use `Sybex.com`. Click Next.

EXERCISE 3.2 *(continued)*

17. At the Domain Controller Options screen, set the following options:

- Function levels: Windows Server 2008 R2 (for both)
- Verify that the DNS and Global Catalog check boxes are checked
- Password: **P@ssw0rd**

Then click Next.

18. At the DNS screen, click Next.
19. At the additional options screen, accept the default NetBIOS domain name and click Next.
20. At the Paths screen, accept the default file locations and click Next.
21. At the Review Options screen, verify your settings and click Next.
22. At the Prerequisites Check screen, click the Install button (as long as there are no errors).

23. After the installation completes, the machine will automatically reboot. Log in as the administrator.
24. Close Server Manager.
25. Click the Start button on the keyboard and choose Administrative Tools.
26. You should see new MMC snap-ins for Active Directory.

EXERCISE 3.2 *(continued)*

27. Close the Administrative Tools window.

In Exercise 3.3, you will learn how to install Active Directory on a Server Core installation. You will use Windows Server 2012 R2 Datacenter Server Core. Before actually installing AD DS, you will learn how to configure the computer name, the time, the administrator password, and a static TCP/IP address, and then you will install DNS.

EXERCISE 3.3

Installing AD DS on Server Core

1. At the Server Core command prompt, type **`cd\windows\system32`** and press Enter.
2. Type **`timedate.cpl`** and set your date, local time zone, and time. Click OK.
3. Type **`Netsh`** and press Enter.
4. Type **`Interface`**, and press Enter.

5. Type **`IPv4`**, and press Enter.

6. Type **`Show IP`** and press Enter. This will show you the current TCP/IP address and the interface with which the TCP/IP address is associated.

7. As you can see, interface 12 is my Ethernet interface. To change this interface, type the following command and press Enter:

   ```
   Set address name="12" source=static address=192.168.15.165
   mask=255.255.255.0 gateway=192.168.15.1
   ```

   I used 192.168.15.x for my address. You can replace the address, mask, and gateway based on your local settings.

8. Type **`Show IP`** and press Enter. You should see that the new address is now manual and set to the IP address you set.

EXERCISE 3.3 *(continued)*

9. Type **`Exit`** and press Enter.
10. Type **`Net User Administrator *`** and press Enter.
11. Type in your password and then confirm the password. I used `P@ssw0rd` for my password.

12. Type the following command and press Enter:

    `Netdom renamecomputer %computername% /newname:ServerA`

13. Type **`Y`** and press Enter.
14. Type **`Shutdown /R /T 0`** and press Enter. This will reboot the machine. After the reboot, log back into the system.
15. Type **`PowerShell`** and press Enter.
16. At the PowerShell prompt, type **`Add-WindowsFeature DNS`** and press Enter. This will add DNS to the server.

17. At the PowerShell prompt, type **`Add-WindowsFeature AD-Domain-Services`** and press Enter.
18. At the PowerShell prompt, type **`Import-Module ADDSDeployment`**.
19. At the PowerShell prompt, type **`Install-ADDSForest`**.

20. Type in your domain name and press Enter. I used `Sybex.com`.
21. Next you will be asked for your Safe mode administrator password. Type in **`P@ssw0rd`** and then confirm it.
22. Type **`Y`** and press Enter.

Active Directory will install, and the machine will automatically reboot.

Deploying Active Directory IaaS in Windows Azure

Well before I jump into this topic, I must first explain what I am talking about. Windows Azure is a Microsoft cloud platform that allows you to put your server data into the cloud. Deploying Active Directory with IaaS means you are using virtualization for the deployment.

So, to put this in a nutshell, when doing this type of install, it's actually not too far off from the install you already did. You create a virtual server and then install Active Directory. Then you upload that virtual server to the cloud.

NOTE

I understand that I have not explained virtualization, but Hyper-V and virtualization will be covered in detail in Chapter 9, "Use Virtualization in Windows Server 2012 R2."

Now that you understand what this section is about, let's talk about some of the tasks that are different from the normal way you install Active Directory virtually. There are three main differences when installing Active Directory IaaS on Windows Azure.

Windows Azure virtual machines may need to have connectivity to the corporate network. Microsoft states that you don't have to have connectivity to your on-site corporate network, but you will lose functionality. Thus, Microsoft recommends that you set up connectivity, and to do that, you must use Windows Azure Virtual Network. Windows Azure Virtual Network includes a site-to-site or site-to-point virtual private network (VPN) component capable of seamlessly connecting Windows Azure virtual machines and on-site machines.

Static IP addresses are *not* supported on Windows Azure virtual machines. Normally, when setting up a server, we all use static IP addresses. This is actually required on a DHCP server, DNS server, and so on. But when you deploy Active Directory IaaS in Windows Azure, you must use Dynamic TCP/IP addressing, and this requires that you set up Windows Azure Virtual Network.

IP addresses for Windows Azure virtual machines are attached to Windows Azure Virtual Network, and that TCP/IP address persists for the lifetime of the virtual machine. Because of this, the Windows Server Active Directory requirements for IP addressing are met, and the requirements for DNS are also met if you want the server to have both roles.

Windows Azure allows for two distinct disk types for virtual machines. As you will learn in Chapter 9, the selection of the virtual machine disk type is important when deploying domain controllers. Windows Azure allows both "operating system disks" and "data disks." Most of the time you will use data disks when installing Active Directory on the virtual machine. Data disks use write-through caching, guaranteeing durability of writes, and this is important to the integrity of any Windows Server active machine. There are some other factors of which you should be aware when choosing your disk type. Please check Microsoft's website for more details when choosing a disk type.

Verifying Active Directory Installation

Once you have installed and configured Active Directory, you'll want to verify that you have done so properly. In the following sections, you'll look at methods for doing this.

Using Event Viewer

The first (and perhaps most informative) way to verify the operations of Active Directory is to query information stored in the Windows Server 2012 R2 event log. You can do this using the Windows Server 2012 R2 Event Viewer. Exercise 3.4 walks you through this procedure. Entries seen with the Event Viewer include errors, warnings, and informational messages.

To complete the steps in Exercise 3.4, you must have configured the local machine as a domain controller.

EXERCISE 3.4

Viewing the Active Directory Event Log

1. Open Administrative tools by pressing the Windows key and choosing Administrative Tools.
2. Open the Event Viewer snap-in from the Administrative Tools program group.
3. In the left pane, under Applications And Services Logs, select Directory Service.
4. In the right pane, you can sort information by clicking column headings. For example, you can click the Source column to sort by the service or process that reported the event.
5. Double-click an event in the list to see the details for that item. Note that you can click the Copy button to copy the event information to the Clipboard. You can then paste the data into a document for later reference. Also, you can move between items using the up and down arrows. Click OK when you have finished viewing an event.
6. Filter an event list by right-clicking the Directory Service item in the left pane and selecting Filter Current Log. Note that filtering does not remove entries from the event logs—it only restricts their display.
7. To verify Active Directory installation, look for events related to the proper startup of Active Directory, such as Event ID 1000 (Active Directory Startup Complete) and 1394 (Attempts To Update The Active Directory Database Are Succeeding). Also, be sure to examine any error or warning messages because they could indicate problems with DNS or other necessary services.
8. When you've finished viewing information in the Event Viewer, close the application.

Gaining Insight Through Event Viewer

Despite its simple user interface and somewhat limited GUI functionality, the Event Viewer tool can be your best ally in isolating and troubleshooting problems with Windows Server 2012 R2. The Event Viewer allows you to view information that is stored in various log files that are maintained by the operating system. This includes information from the following logs:

Application Stores messages generated by programs running on your system. For example, SQL Server 2012 might report the completion of a database backup job within the Application log.

Security Contains security-related information as defined by your auditing settings. For example, you could see when users have logged onto the system or when particularly sensitive files have been accessed.

System Contains operating system-related information and messages. Common messages might include a service startup failure or information about when the operating system was last rebooted.

Directory Service Stores messages and events related to how Active Directory functions. For example, you might find details related to replication here.

DNS Server Contains details about the operations of the DNS service. This log is useful for troubleshooting replication or name-resolution problems.

Other Log Files Contain various features of Windows Server 2012 R2 and the applications that may run on this operating system, which can create additional types of logs. These files allow you to view more information about other applications or services through the familiar Event Viewer tool.

Additionally, developers can easily send custom information from their programs to the Application log. Having all of this information in one place really makes it easy to analyze operating system and application messages. Also, many third-party tools and utilities are available for analyzing log files.

Although the Event Viewer GUI does a reasonably good job of letting you find the information you need, you might want to extract information to analyze other systems or applications. One especially useful feature of the Event Viewer is its ability to save a log file in various formats. You can access this feature by clicking Action ➢ Save As. You'll be given the option of saving in various formats, including tab- and comma-delimited text files. You can then open these files in other applications (such as Microsoft Excel) for additional data analysis.

Overall, in the real world, the Event Viewer can be an excellent resource for monitoring and troubleshooting your important servers and workstations.

In addition to providing information about the status of events related to Active Directory, the Event Viewer shows you useful information about other system services and applications. You should routinely use this tool.

Using Active Directory Administrative Tools

After a server has been promoted to a domain controller, you will see that various tools are added to the Administrative Tools program group, including the following:

Active Directory Administrative Center This is a *Microsoft Management Console (MMC)* snap-in that allows you to accomplish many Active Directory tasks from one central location. This MMC snap-in allows you to manage your directory services objects, including doing the following tasks:

- Reset user passwords
- Create or manage user accounts
- Create or manage groups
- Create or manage computer accounts
- Create or manage organizational units (OUs) and containers
- Connect to one or several domains or domain controllers in the same instance of Active Directory Administrative Center
- Filter Active Directory data

Active Directory Domains and Trusts Use this tool to view and change information related to the various domains in an Active Directory environment. This MMC snap-in also allows you to set up shortcut trusts.

Active Directory Sites and Services Use this tool to create and manage Active Directory sites and services to map to an organization's physical network infrastructure. Sites and services are covered in detail in Chapter 5, "Administer Active Directory."

Active Directory Users and Computers User and computer management is fundamental for an Active Directory environment. The Active Directory Users and Computers tool allows you to set machine- and user-specific settings across the domain. This tool is discussed throughout this book.

Active Directory Module for Windows PowerShell *Windows PowerShell* is a command-line shell and scripting language. The Active Directory Module for Windows PowerShell is a group of cmdlets used to manage your Active Directory domains, Active Directory Lightweight Directory Services (AD LDS) configuration sets, and Active Directory Database Mounting Tool instances in a single, self-contained package.

A good way to make sure that Active Directory is accessible and functioning properly is to run the Active Directory Users and Computers tool. When you open the tool, you should see a configuration similar to that shown in Figure 3.3. Specifically, you should make sure the name of the domain you created appears in the list. You should also click the `Domain Controllers` folder and make sure that the name of your local server appears in the right pane. If your configuration passes these two checks, Active Directory is present and configured.

Testing from Clients

The best test of any solution is simply to verify that it works the way you had intended in your environment. When it comes to using Active Directory, a good test is to ensure that clients can view and access the various resources presented by Windows Server 2012 R2 domain controllers. In the following sections, you'll look at several ways to verify that Active Directory is functioning properly.

FIGURE 3.3 Viewing Active Directory information using the Active Directory Users and Computers tool

Verifying Client Connectivity

If you are unable to see the recently promoted server on the network, there is likely a network configuration error. If only one or a few clients are unable to see the machine, the problem is probably related to client-side configuration. To fix this, make sure that the client computers have the appropriate TCP/IP configuration (including DNS server settings) and that they can see other computers on the network.

If the new domain controller is unavailable from any of the other client computers, you should verify the proper startup of Active Directory using the methods mentioned earlier in this chapter. If Active Directory has been started, ensure that the DNS settings are correct. Finally, test network connectivity between the server and the clients by accessing the network or by using the `ping` command.

Joining a Domain

If Active Directory has been properly configured, clients and other servers should be able to join the domain. Exercise 3.5 outlines the steps you need to take to join a Windows 7 or Windows 8 computer to the domain.

To complete this exercise, you must have already installed and properly configured at least one Active Directory domain controller and a DNS server that supports SRV records in your environment. In addition to the domain controller, you need at least one other computer, not configured as a domain controller, running one of the following operating systems: Windows 2000, Windows XP Professional (Windows XP Home Edition cannot join a domain), Windows Vista, Windows 7, Windows 8, Windows Server 2003,

Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.

Once clients are able to join the domain successfully, they should be able to view Active Directory resources using the Network icon. This test validates the proper functioning of Active Directory and ensures that you have connectivity with client computers.

Exercise 3.5 is being done from a Windows 7 Enterprise computer.

EXERCISE 3.5

Joining a Computer to an Active Directory Domain

1. Right-click the Computer icon on the Start menu, and click Properties.
2. Go to the section called Computer Name. On the right side, click the Change Settings link.
3. Next to the section To Rename This Computer Or Change Its Domain Or Workgroup, click the Change button.
4. In the Member Of section, choose the Domain option. Type the name of the Active Directory domain that this computer should join. Click OK.
5. When prompted for the username and password of an account that has permission to join computers to the domain, enter the information for an administrator of the domain. Click OK to commit the changes. If you successfully joined the domain, you will see a dialog box welcoming you to the new domain.
6. You will be notified that you must reboot the computer before the changes take place. Select Yes when prompted to reboot.

Creating and Configuring Application Data Partitions

Organizations store many different kinds of information in various places. For the IT departments that support this information, it can be difficult to ensure that the right information is available when and where it is needed. Windows Server 2012 R2 uses a feature called *application data partitions*, which allows system administrators and application

developers to store custom information within Active Directory. The idea behind application data partitions is that since you already have a directory service that can replicate all kinds of information, you might as well use it to keep track of your own information.

Developing distributed applications that can, for example, synchronize information across an enterprise is not a trivial task. You have to come up with a way to transfer data between remote sites (some of which are located across the world), and you have to ensure that the data is properly replicated. By storing application information in Active Directory, you can take advantage of its storage mechanism and replication topology. Application-related information stored on domain controllers benefits from having fault-tolerance features and availability.

Consider the following simple example to understand how this can work. Suppose your organization has developed a customer Sales Tracking and Inventory application. The company needs to make the information that is stored by this application available to all of its branch offices and users located throughout the world. However, the goal is to do this with the least amount of IT administrative effort. Assuming that Active Directory has already been deployed throughout the organization, developers can build support into the application for storing data within Active Directory. They can then rely on Active Directory to store and synchronize the information among various sites. When users request updated data from the application, the application can obtain this information from the nearest domain controller that hosts a replica of the Sales Tracking and Inventory data.

Other types of applications can also benefit greatly from the use of application data partitions. Now that you have a good understanding of the nature of application data partitions, let's take a look at how you can create and manage them using Windows Server 2012 R2 and Active Directory.

Creating Application Data Partitions

By default, after you create an Active Directory environment, you will not have any customer application data partitions. Therefore, the first step in making this functionality available is to create a new application data partition. You can use several tools to do this:

Third-Party Applications or Application-Specific Tools Generally, if you are planning to install an application that can store information in the Active Directory database, you'll receive some method of administering and configuring that data along with the application. For example, the setup process for the application might assist you in the steps you need to take to set up a new application data partition and to create the necessary structures for storing data.

Creating and managing application data partitions are advanced Active Directory–related functions. Be sure that you have a solid understanding of the Active Directory schema, Active Directory replication, LDAP, and your applications' needs before you attempt to create new application data partitions in a live environment.

Active Directory Service Interfaces ADSI is a set of programmable objects that can be accessed through languages such as Visual Basic Scripting Edition (VBScript), Visual C#, Visual Basic .NET, and many other language technologies that support the Component Object Model (COM) standard. Through the use of ADSI, developers can create, access, and update data stored in Active Directory and in any application data partitions.

The LDP Tool You can view and modify the contents of the Active Directory schema using LDAP-based queries. The LDP tool allows you to view information about application data partitions.

`Ldp.exe` is a graphical user interface (GUI) tool that allows an administrator to configure Lightweight Directory Access Protocol (LDAP) directory service. Administrators have the ability to use the LDP tool to administer an Active Directory Lightweight Directory Services (AD LDS) instance. To use the LDP tool, you must be an administrator or equivalent.

Figure 3.4 shows an example of connecting to a domain controller and browsing Active Directory information.

FIGURE 3.4 Using the LDP tool to view Active Directory schema information

`Ntdsutil` The `ntdsutil` utility is the main method by which system administrators create and manage application data partitions on their Windows Server 2012 R2 domain controllers. This utility's specific commands are covered later in this chapter.

Creating and managing application data partitions can be fairly complex. Such a project's success depends on the quality of the architecture design. This is a good example of where IT staff and application developers must cooperate to ensure that data is stored effectively and that it is replicated efficiently.

You can create an application data partition in one of three different locations within an Active Directory forest:

- As a new tree in an Active Directory forest
- As a child of an Active Directory domain partition

  For example, you can create an Accounting application data partition within the `Finance.MyCompany.com` domain.

- As a child of another application data partition

This method allows you to create a hierarchy of application data partitions.

As you might expect, you must be a member of the Enterprise Admins or Domain Admins group to be able to create application data partitions. Alternatively, you can be delegated the appropriate permissions to create new partitions.

Now that you have a good idea of the basic ways in which you can create application data partitions, let's look at how replicas (copies of application data partition information) are handled.

Managing Replicas

A *replica* is a copy of any data stored within Active Directory. Unlike the basic information that is stored in Active Directory, application partitions cannot contain security principals. Also, not all domain controllers automatically contain copies of the data stored in an application data partition. System administrators can define which domain controllers host copies of the application data. This is an important feature because, if replicas are used effectively, administrators can find a good balance between replication traffic and data consistency. For example, suppose that three of your organization's 30 locations require up-to-date accounting-related information. You might choose to replicate the data only to domain controllers located in the places that require the data. Limiting replication of this data reduces network traffic.

Replication is the process by which replicas are kept up-to-date. Application data can be stored and updated on designated servers in the same way basic Active Directory information (such as users and groups) is synchronized between domain controllers. Application data partition replicas are managed using the *Knowledge Consistency Checker (KCC)*, which ensures that the designated domain controllers receive updated replica information. Additionally, the KCC uses all Active Directory sites and connection objects (covered in Chapter 5) that you create to determine the best method to handle replication.

Removing Replicas

When you perform a *demotion* on a domain controller, that server can no longer host an application data partition. If a domain controller contains a replica of application data partition information, you must remove the replica from the domain controller before you demote it. If a domain controller is the machine that hosts a replica of the application data partition, then the entire application data partition is removed and will be permanently lost. Generally, you want to do this only after you're absolutely sure that your organization no longer needs access to the data stored in the application data partition.

Using *ntdsutil* to Manage Application Data Partitions

The primary method by which system administrators create and manage application data partitions is through the `ntdsutil` command-line tool. You can launch this tool simply by entering **`ntdsutil`** at a command prompt. The `ntdsutil` command is both interactive

and context sensitive. That is, once you launch the utility, you'll see an `ntdsutil` command prompt. At this prompt, you can enter various commands that set your context within the application. For example, if you enter the `domain management` command, you'll be able to use domain-related commands. Several operations also require you to connect to a domain, a domain controller, or an Active Directory object before you perform a command.

For complete details on using `ntdsutil`, see the Windows Server 2012 R2 Help and Support Center.

Table 3.3 describes the domain management commands supported by the `ntdsutil` tool. You can access this information by typing in the following sequence of commands at a command prompt:

```
ntdsutil
domain management
Help
```

TABLE 3.3 `ntdsutil` domain management commands

ntdsutil domain management command	**Purpose**
`Help` or `?`	Displays information about the commands that are available within the Domain Management menu of the `ntdsutil` command.
`Connection` or `Connections`	Allows you to connect to a specific domain controller. This will set the context for further operations that are performed on specific domain controllers.
`Create NC` *`PartitionDistinguishedName DNSName`*	Creates a new application directory partition.
`Delete NC` *`PartitionDistinguishedName`*	Removes an application data partition.
`List NC Information` *`Partition DistinguishedName`*	Shows information about the specified application data partition.
`List NC Replicas` *`PartitionDistinguishedName`*	Returns information about all replicas for the specific application data partition.
`Precreate` *`PartitionDistinguished NameServerDNSName`*	Pre-creates cross-reference application data partition objects. This allows the specified DNS server to host a copy of the application data partition.

TABLE 3.3 `ntdsutil` domain management commands *(continued)*

`ntdsutil` domain management command	**Purpose**
`Remove NC Replica` *`PartitionDistinguishedName DCDNSName`*	Removes a replica from the specified domain controller.
`Select Operation Target`	Selects the naming context that will be used for other operations.
`Set NC Reference Domain` *`PartitionDistinguishedName DomainDistinguishedName`*	Specifies the reference domain for an application data partition.
`Set NC Replicate NotificationDelay` *`PartitionDistinguishedName FirstDCNotificationDelay OtherDCNotificationDelay`*	Defines settings for how often replication will occur for the specified application data partition.

NOTE

The `ntdsutil` commands are all case insensitive. Mixed case was used in the table to make them easier to read. `NC` in commands stands for "naming context," referring to the fact that this is a partition of the Active Directory schema.

Figure 3.5 provides an example of working with `ntdsutil`. The following commands were entered to set the context for further operations:

```
ntdsutil
domain management
connections
connect to server localhost
connect to domain ADTest
quit
list
```

FIGURE 3.5 Viewing naming contexts on the local domain controller

Configuring DNS Integration with Active Directory

There are many benefits to integrating Active Directory and DNS services:

- You can configure and manage replication along with other Active Directory components.
- You can automate much of the maintenance of DNS resource records through the use of dynamic updates.
- You will be able to set specific security options on the various properties of the DNS service.

Exercise 3.6 shows the steps that you must take to ensure that these integration features are enabled. You'll look at the various DNS functions that are specific to interoperability with Active Directory.

Before you begin this exercise, make sure that the local machine is configured as an Active Directory domain controller and that DNS services have been properly configured. If you instructed the Active Directory Installation Wizard to configure DNS automatically, many of the settings mentioned in this section may already be enabled. However, you should verify the configuration and be familiar with how the options can be set manually.

EXERCISE 3.6

Configuring DNS Integration with Active Directory

1. Open Administrative tools by pressing the Windows key and choosing Administrative Tools.
2. Open the DNS snap-in from the Administrative Tools program group.
3. Right-click the icon for the local DNS server and select Properties. Click the Security tab. Notice that you can now specify which users and groups have access to modify the configuration of the DNS server. Make any necessary changes and click OK.
4. Expand the local server branch and the `Forward Lookup Zones` folder.
5. Right-click the name of the Active Directory domain you created and select Properties.
6. On the General tab, verify that the type is Active Directory–Integrated and that the Data Is Stored In Active Directory message is displayed. If this option is not currently selected, you can change it by clicking the Change button next to Type and choosing the Store The Zone In Active Directory check box on the bottom.
7. Verify that the Dynamic Updates option is set to Secure Only. This ensures that all updates to the DNS resource records database are made through authenticated Active Directory accounts and processes.

EXERCISE 3.6 *(continued)*

The other options are Nonsecure And Secure (accepts all updates) and None (to disallow dynamic updates).

8. Finally, notice that you can define the security permissions at the zone level by clicking the Security tab. Make any necessary changes and click OK.

Summary

This chapter covered the basics of implementing an Active Directory forest and domain structure, creating and configuring application data partitions, and setting the functional level of your domain and forest.

You are now familiar with how you can implement Active Directory. We carefully examined all of the necessary steps and conditions that you need to follow to install Active Directory on your network. First you need to prepare for the Domain Name System because Active Directory cannot be installed without the support of a DNS server.

You also need to verify that the computer you upgrade to a domain controller meets some basic file system and network connectivity requirements so that Active Directory can run smoothly and efficiently in your organization. These are some of the most common things you will have to do when you deploy Active Directory.

The chapter also covered the concept of domain functional levels, which essentially determine the kinds of domain controllers you can use in your environment. For instance, in the Windows 2003 functional level, you can include Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003 domain controllers, but the functionality of the domain is severely limited.

In this chapter, you also learned how to install Active Directory, which you accomplish by promoting a Windows Server 2012 computer to a domain controller using Server Manager. You also learned how to verify the installation by testing Active Directory from a client computer.

This chapter was limited in scope to examining the issues related to installing and configuring the first domain in an Active Directory environment. In later chapters, you'll see how to create and manage more complex configurations.

Exam Essentials

Know the prerequisites for promoting a server to a domain controller. You should understand the tasks that you must complete before you attempt to upgrade a server to a domain controller. Also, you should have a good idea of the information you need in order to complete the domain controller promotion process.

Understand the steps of the Active Directory Installation Wizard. When you run the Active Directory Installation Wizard, you'll be presented with many different choices. You should understand the effects of the various options provided in each step of the wizard.

Be familiar with the tools that you will use to administer Active Directory. Three main administrative tools are installed when you promote a Windows Server 2012 R2 to a domain controller. Be sure that you know which tools to use for which types of tasks.

Understand the purpose of application data partitions. The idea behind application data partitions is that since you already have a directory service that can replicate all kinds of security information, you can also use it to keep track of application data. The main benefit of storing application information in Active Directory is that you can take advantage of its storage mechanism and replication topology. Application-related information stored on domain controllers benefits from having fault-tolerance features and availability.

Review Questions

1. You are the system administrator of a large organization that has recently implemented Windows Server 2012 R2. You have a few remote sites that do not have very tight security. You have decided to implement read-only domain controllers (RODCs). What forest and function levels does the network need for you to do the install? (Choose all that apply.)
   - **A.** Windows 2000 Mixed
   - **B.** Windows 2008 R2
   - **C.** Windows 2003
   - **D.** Windows 2008

2. What is the maximum number of domains that a Windows Server 2012 R2 computer configured as a domain controller may participate in at one time?
   - **A.** Zero
   - **B.** One
   - **C.** Two
   - **D.** Any number of domains

3. A system administrator is trying to determine which file system to use for a server that will become a Windows Server 2012 R2 file server and domain controller. The company has the following requirements:
   - The file system must allow for file-level security from within Windows 2012 R2 Server.
   - The file system must make efficient use of space on large partitions.
   - The domain controller Sysvol must be stored on the partition.

   Which of the following file systems meets these requirements?
   - **A.** FAT
   - **B.** FAT32
   - **C.** HPFS
   - **D.** NTFS

4. For security reasons, you have decided that you must convert the system partition on your removable drive from the FAT32 file system to NTFS. Which of the following steps must you take in order to convert the file system? (Choose two.)
   - **A.** Run the command `CONVERT /FS:NTFS` from the command prompt.
   - **B.** Rerun Windows Server 2008 R2 Setup and choose to convert the partition to NTFS during the reinstallation.

C. Boot Windows Server 2008 R2 Setup from the installation CD-ROM and choose Rebuild File System.

D. Reboot the computer.

5. Windows Server 2012 R2 requires the use of which of the following protocols or services in order to support Active Directory? (Choose two.)

A. DHCP

B. TCP/IP

C. NetBEUI

D. IPX/SPX

E. DNS

6. You are promoting a Windows Server 2012 R2 computer to an Active Directory domain controller for test purposes. The new domain controller will be added to an existing domain. While you are using the Active Directory Installation Wizard, you receive an error message that prevents the server from being promoted. Which of the following might be the cause of the problem? (Choose all that apply.)

A. The system does not contain an NTFS partition on which the Sysvol directory can be created.

B. You do not have a Windows Server 2012 R2 DNS server on the network.

C. The TCP/IP configuration on the new server is incorrect.

D. The domain has reached its maximum number of domain controllers.

7. Your network contains a single Active Directory domain. The domain contains five Windows Server 2008 R2 domain controllers. You plan to install a new Windows Server 2012 R2 domain controller. Which two actions would you need to perform? (Each correct answer presents part of the solution. Choose two.)

A. Run `adprep.exe /rodcprep` at the command line.

B. Run `adprep.exe /forestprep` at the command line.

C. Run `adprep.exe /domainprep` at the command line.

D. From Active Directory Domains and Trusts, raise the functional level of the domain.

E. From Active Directory Users and Computers, prestage the RODC computer account.

8. You are the network administrator for a large company that creates widgets. Management asks you to implement a new Windows Server 2012 R2 system. You need to implement federated identity management. Which of the following will help you do this?

A. Active Directory Federation Services

B. Active Directory DNS Services

C. Active Directory IIS Services

D. Active Directory IAS Services

9. You are the system administrator responsible for your company's infrastructure. You think you have an issue with name resolution, and you need to verify that you are using the correct hostname. You want to test DNS on the local system and need to see whether the hostname server-1 resolves to the IP address 10.1.1.1. Which of the following actions provides a solution to the problem?

A. Add a DNS server to your local subnet.

B. Add the mapping for the hostname server-1 to the IP address 10.1.1.1 in the local system's HOSTS file.

C. Add an A record to your local WINS server.

D. Add an MX record to your local DNS server.

10. You have one Active Directory forest in your organization that contains one domain named `Stellacon.com`. You have two domain controllers configured with the DNS role installed. There are two Active Directory Integrated zones named `Stellacon.com` and `Stellatest.com`. One of your IT members (who is not an administrator) needs to be able to modify the `Stellacon.com` DNS server, but you need to prevent this user from modifying the `Stellatest.com` SOA record. How do you accomplish this?

A. Modify the permissions of the `Stellacon.com` zone from the DNS Manager snap-in.

B. Modify the permissions of the `Stellatest.com` zone from the DNS Manager snap-in.

C. Run the Delegation Of Control Wizard in Active Directory.

D. Run the Delegation Of Control Wizard in the DNS snap-in.

Chapter

4

Configure Windows Server 2012 R2

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure file and share access**

- Create and configure shares
- Configure share permissions
- Configure offline files
- Configure NTFS permissions
- Configure access-based enumeration (ABE)
- Configure Volume Shadow Copy Service (VSS)
- Configure NTFS quotas
- Create and configure Work Folders

✓ **Configure print and document services**

- Configure the Easy Print print driver
- Configure Enterprise Print Management
- Configure drivers
- Configure printer pooling
- Configure print priorities
- Configure printer permissions

✓ **Configure servers for remote management**

- Configure WinRM
- Configure down-level server management
- Configure servers for day-to-day management tasks
- Configure multi-server management
- Configure Server Core
- Configure Windows Firewall
- Manage non-domain joined servers

This chapter explains how to set up your servers so that your network users have something to access. Before you can set up a server, you have to determine the purpose of it. Is it going to be a print server, a file storage server, a remote access server, or a domain controller?

After you have decided how the machine is going to help your network, you must implement your decision. In this chapter, I'll show you how to set up a print server and a file server. In addition, I will discuss how to set up permissions and security for these servers and how you can limit the amount of space your users can have on a server.

NOTE

Microsoft Windows Server 2012 and Windows Server 2012 R2 are used for all of the server types in this chapter. Although other operating systems can be used, this chapter refers only to Windows Server 2012 and Windows Server 2012 R2.

Understanding File Servers

Before you configure a file server, you must understand what a file server actually does. *File servers* are machines on your network that store data files to share among network clients. The same machine can be a file server and another type of server. For example, a machine can both host network files and run Exchange Server 2013. Such a machine would have both file server and application server functions. (*Application servers* are machines that host applications used by network clients.)

Real World Scenario

Multiple Server Types on One Machine

More than ever, in today's world most IT departments have to worry about budgets. The problem is that the IT department often has the smallest budget in a company. You are typically stuck between a rock and a hard place because if your network is running well, people (including executives) forget about you. This makes it hard when you ask for anything that may impact the budget.

Because of the lack of funds, often you will leverage one machine to perform many server tasks. I have seen several companies where the IT department had to have the same machine running both as an application server and as a file server.

You must consider various factors before allowing a machine to run multiple server types. How many processors do you have? What are the processor speeds? How much RAM does the machine have? What is the hard drive speed? What type of applications will be hosted on the machine?

After you have gathered all of the information about the machine, then you can decide whether the machine can host multiple server types. Keep this one fact in mind, however—because of the requirements and demands on the computer system, it's always a good idea to host SQL Server on a dedicated machine.

When setting up a file server, one of the most important things you will do is to set up work and personal folders for your users. I have been consulting for many years, and one thing I always stress to all of my clients is to perform regular backups. After all, most organizations would not be able to recover after losing all of their data. Usually, companies back up only their servers, and this is why home folders are so important. *Home folders* are one of the most common file types on a file server; they are folders set up on the server for users to store information. Users have a location on the server to store their important data, and therefore that data will be backed up when the company does its regular backups.

Home folders are just one example of how to use work folders on a file server. I will be discussing other examples throughout this chapter.

Configuring File Servers

Now that you have an understanding of what a file server does, it's time to discuss how to configure these servers. Setting up a file server properly encompasses many steps. As always, one major concern is security. In the following sections, I will first describe how to share and publish online and offline files and folders. Then I will discuss the two types of security—shared permissions and NTFS security—that an administrator can set when sharing files or folders.

Sharing Folders

A file server is for sharing and storing data. To use one, you need to know how to set up a share, or a shared folder, on your server. A *shared folder* is exactly what it says; it's a folder that is shared on your network so that users can access the data within that folder. As an administrator, you have the ability to determine which users can access which files within a shared folder.

One of the main goals of Active Directory is to make resources easy to find. Active Directory also makes it easy to determine which files are available to users. That being said, I will explain how Active Directory manages to publish shared folders.

Making Active Directory Objects Available to Users

With Active Directory, a system administrator can control which objects users can see. The act of making an Active Directory object available is known as *publishing*. The two main publishable objects are Printer objects and Shared work folder objects. The reason I list Shared work folders here is because personal folders for users are not normally published in Active Directory. You publish an object in Active Directory because you want an easy way for everyone to find resources. Ordinarily, you don't want everyone accessing someone's home folder, and this is why you don't normally publish home folders.

The general process for creating server shares and shared printers has remained unchanged from previous versions of Windows. You create the various objects (printers or folders) and then enable them for sharing.

To make these resources available via Active Directory, however, there's an additional step: You must publish the resources. Once an object has been published in Active Directory, clients will be able to find it.

When you publish objects in Active Directory, you should know the server name and share name of the resource. This information, however, doesn't matter to your users. A system administrator can change the resource to which an object points without having to reconfigure or even notify clients. For example, if you move a share from one server to another, all you need to do is update the Shared Folder's object's properties to point to the new location. Active Directory clients still refer to the resource with the same path and name as they used before.

Exercise 4.1 will walk you through the steps for sharing and publishing a folder for use on your network.

EXERCISE 4.1

Creating and Publishing a Shared Work Folder

1. Create a new folder in the root directory of your `C:` partition, and name it **`Test Share`**.
2. Right-click the `Test Share` folder, and choose Share With ➢ Specific People.

3. In the File Sharing dialog box, enter the names of users with whom you want to share this folder. In the upper box, enter **Everyone** and then click Add. Note that Everyone appears in the lower box. Click in the Permission Level column next to Everyone, and choose Read/Write from the drop-down menu. Then click Share.

4. You see a message that your folder has been shared. Click Done.
5. Open the Active Directory Users and Computers tool. Expand the current domain. Select New ➢ Shared Folder.
6. In the New Object – Shared Folder dialog box, type **Shared Folder Test** for the name of the folder. Then type the UNC path to the share (for example, **`\\serverA\Test Share`**). Click OK to create the share.

One of the main benefits of having all of your resource information in Active Directory is that you can easily find the information that you're seeking using the Find dialog box. When setting up objects in Active Directory, I recommend you always enter as much information as possible for the objects you're creating. The extra effort will pay off when your users start doing searches for these objects. The more information you enter, the more users can search to find the appropriate resource they need.

Access-Based Enumeration

Access-Based Enumeration (ABE) is a feature included with Windows Server 2012/2012 R2. ABE allows your domain users to list only the files and folders to which they have access when browsing content on the file server.

ABE helps eliminate domain users' issues that are caused by users connecting to file servers and seeing large numbers of files and folders the user cannot connect. ABE allows users only to see files and folders to which they have access.

Knowing that ABE is working on the Windows Server helps you set up your permissions properly. If you need to give a user the ability to see files and folders that they might not be able to change, you need to allow them at least to read or view the directories. As an administrator, it's important that you understand that Access-Based Enumeration is working on the server and what you need to do to get a user around it when needed.

Configuring Offline Files

If you have been in this industry long enough, you have seen a major change in end-user computers. Years ago, only a few select users had laptops. They were big and bulky, and they weighed almost as much as today's desktop computers.

The pendulum has swung in the opposite direction. It probably seems like every one of your end users now has a laptop. As an IT administrator, this gives you a whole new set of challenges and problems to address.

One challenge that you have to address is how users can work on files while outside of the office. If you have a user who wants to work at home, how do you give them the files they need to get their work done?

The answer is *offline folders*. These folders contain data that can be worked on by users while outside the office. An IT administrator can set up offline folders through the use of *Group Policy objects (GPOs)*.

When you decide to make folders available for offline use, these folders need to synchronize with the laptops so that all of the data matches between both systems. As an administrator, one decision that you will need to make is when the offline folders will

be synchronized. There are three synchronization options that you can set in a GPO (see Figure 4.1).

FIGURE 4.1 Synchronization options in a GPO

You can set up any combination of these options:

- When you select Synchronize All Offline Files Before Logging Off, offline folders are synchronized when the user logs off the network.
- When you select Synchronize All Offline Files When Logging On, offline folders are synchronized when the user logs on to the network.
- When you select Synchronize Offline Files Before Suspend, offline folders are synchronized before the user does a system suspend.

In Exercise 4.2, I will show you the steps necessary to configure offline folder options by using a GPO. This exercise uses the Group Policy Management Console (GPMC). If your GPMC is not installed, use the Server Manager MMC (under Features) to install it.

Group Policy objects will be covered in full detail in Chapter 6 "Manage GPOs."

EXERCISE 4.2

Configuring Offline Folder Options

1. Open the Group Policy Management Console.
2. In the left pane, expand your forest and then your domain. Under your domain name, there should be a default domain policy.
3. Right-click the default domain policy and choose Edit.
4. In the User Configuration section, expand Policies ➢ Administrative Templates ➢ Network and then click Offline Files.
5. Right-click Synchronize All Offline Files Before Logging Off and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.

6. Right-click Synchronize All Offline Files When Logging On and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.
7. Right-click Synchronize Offline Files Before Suspend and choose Edit. The GPO setting dialog box appears. Choose the Enabled option. In the Action drop-down box, make sure Quick is selected. Click OK.
8. Close the GPMC.

Now that you have set up a GPO for synchronization, it's time to share a folder for offline usage. In Exercise 4.3, you will set up a folder for offline access. You must complete Exercise 4.1 before doing this exercise.

EXERCISE 4.3

Configuring a Shared Network Folder for Offline Access

1. Right-click the `Test Share` folder that you created in Exercise 4.1 and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button.
3. When the Advanced Sharing dialog box appears, click the Caching button.
4. When the Offline Settings dialog box appears, choose the All Files And Programs That Users Open From The Shares Will Be Automatically Available Offline option. Click OK.

5. Click OK twice more to close the Properties dialog box.

Volume Shadow Copy Services

Windows includes a feature that allows you to create a point-in-time image of one or more volumes. The *Volume Shadow Copy Service (VSS)* is the feature within Windows that allows an administrator take an image (shadow copy) of one or more volumes. Shadow copies have the ability to provide both file system and application.

Shadow copies allow an administrator to back up shared folders to a remote location. Shadow copies are designed to help recover files that were accidentally deleted, that were overwritten, or that have become corrupt. One major advantage to shadow copies is that

open files can be backed up. This means that even if users are currently working on files in a shared folder that has shadow copies enabled, the shadow copies will continue to function.

Once administrators have configured and enabled shadow copies (using the Computer Management snap-in), network users can restore earlier versions of files. After the initial shadow copy of the shared folder is created, only changes are copied and not the entire file.

You can enable shadow copies of entire volumes.

The following are some of the settings that you can configure when setting up shadow copies:

Schedule You have the ability to set the schedule of the shadow copies. You can set this schedule to run daily, weekly, monthly, once, at system startup, at logon, or when the system is idle. You can also set the time at which the shadow copy will run.

Storage Locations An administrator needs to set the location of the shadow copy backup. If you are on a network, it is a good idea to place the shadow copy on a network drive.

Maximum Size You can set a maximum size on your shadow copies, or you can specify that they have no size limit. One of the predetermined settings is 64 shadow copies per volume.

In Exercise 4.4, you'll set up a volume to make shadow copies every Monday at 7 a.m. To set up the shadow copies, you will use the Computer Management MMC snap-in.

EXERCISE 4.4

Configuring a Shadow Copy on a Volume

1. Open Computer Management by pressing the Windows key and selecting Administrative Tools ➢ Computer Management.
2. Expand Storage and then right-click Disk Management. Choose All Tasks ➢ Configure Shadow Copies.
3. When the Shadow Copies dialog box appears, click the Settings button.
4. When the Settings windows appears, click the Schedule button.
5. In the Schedule window, set the schedule task to weekly and the start time for 7 a.m. Uncheck all of the days-of-the-week boxes except Mon. Click OK.
6. When the Settings window reappears, click OK.
7. If the Enable button is enabled, click it. Then click OK.
8. Exit the Computer Management MMC.

To recover a previous version of a file from a shadow copy, you use the `\\server_name\share_name` path. The operating system determines how you will gain access to the shared folders and shadow copies. Shadow copies are built into Windows XP (SP1), Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2. If you are using a different Microsoft operating system, you need to download the Shadow Copy Client Pack from the Microsoft download center.

VssAdmin Command

Another way to create, configure, and manage shadow copies is by using the `vssadmin.exe` command-line utility. The `vssadmin.exe` command allows you to create, delete, list, and resize shadow copies and shadow storage.

One area where the VSS is very important is during backups. When you back up open files, the VSS copies the data and helps back up open files. For example, when you are backing up a Microsoft Exchange server using a Unitrends backup server, the VSS Exchange writer is used. To see if the VSS writers are functioning properly, you can open a command prompt (with administrative privileges) and type in the following statement:

```
VSSAdmin list writers
```

This command will show you all the different VSS service writers and how those VSS writers are functioning properly.

Table 4.1 describes the `vssadmin.exe` command and the different commands associated with the `vssadmin` utility.

TABLE 4.1 `Vssadmin.exe` commands

Command	Description
Add ShadowStorage	Adds a new volume shadow copy storage association
Create Shadow	Creates a new volume shadow copy
Delete Shadows	Deletes volume shadow copies
Delete ShadowStorage	Deletes the volume shadow copy storage associations
List Providers	Lists registered volume shadow copy providers
List Shadows	Lists existing volume shadow copies
List ShadowStorage	Lists volume shadow copy storage associations
List Volumes	Lists volumes eligible for shadow copies
List Writers	Lists subscribed volume shadow copy writers
Resize ShadowStorage	Resizes a volume shadow copy storage association
Revert Shadow	Reverts a volume to a shadow copy
Query Reverts	Queries the progress of in-progress revert operations

Configuring Permissions

You have gone through the steps necessary to set up a shared folder, publish it to Active Directory, and set it up for offline access. Now you will see how you can protect these files and folders by using permissions.

You can secure folders using permissions in two ways, and you can secure files in one way. You can set up permissions and security through NTFS or through sharing.

Understanding NTFS

NTFS is an option that you have when you are formatting a hard drive. You can format a hard drive for a Microsoft operating system in three ways.

- File Allocation Table (FAT) is supported on older operating systems only (Server 2003, Server 2000, XP, and so on).
- FAT32 is supported in Windows Server 2012 R2.
- NTFS is supported in Windows Server 2012 R2.

NTFS has many advantages over FAT and FAT32. They include the following:

Compression Compression helps compact files or folders to allow for more efficient use of hard drive space. For example, a file that usually takes up 20MB of space might use only 13MB after compression. To enable compression, just open the Advanced Attributes dialog box for a folder and check the Compress Contents To Save Disk Space box (see Figure 4.2).

FIGURE 4.2 Setting up compression on a folder

Quotas *Quotas* allow you to limit how much hard drive space users can have on a server. Quotas are discussed in greater detail in the section "Configuring Disk Quotas."

Encryption *Encrypting File System (EFS)* allows a user or administrator to secure files or folders by using encryption. Encryption employs the user's security identification

(SID) number to secure the file or folder. To implement encryption, open the Advanced Attributes dialog box for a folder and check the Encrypt Contents To Secure Data box (see Figure 4.3).

FIGURE 4.3 Setting up encryption on a folder

If files are encrypted using EFS and an administrator has to unencrypt the files, there are two ways to do this. First, you can log in using the user's account (the account that encrypted the files) and unencrypt the files. Second, you can become a recovery agent and manually unencrypt the files.

If you use EFS, it's best not to delete users immediately when they leave a company. Administrators have the ability to recover encrypted files, but it is much easier to gain access to the user's encrypted files by logging in as the user who left the company and unchecking the encryption box.

Security One of the biggest advantages of NTFS is security. Security is one of the most important aspects of an IT administrator's job. An advantage of NTFS security is that the security can be placed on individual files and folders. It does not matter whether you are local to the share (in front of the machine where the data is stored) or remote to the share (coming across the network to access the data); the security is always in place with NTFS.

The default security permission is `Users = Read` on new folders or shares.

NTFS security is *additive*. In other words, if you are a member of three groups (Marketing, Sales, and R&D) and these three groups have different security settings, you get the highest level of permissions. For example, let's say you have a user by the name of wpanek who belongs to all three groups (Marketing, Sales, and R&D).

Figure 4.4 shows this user's permissions. The Marketing group has Read and Execute permissions to the `Stellacon Documents` folder. The Sales group has Read and Write, and the R&D group has Full Control. Since wpanek is a member of all three groups, wpanek would get Full Control (the highest level).

FIGURE 4.4 Security settings on the `Stellacon Documents` folder

The only time this does not apply is with the Deny permission. Deny overrides any other group setting. Taking the same example, if Sales has Deny permission for the `Stellacon Documents` folder, the user wpanek would be denied access to that folder. The only way around this Deny is if you added wpanek directly to the folder and gave him individual permissions (see Figure 4.5). Individual permissions override a group Deny. In this example, the individual right of wpanek would override the Sales group's Deny. The user's security permission for the `Stellacon Documents` folder would be Full Control.

FIGURE 4.5 Individual permissions

WARNING Give users only the permissions necessary to do their jobs. Do not give them higher levels than they need.

Understanding Shared Permissions

When you set up a folder to be shared, you have the ability to assign that folder's permissions. *Shared permissions* can be placed only on the folder and not on individual files. Files have the ability to inherit their permissions from the parent folder.

Shared folder permissions are in effect only when users are remote to the shared data. In other words, if computer A shares a folder called `Downloads` and assigns that folder shared permissions, those permissions would apply only if you connected to that share from a machine other than computer A. If you were sitting in front of computer A, the shared permissions would not apply.

Like NTFS permissions (discussed in the previous section), shared permissions are additive, so users receive the highest level of permissions granted by the groups of which they are members.

Also, as with NTFS permissions, the Deny permission (see Figure 4.6) overrides any group permission, and an individual permission overrides a group Deny.

FIGURE 4.6 Setting up permissions on a shared folder

The default shared permission is `Administrators = Full Control`. The shared permissions going from lowest to highest are Read, Change, Full Control, and Deny. Table 4.2 compares the two different types of permissions and security.

TABLE 4.2 NTFS security vs. shared permissions

Description	NTFS	Shared
Folder-level security.	Yes	Yes
File-level security.	Yes	No
In effect when local to the data.	Yes	No
In effect when remote to the data.	Yes	Yes
Permissions are additive.	Yes	Yes
Group Deny overrides all other group settings.	Yes	Yes
Individual settings override group settings.	Yes	Yes

How NTFS Security and Shared Permissions Work Together

When you set up a shared folder, you need to set up shared permissions on that folder. If you're using NTFS, you will also need to set up NTFS security on the folder. Since both shared permissions and NTFS security are in effect when the user is remote, what happens when the two conflict?

These are the two basic rules of thumb:

- The local permission is the NTFS permission.
- The remote permission is the more restrictive set of permissions between NTFS and shared.

This is easy to do as long as you do it in steps. Let's look at Figure 4.7 and walk through the process of figuring out what wpanek has for rights.

FIGURE 4.7 NTFS security and shared permissions example

As you can see, wpanek belongs to three groups (Marketing, Sales, and R&D), and all three groups have settings for the `Stellacon Documents` folder. In the figure, you will notice that there are two questions: Remote = ? and Local = ? That's what you need to figure out—what are wpanek's effective permissions when he is sitting at the computer that shares the folder, and what are his effective permissions when he connects to the folder from another computer (remotely)? To figure this out, follow these steps:

1. Add up the permissions on each side separately.

   Remember, permissions and security are *additive*. You get the highest permission. So, if you look at each side, the highest shared permission is the Read permission. The NTFS security side should add up to equal Full Control. Thus, now you have Read permission on shared and Full Control on NTFS.
2. Determine the local permissions.

   Shared permissions do not apply when you are local to the data. Only NTFS would apply. Thus, the local permission would be Full Control.

3. Determine the remote permissions.

   Remember, the remote permission is the most restrictive set of permissions between NTFS and shared. Since Read is more restrictive than Full Control, the remote permission would be Read.

Let's try another. Look at Figure 4.8, and see whether you can come up with wpanek's local and remote permissions.

FIGURE 4.8 NTFS security and shared permissions

Your answer should match the following:

Local = Read

Remote = Read

Remember, first you add up each side to get the highest level of rights. NTFS would be Read, and shared would be Full Control. The local permission is always just NTFS (shared does not apply to local permissions), and remote permission is whichever permission (NTFS or shared) is the most restrictive (which would be Read on the NTFS side).

Exercise 4.5 walks you through the process of setting both NTFS and shared permissions. You must complete Exercise 4.1 before doing this exercise.

EXERCISE 4.5

Configuring Shared and NTFS Settings

1. Right-click the `Test Share` folder you created in Exercise 4.1 and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button. (You will set the shared permissions first.)
3. Click the Permissions button. Click the Add button. When the Select User page appears, choose a group from Active Directory. (I used the Sales group.) Once you find your group, click OK.

EXERCISE 4.5 *(continued)*

4. The Permissions dialog box appears. With your group highlighted, click the Allow check box next to Full Control and click OK. (All of the other Allow check boxes will automatically become checked.)
5. On the Advanced Sharing page, click OK. Now click the Security tab. (This allows you to set the NTFS security settings.)
6. Click the Edit button. That takes you to the Permissions page. Now click the Add button. When the Select User page appears, choose a group from Active Directory. (I used the Everyone group.) Once you find your group, choose OK.
7. The Permissions dialog box appears. With your group highlighted, click the Allow check box next to Modify, and click OK. (All of the check boxes below Modify will automatically become checked.)
8. Click Close.

Configuring Disk Quotas

In this chapter so far, you have seen how to set up a share and publish it to Active Directory. You've also learned how to set up permissions and security and how NTFS and shared permissions work with each other. It's time to learn how to limit users' hard drive space on the servers.

Disk quotas give administrators the ability to limit how much storage space a user can have on a hard drive. As mentioned earlier in this chapter, disk quotas are an advantage of using NTFS over FAT32. If you decide to use FAT32 on a volume or partition, quotas will not be available.

You have a few options available to you when you set up disk quotas. You can set up disk quotas based on volume or on users.

A good rule of thumb is to set up an umbrella quota policy that covers the entire volume and then let individual users exceed the umbrella as needed.

Setting Quotas by Volume One way to set up disk quotas is by setting the quota by volume, on a per-volume basis. This means that if you have a hard drive with `C:`, `D:`, and `E:` volumes, you would have to set up three individual quotas—one for each volume. This is your umbrella. This is where you set up an entire disk quota based on the volume for all users.

Setting Quotas by User You have the ability to set up quotas on volumes by user. Here is where you would individually let users have independent quotas that exceed your umbrella quota.

Specifying Quota Entries You use quota entries to configure the volume and user quotas. You do this on the Quotas tab of the volume's Properties dialog box. (See Exercise 4.6.)

Creating Quota Templates Quota templates are predefined ways to set up quotas. Templates allow you to set up disk quotas without needing to create a disk quota from scratch. One advantage of using a template is that when you want to set up disk quotas on multiple volumes (`C:`, `D:`, and `E:`) on the same hard drive, you do not need to re-create the quota on each volume.

Exercise 4.6 will show you how to set up an umbrella quota for all users and then have an individual account in your Active Directory exceed this quota.

EXERCISE 4.6

Configuring Disk Quotas

1. Open Windows Explorer.
2. Right-click the local disk (`C:`) and choose Properties.
3. Click the Quotas tab.
4. Check the Enable Quota Management check box. Also check the Deny Disk Space To Users Exceeding Quota Limit box.
5. Click the Limit Disk Space To option and enter **1000MB** in the box.
6. Enter **750MB** in the Set Warning Level To boxes.
7. Click the Apply button. If a warning box appears, click OK. This warning is just informing you that the disk may need to be rescanned for the quota.
8. Now that you have set up an umbrella quota to cover everyone, you'll set up a quota that exceeds the umbrella. Click the Quota Entries button.
9. The Quotas Entries for (`C:`) window appears. You will see some users already listed. These are users who are already using space on the volume. Click the Quota menu at the top and choose New Quota Entry.

   Notice the N/A entry in the Percent Used column. This belongs to the administrator account, which by default has no limit.
10. On the Select User page, choose a user that you want to allow to exceed the quota (for this example, I used the wpanek account). Click OK.
11. This opens the Add New Quota Entry dialog box. Click the Do Not Limit Disk Usage option and click OK.
12. You will notice that the new user has no limit. Close the disk quota tool.

Configuring Print Services

One of the most important components on a network is the printer. Printers today are almost as important as the computers themselves. Think about your network. What would your network be like without a printer? Even small networks or home networks have a printer today.

How many printers do you want on your network? It is not feasible to put a printer on every user's desk. What if some users need black and white while others need color? Do you give each user two printers? What if they need laser printing for reports but ink-jets will work fine for every other type of print job? These are all questions that you must answer before buying any printers for your networks.

This is also where network printers and print servers come into play. *Network printers* are printers that can be directly connected to the network through some form of network interface card. These printers usually have settings that can be configured for your network needs. For example, if your network uses DHCP, you can set the printer to be a DHCP client.

Print servers are servers that have a connected printer, where the server handles all printing issues. This is an excellent solution for printers that cannot directly connect to the network. Once the printer is connected to the network (through the use of a NIC or a server), the end user just connects to the printer and prints. To the end user, there is no real difference between the two options.

Before an end user can print to a network printer, an administrator must connect, set up, share, and publish the printer for use. An administrator must also set the permissions on the printer to allow users to print to that printer. The following sections will discuss these items in detail.

Creating and Publishing Printers

Once your printer is installed, you must share the printer and then publish the printer to Active Directory before users can print to it. Printers can be published easily within Active Directory. This makes them available to users in your domain.

Exercise 4.7 walks you through the steps you need to take to share and publish a Printer object by having you create and share a printer. To complete the printer installation, you need access to the Windows Server 2012 installation media (via the hard disk, a network share, or the CD/DVD drive). If you do not have a printer for this exercise, just choose one from the list and continue the exercise.

EXERCISE 4.7

Creating and Publishing a Printer

1. Press the Windows key and select ➢ Control Panel ➢ Devices and Printers ➢ Add Printer. This starts the Add Printer Wizard.

2. On the Add Printer page, click the link The Printer That I Want Isn't Listed.
3. Choose Add A Local Printer and click Next.
4. On the Choose A Printer Port page, select Use An Existing Port. From the drop-down list beside that option, make sure LPT1: (Printer Port) is selected. Click Next.
5. On the Install The Printer Driver page, select Generic for the manufacturer, and for the printer, highlight Generic/Text Only. Click Next.
6. If a driver page appears, choose Use The Driver That Is Currently Installed and click Next.
7. On the Type A Printer Name page, enter **Text Printer**. Uncheck the Set As The Default Printer box and then click Next.
8. The Installing Printer page appears. After the system is finished, the Printer Sharing page appears. Make sure the Share This Printer So That Others On Your Network Can Find And Use It box is selected, and accept the default share name of Text Printer.
9. In the Location section, type **Building 203**, and in the Comment section, add the following comment: **This is a text-only printer**. Click Next.
10. On the You've Successfully Added Text Printer page, click Finish.
11. Next you need to verify that the printer will be listed in Active Directory. Right-click the Text Printer icon, and select Text Printer Properties.
12. Next select the Sharing tab and make sure that the List In The Directory box is checked. Click OK to accept the settings.

13. Close the printer Properties box, and close Devices And Printers.

Note that when you create and share a printer this way, an Active Directory Printer object is not displayed within the Active Directory Users and Computers tool.

Configuring Printers

The printer has now been installed and published to Active Directory. It's time to set all of the different configuration options. To get to the options, right-click the Printer object and choose Properties.

The following are just some of the tabs you can configure:

The General Tab The General tab (see Figure 4.9) allows you to set some basic printer attributes.

- The field at the top of the dialog box contains the display name of the Printer object.
- The Location field should contain text that helps users physically locate the printer. This allows users to search for printers based on location (location-aware printing).
- The Comment field allows an administrator to put in any additional information, such as the printer type.
- The Printing Preferences button takes you to controls that allow you to change the layout and paper type of the printer.

FIGURE 4.9 The General tab of the printer's Properties dialog box

The Sharing Tab The Sharing tab (see Figure 4.10) allows you to configure your printer for sharing on your network. This is what allows users to use a network printer (if they have the proper permissions on the printer).

- The Share This Printer check box allows you to share the printer on the network.
- Share Name is the name your users will see on the network.
- When Render Print Jobs On Client Computers is checked, the client computer caches the print job until the printer is ready to print. If unchecked, the print server will cache the entire job before it prints to the printer.
- When List In The Directory is checked, users can search the directory for the printer.
- The Additional Drivers button allows you to load additional drivers for your clients. It is especially useful for giving access to drivers for older client systems. One advantage of a print server is that the server will automatically download drivers to client computers.

FIGURE 4.10 The Sharing tab of the printer's Properties dialog box

The Ports Tab The Ports tab (see Figure 4.11) allows you to configure the port to which your printer is connected. You can add ports or configure existing ports.

- The Port check boxes allow you to choose to which port your printer is connected. Options are the printer port, serial port, local port, and print to file port.
- The Add Port button allows you to add a custom port (for example, a TCP/IP port).

- The Delete Port button allows you to remove a port from the Port list.
- The Configure Port button gives you settings to configure an existing port. For example, if you use TCP/IP, this button allows you to change the TCP/IP options.
- Enable Bidirectional Support allows your printer and computer to communicate back and forth. If this check box is disabled, your printer cannot support two-way communications.
- A *printer pool* allows two or more identical printers to share the print load. When a document is sent to the printer pool, the first available printer receives the print job and prints it. Enable Printer Pooling allows a large department or organization to get print jobs done faster. Users do not have to wait for one printer to get their print job. You should follow these rules when setting up a printer pool:
  - All printers in the pool need to be the same model and type.
  - All printers in the pool should be in the same physical location. Print jobs will be printed to the first available printer. If these printers are located all over the company, it may take a user too long to find their print job.

FIGURE 4.11 The Ports tab of the printer's Properties dialog box

The Advanced Tab The Advanced tab (see Figure 4.12) is where you can set availability, priority, and many other options.

- The availability controls let you set the hours when this printer can be used. You can set it to be always available or available only between the hours you set.
- If multiple print shares are set up to go to the same printer, you can specify a printer priority with the Priority field for each share. The higher the number, the faster a print job sent to that share will access the printer. The highest priority is 99, and the default

(lowest) is 1. If two users send jobs to the same printer at the same time, one with a 99 priority and the other with a 1 priority, the 99 priority would print first.

- Driver is the default printer driver that the printer is using.
- The print spooling controls let you decide how the print job will spool. You can choose to have the entire job spool first before printing (this ensures that the entire job is received by the print queue before printing), to start printing immediately while the job is still spooling, or to print directly to the printer without spooling. (The last option requires a printer with a large amount of RAM on the motherboard.)
- Hold Mismatched Documents allows the spooler to hold any print jobs that don't match the setup for the print device.
- Print Spooled Documents First allows a completely spooled printer job to be printed first even if it has a lower priority number than a job that is still spooling.
- Usually, after a print job has been printed, the print queue deletes the print job. If you check the Keep Printed Documents box, the print queue will not delete the print job after it is printed.
- Enable Advanced Printing Features allows you to set some advanced features such as the Page Order and Pages Per Sheet settings.

FIGURE 4.12 Advanced tab of the printer's Properties dialog box

The Color Management Tab This tab allows you to adjust the color of your printing jobs.

The Security Tab The Security tab (see Figure 4.13) is where you can set the permissions for your printer. This allows users to print, manage printers, manage documents, and take advantage of special permissions.

- The Add button allows you to add users and groups to the printer.
- The Remove button allows you to remove users and groups from the printer.
- The following controls, available in the Permissions For Everyone box, apply to everyone on your network:
    - Print gives everyone the right to print to this printer.
    - Manage Printers gives everyone the right to manage this printer, including deleting print jobs, setting priorities, setting availability, and so on.
    - Manage Documents gives everyone the right to manage print jobs.
    - Special Permissions allows you to set unique permissions such as Print, Manage Printers, Read permissions, Change permissions, and Take Ownership.

FIGURE 4.13 Security tab of the printer's Properties dialog box

Migrating Print Servers

In a network environment, an administrator may find it necessary to replace older print servers or to consolidate multiple print servers into one. To do this print server migration or

replacement, you can use the Printer Migration Wizard or the `Printbrm.exe` command-line tool. These two utilities allow you to export print queues, printer settings, printer ports, and language monitors. These utilities then allow you to import these settings on another print server running Windows Server 2012 R2.

Printer Pooling

In a large organization, one issue that you may run into when you print a document to a print device is that you may have to wait a while for that document to print. If you have hundreds of print jobs being sent to a print device, it could take time until your print job appears on the print device. This is where printer pools can help.

A *printer pool* allows an administrator to associates multiple printers (identical print devices) with a single set of printer software. When you send a print job to a device, the print job will print to the first available device in the printer pool. This allows print jobs to print faster to multiple devices. For this to work, you must make sure that all devices are in the same physical area. You do not want a user traveling all over the company looking for their print job because they don't know which device printed the job.

To set up a printer to print to multiple devices, follow these steps:

1. Open Devices and Printers.
2. Right-click the printer you are using and then click Printer Properties.
3. On the Ports tab, select the Enable Printer Pooling check box.
4. Click each port where the printers you want to pool are connected.

Easy Print Driver

One printer configuration that is a little different from normal is when you are setting up a printer for a Remote Desktop server. However, Microsoft has included a feature to help. That feature is called the *Easy Print Driver*.

Remote Desktop Services gives you the ability to do printer redirection. What this means is Remote Desktop can route printing jobs from a server to a printer that is attached to a client computer. On an RD Session Host server, an administrator has the ability to use the Remote Desktop Easy Print printer driver to help simplify printer configuration.

The RD Session Host server first tries to use the Remote Desktop Easy Print driver, and if the RD client computer does not support this driver, the server looks for a matching printer driver on the server.

Configuring Remote Management

As an administrator, sometimes you might need to manage a server remotely. There are a few different tools you can use to do this task. You can use remote administration to help configure services on a Windows Server 2012 R2 system. The following sections cover Windows Remote Management and Windows PowerShell.

Windows PowerShell does not always have to be used remotely. For example, you can use Windows PowerShell when configuring a Windows Server 2012 R2 Server Core installation locally.

Windows Remote Management

The *Windows Remote Management (WinRM) utility* is Microsoft's version of the WS-Management protocol, an industry-standard protocol that allows different vendors' operating systems and hardware to work together. There are three main ways to access the WinRM utility:

- WinRM command-line tool
- WinRM scripting objects
- Windows Remote Shell command-line tool

The WinRM utility allows you to execute commands remotely and obtain management data from local and remote computers. You can use the WinRM utility on both Windows-based operating systems and non-Windows-based operating systems.

When using the WinRM utility, you can use the `-machine` switch to indicate the remote machine to which you are connecting. When connecting to a machine, you can connect using the localhost name, the NetBIOS name, the fully qualified domain name (FQDN), or the IP address of the remote machine. The following is an example of a WinRM command using a FQDN name on the secure port 443:

```
winrm get -machine:server.stellacon.local -port:443
```

Table 4.3 shows the command-line WinRM commands and descriptions of what each command does.

TABLE 4.3 WinRM commands and descriptions

Command	Description
`WinRM g` or `WinRM get`	Retrieves management information
`WinRM s` or `WinRM set`	Modifies management information
`WinRM c` or `WinRM create`	Creates a new instance on the managed resources
`WinRM d` or `WinRM delete`	Removes an instance from a managed resource
`WinRM e` or `WinRM enumerate`	Lists all instances of a managed resource
`WinRM i` or `WinRM invoke`	Executes a method on a managed resource
`WinRM id` or `WinRM identity`	Determines whether a WS-Management implementation is running on a remote machine

`WinRM quickconfig`	Configures a machine to accept WS-Management commands from a remote machine
`WinRM configSDDL`	Modifies an existing security descriptor for a Uniform Resource Identifier (URI)
`WinRM helpmsg`	Displays error messages for an error code

Now that you have looked at WinRM, let's take a look at how to use the Windows PowerShell utility.

Windows PowerShell

Windows PowerShell is a task-based, command-line scripting utility that allows you to execute commands locally or remotely on a Windows Server 2012 R2 machine. It was specifically designed for system administrators to allow for local or remote administration.

Microsoft asks a lot of questions on the exam about Windows PowerShell. Therefore, I will be discussing PowerShell throughout this book because of its importance on all of the Windows Server 2012 R2 exams.

Most operating system shells, including `Cmd.exe` and the SH, KSH, CSH, and BASH Unix shells, work by running a command or utility in a new process and then presenting the results to the user as text. These system shells also have commands that are built into the shell and execute in the shell process. In most system shells, because there are only a few built-in commands, many utilities have been created over the years to complete tasks.

Windows PowerShell contains an interactive prompt and a scripting environment that can be used independently or in combination. Unlike the previously mentioned system shells, which accept and return text, Windows PowerShell is built using the *.NET Framework common language runtime (CLR)* and the .NET Framework. Because of this, Windows PowerShell accepts and returns .NET Framework objects. This important change in the shell allows you to use entirely new tools and methods to manage and configure Windows.

Windows PowerShell introduced the concept of using cmdlets (pronounced "command-lets"). Cmdlets are simple, single-function command-line tools built into the shell. Administrators can use the cmdlets independently, or they can combine these tools to execute complex tasks and harness the true power of PowerShell. Windows PowerShell includes more than a hundred core cmdlets, but the true advantage of PowerShell is that anyone can write their own cmdlets and share them with other users.

Administrators often automate the management of their multicomputer environments by running sequences of long-running tasks, or *workflows*, which can affect multiple managed computers or devices at the same time. Windows PowerShell can help administrators accomplish workflows in a more effective way. Windows PowerShell includes some of the following advantages:

Windows PowerShell Scripting Syntax Administrators can use Windows PowerShell scripting expertise to create script-based tasks by using the extensible Windows PowerShell language. Windows PowerShell script-based tasks are easy to create, and IT members can share them easily by entering them into an email or publishing them on a web page.

Day-to-Day Management tasks Windows PowerShell allows administrators to configure and maintain servers. PowerShell allows you to pre-create scripts or use ready-to-use scripts to handle day-to-day tasks. This way, an administrator can just run a script to complete server configurations or management.

Multiserver Management Administrators can concurrently apply workflow tasks to hundreds of managed servers and computers. Windows PowerShell includes common parameters to set workflows automatically, such as `PSComputerName`, to enable multicomputer administrative scenarios.

Single Task to Manage Complex, End-to-End Processes Administrators can combine related scripts or commands that act upon an entire scenario into a single workflow. The status of activities within the workflow can be viewed at any time.

Automated Failure Recovery Using Windows PowerShell allows workflows to survive both planned and unplanned interruptions, such as computer restarts. Administrators have the ability to suspend workflow operations and then restart or resume the workflow from the exact point at which it was suspended. Administrators can then create checkpoints as part of their workflow process so that they can resume the workflow from the last persisted task (or checkpoint) instead of restarting the workflow from the beginning.

Activity Retries Administrators can create workflows that also specify activities that must rerun if the activity does not get completed on one or more managed computers (for example, if a target node was not online at the time the activity was running).

Connect and Disconnect Administrators can connect and disconnect from the node that is executing the workflow, but the workflow will continue to run.

Configuring Non-Domain Servers Another advantage of PowerShell is the ability to configure non-domain servers from a Windows Server 2012 R2 server (domain member). When you are running commands on the non-domain machine, you must have access to the non-domain machine's system administrator account. Another way to configure a non-domain server is to connect through remote desktop into the non-domain server and then configure the machine or run PowerShell commands while connected through remote desktop.

Task Scheduling Workflow tasks have the ability to be scheduled and started when specific conditions are met. This is also true for any other Windows PowerShell cmdlet or script.

Table 4.4 defines a few of the cmdlets available in Windows PowerShell. Again, there are hundreds of cmdlets, and the ones listed in the table are just some of the more common ones. You can retrieve a list of all the cmdlets starting here:

`http://technet.microsoft.com/en-us/scriptcenter/dd772285.aspx`

TABLE 4.4 Windows PowerShell cmdlets

Cmdlet	Definition
`Clear-History`	Deletes entries from the command history
`Invoke-command`	Runs commands on local or remote computers
`Start-job`	Starts a Windows PowerShell background job
`Stop-job`	Stops a Windows PowerShell background job
`Remove-job`	Deletes a Windows PowerShell background job
`Import-Module`	Adds modules to the current session
`Receive-job`	Gets the results of a Windows PowerShell background job
`Format-table`	Shows the results in a table format
`Out-file`	Sends the job results to a file
`Get-Date`	Gets the date and time
`Set-Date`	Sets the system time and date on a computer
`Get-event`	Gets an event in the event queue
`New-event`	Creates a new event
`Trace-command`	Configures and starts a trace of a command on a machine
`Get-WindowsFeature`	Gets a list of available and installed roles and features on the local server
`Get-WindowsFeature -ServerName`	Gets a list of available and installed roles and features on a remote server
`Get-Help Install-WindowsFeature`	Gets the syntax and accepted parameters for the `Install-WindowsFeature` cmdlet
`Uninstall-WindowsFeature`	Removes a role or feature
`Get-NetIPAddress`	Gets information about IP address configuration
`Set-NetIPAddress`	Modifies IP address configuration properties of an existing IP address
`Set-NetIPv4Protocol`	Modifies information about the IPv4 protocol configuration

Windows PowerShell Commands

I will show you Windows PowerShell commands throughout this book. If I show you how to install a role or feature in Server Manager, I will also include the Windows PowerShell equivalent.

Another advantage of Windows PowerShell is that it allows you to gain access to a file system on a computer and to access the registry, digital certificate stores, and other data stores.

Complete Exercise 4.8 to start the Windows PowerShell utility in the Windows Server 2012 R2 Server Core machine installed in the previous exercise.

EXERCISE 4.8

Starting the Windows PowerShell Utility

1. Type **`Start PowerShell`** at the Windows Server 2012 R2 Server Core command prompt.
2. When the Windows PowerShell utility starts, type **`Help`** and press Enter. This will show you the Windows PowerShell syntax and some of the commands included in Windows PowerShell.
3. At the Windows PowerShell command prompt, type **`Get-Date`**. This will show you the system's date and time.
4. At the Windows command prompt, type **`Help *`**. This will show you all of the cmdlets you can use.
5. Close the Windows PowerShell utility by typing **`Exit`**.

Configuring Down-Level Servers

As an administrator, sometimes you might have to configure a Windows Server 2008 R2 server from a Windows Server 2012 R2 machine. This is referred to as configuring a *down-level server*.

When you install Windows Server 2012 R2, Server Manager can be used to configure and manage a down-level server as long as that down-level server is running one of the following operating systems:

- Windows Server 2008 R2 SP1 (either full server or a Server Core installation)
- Windows Server 2008 SP2 (full server only)

To be able to configure the Windows Server 2008/2008 R2 servers remotely, you must first install Windows Management Framework 3.0 (WMF 3.0) and all of its prerequisites on the Windows Server 2008/2008 R2 servers. No special configuration is required on the Windows Server 2012 R2 server.

If you need to install WMF 3.0 on a Windows Server 2008 R2 Server Core installation, you can do this by using the Deployment Image Servicing and Management (DISM) commands. The command names that you would use for these features are as follows:

- MicrosoftWindowsPowerShell
- MicrosoftWindowsPowerShell-WOW64
- NetFx2-ServerCore
- NetFx2-ServerCore-WOW64

To run these commands, you would run the following in Server Core:

```
Dism /online /enable-feature: <Feature Name>
```

It is important to remember that Dism is case-sensitive in the command shown here.

Configuring Server Core

When configuring servers remotely, an administrator may have to configure a Server Core system. Let's take a look at some of the Server Core commands that can be used to do some basic server configurations.

When configuring Server Core, you may need to set the system for a static TCP/IP address. Use the following Windows PowerShell commands:

- `Get-NetIPConfiguration` allows you to view your current network configuration.
- `Get-NetIPAddress` allows you to view the IP addresses you are currently using.

If you want to set your static TCP/IP address, do the following:

1. In Windows PowerShell, run `Get-NetIPInterface`.
2. Write down the number shown in the `IfIndex` column of the output for the IP interface or the `InterfaceDescription` string for the network adapter you want to change.
3. In Windows PowerShell, run `New-NetIPAddress –InterfaceIndex 10 –IPAddress –192.168.15.2 –PrefixLength 24 –DefaultGateway –192.168.15.1`.
   - `InterfaceIndex` is the value of `IfIndex` from step 2 (in this example, `10`).

- `IPAddress` is the static IP address you intend to set (in this example, `192.168.15.2`).
- `PrefixLength` is the prefix length (another form of subnet mask) for the IP address you intend to set (in this example, `24`).
- `DefaultGateway` is the default gateway (in this example, `192.168.15.1`).

4. In Windows PowerShell, run `Set-DNSClientServerAddress -InterfaceIndex 10 -ServerAddresses 192.168.15.4`.
   - `InterfaceIndex` is the value of `IfIndex` from step 2.
   - `ServerAddresses` is the IP address of your DNS server.
5. To add multiple DNS servers, run `Set-DNSClientServerAddress -InterfaceIndex 10 -ServerAddresses 192.168.15.4,192.168.15.5`.
   - In this example, `192.168.15.4` and `192.168.15.5` are both IP addresses of DNS servers.

Another Server Core task that you may need to configure is setting the server name. In PowerShell, run the following command to rename the server: `Rename-Computer`.

As an administrator, you may also want to run PowerShell commands on one system to run on another system. You can enable Windows PowerShell Remoting by using the `Enable-PSRemoting` command.

Configuring the Windows Firewall

The final item to examine is configuring Windows Firewall remotely. Microsoft Server 2012 R2 Windows Firewall will be discussed in full detail in Chapter 6, but since I am discussing remote administration, let's look at the commands needed to configure Windows Firewall remotely.

`Netsh advfirewall` is a command-line (with Administrator privileges) tool for Windows Firewall with Advanced Security that helps with the creation, administration, and monitoring of Windows Firewall and IPsec settings and provides an alternative to console-based management.

To enter into the `netsh advfirewall` prompt, you must first type **`netsh`**. After you enter the `netsh` prompt, you then type **`advfirewall`**, which will bring you to the `netsh advfirewall` prompt. When you enter `netsh advfirewall`, it enters you into a `netsh advfirewall` prompt that looks like the following:

```
netsh advfirewall> prompt
```

Once you are at the `netsh firewall` prompt, you can use the question mark to get a list of all available options (`netsh advfirewall>?`). Figure 4.14 shows you the list of available options.

FIGURE 4.14 Netsh advfirewall options

```
Administrator: Command Prompt - netsh
netsh advfirewall>?

The following commands are available:

Commands inherited from the netsh context:
..              - Goes up one context level.
abort           - Discards changes made while in offline mode.
add             - Adds a configuration entry to a list of entries.
advfirewall     - Changes to the `netsh advfirewall' context.
alias           - Adds an alias.
bridge          - Changes to the `netsh bridge' context.
bye             - Exits the program.
commit          - Commits changes made while in offline mode.
delete          - Deletes a configuration entry from a list of entries.
dhcpclient      - Changes to the `netsh dhcpclient' context.
dnsclient       - Changes to the `netsh dnsclient' context.
exit            - Exits the program.
firewall        - Changes to the `netsh firewall' context.
http            - Changes to the `netsh http' context.
interface       - Changes to the `netsh interface' context.
ipsec           - Changes to the `netsh ipsec' context.
lan             - Changes to the `netsh lan' context.
mbn             - Changes to the `netsh mbn' context.
namespace       - Changes to the `netsh namespace' context.
nap             - Changes to the `netsh nap' context.
netio           - Changes to the `netsh netio' context.
offline         - Sets the current mode to offline.
online          - Sets the current mode to online.
p2p             - Changes to the `netsh p2p' context.
popd            - Pops a context from the stack.
pushd           - Pushes current context on stack.
quit            - Exits the program.
ras             - Changes to the `netsh ras' context.
rpc             - Changes to the `netsh rpc' context.
set             - Updates configuration settings.
show            - Displays information.
trace           - Changes to the `netsh trace' context.
unalias         - Deletes an alias.
wcn             - Changes to the `netsh wcn' context.
wfp             - Changes to the `netsh wfp' context.
winhttp         - Changes to the `netsh winhttp' context.
winsock         - Changes to the `netsh winsock' context.
wlan            - Changes to the `netsh wlan' context.
```

Summary

In this chapter, I discussed file servers and how they can be effective on your network. I also discussed sharing folders for users to access, and then I discussed how to publish those shared folders to Active Directory.

You learned about NTFS security versus shared folder permissions and how to limit users' hard drive space by setting up disk quotas. The chapter also covered the Encrypting File System (EFS) and how users can encrypt and compress files.

I talked about print servers and configuring printers. I talked about how to share and publish printers within Active Directory as well as print permissions, printer priorities, and print pooling.

You then took a look at remote configuration and a few tools that allow you to configure servers.

- Windows Remote Management lets you configure a server remotely from another machine.
- PowerShell is an important tool in the Windows Server 2012 R2 arsenal. Microsoft has been moving the industry toward PowerShell, and there will be many questions on the exam about PowerShell.
- `Netsh` allows you to configure Windows Firewall remotely.

Exam Essentials

Learn How Resources Can Be Published A design goal for Active Directory was to make network resources easier for users to find. With that in mind, you should understand how using published printers and shared folders can simplify network resource management.

Know How to Configure Offline Folders Offline folders give you the opportunity to set up folders so that users can work on the data while outside the office and later synchronize it with a master copy. You can set up GPOs to help with offline folder synchronization.

Know How to Configure NTFS Security One of the major advantages of using NTFS over FAT32 is access to additional security features. NTFS allows you to put security at the file and folder layers. NTFS security is in effect whether the user is remote or local to the computer with the data.

Know How to Configure Shared Permissions Shared permissions allow you to determine the access a user will receive when connecting to a shared folder. Shared permissions are allowed only at the folder layer and are in effect only when the user is remote to the computer with the shared data.

Understand How NTFS and Shared Permissions Work Together NTFS and shared permissions are individually additive—you get the highest level of security and permissions within each type. NTFS is always in effect, and it is the only security available locally. Shared permissions are in effect only when connecting remotely to access the shared data. When the two types of permissions meet, the most restrictive set of permissions applies.

Know How to Configure Disk Quotas Disk quotas allow an organization to determine the amount of disk space that users can have on a volume of a server. An administrator can set up disk quotas based on volumes or by users. Each volume must have its own separate set of disk quotas.

Know How to Configure Printing I discussed network printers versus print servers. Understand that when you create a printer, you want to publish the printer within Active Directory so that your users can find it throughout the domain. Understand the different printer permissions and how to install print drivers.

Understand Windows PowerShell Understanding Windows PowerShell is not only important for the exam; it will also allow you to configure Server Core more efficiently. Windows PowerShell is a command-line utility that allows you run single cmdlets as well as run complex tasks to exploit the full power from PowerShell.

Review Questions

1. The company for which you work has a multilevel administrative team that is segmented by departments and locations. There are four major locations, and you are in the Northeast group. You have been assigned to the administrative group that is responsible for creating and maintaining network shares for files and printers in your region. The last place you worked had a large Windows Server 2003 network, where you had a much wider range of responsibilities. You are excited about the chance to learn more about Windows Server 2012 R2.

   For your first task, you have been given a list of file and printer shares that need to be created for the users in your region. You ask how to create them in Windows Server 2012 R2, and you are told that the process of creating a share is the same as with Windows Server 2003. You create the shares and use `NETUSE` to test them. Everything appears to work fine, so you send out a message that the shares are available. The next day, you start receiving calls from users who say they cannot see any of the resources you created. What is the most likely reason for the calls from the users?

   A. You forgot to enable NetBIOS for the shares.

   B. You need to force replication for the shares to appear in the directory.

   C. You need to publish the shares in the directory.

   D. The shares will appear within the normal replication period.

2. You want to publish a printer to Active Directory. Where would you click in order to accomplish this task?

   A. The Sharing tab

   B. The Advanced tab

   C. The Device Settings tab

   D. The Printing Preferences button

3. A system administrator creates a local Printer object, but it doesn't show up in Active Directory when a user executes a search for all printers. Which of the following are possible reasons for this? (Choose all that apply.)

   A. The printer was not shared.

   B. The printer is offline.

   C. The client does not have permission to view the printer.

   D. The printer is malfunctioning.

4. You are the network administrator for a midsize coffee bean distributor. Your company's network has four Windows 2012 R2 servers, and all of the clients are running either Windows 8 or Windows 7. Most of your end users use laptops to do their work, and many of them work away from the office. What should you configure to help them work on documents when away from the office?

A. Online file access

B. Offline file access

C. Share permissions

D. NTFS permissions

5. Your company has decided to implement a Windows 2012 R2 server. The company IT manager who came before you always used FAT32 as the system partition. Your company wants to know whether it should move to NTFS. Which of the following are some advantages of NTFS? (Choose all that apply.)

A. Security

B. Quotas

C. Compression

D. Encryption

6. Will, the IT manager for your company, has been asked to give Moe the rights to read and change documents in the `Stellacon Documents` folder. The following table shows the current permissions on the shared folder:

Group/User	NTFS	Shared
Sales	Read	Change
Marketing	Modify	Change
R&D	Deny	Full Control
Finance	Read	Read
Tylor	Read	Change

Moe is a member of the Sales and Finance groups. When Moe accesses the `Stellacon Documents` folder, he can read all of the files, but the system won't let him change or delete files. What do you need to do to give Moe the minimum amount of rights to do his job?

A. Give Sales Full Control to shared permissions.

B. Give Moe Full Control to NTFS security.

C. Give Finance Change to shared permissions.

D. Give Finance Modify to NTFS security.

E. Give Moe Modify to NTFS security.

7. You are the administrator of your network, which consists of two Windows Server 2012 R2 systems. One of the servers is a domain controller, and the other server is a file server for data storage. The hard drive of the file server is starting to fill up. You do not have the ability to install another hard drive, so you decide to limit the amount of space everyone gets on the hard drive. What do you need to implement to solve your problem?

A. Disk spacing

B. Disk quotas

C. Disk hardening

D. Disk limitations

8. You are the IT manager for your company. You have been asked to give the Admin group the rights to read, change, and assign permissions to documents in the `Stellacon Documents` folder. The following table shows the current permissions on the `Stellacon Documents` shared folder:

Group/User	NTFS	Shared
Sales	Read	Change
Marketing	Modify	Change
R&D	Deny	Full Control
Finance	Read	Read
Admin	Change	Change

What do you need to do to give the Admin group the rights to do their job? (Choose all that apply.)

A. Give Sales Full Control to shared permissions.

B. Give Full Control to NTFS security.

C. Give Admin Full Control to shared permissions.

D. Give Finance Modify to NTFS security.

E. Give Admin Full Control to NTFS security.

9. You have been asked to configure a Windows Server 2012 R2 Datacenter Server Core machine. Which remote configuration applications can you use to configure this server from your machine? (Choose all that apply.)

A. Windows Remote Management

B. Command prompt

C. Windows PowerShell

D. Microsoft Remote Admin (MRA)

10. You have been hired by a small company to implement new Windows Server 2012 R2 systems. The company wants you to set up a server for users' home folder locations. What type of server would you be setting up?

A. PDC server

B. Web server

C. Exchange server

D. File server

Chapter 5

Administer Active Directory

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Create and manage Active Directory users and computers**

- Automate the creation of Active Directory accounts
- Create, copy, configure, and delete users and computers
- Configure templates
- Perform bulk Active Directory operations
- Configure user rights
- Offline domain join
- Manage inactive and disabled accounts

✓ **Create and manage Active Directory groups and organizational units (OUs)**

- Configure group nesting
- Convert groups including security, distribution, universal, domain local, and domain global
- Manage group membership using Group Policy
- Enumerate group membership
- Delegate the creation and management of Active Directory objects
- Manage default Active Directory containers
- Create, copy, configure, and delete groups and OUs

In previous chapters, you learned how to install Domain Name System (DNS) and Active Directory, but you still haven't been introduced to the lower-level objects that exist in Active Directory.

In this chapter, you will look at the structure of the various components within a domain. You'll see how an organization's business structure can be mirrored within Active Directory through the use of organizational units for ease of use and to create a seamless look and feel. Because the concepts related to organizational units are quite simple, some system administrators may underestimate their importance and not plan to use them accordingly. Make no mistake: one of the fundamental components of a successful Active Directory installation is the proper design and deployment of organizational units.

You'll also see in this chapter the actual steps you need to take to create common Active Directory objects and then learn how to configure and manage them. Finally, you'll look at ways to publish resources and methods for creating user accounts automatically.

An Overview of OUs

An *organizational unit (OU)* is a logical group of Active Directory objects, just as the name implies. OUs serve as containers within which Active Directory objects can be created, but they do not form part of the DNS namespace. They are used solely to create organization within a domain.

OUs can contain the following types of Active Directory objects:

- Users
- Groups
- Computers
- Shared Folder objects
- Contacts
- Printers
- InetOrgPerson objects
- Microsoft Message Queuing (MSMQ) Queue aliases
- Other OUs

Perhaps the most useful feature of OUs is that they can contain other OU objects. As a result, system administrators can hierarchically group resources and objects according to

business practices. The OU structure is extremely flexible and, as you will see later in this chapter, can easily be rearranged to reflect business reorganizations.

Another advantage of OUs is that each can have its own set of policies. Administrators can create individual and unique Group Policy objects (GPOs) for each OU. GPOs are rules or policies that can apply to all of the objects within the OU. GPOs are discussed in detail in Chapter 6 "Manage GPOs."

Each type of object has its own purpose within the organization of Active Directory domains. Later in this chapter, you'll look at the specifics of User, Computer, Group, and Shared Folder objects. For now, let's focus on the purpose and benefits of using OUs.

The Purpose of OUs

OUs are mainly used to organize the objects within Active Directory. Before you dive into the details of OUs, however, you must understand how OUs, users, and groups interact. Most important, you should understand that OUs are simply containers that you can use to group various objects logically. They are not, however, groups in the classical sense. That is, they are not used for assigning security permissions. Another way of stating this is that the user accounts, computer accounts, and group accounts that are contained in OUs are considered security principals while the OUs themselves are not.

OUs do not take the place of standard user and group permissions. A good general practice is to assign users to groups and then place the groups within OUs. This enhances the benefits of setting security permissions and of using the OU hierarchy for making settings. Figure 5.1 illustrates this concept.

FIGURE 5.1 Relationships of users, groups, and OUs

An OU contains objects only from within the domain in which it resides. As you'll see in the section "Delegating Administrative Control" later in this chapter, the OU is the finest level of granularity used for group policies and other administrative settings.

Benefits of OUs

There are many benefits to using OUs throughout your network environment.

- OUs are the smallest unit to which you can assign directory permissions.
- You can easily change the OU structure, and it is more flexible than the domain structure.
- The OU structure can support many different levels of hierarchy.
- Child objects can inherit OU settings.
- You can set Group Policy settings on OUs.
- You can easily delegate the administration of OUs and the objects within them to the appropriate users and groups.

Now that you have a good idea of why you should use OUs, take a look at some general practices you can use to plan the OU structure.

Planning the OU Structure

One of the key benefits of Active Directory is the way in which it can bring organization to complex network environments. Before you can begin to implement OUs in various configurations, you must plan a structure that is compatible with business and technical needs. In this section, you'll learn about several factors that you should consider when planning for the structure of OUs.

Logical Grouping of Resources

The fundamental purpose of using OUs is to group resources (which exist within Active Directory) hierarchically. Fortunately, hierarchical groups are quite intuitive and widely used in most businesses. For example, a typical manufacturing business might divide its various operations into different departments as follows:

- Sales
- Marketing
- Engineering
- Research and Development
- Support
- Information Technology (IT)

Each of these departments usually has its own goals and mission. To make the business competitive, individuals within each of the departments are assigned to various roles. The following role types might be used:

- Managers
- Clerical staff
- Technical staff
- Planners

Each of these roles usually entails specific job responsibilities. For example, managers should provide direction to general staff members. Note that the very nature of these roles suggests that employees may fill many different positions. That is, one employee might be a manager in one department and a member of the technical staff in another. In the modern workplace, such situations are quite common.

All of this information helps you plan how to use OUs. First the structure of OUs within a given network environment should map well to the business's needs, including the political and logical structure of the organization as well as its technical needs. Figure 5.2 shows how a business organization might be mapped to the OU structure within an Active Directory domain.

FIGURE 5.2 Mapping a business organization to an OU structure

Stellacon.com Domain

When naming OUs for your organization, you should keep several considerations and limitations in mind:

Keep the Names and Descriptions Simple The purpose of OUs is to make administering and using resources simple. Therefore, it's always a good idea to keep the names of your objects simple and descriptive. Sometimes, finding a balance between these two goals can be a challenge. For example, although a printer name like "The LaserJet located near Bob's cube" might seem descriptive, it is certainly difficult to type. Also, imagine the naming changes that you might have to make if Bob moves (or leaves the company)!

Pay Attention to Limitations The maximum length for the name of an OU is 64 characters. In most cases, this should adequately describe the OU. Remember, the name of an OU does not have to describe the object uniquely because the OU is generally referenced only as part of the overall hierarchy. For example, you can choose to create an OU named "IT" within two different parent OUs. Even though the OUs have the same name, users and administrators are able to distinguish between them based on their complete pathname.

Pay Attention to the Hierarchical Consistency The fundamental basis of an OU structure is its position in a hierarchy. From a design standpoint, this means you cannot have two OUs with the same name at the same level. However, you can have OUs with the same name at different levels. For example, you could create an OU named "Corporate" within the North America OU and another one within the South America OU. This is because the fully qualified domain name includes information about the hierarchy. When an administrator tries to access resources in a Corporate OU, they must specify which Corporate OU they mean.

For example, if you create a North America OU, the Canada OU should logically fit under it. If you decide that you want to separate the North America and Canada OUs into completely different containers, then you might want to use other, more appropriate names. For example, you could change North America to "U.S." Users and administrators depend on the hierarchy of OUs within the domain, so make sure that it remains logically consistent.

Based on these considerations, you should have a good idea of how best to organize the OU structure for your domain.

Understanding OU Inheritance

When you rearrange OUs within the structure of Active Directory, you can change several settings. When they are moving and reorganizing OUs, system administrators must pay careful attention to automatic and unforeseen changes in security permissions and other configuration options. By default, OUs inherit the permissions of their new parent container when they are moved.

By using the built-in tools provided with Windows Server 2012 R2 and Active Directory, you can move or copy OUs only within the same domain. You cannot use the Active

Directory Users and Computers tool to move OUs between domains. To do this, use the *Active Directory Migration Tool (ADMT)*. This is one of the many Active Directory support tools.

Delegating Administrative Control

I already mentioned that OUs are the smallest component within a domain to which administrative permissions and group policies can be assigned by administrators. Now you'll take a look specifically at how administrative control is set on OUs.

Real World Scenario

Delegation occurs when a higher security authority assigns permissions to a lesser security authority. As a real-world example, assume that you are the director of IT for a large organization. Instead of doing all of the work yourself, you would probably assign roles and responsibilities to other individuals. For example, if you worked within a multidomain environment, you might make one system administrator responsible for all operations within the Sales domain and another responsible for the Engineering domain. Similarly, you could assign the permissions for managing all printers and print queue objects within your organization to one individual user while allowing another individual user to manage all security permissions for users and groups. In this way, you can distribute the various roles and responsibilities of the IT staff throughout the organization.

Businesses generally have a division of labor that handles all of the tasks involved in keeping the company's networks humming. Network operating systems (NOSs), however, often make it difficult to assign just the right permissions; in other words, they do not support very granular permission assignments. Sometimes, fine granularity is necessary to ensure that only the right permissions are assigned. A good general rule of thumb is to provide users and administrators with the minimum permissions they require to do their jobs. This way, you can ensure that accidental, malicious, and otherwise unwanted changes do not occur.

TIP

You can use auditing to log events to the Security log in the Event Viewer. This is a way to ensure that if accidental, malicious, and otherwise unwanted changes do occur, they are logged and traceable.

In the world of Active Directory, you delegate to define responsibilities for OU administrators. As a system administrator, you will occasionally be tasked with having to delegate responsibility to others—you can't do it all, although sometimes administrators believe that they can. You understand the old IT logic of doing all of the tasks yourself for job security, but this can actually make you look worse.

You can delegate control only at the OU level and not at the object level within the OU.

If you do find yourself in a role where you need to delegate, remember that Windows Server 2012 R2 was designed to offer you the ability to do so. In its simplest definition, *delegation* allows a higher administrative authority to grant specific administrative rights for containers and subtrees to individuals and groups. What this essentially does is to eliminate the need for domain administrators with sweeping authority over large segments of the user population. You can break up this control over branches within your tree, within each OU you create.

To understand delegation and rights, you should first understand the concept of *access control entries (ACEs)*. ACEs grant specific administrative rights on objects in a container to a user or group. A container's access control list (ACL) is used to store ACEs.

When you are considering implementing delegation, keep these two concerns in mind:

Parent-Child Relationships The OU hierarchy you create will be important when you consider the maintainability of security permissions. OUs can exist in a parent-child relationship, which means that permissions and group policies set on OUs higher up in the hierarchy (parents) can interact with objects in lower-level OUs (children). When it comes to delegating permissions, this is extremely important. You can allow child containers to inherit the permissions set on parent containers automatically. For example, if the North America division of your organization contains 12 other OUs, you could delegate permissions to all of them at once (saving time and reducing the likelihood of human error) by placing security permissions on the North America division. This feature can greatly ease administration, especially in larger organizations, but it is also a reminder of the importance of properly planning the OU structure within a domain.

Inheritance Settings Now that you've seen how you can use parent-child relationships for administration, you should consider *inheritance*, the process in which child objects take on the permissions of a parent container. When you set permissions on a parent container, all of the child objects are configured to inherit the same permissions. You can override this behavior, however, if business rules do not lend themselves well to inheritance.

Applying Group Policies

One of the strengths of the Windows operating system is that it offers users a great deal of power and flexibility. From installing new software to adding device drivers, users can make many changes to their workstation configurations. However, this level of flexibility is also a potential problem. For instance, inexperienced users might inadvertently change settings, causing problems that can require many hours to fix.

In many cases (and especially in business environments), users require only a subset of the complete functionality the operating system provides. In the past, however, the difficulty associated with implementing and managing security and policy settings has led to lax security policies. Some of the reasons for this are technical—it can be tedious and difficult to implement and manage security restrictions. Other problems have been political—users and management might feel that they should have full permissions on their local machines, despite the potential problems this might cause.

That's where the idea of group policies comes in. Simply defined, *group policies* are collections of rules that you can apply to objects within Active Directory. Specifically, Group Policy settings are assigned at the site, domain, and OU levels, and they can apply to user accounts and computer accounts. For example, a system administrator can use group policies to configure the following settings:

- Restricting users from installing new programs
- Disallowing the use of the Control Panel
- Limiting choices for display and Desktop settings

Creating OUs

Now that you have looked at several different ways in which OUs can be used to bring organization to the objects within Active Directory, it's time to look at how you can create and manage them.

Through the use of the *Active Directory Users and Computers administrative tool*, also called the *MMC (Microsoft Management Console)*, you can quickly and easily add, move, and change OUs. This graphical tool makes it easy to visualize and create the various levels of hierarchy an organization requires.

Figure 5.3 shows a geographically based OU structure that a multinational company might use. Note that the organization is based in North America and that it has a corporate office located there. In general, the other offices are much smaller than the corporate office located in North America.

FIGURE 5.3 A geographically based OU structure

It's important to note that this OU structure could have been designed in several different ways. For example, I could have chosen to group all of the offices located in the United States within an OU named "U.S." However, because of the large size of these offices, I chose to place these objects at the same level as the Canada and Mexico OUs. This prevents an unnecessarily deep OU hierarchy while still logically grouping the offices.

One nice feature when creating an OU is the ability to protect the OU from being accidentally deleted. When you create an OU, you can check the Protect Container From Accidental Deletion check box. This check box protects against an administrator deleting the OU. To delete the OU, you must go into the advanced view of the OU and uncheck the box.

Exercise 5.1 walks you through the process of creating several OUs for a multinational business. You'll be using this OU structure in later exercises within this chapter.

NOTE

To perform the exercises included in this chapter, you must have administrative access to a Windows Server 2012 R2 domain controller.

EXERCISE 5.1

Creating an OU Structure

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers administrative tool.
3. Right-click the name of the local domain and choose New ➢ Organizational Unit. You will see the dialog box shown here. Notice that this box shows you the current context within which the OU will be created. In this case, you're creating a top-level OU, so the full path is simply the name of the domain.

4. Type **North America** for the name of the first OU. Uncheck the box Protect Container From Accidental Deletion and click OK to create this object.
5. Create the following top-level OUs by right-clicking the name of the domain and choosing New ➢ Organizational Unit. Also make sure to uncheck Protect Container From Accidental Deletion for all OUs in these exercises because you'll be deleting some of these OUs in later ones.

   Africa

   Asia

   Europe

   South America

   Note that the order in which you create the OUs is not important. In this exercise, you are simply using a method that emphasizes the hierarchical relationship.

EXERCISE 5.1 *(continued)*

6. Create the following second-level OUs within the North America OU by right-clicking the North America OU and selecting New ➢ Organizational Unit:

   Austin

   Boston

   Canada

   Chicago

   Corporate

   Los Angeles

   Mexico

   New York

   San Francisco

7. Create the following OUs under the Asia OU:

   China

   India

   Malaysia

   Vietnam

8. Create the following OUs under the Europe OU:

   France

   Germany

   Spain

   UK

9. Create the following OUs under the South America OU:

   Argentina

   Brazil

   Chile

   Peru

10. Create the following third-level OUs under the India OU by right-clicking India within the Asia OU and selecting New ➢ Organizational Unit:

    Bombay

    New Delhi

11. Within the North America Corporate OU, create the following OUs:

    Engineering

    HR

    Marketing

    Research

    Sales

12. When you have completed creating the OUs, you should have a structure that looks similar to the one in the left pane shown here.

Managing OUs

Managing network environments would still be challenging, even if things rarely changed. However, in the real world, business units, departments, and employee roles change frequently. As business and technical needs change, so should the structure of Active Directory.

Fortunately, changing the structure of OUs within a domain is a relatively simple process. In the following sections, you'll look at ways to delegate control of OUs and make other changes.

Moving, Deleting, and Renaming OUs

The process of moving, deleting, and renaming OUs is a simple one. Exercise 5.2 shows how you can easily modify and reorganize OUs to reflect changes in the business organization. The specific scenario covered in this exercise includes the following changes:

- The Research and Engineering departments have been combined to form a department known as Research and Development (RD).
- The Sales department has been moved from the Corporate headquarters office to the New York office.
- The Marketing department has been moved from the Corporate headquarters office to the Chicago office.

This exercise assumes you have already completed the steps in Exercise 5.1.

EXERCISE 5.2

Modifying OU Structure

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers administrative tool.
3. Right-click the Engineering OU (located within North America ➢ Corporate) and click Delete. When you are prompted for confirmation, click Yes. Note that if this OU contained objects, they would have all been automatically deleted as well.
4. Right-click the Research OU and select Rename. Type **RD** to change the name of the OU and press Enter.
5. Right-click the Sales OU and select Move. In the Move dialog box, expand the North America branch and click the New York OU. Click OK to move the OU.

6. You will use an alternate method to move the Marketing OU. Drag the Marketing OU and drop it onto the Chicago OU.
7. When you have finished, you should see an OU structure similar to the one shown here. Close the Active Directory Users and Computers administrative tool.

Administering Properties of OUs

Although OUs are primarily created for organizational purposes within the Active Directory environment, they have several settings that you can modify. To modify the properties of an OU using the Active Directory Users and Computers administrative tool, right-click the name of any OU and select Properties. When you do, the OU Properties dialog box appears. In the example shown in Figure 5.4, you'll see the options on the General tab.

FIGURE 5.4 The General tab of the OU's Properties dialog box

In any organization, it helps to know who is responsible for managing an OU. You can set this information on the Managed By tab (see Figure 5.5). The information specified on this tab is convenient because it is automatically pulled from the contact information on a user record. You should consider always having a contact for each OU within your organization so that other system administrators know whom to contact if they need to make any changes.

FIGURE 5.5 The Managed By tab of the OU's Properties dialog box

Delegating Control of OUs

In simple environments, one or a few system administrators may be responsible for managing all of the settings within Active Directory. For example, a single system administrator could manage all users within all OUs in the environment. In larger organizations, however, roles and responsibilities may be divided among many different individuals. A typical situation is one in which a system administrator is responsible for objects within only a few OUs in an Active Directory domain. Alternatively, one system administrator might manage User and Group objects while another is responsible for managing file and print services.

Fortunately, using the Active Directory Users and Computers tool, you can quickly and easily ensure that specific users receive only the permissions they need. In Exercise 5.3, you will use the Delegation of Control Wizard to assign permissions to individuals. To complete these steps successfully, first you must have created the objects in the previous exercises of this chapter.

EXERCISE 5.3

Using the Delegation of Control Wizard

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers administrative tool.
3. Right-click the Corporate OU within the North America OU and select Delegate Control. This starts the Delegation of Control Wizard. Click Next to begin configuring security settings.
4. In the Users Or Groups page, click the Add button. In the Enter The Object Names To Select field, enter **Account Operators** and click the Check Names button. Click OK. Click Next to continue.
5. In the Tasks To Delegate page, select Delegate The Following Common Tasks and place a check mark next to the following items:

   Create, Delete, And Manage User Accounts

   Reset User Passwords And Force Password Change At Next Logon

   Read All User Information

   Create, Delete, And Manage Groups

   Modify The Membership Of A Group
6. Click Next to continue.

EXERCISE 5.3 *(continued)*

7. The Completing The Delegation Of Control Wizard page then provides a summary of the operations you have selected. To implement the changes, click Finish.

Although the common tasks available through the wizard are sufficient for many delegation operations, you may have cases in which you want more control. For example, you might want to give a particular system administrator permissions to modify only Computer objects. Exercise 5.4 uses the Delegation of Control Wizard to assign more granular permissions. To complete these steps successfully, you must have completed the previous exercises in this chapter.

EXERCISE 5.4

Delegating Custom Tasks

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers administrative tool.
3. Right-click the Corporate OU within the North America OU and select Delegate Control. This starts the Delegation of Control Wizard. Click Next to begin making security settings.
4. In the Users Or Groups page, click the Add button. In the Enter The Object Names To Select field, enter **Server Operators** and click the Check Names button. Click OK and then click Next to continue.
5. In the Tasks To Delegate page, select the Create A Custom Task To Delegate radio button and click Next to continue.

6. In the Active Directory Object Type page, choose Only The Following Objects In The Folder and place a check mark next to the following items. (You will have to scroll down to see them all.)

   User Objects

   Computer Objects

   Contact Objects

   Group Objects

   Organizational Unit Objects

   Printer Objects

7. Click Next to continue.

8. In the Permissions page, place a check mark next to the General option and make sure the other options are not checked. Note that if the various objects within your Active Directory schema had property-specific settings, you would see those options here. Place a check mark next to the following items:

   Create All Child Objects

   Read All Properties

   Write All Properties

   This gives the members of the Server Operators group the ability to create new objects within the Corporate OU and the permissions to read and write all properties for these objects.

EXERCISE 5.4 *(continued)*

9. Click Next to continue.
10. The Completing The Delegation Of Control Wizard page provides a summary of the operations you have selected. To implement the changes, click Finish.

Real World Scenario

Delegation: Who's Responsible for What?

You're the IT director for a large, multinational organization. You've been with the company for quite a while, that is, since the environment had only a handful of offices and a few network and system administrators. Times have changed, however. Now system administrators must coordinate the efforts of hundreds of IT staffers in 14 countries.

For years now, a debate has been raging among IT administrators on the question of when to create a new child domain and when to make it just an OU. For example, let's say you have a remote office in Concord, New Hampshire. Do you give the remote office its own domain (as a child domain), or do you just make the Concord office an OU? Well, it really depends on who you want to manage the resources in Concord. Do you want to create domains or OUs based on location?

Fortunately, through the proper use of OUs and delegation, you are given a lot of flexibility in determining how to handle the administration. You can structure the administration in several ways. First, if you choose to create OUs based on a geographic business structure, you could delegate control of these OUs based on the job functions of various system administrators. For example, you could use one user account to administer the

Concord OU. Within the Concord OU, this system administrator could delegate control of resources represented by the Printers and Scanners OUs.

Alternatively, the OU structure may create a functional representation of the business. For example, the Engineering OU might contain other OUs that are based on office locations such as New York and Paris. A system administrator of the Engineering domain could delegate permissions based on geography or job functions to the lower OUs. Regardless of whether you build a departmental, functional, or geographical OU model, keep in mind that each model excludes other models. This is one of the most important decisions you need to make. When you are making this decision or modifying previous decisions, your overriding concern is how it will affect the management and administration of the network. The good news is that, because Active Directory has so many features, the model you choose can be based on specific business requirements rather than imposed by architectural constraints.

Troubleshooting OUs

In general, you will find using OUs to be a relatively straightforward and painless process. With adequate planning, you'll be able to implement an intuitive and useful structure for OU objects.

The most common problems with OU configuration are related to the OU structure. When troubleshooting OUs, pay careful attention to the following factors:

Inheritance By default, Group Policy and other settings are transferred automatically from parent OUs to child OUs and objects. Even if a specific OU is not given a set of permissions, objects within that OU might still get them from parent objects.

Delegation of Administration If you allow the wrong user accounts or groups to perform specific tasks on OUs, you might be violating your company's security policy. Be sure to verify the delegations you have made at each OU level.

Organizational Issues Sometimes, business practices do not easily map to the structure of Active Directory. A few misplaced OUs, user accounts, computer accounts, or groups can make administration difficult or inaccurate. In many cases, it might be beneficial to rearrange the OU structure to accommodate any changes in the business organization. In others, it might make more sense to change business processes.

If you regularly consider each of these issues when troubleshooting problems with OUs, you will be much less likely to make errors in the Active Directory configuration.

Creating and Managing Active Directory Objects

Now that you are familiar with the task of creating OUs, you should find creating and managing other Active Directory objects quite simple. The following sections will examine the details.

Overview of Active Directory Objects

When you install and configure a domain controller, Active Directory sets up an organizational structure for you, and you can create and manage several types of objects.

Active Directory Organization

When you are looking at your Active Directory structure, you will see objects that look like folders in Windows Explorer. These objects are containers, or *organizational units (OUs)*. The difference is that an OU is a container to which you can link a GPO. Normal containers cannot have a GPO linked to them. That's what makes an OU a special container.

By default, after you install and configure a domain controller, you will see the following organizational sections within the Active Directory Users and Computers tool (they look like folders):

Built-In The *Built-In container* includes all of the standard groups that are installed by default when you promote a domain controller. You can use these groups to administer the servers in your environment. Examples include the Administrators group, Backup Operators group, and Print Operators group.

Computers By default, the *Computers container* contains a list of the workstations in your domain. From here, you can manage all of the computers in your domain.

Domain Controllers The *Domain Controllers OU* includes a list of all the domain controllers for the domain.

Foreign Security Principals *Foreign security principals* containers are any objects to which security can be assigned and that are not part of the current domain. *Security principals* are Active Directory objects to which permissions can be applied, and they can be used to manage permissions in Active Directory.

Managed Service Accounts The *Managed Service Accounts container* is a new Windows Server 2012 R2 container. Service accounts are accounts created to run specific services such as Exchange and SQL Server. Having a Managed Service Accounts container allows you to control the service accounts better and thus allows for better service account security.

Users The *Users container* includes all the security accounts that are part of the domain. When you first install the domain controller, there will be several groups in this container.

For example, the Domain Admins group and the administrator account are created in this container.

You want to be sure to protect the administrator account. You should rename the admin account and make sure the password is complex. Protected admin accounts can make your network safer. Every hacker knows that there is an administrator account on the server by default. Be sure to make your network safer by protecting the admin account.

Active Directory Objects

You can create and manage several different types of Active Directory objects. The following are specific object types:

Computer *Computer objects* represent workstations that are part of the Active Directory domain. All computers within a domain share the same security database, including user and group information. Computer objects are useful for managing security permissions and enforcing Group Policy restrictions.

Contact *Contact objects* are usually used in OUs to specify the main administrative contact. Contacts are not security principals like users. They are used to specify information about individuals outside the organization.

Group *Group objects* are logical collections of users primarily for assigning security permissions to resources. When managing users, you should place them into groups and then assign permissions to the group. This allows for flexible management without the need to set permissions for individual users.

InetOrgPerson The *InetOrgPerson object* is an Active Directory object that defines attributes of users in Lightweight Directory Access Protocol (LDAP) and X.500 directories.

MSIMaging-PSPs *MSIMaging-PSPs* is a container for all Enterprise Scan Post Scan Process objects.

MSMQ Queue Alias An *MSMQ Queue Alias object* is an Active Directory object for the MSMQ-Custom-Recipient class type. The Microsoft Message Queuing (MSMQ) Queue Alias object associates an Active Directory path and a user-defined alias with a public, private, or direct single-element format name. This allows a queue alias to be used to reference a queue that might not be listed in Active Directory Domain Services (AD DS).

Organizational Unit An *OU object* is created to build a hierarchy within the Active Directory domain. It is the smallest unit that can be used to create administrative groupings, and it can be used to assign group policies. Generally, the OU structure within a domain reflects a company's business organization.

Printer *Printer objects* map to printers.

Shared Folder *Shared Folder objects* map to server shares. They are used to organize the various file resources that may be available on file/print servers. Often, Shared Folder objects are used to give logical names to specific file collections. For example, system

administrators might create separate shared folders for common applications, user data, and shared public files.

User A *User object* is the fundamental security principal on which Active Directory is based. User accounts contain information about individuals as well as password and other permission information.

Creating Objects Using the Active Directory Users and Computers Tool

Exercise 5.5 walks you through the steps necessary to create various objects within an Active Directory domain. In this exercise, you create some basic Active Directory objects. To complete this exercise, you must have access to at least one Active Directory domain controller, and you should have also completed the previous exercises in this chapter.

EXERCISE 5.5

Creating Active Directory Objects

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers tool.
3. Expand the current domain to list the objects currently contained within it. For this exercise, you will use the second- and third-level OUs contained within the North America top-level OU, as shown here.

4. Right-click the Corporate OU and select New ➢ User. Fill in the following information:

   First Name: **Maria**

   Initial: **D**

   Last Name: **President**

   Full Name: (leave as default)

   User Logon Name: **mdpresident** (leave default domain)

   Click Next to continue.

5. Enter **P@ssw0rd** for the password for this user and then confirm it. Note that you can also make changes to password settings here. Click Next.

6. You will see a summary of the user information. Click Finish to create the new user.

7. Click the RD container and create another user in that container with the following information:

   First Name: **John**

   Initial: **Q**

   Last Name: **Adams**

   Full Name: (leave as default)

   User Logon Name: **jqadams** (leave default domain)

   Click Next to continue.

8. Assign the password **P@ssw0rd**. Click Next and then click Finish to create the user.

9. Right-click the RD OU and select New ➢ Contact. Use the following information to fill in the properties of the Contact object:

   First Name: **Jane**

   Initials: **R**

   Last Name: **Admin**

   Display Name: **jradmin**

   Click OK to create the new Contact object.

10. Right-click the RD OU and select New ➢ Shared Folder. Enter **Software** for the name and **\\server1\applications** for the network path (also known as the Universal Naming Convention [UNC] path). Note that you can create the object even though this resource (the physical server) does not exist. Click OK to create the Shared Folder object.

11. Right-click the HR OU and select New ➢ Group. Type **All Users** for the group name. Do not change the value in the Group Name (Pre–Windows 2000) field. For Group Scope, select Global, and for Group Type, select Security. To create the group, click OK.

EXERCISE 5.5 *(continued)*

12. Right-click the Sales OU and select New ➢ Computer. Type **Workstation1** for the name of the computer. Notice that the pre–Windows 2000 name is automatically populated and that, by default, the members of the Domain Admins group are the only ones who can add this computer to the domain. Place a check mark in the Assign This Computer Account As A Pre-Windows 2000 Computer box and then click OK to create the Computer object.
13. Close the Active Directory Users and Computers tool.

Configuring the User Principal Name

When you log into a domain, your logon name looks like an email address (for example, `wpanek@willpanek.com`). This is called your *user principal name (UPN)*. A UPN is the username followed by the @ sign and the domain name. At the time that the user account is created, the UPN suffix is generated by default. The UPN is created as *`userName@Domain Name`*, but an administrator can alter or change the default UPN. If your forest has multiple domains and you need to change the UPN to a different domain, you have that ability. To change the UPN suffix, in Active Directory Users and Computers, choose a user and go into their properties. Choose the Attribute Editor tab. Scroll down to the `userPrincipalName` attribute and make your changes. These changes then get replicated to the global catalog.

If your organization has multiple forests set up by a trust, you can't change the UPN to a domain in the other forest. Global catalogs are used to log on users. Because UPNs get replicated to the local forest global catalog servers, you cannot log onto other forests using the UPN.

Using Templates

Now you are going to dive into user templates. *User templates* allow an Active Directory administrator to create a default account (for example, template_sales) and use that account to create all of the other users who match it (all the salespeople).

If you are creating multiple accounts, this can save you a lot of time and resources. For example, if you need to add 35 new salespeople to your company, you'll create one template for sales and use a copy of that template for all of the other new accounts. This saves you the trouble of filling out many of the same fields over and over again. When you copy a template, some of the information does *not* get copied over. This is because it is user-specific information. Here are some of the fields that do not get copied over from a template:

- Name
- Logon Name
- Password
- Email

- Phone Numbers
- Description
- Office
- Web Page

Many of the important fields such as Member Of (groups to which the user belongs), Profile Path, Department, and Company all get copied over. There is one important item that needs to be done when creating a template: the template account needs to be disabled after creation. You do not want anyone using this account to access your network. In Exercise 5.6, you will create a Sales template to use for your Sales department.

EXERCISE 5.6

Creating a User Template

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers snap-in.
3. Expand the current domain to list the objects contained within it. For this exercise, you will use the Sales OU. Right-click the Sales OU and choose New ➢ User.
4. Use the following properties:

   First Name: **Sales**

   Last Name: **Template**

   Username: **sales_template**

   Password: **P@ssw0rd**
5. Click Next and then click Finish.
6. In the right window, double-click the Sales Template user to open the properties.
7. On the General tab, complete the following items:

   Description: **Template Account**

   Office: **Corporate**

   Telephone: **999-999-9999**

   Email: **Salet@abc.com**

   Web: **www.abc.com**
8. Click the Profile tab. In the Profile Path field, type **\\ServerA\%username%**.
9. On the Members Of tab, click the Add button. At the Enter The Object Name To Select box, type **Administrator** and click the Check Names button. (Normally you would not

EXERCISE 5.6 *(continued)*

add salespeople to the Administrators group, but you are doing so just for this exercise.) Click OK.

10. Click the Account tab. Scroll down in the Account Options box and check the Account Is Disabled check box.
11. Click OK in the user's Properties window to go back to the Sales OU.
12. Right-click the Sales Template account and choose Copy.
13. Enter the following information:

    First Name: **Jenny**

    Last Name: **Sales**

    Username: **jsales**

    Password: **P@ssw0rd**

    Uncheck the Account Is disabled check box.
14. In the right window, double-click the Jenny Sales user to open the properties.
15. Take a look at the Members Of tab, the General tab, and the Profile tab, and you will see that some of the fields are prefilled (including the Administrators group).
16. Close Jenny Sales Properties and exit Active Directory Users and Computers.

Importing Objects from a File

In Exercise 5.5, you created an account using the Active Directory Users and Computers tool. But what if you need to bulk import accounts? There are two main applications for doing bulk imports of accounts: the `ldifde.exe` utility and the `csvde.exe` utility. Both utilities import accounts from files.

The `ldifde` utility imports from line-delimited files. This utility allows an administrator to export and import data, thus allowing batch operations such as Add, Modify, and Delete to be performed in Active Directory. Windows Server 2012 R2 includes `ldifde.exe` to help support batch operations.

The `csvde.exe` utility performs the same export functions as `ldifde.exe`, but `csvde.exe` uses a comma-separated value file format. The `csvde.exe` utility does not allow administrators to modify or delete objects. It only supports adding objects to Active Directory.

Active Directory Migration Tool

Another tool that administrators have used in the past is *Active Directory Migration Tool (ADMT)*. ADMT allows an administrator to migrate users, groups, and computers from a previous version of the server to a current version of the server.

Administrators also used the ADMT to migrate users, groups, and computers between Active Directory domains in different forests (interforest migration) and between Active Directory domains in the same forest (intraforest migration).

At the time this book was written, Microsoft had not yet released a new version of ADMT that is supported by Windows Server 2012 R2. The reason I even mention it in this book is because Microsoft may be releasing a version of it soon, and I wanted you to understand what it can do. Continue to check the Microsoft website to see whether a new version has been released.

Offline Domain Join of a Computer

Offline domain join gives administrators the ability to preprovision computer accounts in the domain to prepare operating systems for deployments. At startup, computers can then join the domain without the need to contact a domain controller. This helps reduce the time it takes to deploy computers in a datacenter.

Let's say your datacenter needs to have multiple virtual machines deployed. This is where offline domain join can be useful. Upon initial startup after the operating system is installed, offline domain join allows the virtual machines to join the domain automatically. No additional steps or restart are needed.

The following are some of the benefits of using offline domain join:

- There is no additional network traffic for Active Directory state changes.
- There is no additional network traffic for computer state changes to the domain controller.
- Changes for both the Active Directory state and the computer state can be completed at a different times.

Managing Object Properties

Once you've created the necessary Active Directory objects, you'll probably need to make changes to their default properties. In addition to the settings you made when you were creating Active Directory objects, you can configure several more properties. You can also access object properties by right-clicking any object and selecting Properties from the pop-up menu.

Each object type contains a unique set of properties.

User Object Properties The following list describes some of the properties of a User object:

General General account information about this user

Address Physical location information about this user

Account User logon name and other account restrictions, such as workstation restrictions and logon hours

Profile Information about the user's roaming profile settings

Telephones Telephone contact information for the user

Organization The user's title, department, and company information

Member Of Group membership information for the user

Dial-In Remote Access Service (RAS) permissions for the user

Environment Logon and other network settings for the user

Sessions Session limits, including maximum session time and idle session settings

Remote Control Remote control options for this user's session

Remote Desktop Services Profile Information about the user's profile for use with Remote Desktop Services

Personal Virtual Desktop Allows you to assign a user a specific virtual machine to use as a personal virtual desktop

COM+ Specifies a COM+ partition set for the user

Computer Object Properties

Computer objects have different properties than User objects. Computer objects refer to the systems that clients are operating to be part of a domain. The following list describes some Computer object properties:

General Information about the name of the computer, the role of the computer, and its description

(You can enable an option to allow the Local System account of this machine to request services from other servers. This is useful if the machine is a trusted and secure computer.)

Operating System The name, version, and service pack information for the operating system running on the computer

Member Of Active Directory groups of which this Computer object is a member

Delegation Allows you to set services that work on behalf of another user

Location A description of the computer's physical location

Managed By Information about the User or Contact object that is responsible for managing this computer

Dial-In Sets dial-in options for the computer

Setting Properties for Active Directory Objects

Now that you have seen the various properties that can be set for the Active Directory objects, let's complete an exercise on how to configure some of these properties. Exercise 5.7 walks you through how to set various properties for Active Directory objects. To complete the steps in this exercise, first you must have completed Exercise 5.5.

Although it may seem a bit tedious, it's always a good idea to enter as much information as you know about Active Directory objects when you create them. Although the name Printer1 may be meaningful to you, users will appreciate the additional information, such as location, when they are searching for objects.

EXERCISE 5.7

Managing Object Properties

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers tool.
3. Expand the name of the domain and select the RD container. Right-click the John Q. Adams user account and select Properties.
4. Here you will see the various Properties tabs for the User account. Make some configuration changes based on your personal preferences. Click OK to continue.

5. Select the HR OU. Right-click the All Users group and click Properties. In the All Users Properties dialog box, you will be able to modify the membership of the group.

EXERCISE 5.7 *(continued)*

Click the Members tab and then click Add. Add the Maria D. President and John Q. Admin user accounts to the group. Click OK to save the settings and then OK to accept the group modifications.

6. Select the Sales OU. Right-click the Workstation1 Computer object. Notice that you can choose to disable the account or reset it (to allow another computer to join the domain under that same name). From the context menu, choose Properties. You'll see the properties for the Computer object.

   Examine the various options and make changes based on your personal preference. After you have examined the available options, click OK to continue.

7. Select the Corporate OU. Right-click the Maria D. President user account and choose Reset Password. You will be prompted to enter a new password, and then you'll be asked to confirm it. Note that you can also force the user to change this password upon the next logon, and you can also unlock the user's account from here. For this exercise, do not enter a new password; just click Cancel.

8. Close the Active Directory Users and Computers tool.

By now, you have probably noticed that Active Directory objects have a lot of common options. For example, Group and Computer objects both have a Managed By tab.

Windows Server 2012 R2 allows you to manage many User objects at once. For instance, you can select several User objects by holding down the Shift or Ctrl key while selecting. You can then right-click any one of the selected objects and select Properties to display the properties that are available for multiple users. Notice that not every user property is available because some properties are unique to each user. You can configure the Description field for multiple object selections that include both users and nonusers, such as computers and groups.

NOTE

An important thing to think about when it comes to accounts is the difference between disabling an account and deleting an account. When you delete an account, the security ID (SID) gets deleted. Even if you later create an account with the same username, it will have a different SID number, and therefore it will be a different account. It is sometimes better to disable an account and place it into a nonactive OU called *Disabled.* This way, if you ever need to reaccess the account, you can do so.

Another object management task is the process of deprovisioning. *Deprovisioning* is the management of Active Directory objects in the container. When you remove an object from an Active Directory container, the deprovisioning process removes the object and synchronizes the container to stay current.

Understanding Groups

Now that you know how to create user accounts, it's time to learn how to create group accounts. As an instructor, I am always amazed when students (who work in the IT field) have no idea why they should use groups. This is something every organization should be using.

To illustrate their usefulness, let's say you have a Sales department user by the name of wpanek. Your organization has 100 resources shared on the network for users to access. Because wpanek is part of the Sales department, he has access to 50 of the resources. The Marketing department uses the other 50. If the organization is not using groups and wpanek moves from Sales to Marketing, how many changes do you have to make? The answer is 100. You have to move him out of the 50 resources he currently can use and place his account into the 50 new resources that he now needs.

Now let's say that you use groups. The Sales group has access to 50 resources, and the Marketing group has access to the other 50. If wpanek moves from Sales to Marketing, you need to make only two changes. You just have to take wpanek out of the Sales group and place him in the Marketing group. Once this is done, wpanek can access everything he needs to do his job.

Group Properties

Now that you understand why you should use groups, let's go over setting up groups and their properties. When you are creating groups, it helps to understand some of the options that you need to use.

Group Type You can choose from two group types: security groups and distribution groups.

Security Groups These groups can have rights and permissions placed on them. For example, if you want to give a certain group of users access to a particular printer, but you want to control what they are allowed to do with this printer, you'd create a security group and then apply certain rights and permissions to this group.

Security groups can also receive emails. If someone sent an email to the group, all users within that group would receive it (as long as they have a mail system that allows for mail-enabled groups, like Exchange).

Distribution Groups These groups are used for email *only* (as long as they have a mail system that allows for mail-enabled groups, like Exchange). You cannot place permissions and rights for objects on this group type.

Group Scope When it comes to group scopes, you have three choices.

Domain Local Groups Domain local groups are groups that remain in the domain in which they were created. You use these groups to grant permissions within a single domain. For example, if you create a domain local group named HPLaser, you cannot use that group in any other domain, and it has to reside in the domain in which you created it.

Global Group Global groups can contain other groups and accounts from the domain in which the group is created. In addition, you can give them permissions in any domain in the forest.

Universal Groups Universal groups can include other groups and accounts from any domain in the domain tree or forest. You can give universal groups permissions in any domain in the domain tree or forest.

Creating Group Strategies

When you are creating a group strategy, think of this acronym that Microsoft likes to use in the exam: AGDLP (or AGLP). This acronym stands for a series of actions you should perform. Here is how it expands:

A Accounts (Create your user accounts.)

G Global groups (Put user accounts into global groups.)

DL Domain local groups (Put global groups into domain local groups.)

P Permissions (Assign permissions such as Deny or Apply on the domain local group.)

Another acronym that stands for a strategy you can use is AGUDLP (or AULP). Here is how it expands:

A Accounts (Create your user accounts.)

G Global groups (Put user accounts into global groups.)

U Universal groups (Put the global groups into universal groups.)

DL Domain local groups (Put universal groups into domain local groups.)

P Permissions (Place permissions on the local group.)

Creating a Group

To create a new group, open the Active Directory Users and Computers snap-in. Click the OU where the group is going to reside. Right-click and choose New and then Group. After you create the group, just click the Members tab and choose Add. Add the users you want to reside in that group, and that's all there is to it.

Filtering and Advanced Active Directory Features

The Active Directory Users and Computers tool has a couple of other features that come in quite handy when you are managing many objects. You can access the Filter Options dialog box by clicking the View menu in the MMC and choosing Filter Options. You'll see a dialog box similar to the one shown in Figure 5.6. Here you can choose to filter objects by their specific types within the display. For example, if you are an administrator who works primarily with user accounts and groups, you can select those specific items by placing check marks in the list. In addition, you can create more complex filters by choosing Create Custom. Doing so provides you with an interface that looks similar to that of the Find command.

FIGURE 5.6 The Filter Options dialog box

Another option in the Active Directory Users and Computers tool is to view advanced options. You can enable the advanced options by choosing Advanced Features in the View menu. This adds some top-level folders to the list under the name of the domain. Let's take a look at a couple of the new top-level folders.

The `System` folder (shown in Figure 5.7) provides additional features that you can configure to work with Active Directory. You can configure settings for the Distributed File System (DFS), IP Security (IPSec) policies, the File Replication Service (FRS), and more. In addition to the `System` folder, you'll see the `LostAndFound` folder. This folder contains any files that may not have been replicated properly between domain controllers. You should check this folder periodically for any files so that you can decide whether you need to move them or copy them to other locations.

FIGURE 5.7 Advanced Features in the `System` folder of the Active Directory Users and Computers tool

As you can see, managing Active Directory objects is generally a simple task. The Active Directory Users and Computers tool allows you to configure several objects. Let's move on to look at one more common administration function: moving objects.

Moving, Renaming, and Deleting Active Directory Objects

One of the extremely useful features of the Active Directory Users and Computers tool is its ability to move users and resources easily.

Exercise 5.8 walks you through the process of moving Active Directory objects. In this exercise, you will make several changes to the organization of Active Directory objects. To complete this exercise, first you must have completed Exercise 5.5.

EXERCISE 5.8

Moving Active Directory Objects

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers tool and expand the name of the domain.
3. Select the Sales OU (under the New York OU), right-click Workstation1, and select Move. A dialog box appears. Select the RD OU and click OK to move the Computer object to that container.
4. Click the RD OU and verify that Workstation1 was moved.
5. Close the Active Directory Users and Computers tool.

In addition to moving objects within Active Directory, you can easily rename them by right-clicking an object and selecting Rename. Note that this option does not apply to all objects. You can remove objects from Active Directory by right-clicking them and choosing Delete.

WARNING

Deleting an Active Directory object is an irreversible action. When an object is destroyed, any security permissions or other settings made for that object are removed as well. Because each object within Active Directory contains its own security identifier (SID), simply re-creating an object with the same name does not place any permissions on it. Before you delete an Active Directory object, be sure that you will never need it again. Windows Server 2012 R2 has an Active Directory Recycle Bin to allow an administrator to retrieve a deleted object, but in case the Recycle Bin gets cleared, it's better to be safe than sorry. Also, the AD Recycle Bin is disabled by default, so it will be unavailable unless you turn that feature on. So, what is the moral of this story? Don't delete AD objects unless you are absolutely sure you want them gone.

Windows Server 2012 R2 has a check box called Protect Container From Accidental Deletion for all OUs. If this check box is checked, to delete or move an OU, you must go into the Active Directory Users and Computers advanced options. Once you are in the advanced options, you can uncheck the box to move or delete the OU.

Resetting an Existing Computer Account

Every computer on the domain establishes a discrete channel of communication with the domain controller at logon time. The domain controller stores a randomly selected password (different from the user password) for authentication across the channel. The password is updated every 30 days.

Sometimes the computer's password and the domain controller's password don't match, and communication between the two machines fails. Without the ability to reset the computer account, you wouldn't be able to connect the machine to the domain. Fortunately, you can use the Active Directory Users and Computers tool to reestablish the connection.

Exercise 5.9 shows you how to reset an existing computer account. You should have completed the previous exercises in this chapter before you begin this exercise.

EXERCISE 5.9

Resetting an Existing Computer Account

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers tool and expand the name of the domain.
3. Click the RD OU and then right-click the Workstation1 computer account.
4. Select Reset Account from the context menu. Click Yes to confirm your selection. Click OK at the success prompt.
5. When you reset the account, you break the connection between the computer and the domain. So, after performing this exercise, reconnect the computer to the domain if you want it to continue working on the network.

Throughout this book, I have tried to show you the PowerShell way of doing a task shown previously using an MMC snap-in. Well, this is going to be no different.

This example shows you how to reset the secure connection between the local computer and the domain to which it is joined using a PowerShell command. In this example, the

domain controller that performs the operation is specified as `StellaDC1.Stellacon.com`. To execute this PowerShell command, you must run this command on the local computer:

```
Test-ComputerSecureChannel -Repair -Server StellaDC1.Stellacon.com
```

Publishing Active Directory Objects

One of the main goals of Active Directory is to make resources easy to find. Two of the most commonly used resources in a networked environment are server file shares and printers. These are so common, in fact, that most organizations have dedicated file and print servers. When it comes to managing these types of resources, Active Directory makes it easy to determine which files and printers are available to users.

With that being said, take a look at how Active Directory manages to publish shared folders and printers.

Making Active Directory Objects Available to Users

An important aspect of managing Active Directory objects is that a system administrator can control which objects users can see. The act of making an Active Directory object available is known as *publishing*. The two main types of publishable objects are Printer objects and Shared Folder objects.

The general process for creating server shares and shared printers has remained unchanged from previous versions of Windows: you create the various objects (a printer or a file system folder) and then enable them for sharing. To make these resources available via Active Directory, however, there's an additional step: you must publish the resources. Once an object has been published in Active Directory, clients will be able to use it.

When you publish objects in Active Directory, you should know the server name and share name of the resource. When system administrators use Active Directory objects, they can change the resource to which the object points, without having to reconfigure or even notify clients. For example, if you move a share from one server to another, all you need to do is to update the Shared Folder object's properties to point to the new location. Active Directory clients still refer to the resource with the same path and name that they used before.

Publishing Printers

Printers can be published easily within Active Directory. This makes them available to users in your domain.

Exercise 5.10 walks you through the steps you need to take to share and publish a Printer object by having you create and share a printer. To complete the printer installation, you need access to the Windows Server 2012 R2 installation media (via the hard disk, a network share, or the CD-ROM drive).

EXERCISE 5.10

Creating and Publishing a Printer

1. Click the Windows key on the keyboard and choose Control Panel.
2. Click Devices And Printers ➢ Add A Printer. This starts the Add Printer Wizard. Then click the Next button.
3. In the Choose A Local Or Network Printer page, select Add A Local Printer. This should automatically take you to the next page. If it does not, click Next.
4. On the Choose A Printer Port page, select Use An Existing Port. From the drop-down list beside that option, make sure LPT1: (Printer Port) is selected. Click Next.
5. On the Install The Printer Driver page, select Generic for the manufacturer. For the printer, highlight Generic/Text Only. Click Next.
6. On the Type A Printer Name page, type **Text Printer**. Uncheck the Set As The Default Printer box and then click Next.
7. The Installing Printer screen appears. After the system is finished, the Printer Sharing page appears. Make sure the box labeled "Share this printer so that others on your network can find and use it" is selected, and accept the default share name of Text Printer.
8. In the Location section, type **Building 203**, and in the Comment section, add the following comment: **This is a text-only Printer**. Click Next.

9. On the You've Successfully Added Text Printer page, click Finish.
10. Next you need to verify that the printer will be listed in Active Directory. Right-click the Text Printer icon and select Printer Properties.

EXERCISE 5.10 *(continued)*

11. Select the Sharing tab and make sure that the List In The Directory box is checked. Note that you can also add additional printer drivers for other operating systems using this tab. Click OK to accept the settings.

Note that when you create and share a printer this way, an Active Directory Printer object is not displayed within the Active Directory Users and Computers tool. The printer is actually associated with the Computer object to which it is connected.

Publishing Shared Folders

Now that you've created and published a printer, you'll see how the same thing can be done to shared folders.

Exercise 5.11 walks through the steps required to create a folder, share it, and then publish it in Active Directory. This exercise assumes you are using the `C:` partition; however, you may want to change this based on your server configuration. This exercise assumes you have completed Exercise 5.5.

EXERCISE 5.11

Creating and Publishing a Shared Folder

1. Create a new folder in the root directory of your `C:` partition and name it `Test Share`. To do this, click the File Explorer link on the toolbar.
2. Right-click the `Test Share` folder. Choose Share With ➢ Specific People.

3. In the File Sharing dialog box, enter the names of users with whom you want to share this folder. In the upper box, enter **Everyone** and then click Add. Note that Everyone appears in the lower box. Click in the Permission Level column next to Everyone and choose Read/Write from the pop-up menu. Then click Share.
4. You'll see a message that your folder has been shared. Click Done.
5. Click the Windows key on the keyboard and choose Administrative Tools.
6. Open the Active Directory Users and Computers tool. Expand the current domain and right-click the RD OU. Select New ➢ Shared Folder.
7. In the New Object - Shared Folder dialog box, type **Shared Folder Test** for the name of the folder. Then type the UNC path to the share (for example, **\\server1\Test Share**). Click OK to create the share.

Once you have created and published the Shared Folder object, clients can use the My Network Places icon to find it. The Shared Folder object will be organized based on the OU in which you created it. When you use publication, you can see how this makes it easy to manage shared folders.

Querying Active Directory

So far you've created several Active Directory resources. One of the main benefits of having all of your resource information in Active Directory is that you can easily find what you're looking for using the Find dialog box. Recall that I recommended that you always enter as much information as possible when creating Active Directory objects. This is where that extra effort begins to pay off.

Exercise 5.12 walks you through the steps to find specific objects in Active Directory. To complete this exercise, you must have completed Exercise 5.5.

EXERCISE 5.12

Finding Objects in Active Directory

1. Click the Windows key on the keyboard and choose Administrative Tools.
2. Open the Active Directory Users and Computers tool.
3. Right-click the name of the domain and select Find.
4. In the Find Users, Contacts, And Groups dialog box, select Users, Contacts, And Groups from the Find drop-down list. For the In setting, choose Entire Directory. This searches the entire Active Directory environment for the criteria you enter.

   Note that if this is a production domain and there are many objects, searching the whole directory may be a time-consuming and network-intensive operation.

EXERCISE 5.12 *(continued)*

5. In the Name field, type **admin** and then click Find Now to obtain the results of the search.

6. Now that you have found several results, you can narrow down the list. Click the Advanced tab of the Find Users, Contacts, And Groups dialog box.

In the Field drop-down list, select User ➢ Last Name. For Condition, select Starts With, and for Value, type **admin**. Click Add to add this condition to the search criteria. Click Find Now. Now only the users that have the last name Admin are shown.

7. When you have finished searching, close the Find Users, Contacts, And Groups dialog box and exit the Active Directory Users and Computers tool.

Using the many options available in the Find dialog box, you can usually narrow down the objects for which you are searching quickly and efficiently. Users and system administrators alike find this tool useful in environments of any size. Now that you have seen how to create objects in Active Directory, let's take a look at a new Windows Server 2012 R2 feature called Active Directory Administrative Center.

Using the Active Directory Administrative Center

Windows Server 2012 R2 has a feature called the *Active Directory Administrative Center* (see Figure 5.8). This feature allows you to manage many Active Directory tasks from one central location (see Figure 5.9).

FIGURE 5.8 Active Directory Administrative Center

FIGURE 5.9 Administrative Center Overview screen

Using the Active Directory Administrative Center, here are some of the tasks that an administrator can perform:

- Reset passwords
- Create new objects
- Delete objects
- Move objects
- Perform global searches
- Configure properties for Active Directory objects

In Windows Server 2012 R2, the Active Directory Administrative Center is just another tool in your Active Directory tool belt. It does not matter which way you create your Active Directory objects as long as you have a good understanding of how to create them.

Using the Command Prompt for Active Directory Configuration

Many IT administrators like to use command-line commands to configure and maintain their Active Directory environment. One advantage of using command-line commands is the ability to do multiple changes at once using batch files.

Another advantage of knowing how to manipulate Active Directory using the command prompt is working with Windows Server 2012 R2 Server Core. Server Core is an installation of Windows Server 2012 R2 that has no GUI windows. One of the ways to configure Server Core is to use commands in the command prompt window.

Table 5.1 shows you many of the command prompt commands and explains how each command affects Active Directory.

TABLE 5.1 Command prompt commands

Command	Explanation
`Csvde`	This command allows you to import and export data from Active Directory. The data gets stored in a comma-separated value (CSV) format.
`Dcdiag`	This troubleshooting command checks the state of your domain controllers in your forest and sends back a report of any problems.

`Djoin`	This command allows a computer account to join a domain, and it runs an offline domain join when a computer restarts.
`Dsacls`	This command allows you to see and change permissions in the access control list for objects in Active Directory Domain Services (AD DS).
`Dsadd`	This command allows you to add an object to the AD DS directory.
`Dsamain`	This command shows the Active Directory data stored in either a snapshot or a backup as if it were in a Lightweight Directory Access Protocol (LDAP) server.
`Dsdbutil`	This command provides database utilities for Active Directory Lightweight Directory Services (AD LDS).
`Dsget`	This command shows the properties of an object in the AD DS directory.
`Dsmgmt`	This command gives an administrator management utilities for AD LDS.
`Dsmod`	This command allows you to modify an AD DS object.
`Dsmove`	This command allows you to move an object in an Active Directory domain from its current OU to a new OU within the same forest.
`Dsquery`	This command allows you to query AD DS.
`Dsrm`	This command removes an object from the AD DS directory.
`Ldifde`	This command allows you to import and export data from Active Directory. The data is stored as LDAP Data Interchange Format (LDIF).
`Ntdsutil`	This is one of the most important commands for Active Directory. It allows you to do maintenance on the Active Directory database.
`Repadmin`	This command allows administrators to diagnose Active Directory replication problems between domain controllers.

Summary

This chapter covered the fundamentals of administering Active Directory. The most important part of administering Active Directory is learning about how to work with OUs. Therefore, you should be aware of the purpose of OUs; that is, they help you to organize and manage the directory. For instance, think of administrative control. If you wanted to delegate rights to another administrator (such as a sales manager), you could delegate that authority to that user within the Sales OU. As the system administrator, you would retain the rights to the castle.

You also looked at how to design an OU structure from an example. The example showed you how to design a proper OU layout. You can also create, organize, and reorganize OUs if need be.

In addition, you took a look at groups and group strategies. There are different types of groups (domain local, global, and universal groups), and you should know when each group is available and when to use each group.

Finally, this chapter covered how to use the Active Directory Users and Computers tool to manage Active Directory objects. If you're responsible for day-to-day system administration, there's a good chance that you are already familiar with this tool; if not, you should be after reading this chapter. Using this tool, you learned how to work with Active Directory objects such as User, Computer, and Group objects. You also learned how to import users by doing a bulk import, and you studied the two different file types that work for bulk imports. Bulk imports allow you to import multiple users without the need to add one user at a time.

Exam Essentials

Understand the purpose of OUs. OUs are used to create a hierarchical, logical organization for objects within an Active Directory domain.

Know the types of objects that can reside within OUs. OUs can contain Active Directory User, Computer, Shared Folder, and other objects.

Understand how to use the Delegation of Control Wizard. The Delegation of Control Wizard is used to assign specific permissions at the level of OUs.

Understand the concept of inheritance. By default, child OUs inherit permissions and Group Policy assignments set for parent OUs. However, these settings can be overridden for more granular control of security.

Know groups and group strategies. You can use three groups in Native mode: domain local, global, and universal. Understand the group strategies and when they apply.

Understand how Active Directory objects work. Active Directory objects represent some piece of information about components within a domain. The objects themselves have attributes that describe details about them.

Understand how Active Directory objects can be organized. By using the Active Directory Users and Computers tool, you can create, move, rename, and delete various objects.

Understand how to import bulk users. You can import multiple accounts by doing a bulk import. Bulk imports use files to import the data into Active Directory. Know the two utilities (`ldifde.exe` and `csvde.exe`) you need to perform the bulk imports and how to use them.

Learn how resources can be published. A design goal for Active Directory was to make network resources easier for users to find. With that in mind, you should understand how using published printers and shared folders can simplify network resource management.

Review Questions

1. You are the administrator of an organization with a single Active Directory domain. A user who left the company returns after 16 weeks. The user tries to log onto their old computer and receives an error stating that authentication has failed. The user's account has been enabled. You need to ensure that the user is able to log onto the domain using that computer. What do you do?
   - **A.** Reset the computer account in Active Directory. Disjoin the computer from the domain and then rejoin the computer to the domain.
   - **B.** Run the `ADadd` command to rejoin the computer account.
   - **C.** Run the MMC utility on the user's computer, and add the Domain Computers snap-in.
   - **D.** Re-create the user account and reconnect the user account to the computer account.

2. You are the administrator of an organization with a single Active Directory domain. One of your senior executives tries to log onto a machine and receives the error "This user account has expired. Ask your administrator to reactivate your account." You need to make sure that this doesn't happen again to this user. What do you do?
   - **A.** Configure the domain policy to disable account lockouts.
   - **B.** Configure the password policy to extend the maximum password age to 0.
   - **C.** Modify the user's properties to set the Account Never Expires setting.
   - **D.** Modify the user's properties to extend the maximum password age to 0.

3. You need to create a new user account using the command prompt. Which command would you use?
   - **A.** `dsmodify`
   - **B.** `dscreate`
   - **C.** `dsnew`
   - **D.** `dsadd`

4. Maria is a user who belongs to the Sales distribution global group. She is not able to access the laser printer that is shared on the network. The Sales global group has full access to the laser printer. How do you fix the problem?
   - **A.** Change the group type to a security group.
   - **B.** Add the Sales global group to the Administrators group.
   - **C.** Add the Sales global group to the Printer Operators group.
   - **D.** Change the Sales group to a local group.

5. You are a domain administrator for a large domain. Recently, you have been asked to make changes to some of the permissions related to OUs within the domain. To restrict security for the Texas OU further, you remove some permissions at that level. Later, a junior system administrator mentions that she is no longer able to make changes to objects within the Austin OU (which is located within the Texas OU). Assuming that no other changes have been made to Active Directory permissions, which of the following characteristics of OUs might have caused the change in permissions?
   - **A.** Inheritance
   - **B.** Group Policy
   - **C.** Delegation
   - **D.** Object properties

6. Isabel, a system administrator, created a new Active Directory domain in an environment that already contains two trees. During the promotion of the domain controller, she chose to create a new Active Directory forest. Isabel is a member of the Enterprise Administrators group and has full permissions over all domains. During the organization's migration to Active Directory, many updates were made to the information stored within the domains. Recently, users and other system administrators have complained about not being able to find specific Active Directory objects in one or more domains (although the objects exist in others). To investigate the problem, Isabel wants to check for any objects that have not been properly replicated among domain controllers. If possible, she would like to restore these objects to their proper place within the relevant Active Directory domains.

   Which two of the following actions should she perform to be able to view the relevant information? (Choose two.)
   - **A.** Change Active Directory permissions to allow object information to be viewed in all domains.
   - **B.** Select the Advanced Features item in the View menu.
   - **C.** Promote a member server in each domain to a domain controller.
   - **D.** Rebuild all domain controllers from the latest backups.
   - **E.** Examine the contents of the `LostAndFound` folder using the Active Directory Users and Computers tool.

7. You are a consultant hired to evaluate an organization's Active Directory domain. The domain contains more than 200,000 objects and hundreds of OUs. You begin examining the objects within the domain, but you find that the loading of the contents of specific OUs takes a long time. Furthermore, the list of objects can be large. You want to do the following:
   - Use the built-in Active Directory administrative tools and avoid the use of third-party tools or utilities.
   - Limit the list of objects within an OU to only the type of objects that you're examining (for example, only Computer objects).
   - Prevent any changes to the Active Directory domain or any of the objects within it.

Which one of the following actions meets these requirements?

A. Use the Filter option in the Active Directory Users and Computers tool to restrict the display of objects.

B. Use the Delegation of Control Wizard to give yourself permissions over only a certain type of object.

C. Implement a new naming convention for objects within an OU and then sort the results using this new naming convention.

D. Use the Active Directory Domains and Trusts tool to view information from only selected domain controllers.

E. Edit the domain Group Policy settings to allow yourself to view only the objects of interest.

8. You are the administrator for a small organization with four servers. You have one file server named Paniva that runs Windows Server 2012 R2. You have a junior administrator who needs to do backups on this server. You need to ensure that the junior admin can use Windows Server Backup to create a complete backup of Paniva. What should you configure to allow the junior admin to do the backups?

A. The local groups by using Computer Management

B. A task by using Authorization Manager

C. The User Rights Assignment by using the Local Group Policy Editor

D. The Role Assignment by using Authorization Manager

9. Miguel is a junior-level system administrator, and he has basic knowledge about working with Active Directory. As his supervisor, you have asked Miguel to make several security-related changes to OUs within the company's Active Directory domain. You instruct Miguel to use the basic functionality provided in the Delegation of Control Wizard. Which of the following operations are represented as common tasks within the Delegation of Control Wizard? (Choose all that apply.)

A. Reset passwords on user accounts.

B. Manage Group Policy links.

C. Modify the membership of a group.

D. Create, delete, and manage groups.

10. You are the primary system administrator for a large Active Directory domain. Recently, you have hired another system administrator upon whom you intend to offload some of your responsibilities. This system administrator will be responsible for handling help desk calls and for basic user account management. You want to allow the new employee to have permissions to reset passwords for all users within a specific OU. However, for security reasons, it's important that the user not be able to make permissions changes for objects within other OUs in the domain. Which of the following is the best way to do this?

A. Create a special administration account within the OU and grant it full permissions for all objects within Active Directory.

B. Move the user's login account into the OU that the new employee is to administer.

C. Move the user's login account to an OU that contains the OU (that is, the parent OU of the one that the new employee is to administer).

D. Use the Delegation of Control Wizard to assign the necessary permissions on the OU that the new employee is to administer.

Chapter

6

Manage GPOs

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Create Group Policy Objects (GPOs)**

- Configure a Central Store
- Manage starter GPOs
- Configure GPO links
- Configure multiple local group policies
- Configure security filtering

✓ **Configure application restriction policies**

- Configure rule enforcement
- Configure applocker rules
- Configure Software Restriction Policies

For many years, making changes to computer or user environments was a time-consuming process. If you wanted to install a service pack or a piece of software, unless you had a third-party utility, you had to use the *sneakernet* (that is, you had to walk from one computer to another with a disk containing the software).

Installing any type of software or companywide security change was one of the biggest challenges faced by system administrators. It was difficult enough just to deploy and manage workstations throughout the environment. Combine this with the fact that users were generally able to make system configuration changes to their own machines, it quickly became a management nightmare!

For example, imagine that a user noticed that they did not have enough disk space to copy a large file. Instead of seeking assistance from the IT help desk, they may have decided to do a little cleanup on their own. Unfortunately, this cleanup operation may have resulted in deleting critical system files! Or, consider the case of users who changed system settings "just to see what they did." Relatively minor changes, such as modifying TCP/IP bindings or Desktop settings, could cause hours of support headaches. Now multiply these (or other common) problems by hundreds (or even thousands) of end users. Clearly, system administrators needed to have a secure way to limit the options available to users of client operating systems.

How do you prevent problems such as these from occurring in a Windows Server 2012 R2 environment? Fortunately, there's a readily available solution delivered with the base operating system that's easy to implement. Two of the most important system administration features in Windows Server 2012 R2 and Active Directory are *Group Policy* and *Security Policy*. By using *Group Policy objects (GPOs)*, administrators can quickly and easily define restrictions on common actions and then apply them at the site, domain, or organizational unit (OU) level. In this chapter, you will see how group and security policies work, and then you will look at how to implement them within an Active Directory environment.

Introducing Group Policy

One of the strengths of Windows-based operating systems is their flexibility. End users and system administrators can configure many different options to suit the network environment and their personal tastes. However, this flexibility comes at a price—generally, end users on a network should not change many of these options. For example, TCP/IP configuration and security policies should remain consistent for all client computers. In fact, end

users really don't need to be able to change these types of settings in the first place because many of them do not understand the purpose of these settings.

Windows Server 2012 R2 *group policies* are designed to provide system administrators with the ability to customize end-user settings and to place restrictions on the types of actions that users can perform. Group policies can be easily created by system administrators and then later applied to one or more users or computers within the environment. Although they ultimately do affect registry settings, it is much easier to configure and apply settings through the use of Group Policy than it is to make changes to the registry manually. To make management easy, Microsoft has set up Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 so that Group Policy settings are all managed from within the Microsoft Management Console (MMC) in the Group Policy Management Console (GPMC).

Group policies have several potential uses. I'll cover the use of group policies for software deployment, and I'll also focus on the technical background of group policies and how they apply to general configuration management.

Let's begin by looking at how group policies function.

Understanding Group Policy Settings

Group Policy settings are based on *Group Policy administrative templates*. These templates provide a list of user-friendly configuration options and specify the system settings to which they apply. For example, an option for a user or computer that reads Require A Specific Desktop Wallpaper Setting would map to a key in the registry that maintains this value. When the option is set, the appropriate change is made in the registry of the affected users and computers.

By default, Windows Server 2012 R2 comes with several administrative template files that you can use to manage common settings. Additionally, system administrators and application developers can create their own administrative template files to set options for specific functionality.

Most Group Policy items have three different settings options:

Enabled Specifies that a setting for this GPO has been configured. Some settings require values or options to be set.

Disabled Specifies that this option is disabled for client computers. Note that disabling an option *is* a setting. That is, it specifies that the system administrator wants to disallow certain functionality.

Not Configured Specifies that these settings have been neither enabled nor disabled. Not Configured is the default option for most settings. It simply states that this group policy will not specify an option and that other policy settings may take precedence.

The specific options available (and their effects) will depend on the setting. Often, you will need additional information. For example, when setting the Account Lockout policy, you must specify how many bad login attempts may be made before the account is locked out. With this in mind, let's look at the types of user and computer settings that can be managed.

Group Policy settings can apply to two types of Active Directory objects: User objects and Computer objects. Because both users and computers can be placed into groups and organized within OUs, this type of configuration simplifies the management of hundreds, or even thousands, of computers.

The main options you can configure within user and computer group policies are as follows:

Software Settings The *Software Settings* options apply to specific applications and software that might be installed on the computer. System administrators can use these settings to make new applications available to end users and to control the default configuration for these applications.

Windows Settings The *Windows Settings* options allow system administrators to customize the behavior of the Windows operating system. The specific options that are available here are divided into two types: user and computer. User-specific settings let you configure Internet Explorer (including the default home page and other settings). Computer settings include security options, such as Account Policy and Event Log options.

Administrative Templates *Administrative templates* are used to configure user and computer settings further. In addition to the default options available, system administrators can create their own administrative templates with custom options.

Group Policy Preferences The Windows Server 2012 R2 operating system includes *Group Policy preferences (GPPs)*, which give you more than 20 new Group Policy extensions. These extensions, in turn, give you a vast range of configurable settings within a Group Policy object. Included in the new Group Policy preference extensions are settings for folder options, mapped drives, printers, the registry, local users and groups, scheduled tasks, services, and the Start menu.

Besides providing easier management, Group Policy preferences give an administrator the ability to deploy settings for client computers without restricting the users from changing the settings. This gives an administrator the flexibility needed to decide which settings to enforce and which not to enforce.

Figure 6.1 shows some of the options you can configure with Group Policy.

ADMX Central Store Another consideration in GPO settings is whether to set up an *ADMX Central Store*. GPO administrative template files are saved as ADMX (`.admx`) files and AMXL (`.amxl`) for the supported languages. To get the most benefit out of using administrative templates, you should create an ADMX Central Store.

You create the Central Store in the `SYSVOL` folder on a domain controller. The Central Store is a repository for all of your administrative templates, and the Group Policy tools check it. The Group Policy tools then use any ADMX files that they find in the Central Store. These files then replicate to all domain controllers in the domain.

If you want your clients to be able to edit domain-based GPOs by using the ADMX files that are stored in the ADMX Central Store, you must be using Windows Vista, Windows 7, Windows 8, Server 2008, Server 2008 R2, Server 2012, or Server 2012 R2.

Security Template *Security templates* are used to configure security settings through a GPO. Some of the security settings that can be configured are settings for account policies, local policies, event logs, restricted groups, system services, and the registry.

FIGURE 6.1 Group Policy configuration options

Starter GPOs *Starter Group Policy objects* give administrators the ability to store a collection of administrative template policy settings in a single object. Administrators then have the ability to import and export starter GPOs to distribute the GPOs easily to other environments. When a GPO is created from a starter GPO, as with any template, the new GPO receives the settings and values that were defined from the administrative template policy in the starter GPO.

WARNING

Group Policy settings do not take effect immediately. You must run the `gpupdate` command at the command prompt or wait for the regular update cycle in order for the policy changes to take effect.

The Security Settings Section of the GPO

One of the most important sections of a GPO is the Security Settings section. The Security Settings section, under the Windows Settings section, allows an administrator to secure many aspects of the computer and user policies. The following are some of the configurable options for the Security Settings section:

Computer Section Only of the GPO

- Account Policies
- Local Policies
- Event Policies

- Restricted Groups
- System Services
- Registry
- File System
- Wired Network
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Wireless Networks
- Network Access Protection
- Application Control Policies
- IP Security Policies
- Advanced Audit Policy Configuration

Computer and User Sections of the GPO

- Public Key Policies
- Software Restriction Policy

Restricted Groups

The *Restricted Groups* settings allow you to control group membership by using a GPO. The group membership I am referring to is the normal Active Directory groups (domain local, global, and universal). The settings offer two configurable properties: Members and Members Of.

The users on the Members list do not belong to the restricted group. The users on the Members Of list do belong to the restricted group. When you configure a Restricted Group policy, members of the restricted group that are not on the Members list are removed. Users who are on the Members list who are not currently a member of the restricted group are added.

Software Restriction Policy

Software restriction policies allow administrators to identify software and to control its ability to run on the user's local computer, organizational unit, domain, or site. This prevents users from installing unauthorized software. Software Restriction Policy is discussed in greater detail in this chapter in the "Implementing Software Deployment" section.

Group Policy Objects

So far, I have discussed what group policies are designed to do. Now it's time to drill down to determine exactly how you can set up and configure them.

To make them easier to manage, group policies may be placed in items called *Group Policy objects (GPOs)*. GPOs act as containers for the settings made within Group Policy files, which simplifies the management of settings. For example, as a system administrator, you might have different policies for users and computers in different departments. Based

on these requirements, you could create a GPO for members of the Sales department and another for members of the Engineering department. Then you could apply the GPOs to the OU for each department. Another important concept you need to understand is that Group Policy settings are hierarchical; that is, system administrators can apply Group Policy settings at four different levels. These levels determine the GPO processing priority.

Local Every Windows operating system computer has one Group Policy object that is stored locally. This GPO functions for both the computer and user Group Policy processing.

Sites At the highest level, system administrators can configure GPOs to apply to entire sites within an Active Directory environment. These settings apply to all of the domains and servers that are part of a site. Group Policy settings managed at the site level may apply to more than one domain within the same forest. Therefore, they are useful when you want to make settings that apply to all of the domains within an Active Directory tree or forest.

Domains Domains are the third level to which system administrators can assign GPOs. GPO settings placed at the domain level will apply to all of the User and Computer objects within the domain. Usually, system administrators make master settings at the domain level.

Organizational Units The most granular level of settings for GPOs is the OU level. By configuring Group Policy options for OUs, system administrators can take advantage of the hierarchical structure of Active Directory. If the OU structure is planned well, you will find it easy to make logical GPO assignments for various business units at the OU level.

Based on the business need and the organization of the Active Directory environment, system administrators might decide to set up Group Policy settings at any of these four levels. Because the settings are cumulative by default, a User object might receive policy settings from the site level, from the domain level, and from the OUs in which it is contained.

You can also apply Group Policy settings to the local computer (in which case Active Directory is not used at all), but this limits the manageability of the Group Policy settings.

Group Policy Inheritance

In most cases, Group Policy settings are cumulative. For example, a GPO at the domain level might specify that all users within the domain must change their password every 60 days, and a GPO at the OU level might specify the default desktop background for all users and computers within that OU. In this case, both settings apply, so users within the OU are forced to change their password every 60 days and have the default Desktop setting.

What happens if there's a conflict in the settings? For example, suppose you create a scenario where a GPO at the site level specifies that users are to use red wallpaper and another GPO at the OU level specifies that they must use green wallpaper. The users at the OU layer would have green wallpaper by default. Although hypothetical, this raises an important point about *inheritance*. By default, the settings at the most specific level (in this case, the OU that contains the User object) override those at more general levels. As a friend of mine from Microsoft always says, "Last one to apply wins."

Although the default behavior is for settings to be cumulative and inherited, system administrators can modify this behavior. They can set two main options at the various levels to which GPOs might apply.

Block Policy Inheritance The *Block Policy Inheritance* option specifies that Group Policy settings for an object are not inherited from its parents. You might use this, for example, when a child OU requires completely different settings from a parent OU. Note, however, that you should manage blocking policy inheritance carefully because this option allows other system administrators to override the settings made at higher levels.

Force Policy Inheritance The *Enforced option* (sometimes referred as *No Override*) can be placed on a parent object, and it ensures that all lower-level objects inherit these settings. In some cases, system administrators want to ensure that Group Policy inheritance is not blocked at other levels. For example, suppose it is corporate policy that all network accounts are locked out after five incorrect password attempts. In this case, you would not want lower-level system administrators to override the option with other settings.

System administrators generally use this option when they want to enforce a specific setting globally. For example, if a password expiration policy should apply to all users and computers within a domain, a GPO with the *Force Policy Inheritance* option enabled could be created at the domain level.

You must consider one final case: If a conflict exists between the computer and user settings, the user settings take effect. If, for instance, a system administrator applies a default desktop setting for the Computer policy and a different default desktop setting for the User policy, the one they specify in the User policy takes effect. This is because the user settings are more specific, and they allow system administrators to make changes for individual users regardless of the computer they're using.

Planning a Group Policy Strategy

Through the use of Group Policy settings, system administrators can control many different aspects of their network environment. As you'll see throughout this chapter, system administrators can use GPOs to configure user settings and computer configurations. Windows Server 2012 R2 includes many different administrative tools for performing these tasks. However, it's important to keep in mind that, as with many aspects of using Active Directory, a successful Group Policy strategy involves planning.

Because there are thousands of possible Group Policy settings and many different ways to implement them, you should start by determining the business and technical needs of your organization. For example, you should first group your users based on their work functions. You might find, for example, that users in remote branch offices require particular network configuration options. In that case, you might implement Group Policy settings best at the site level. In another instance, you might find that certain departments have varying requirements for disk quota settings. In this case, it would probably make the most sense to apply GPOs to the appropriate department OUs within the domain.

The overall goal should be to reduce complexity (for example, by reducing the overall number of GPOs and GPO links) while still meeting the needs of your users. By taking into

account the various needs of your users and the parts of your organization, you can often determine a logical and efficient method of creating and applying GPOs. Although it's rare that you'll come across a right or wrong method of implementing Group Policy settings, you will usually encounter some that are either better or worse than others.

By implementing a logical and consistent set of policies, you'll also be well prepared to troubleshoot any problems that might come up or to adapt to your organization's changing requirements. Later in this chapter, you'll learn about some specific methods for determining effective Group Policy settings before you apply them.

Implementing Group Policy

Now that I've covered the basic layout and structure of group policies and how they work, let's look at how you can implement them in an Active Directory environment. In the following sections, you'll start by creating GPOs. Then you'll apply these GPOs to specific Active Directory objects, and you'll take a look at how to use administrative templates.

Creating GPOs

In Windows Server 2000 and Windows Server 2003, you could create GPOs from many different locations. For example, you could use Active Directory Users and Computers to create GPOs on your OUs along with other GPO tools. In Windows Server 2012 R2, things are simpler. You can create GPOs for OUs in only one location: the Group Policy Management Console (GPMC). You have your choice of three applications for setting up policies on your Windows Server 2012 R2 computers.

Local Computer Policy Tool This administrative tool allows you to quickly access the Group Policy settings that are available for the local computer. These options apply to the local machine and to users who access it. You must be a member of the local Administrators group to access and make changes to these settings.

Administrators may need the ability to work on multiple local group policy objects (MLGPOs) at the same time. To do this, you would complete the following steps. (You can't configure MLGPOs on domain controllers.)

1. Open the MMC by typing **MMC** in the Run command box.
2. Click File and then click Add/Remove Snap-in.
3. From the available snap-ins list, choose Group Policy Object Editor and click Add.
4. In the Select Group Policy Object dialog box, click the Browse button.
5. Click the Users tab in the Browse For The Group Policy Object dialog box.
6. Click the user or group for which you want to create or edit a local Group Policy and click OK.
7. Click Finish and then click OK.
8. Configure the multiple policy settings.

Group Policy Management Console You must use the GPMC to manage Group Policy deployment. The GPMC provides a single solution for managing all Group Policy–related tasks, and it is also best suited to handle enterprise-level tasks, such as forest-related work.

The GPMC allows administrators to manage Group Policy and GPOs all from one easy-to-use console whether their enterprise solution spans multiple domains and sites within one or more forests or is local to one site. The GPMC adds flexibility, manageability, and functionality. Using this console, you can also perform other functions, such as backup and restore, importing, and copying.

`Auditpol.exe` `Auditpol.exe` is a command-line utility that works with Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. An administrator has the ability to display information about policies and also to perform some functions to manipulate audit policies. Table 6.1 shows some of the switches available for `auditpol.exe`.

TABLE 6.1 `Auditpol.exe` switches

Switch	Description
`/?`	This is the `Auditpol.exe` help command.
`/get`	This allows you to display the current audit policy.
`/set`	This allows you to set a policy.
`/list`	This displays selectable policy elements.
`/backup`	This allows you to save the audit policy to a file.
`/restore`	This restores a policy from previous backup.
`/clear`	This clears the audit policy.
`/remove`	This removes all per-user audit policy settings and disables all system audit policy settings.
`/ResourceSACL`	This configures the Global Resource SACL.

WARNING

You should be careful when making Group Policy settings because certain options might prevent the proper use of systems on your network. Always test Group Policy settings on a small group of users before you deploy them throughout your organization. You'll probably find that some settings need to be changed to be effective.

Exercise 6.1 walks you through the process of installing the Group Policy Management MMC snap-in for editing Group Policy settings and creating a GPO.

EXERCISE 6.1

Creating a Group Policy Object Using the GPMC

1. Click the Windows button and choose Administrative Tools ➢ Group Policy Management. The Group Policy Management tool opens.
2. Expand the Forest, Domains, *your domain name,* and North America containers. Right-click the Corporate OU and then choose Create A GPO In This Domain, And Link It Here.
3. When the New GPO dialog box appears, type **Warning Box** in the Name field. Click OK.
4. The New GPO will be listed on the right side of the Group Policy Management window. Right-click the GPO and choose Edit.

5. In the Group Policy Management Editor, expand the following: Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options. On the right side, scroll down and double-click Interactive Logon: Message Text For Users Attempting To Log On.
6. Click the box Define This Policy Setting In The Template. In the text box, type **Unauthorized use of this machine is prohibited** and then click OK. Close the GPO and return to the GPMC main screen.
7. Under the domain name (in the GPMC), right-click Group Policy Objects and choose New.
8. When the New GPO dialog box appears, type **Unlinked Test GPO** in the Name field. Click OK.
9. On the right side, the new GPO will appear. Right-click Unlinked Test GPO and choose Edit.
10. Under the User Configuration section, click Policies ➢ Administrative Templates ➢ Desktop. On the right side, double-click Hide And Disable All Items On The Desktop and then click Enabled. Click OK and then close the GPMC.

EXERCISE 6.1 *(continued)*

Note that Group Policy changes may not take effect until the next user logs in (some settings may even require that the machine be rebooted). That is, users who are currently working on the system will not see the effects of the changes until they log off and log in again. GPOs are reapplied every 90 minutes with a 30-minute offset. In other words, users who are logged in will have their policies reapplied every 60 to 120 minutes. Not all settings are reapplied (for example, software settings and password policies).

Linking Existing GPOs to Active Directory

Creating a GPO is the first step in assigning group policies. The second step is to link the GPO to a specific Active Directory object. As mentioned earlier in this chapter, GPOs can be linked to sites, domains, and OUs.

Exercise 6.2 walks you through the steps that you must take to assign an existing GPO to an OU within the local domain. In this exercise, you will link the Test Domain Policy GPO to an OU. To complete the steps in this exercise, you must have completed Exercise 6.1.

EXERCISE 6.2

Linking Existing GPOs to Active Directory

1. Open the Group Policy Management Console.
2. Expand the Forest and Domain containers and right-click the Africa OU.
3. Choose Link An Existing GPO.
4. The Select GPO dialog box appears. Click Unlinked Test GPO and click OK.
5. Close the Group Policy Management Console.

Note that the GPMC tool offers a lot of flexibility in assigning GPOs. You can create new GPOs, add multiple GPOs, edit them directly, change priority settings, remove links, and delete GPOs all from within this interface. In general, creating new GPOs using the GPMC tool is the quickest and easiest way to create the settings you need.

To test the Group Policy settings, you can simply create a user account within the Africa OU that you used in Exercise 6.2. Then, using another computer that is a member of the same domain, you can log on as the newly created user.

Managing Group Policy

Now that you have implemented GPOs and applied them to sites, domains, and OUs within Active Directory, it's time to look at some ways to manage them. In the following sections, you'll look at how multiple GPOs can interact with one another and ways that you can

provide security for GPO management. Using these features is an important part of working with Active Directory, and if you properly plan Group Policy, you can greatly reduce the time the help desk spends troubleshooting common problems.

Managing GPOs

One of the benefits of GPOs is that they're modular and can apply to many different objects and levels within Active Directory. This can also be one of the drawbacks of GPOs if they're not managed properly. A common administrative function related to using GPOs is finding all of the Active Directory links for each of these objects. You can do this when you are viewing the Linked Group Policy Objects tab of the site, domain, or OU in the GPMC (shown in Figure 6.2).

FIGURE 6.2 Viewing GPO links to an Active Directory OU

In addition to the common action of delegating permissions on OUs, you can set permissions regarding the modification of GPOs. The best way to accomplish this is to add users to the Group Policy Creator/Owners built-in security group. The members of this group are able to modify security policy. You saw how to add users to groups back in Chapter 5, "Administer Active Directory."

Windows Management Instrumentation

Windows Management Instrumentation (WMI) scripts are used to gather information or to help GPOs deploy better. The best way to explain this is to give an example. Let's say you wanted to deploy Microsoft Office 2013 to everyone in the company. You would first

set up a GPO to deploy the Office package (explained later in the section "Deploying Software Through a GPO").

You can then place a WMI script on the GPO stating that only computers with 10GB of hard disk space actually deploy Office. Now if a computer has 10GB of free space, the Office GPO would get installed. If the computer does not have the 10GB of hard disk space, the GPO will not deploy. You can use WMI scripts to check for computer information such as MAC addresses. WMI is a powerful tool because if you know how to write scripts, the possibilities are endless. The following script is a sample of a WMI that is checking for at least 10GB of free space on the `C:` partition/volume:

```
Select * from Win32_LogicalDisk where FreeSpace > 10737418240 AND
Caption = "C:"
```

Security Filtering of a Group Policy

Another method of securing access to GPOs is to set permissions on the GPOs themselves. You can do this by opening the GPMC, selecting the GPO, and clicking the Advanced button in the Delegation tab. The Unlinked Test GPO Security Settings dialog box appears (see Figure 6.3).

FIGURE 6.3 A GPO's Security Settings dialog box

The following permissions options are available:

- Full Control
- Read
- Write

- Create All Child Objects
- Delete All Child Objects
- Apply Group Policy

You might have to scroll the Permissions window to see the Apply Group Policy item. Of these, the Apply Group Policy setting is particularly important because you use it to filter the scope of the GPO. *Filtering* is the process by which selected security groups are included or excluded from the effects of the GPOs. To specify that the settings should apply to a GPO, you should select the Allow check box for both the Apply Group Policy setting and the Read setting. These settings will be applied only if the security group is also contained within a site, domain, or OU to which the GPO is linked. To disable GPO access for a group, choose Deny for both of these settings. Finally, if you do not want to specify either Allow or Deny, leave both boxes blank. This is effectively the same as having no setting.

In Exercise 6.3, you will filter Group Policy using security groups. To complete the steps in this exercise, you must have completed Exercises 6.1 and 6.2.

EXERCISE 6.3

Filtering Group Policy Using Security Groups

1. Open the Active Directory Users and Computers administrative tool.
2. Create a new OU called **Group Policy Test**.
3. Create two new global security groups within the Group Policy Test OU and name them **PolicyEnabled** and **PolicyDisabled**.
4. Exit Active Directory Users and Computers and open the GPMC.
5. Right-click the Group Policy Test OU and select Link An Existing GPO.
6. Choose Unlinked Test GPO and click OK.
7. Expand the Group Policy Test OU so that you can see the GPO (Unlinked Test GPO) underneath the OU.
8. Click the Delegation tab and then click the Advanced button in the lower-right corner of the window.
9. Click the Add button and type **PolicyEnabled** in the Enter The Object Names To Select field. Click the Check Names button. Then click OK.
10. Add a group named **PolicyDisabled** in the same way.
11. Highlight the PolicyEnabled group and select Allow for the Read and Apply Group Policy permissions. This ensures that users in the PolicyEnabled group will be affected by this policy.

12. Highlight the PolicyDisabled group and select Deny for the Read and Apply Group Policy permissions. This ensures that users in the PolicyDisabled group will not be affected by this policy.
13. Click OK. You will see a message stating that you are choosing to use the Deny permission and that the Deny permission takes precedence over the Allow entries. Click the Yes button to continue.
14. When you have finished, close the GPMC tool.

Delegating Administrative Control of GPOs

So far, you have learned about how to use Group Policy to manage user and computer settings. What you haven't done yet is to determine who can modify GPOs. It's important to establish the appropriate security on GPOs themselves for two reasons.

- If the security settings aren't set properly, users and system administrators can easily override them. This defeats the purpose of having the GPOs in the first place.
- Having many different system administrators creating and modifying GPOs can become extremely difficult to manage. When problems arise, the hierarchical nature of GPO inheritance can make it difficult to pinpoint the problem.

Fortunately, through the use of delegation, determining security permissions for GPOs is a simple task. Exercise 6.4 walks you through the steps that you must take to grant the appropriate permissions to a user account. Specifically, the process involves delegating the ability to manage Group Policy links on an Active Directory object (such as an OU). To complete this exercise, you must have completed Exercises 6.1 and 6.2.

EXERCISE 6.4

Delegating Administrative Control of Group Policy

1. Open the Active Directory Users and Computers tool.
2. Expand the local domain and create a user named **Policy Admin** within the Group Policy Test OU.
3. Exit Active Directory Users and Computers and open the GPMC.
4. Click the Group Policy Test OU and select the Delegation tab.
5. Click the Add button. In the field Enter The Object Name To Select, type **Policy Admin** and click the Check Names button.
6. The Add Group Or User dialog box appears. In the Permissions drop-down list, make sure that the item labeled Edit Settings, Delete, Modify Security is chosen. Click OK.

EXERCISE 6.4 *(continued)*

7. At this point you should be looking at the Group Policy Test Delegation window. Click the Advanced button in the lower-right corner.
8. Highlight the Policy Admin account and check the Allow Full Control box. This user now has full control of these OUs and all child OUs and GPOs for these OUs. Click OK.

   If you just want to give this user individual rights, then, in the Properties window (step 8), click the Advanced button and then the Effective Permissions tab. This is where you can also choose a user and give them only the rights that you want them to have.
9. When you have finished, close the GPMC tool.

Understanding Delegation

Although I have talked about delegation throughout the book, it's important to discuss it again in the context of OUs, Group Policy, and Active Directory.

Once configured, Active Directory administrative delegation allows an administrator to delegate tasks (usually administration related) to specific user accounts or groups. What this means is that if you don't manage it all, the user accounts (or groups) you choose will be able to manage their portions of the tree.

It's important to be aware of the benefits of Active Directory Delegation (AD Delegation). *AD Delegation* will help you manage the assigning of administrative control over objects in Active Directory, such as users, groups, computers, printers, domains, and sites. AD Delegation is used to create more administrators, which essentially saves time.

For example, let's say you have a company whose IT department is small and situated in a central location. The central location connects three other smaller remote sites. These sites do not each warrant a full-time IT person, but the manager on staff (for example) at each remote site can become an administrator for their portion of the tree. If that manager administers the user accounts for the staff at the remote site, this reduces the burden on the system administrator of doing trivial administrative work, such as unlocking user accounts or changing passwords, and thus it reduces costs.

Controlling Inheritance and Filtering Group Policy

Controlling inheritance is an important function when you are managing GPOs. Earlier in this chapter, you learned that, by default, GPO settings flow from higher-level Active Directory objects to lower-level ones. For example, the effective set of Group Policy settings for a user might be based on GPOs assigned at the site level, at the domain level, and in the OU hierarchy. In general, this is probably the behavior you would want.

In some cases, however, you might want to block Group Policy inheritance. You can accomplish this easily by selecting the object to which a GPO has been linked. Right-click the object and choose Block Inheritance (see Figure 6.4). By enabling this option, you are effectively specifying that this object starts with a clean slate; that is, no other Group Policy settings will apply to the contents of this Active Directory site, domain, or OU.

FIGURE 6.4 Blocking GPO inheritance

System administrators can also force inheritance. By setting the Enforced option, they can prevent other system administrators from making changes to default policies. You can set the Enforced option by right-clicking the GPO and choosing the Enforced item (see Figure 6.5).

FIGURE 6.5 Setting the Enforced GPO option

Assigning Script Policies

System administrators might want to make several changes and implement certain settings that would apply while the computer is starting up or the user is logging on. Perhaps the most common operation that logon scripts perform is mapping network drives. Although users can manually map network drives, providing this functionality within login scripts ensures that mappings stay consistent and that users only need to remember the drive letters for their resources.

Script policies are specific options that are part of Group Policy settings for users and computers. These settings direct the operating system to the specific files that should be processed during the startup/shutdown or logon/logoff processes. You can create the scripts by using the *Windows Script Host (WSH)* or with standard batch file commands. WSH allows developers and system administrators to create scripts quickly and easily using Visual Basic Scripting Edition (VBScript) or JScript (Microsoft's implementation of JavaScript). Additionally, WSH can be expanded to accommodate other common scripting languages.

To set script policy options, you simply edit the Group Policy settings. As shown in Figure 6.6, there are two main areas for setting script policy settings.

Startup/Shutdown Scripts These settings are located within the Computer Configuration ➢ Windows Settings ➢ Scripts (Startup/Shutdown) object.

Logon/Logoff Scripts These settings are located within the User Configuration ➢ Windows Settings ➢ Scripts (Logon/Logoff) object.

FIGURE 6.6 Viewing Startup/Shutdown script policy settings

To assign scripts, simply double-click the setting, and its Properties dialog box appears. For instance, if you double-click the Startup setting, the Startup Properties dialog box appears (see Figure 6.7). To add a script filename, click the Add button. When you do, you will be asked to provide the name of the script file (such as `MapNetworkDrives.vbs` or `ResetEnvironment.bat`).

FIGURE 6.7 Setting scripting options

Note that you can change the order in which the scripts are run by using the Up and Down buttons. The Show Files button opens the directory folder in which you should store the Logon script files. To ensure that the files are replicated to all domain controllers, you should be sure you place the files within the SYSVOL share.

Understanding the Loopback Policy

There may be times when the user settings of a Group Policy object should be applied to a computer based on its location instead of the user object. Usually, the user Group Policy processing dictates that the GPOs be applied in order during computer startup based on the computers located in their organizational unit. User GPOs, on the other hand, are applied in order during logon, regardless of the computer to which they log on.

In some situations, this processing order may not be appropriate. A good example is a kiosk machine. You would not want applications that have been assigned or published to a user to be installed when the user is logged on to the kiosk machine. *Loopback Policy* allows two ways to retrieve the list of GPOs for any user when they are using a specific computer in an OU.

Merge Mode The GPOs for the computer are added to the end of the GPOs for the user. Because of this, the computer's GPOs have higher precedence than the user's GPOs.

Replace Mode In Replace mode, the user's GPOs are not used. Only the GPOs of the Computer object are used.

Managing Network Configuration

Group policies are also useful in network configuration. Although administrators can handle network settings at the protocol level using many different methods, such as Dynamic Host Configuration Protocol (DHCP), Group Policy allows them to set which functions and operations are available to users and computers.

Figure 6.8 shows some of the features that are available for managing Group Policy settings. The paths to these settings are as follows:

Computer Network Options These settings are located within the Computer Configuration ➢ Administrative Templates ➢ Network ➢ Network Connections folder.

User Network Options These settings are located within User Configuration ➢ Administrative Templates ➢ Network.

Here are some examples of the types of settings available:

- The ability to allow or disallow the modification of network settings.

  In many environments, the improper changing of network configurations and protocol settings is a common cause of help desk calls.
- The ability to allow or disallow the creation of Remote Access Service (RAS) connections.

FIGURE 6.8 Viewing Group Policy User network configuration options

This option is useful, especially in larger networked environments, because the use of modems and other WAN devices can pose a security threat to the network.

- The ability to set offline files and folders options.

  This is especially useful for keeping files synchronized for traveling users, and it is commonly configured for laptops.

Each setting includes detailed instructions in the description area of the GPO Editor window. By using these configuration options, system administrators can maintain consistency for users and computers and avoid many of the most common troubleshooting calls.

Automatically Enrolling User and Computer Certificates in Group Policy

You can also use Group Policy to enroll user and computer certificates automatically, making the entire certificate process transparent to your end users. Before proceeding, you should understand what certificates are and why they are an important part of network security.

Think of a digital certificate as a carrying case for a public key. A certificate contains the public key and a set of attributes, including the key holder's name and email address.

These attributes specify something about the holder: their identity, what they're allowed to do with the certificate, and so on. The attributes and the public key are bound together because the certificate is digitally signed by the entity that issued it. Anyone who wants to verify the certificate's contents can verify the issuer's signature.

Certificates are one part of what security experts call a *public-key infrastructure (PKI)*. A PKI has several different components that you can mix and match to achieve the desired results. Microsoft's PKI implementation offers the following functions:

Certificate Authorities CAs issue certificates, revoke certificates they've issued, and publish certificates for their clients. Big CAs like Thawte and VeriSign do this for millions of users. If you want, you can also set up your own CA for each department or workgroup in your organization. Each CA is responsible for choosing which attributes it will include in a certificate and what mechanism it will use to verify those attributes before it issues the certificate.

Certificate Publishers They make certificates publicly available, inside or outside an organization. This allows widespread availability of the critical material needed to support the entire PKI.

PKI-Savvy Applications These allow you and your users to do useful things with certificates, such as encrypt email or network connections. Ideally, the user shouldn't have to know (or even be aware of) what the application is doing—everything should work seamlessly and automatically. The best-known examples of PKI-savvy applications are web browsers such as Internet Explorer and Firefox and email applications such as Outlook.

Certificate Templates These act like rubber stamps. By specifying a particular template as the model you want to use for a newly issued certificate, you're actually telling the CA which optional attributes to add to the certificate as well as implicitly telling it how to fill some of the mandatory attributes. Templates greatly simplify the process of issuing certificates because they keep you from having to memorize the names of all of the attributes you may potentially want to put in a certificate.

Learn More About PKI

When discussing certificates, it's also important to mention PKI and its definition. The exam doesn't go deeply into PKI, but I recommend you do some extra research on your own because it is an important technology and shouldn't be overlooked. PKI is actually a simple concept with a lot of moving parts. When broken down to its bare essentials, PKI is nothing more than a server and workstations utilizing a software service to add security to your infrastructure. When you use PKI, you are adding a layer of protection. The auto-enrollment Settings policy determines whether users and/or computers are automatically enrolled for the appropriate certificates when necessary. By default, this policy is enabled if a certificate server is installed, but you can make changes to the settings, as shown in Exercise 6.5.

In Exercise 6.5, you will learn how to configure automatic certificate enrollment in Group Policy. You must have first completed the other exercises in this chapter in order to proceed with Exercise 6.5.

EXERCISE 6.5

Configuring Automatic Certificate Enrollment in Group Policy

1. Open the Group Policy Management Console tool.
2. Right-click the North America OU that you created in the previous exercises in this book.
3. Choose Create A GPO In This Domain And Link It Here and name it **Test CA**. Click OK.
4. Right-click the Test CA GPO and choose Edit.
5. Open Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Public Key Policies.
6. Double-click Certificate Services Client – Auto-Enrollment in the right pane.

7. The Certificate Services Client – Auto-Enrollment Properties dialog box will appear.
8. For now, don't change anything. Just become familiar with the settings in this dialog box. Click OK to close it.

Redirecting Folders

Another set of Group Policy settings that you will learn about are the *folder redirection settings*. Group Policy provides a means for redirecting the `Documents`, `Desktop`, and `Start Menu` folders, as well as cached application data, to network locations. Folder redirection is particularly useful for the following reasons:

- When they are using roaming user profiles, a user's `Documents` folder is copied to the local machine each time they log on. This requires high bandwidth consumption and time if the `Documents` folder is large. If you redirect the `Documents` folder, it stays in the redirected location, and the user opens and saves files directly to that location.
- Documents are always available no matter where the user logs on.
- Data in the shared location can be backed up during the normal backup cycle without user intervention.
- Data can be redirected to a more robust server-side administered disk that is less prone to physical and user errors.

When you decide to redirect folders, you have two options: basic and advanced.

- Basic redirection redirects everyone's folders to the same location (but each user gets their own folder within that location).
- Advanced redirection redirects folders to different locations based on group membership. For instance, you could configure the Engineers group to redirect their folders to `//Engineering1/Documents/` and the Marketing group to `//Marketing1/Documents/`. Again, individual users still get their own folder within the redirected location.

To configure folder redirection, follow the steps in Exercise 6.6. You must have completed the other exercises in this chapter to proceed with this exercise.

EXERCISE 6.6

Configuring Folder Redirection in Group Policy

1. Open the GPMC tool.
2. Open the North America OU and then edit the Test CA GPO.
3. Open User Configuration ➢ Policies ➢ Windows Settings ➢ Folder Redirection ➢ Documents.
4. Right-click Documents, and select Properties.
5. On the Target tab of the Documents Properties dialog box, choose the Basic – Redirect Everyone's Folder To The Same Location selection from the Settings drop-down list.
6. Leave the default option for the Target Folder Location drop-down list and specify a network path in the Root Path field.

7. Click the Settings tab. All of the default settings are self-explanatory and should typically be left at the default setting. Click OK when you have finished.

Folder Redirection Facts

Try not to mix up the concepts of *folder redirection* and *offline folders*, especially in a world with ever-increasing numbers of mobile users. Folder redirection and offline folders are different features.

Windows Server 2012 R2 folder redirection works as follows: The system uses a pointer that moves the folders you want to a location you specify. Users do not see any of this—it is transparent to them. One problem with folder redirection is that it does not work for mobile users (users who will be offline and who will not have access to files they may need).

Offline folders, however, are copies of folders that were local to you. Files are now available locally to you on the system you have with you. They are also located back on the server where they are stored. The next time you log in, the folders are synchronized so that both folders contain the latest data. This is a perfect feature for mobile users, whereas folder redirection provides no benefit for the mobile user.

Managing GPOs with Windows PowerShell Group Policy Cmdlets

As stated earlier in this book, *Windows PowerShell* is a Windows command-line shell and scripting language. Windows PowerShell can also help an administrator automate many of the same tasks that you perform using the Group Policy Management Console.

Windows Server 2012 R2 helps you perform many of the Group Policy tasks by providing more than 25 cmdlets. Each of these cmdlets is a simple, single-function command-line tool.

The Windows PowerShell Group Policy cmdlets can help you perform some of the following tasks for domain-based Group Policy objects:

- Maintain, create, remove, back up, and import GPOs
- Create, update, and remove GPO links to Active Directory containers
- Set Active Directory OUs and domain permissions and inheritance flags
- Configure Group Policy registry settings
- Create and edit Starter GPOs

The requirement for Windows PowerShell Group Policy cmdlets is Windows Server 2012 R2 on either a domain controller or a member server that has the GPMC installed. Windows 7 and Windows 8 also have the ability to use Windows PowerShell Group Policy cmdlets if they have Remote Server Administration Tools (RSAT) installed. RSAT includes the GPMC and its cmdlets. PowerShell is also a requirement.

Deploying Software Through a GPO

It's difficult enough to manage applications on a stand-alone computer. It seems that the process of installing, configuring, and uninstalling applications is never finished. Add in the hassle of computer reboots and reinstalling corrupted applications, and the reduction in productivity can be substantial.

Software administrators who manage software in network environments have even more concerns.

- First, they must determine which applications specific users require.
- Then, IT departments must purchase the appropriate licenses for the software and acquire any necessary media.
- Next, the system administrators need to install the applications on users' machines. This process generally involves help desk staff visiting computers, or it requires end users to install the software themselves. Both processes entail several potential problems, including installation inconsistency and lost productivity from downtime experienced when applications were installed.
- Finally, software administrators still need to manage software updates and remove unused software.

One of the key design goals for Active Directory was to reduce some of the headaches involved in managing software and configurations in a networked environment. To that end, Windows Server 2012 R2 offers several features that can make the task of deploying software easier and less error prone. Before you dive into the technical details, however, you need to examine the issues related to software deployment.

The Software Management Life Cycle

Although it may seem that the use of a new application requires only the installation of the necessary software, the overall process of managing applications involves many more steps. When managing software applications, there are three main phases to their life cycle, as follows:

Phase 1: Deploying Software The first step in using applications is to install them on the appropriate client computers. Generally, some applications are deployed during the initial configuration of a PC, and others are deployed when they are requested. In the latter case, this often used to mean that system administrators and help desk staffs have to visit client computers and manually walk through the installation process. With Windows Server 2012 R2 and GPOs, the entire process can be automated.

Before You Install, Stop

It is important to understand that just because you can easily deploy software, it does not necessarily mean you have the right to do so. Before you install software on client computers, you must make sure you have the appropriate licenses for the software. Furthermore, it's important to take the time to track application installations. As many system administrators have discovered, it's much more difficult to inventory software installations after they've been performed. Another issue you may encounter is that you lack available resources (for instance, your system does not meet the minimum hardware requirements) and that you face problems such as limited hard disk space or memory that may not be able to handle the applications that you want to load and use. You may also find that your user account does not have the permission to install software. It's important to consider not only how you will install software but also whether you can.

Phase 2: Maintaining Software Once an application is installed and in use on client computers, you need to ensure that the software is maintained. You must keep programs up-to-date by applying changes due to bug fixes, enhancements, and other types of updates. This is normally done with service packs, hot fixes, and updates. As with the initial software deployment, software maintenance can be tedious. Some programs require older versions to be uninstalled before updates are added. Others allow for automatically upgrading over existing installations. Managing and deploying software updates can consume a significant amount of the IT staff's time.

Using Windows Update

Make sure that you learn about Windows Update, a service that allows you to connect to Microsoft's website and download what your system may need to bring it up to compliance. This tool is helpful if you are running a stand-alone system, but if you want to deploy software across the enterprise, the best way to accomplish this is first to test the updates you are downloading and make sure you can use them and that they are not bug ridden. Then you can use a tool such as the Windows Server Update Service (WSUS), which was formerly called the Software Update Services (SUS).

You can check for updates at Microsoft's website (`http://update.microsoft.com`). Microsoft likes to ask many types of questions about WSUS on its certification exams. WSUS is described in detail in other Sybex certification books.

Phase 3: Removing Software The end of the life cycle for many software products involves the actual removal of unused programs. Removing software is necessary when applications become outdated or when users no longer require their functionality. One of the traditional problems with uninstalling applications is that many of the installed files may not be removed. Furthermore, the removal of shared components can sometimes cause other programs to stop functioning properly. Also, users often forget to uninstall applications that they no longer need, and these programs continue to occupy disk space and consume valuable system resources.

The Microsoft Windows Installer (MSI) manages each of these three phases of the software maintenance life cycle. Now that you have an overview of the process, let's move forward to look at the steps involved in deploying software using Group Policy.

The *Microsoft Windows Installer* (sometimes referred to as Microsoft Installer or Windows Installer) is an application installation and configuration service. An instruction file (the Microsoft Installer package) contains information about what needs to be done to install a product. It's common to confuse the two.

The Windows Installer

If you've installed newer application programs (such as Microsoft Office 2013), you've probably noticed the updated setup and installation routines. Applications that comply with the updated standard use the *Windows Installer specification* and MSI software packages for deployment. Each package contains information about various setup options and the files required for installation. Although the benefits may not seem dramatic on the surface, there's a lot of new functionality under the hood.

The Windows Installer was created to solve many of the problems associated with traditional application development. It has several components, including the Installer service (which runs on Windows 2000, XP, Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 computers), the Installer program (`msiexec.exe`) that is responsible for executing the instructions in a *Windows Installer package*, and the specifications third-party developers use to create their own packages. Within each installation package file is a relational structure (similar to the structure of tables in databases) that records information about the programs contained within the package.

To appreciate the true value of the Windows Installer, you'll need to look at some of the problems with traditional software deployment mechanisms and then at how the Windows Installer addresses many of them.

Application Installation Issues

Before the Windows Installer, applications were installed using a setup program that managed the various operations required for a program to operate. These operations included copying files, changing registry settings, and managing any other operating system changes that might be required (such as starting or stopping services). However, this method had several problems:

- The setup process was not robust, and aborting the operation often left many unnecessary files in the file system.
- The process included uninstalling an application (this also often left many unnecessary files in the file system) and remnants in the Windows registry and operating system folders. Over time, these remnants would result in reduced overall system performance and wasted disk space.
- There was no standard method for applying upgrades to applications, and installing a new version often required users to uninstall the old application, reboot, and then install the new program.
- Conflicts between different versions of *dynamic link libraries (DLLs)*—shared program code used across different applications—could cause the installation or removal of one application to break the functionality of another.

Benefits of the Windows Installer

Because of the many problems associated with traditional software installation, Microsoft created the *Windows Installer*. This system provides for better manageability of the software installation process and allows system administrators more control over the deployment process. Specifically, the Windows Installer provides the following benefits:

Improved Software Removal The process of removing software is an important one because remnants left behind during the uninstall process can eventually clutter up the registry and file system. During the installation process, the Windows Installer keeps track of all of the changes made by a setup package. When it comes time to remove an application, all of these changes can then be rolled back.

More Robust Installation Routines If a typical setup program is aborted during the software installation process, the results are unpredictable. If the actual installation hasn't yet begun, then the installer generally removes any temporary files that may have been created. However, if the file copy routine starts before the system encounters an error, it is likely that the files will not be automatically removed from the operating system. In contrast, the Windows Installer allows you to roll back any changes when the application setup process is aborted.

Ability to Use Elevated Privileges Installing applications usually requires the user to have Administrator permissions on the local computer because file system and registry changes are required. When installing software for network users, system administrators have two options. First, they can log off of the computer before installing the software and then log back on as a user who has Administrator permissions on the local computer. This method is tedious and time-consuming. The second option is to give users Administrator permissions temporarily on their own machines. This method could cause security problems and requires the attention of a system administrator.

Through the use of the Installer service, the Windows Installer is able to use temporarily elevated privileges to install applications. This allows users, regardless of their security settings, to execute the installation of authorized applications. This saves time and preserves security.

Support for Repairing Corrupted Applications Regardless of how well a network environment is managed, critical files are sometimes lost or corrupted. Such problems can prevent applications from running properly and can cause crashes. Windows Installer packages provide you with the ability to verify the installation of an application and, if necessary, replace any missing or corrupted files. This support saves time and lessens end-user headaches associated with removing and reinstalling an entire application to replace just a few files.

Prevention of File Conflicts Generally, different versions of the same files should be compatible with each other. In the real world, however, this isn't always the case. A classic problem in the Windows world is the case of one program replacing DLLs that are used by several other programs. Windows Installer accurately tracks which files are used by certain programs and ensures that any shared files are not improperly deleted or overwritten.

Automated Installations A typical application setup process requires end users or system administrators to respond to several prompts. For example, a user may be able to choose the program group in which icons will be created and the file system location to which the program will be installed. Additionally, they may be required to choose which options are installed. Although this type of flexibility is useful, it can be tedious when you are rolling out multiple applications. By using features of the Windows Installer, however, users are able to specify setup options before the process begins. This allows system administrators to ensure consistency in installations, and it saves users time.

Advertising and On-Demand Installations One of the most powerful features of the Windows Installer is its ability to perform on-demand software installations. Prior to the

Windows Installer, application installation options were quite basic—either a program was installed or it was not. When setting up a computer, system administrators would be required to guess which applications the user might need and install all of them.

The Windows Installer supports a function known as advertising. *Advertising* makes applications appear to be available via the Start menu. However, the programs themselves may not actually be installed on the system. When a user attempts to access an advertised application, the Windows Installer automatically downloads the necessary files from a server and installs the program. The result is that applications are installed only when they are needed, and the process requires no intervention from the end user. We'll cover the details of this process later in this chapter.

To anyone who has managed many software applications in a network environment, all of these features of the Windows Installer are likely welcome ones. They also make life easier for end users and application developers; they can focus on the "real work" that their jobs demand.

Windows Installer File Types

When performing software deployment with the Windows Installer in Windows Server 2012 R2, you may encounter several different file types.

Microsoft Windows Installer Packages To take full advantage of Windows Installer functionality, applications must include Microsoft Windows Installer packages. Third-party application vendors and software developers normally create these packages, and they include the information required to install and configure the application and any supporting files.

Microsoft Transformation Files *Microsoft Transformation (MST) files* are useful when you are customizing the details of how applications are installed. When a system administrator chooses to assign or publish an application, they may want to specify additional options for the package. For example, if a system administrator wants to allow users to install only the Microsoft Word and Microsoft PowerPoint components of Office 2013, they could specify these options within a transformation file. Then, when users install the application, they will be provided only with the options related to these components.

Microsoft Patches To maintain software, patches are often required. Patches may make registry and/or file system changes. *Patch files (MSP)* are used for minor system changes and are subject to certain limitations. Specifically, a patch file cannot remove any installed program components and cannot delete or modify any shortcuts created by the user.

Initialization Files To provide support for publishing non-Windows Installer applications, *initialization files* can be used. These files provide links to a standard executable file that is used to install an application. An example might be `\\server1\software\program1\setup.exe`. These files can then be published and advertised, and users can access the *Add Or Remove Programs* icon to install them over the network.

Application Assignment Scripts *Application assignment scripts (AAS)* store information regarding assigning programs and any settings that the system administrator makes. These files are created when Group Policy is used to create software package assignments for users and computers.

Each of these types of files provides functionality that allows the system administrator to customize software deployment. Windows Installer packages have special properties that you can view by right-clicking the file in Windows Explorer and choosing Properties (see Figure 6.9).

FIGURE 6.9 Viewing the properties of an MSI package file

Deploying Applications

The functionality provided by Windows Installer offers many advantages to end users who install their own software. However, that is just the beginning in a networked environment. As you'll see later in this chapter, the various features of Windows Installer and compatible packages allow system administrators to determine centrally applications that users will be able to install.

There are two main methods of making programs available to end users using Active Directory: assigning and publishing. Both assigning and publishing applications greatly ease the process of deploying and managing applications in a network environment.

In the following sections, you'll look at how the processes of assigning and publishing applications can make life easier for IT staff and users alike. The various settings for assigned and published applications are managed through the use of GPOs.

Assigning Applications

Software applications can be assigned to users and computers. *Assigning* a software package makes the program available for automatic installation. The applications advertise their availability to the affected users or computers by placing icons within the `Programs` folder of the Start menu for Windows 8 (and before) and Windows Server 2012, and within the Apps area on Windows 8.1 and Windows Server 2012 R2.

When applications are assigned to a user, programs will be advertised to the user regardless of which computer they are using. That is, icons for the advertised program will appear regardless of whether the program is installed on that computer. If the user clicks an icon for a program that has not yet been installed on the local computer, the application will automatically be accessed from a server and it will be installed.

When an application is assigned to a computer, the program is made available to any users of the computer. For example, all users who log on to a computer that has been assigned Microsoft Office 2013 will have access to the components of the application. If the user did not previously install Microsoft Office 2013, they will be prompted for any required setup information when the program first runs.

Generally, applications that are required by the vast majority of users should be assigned to computers. This reduces the amount of network bandwidth required to install applications on demand and improves the end-user experience by preventing the delay involved when installing an application the first time it is accessed. Any applications that may be used by only a few users (or those with specific job tasks) should be assigned to users.

Publishing Applications

When applications are *published*, they are advertised, but no icons are automatically created. Instead, the applications are made available for installation using the Add Or Remove Programs icon in Control Panel.

Windows Vista, Windows 7, and Windows 8 do not have the Add Or Remove Programs feature. They use the Programs icon in Control Panel to install the software.

Implementing Software Deployment

So far, you have become familiar with the issues related to software deployment and management from a theoretical level. Now it's time to drill down into the actual steps required to deploy software using the features of Active Directory and the GPMC. In the following

sections, you will walk through the steps required to create an application distribution share point, to publish and assign applications, to update previously installed applications, to verify the installation of applications, and to update Windows operating systems.

Preparing for Software Deployment

Before you can install applications on client computers, you must make sure that the necessary files are available to end users. In many network environments, system administrators create shares on file servers that include the installation files for many applications. Based on security permissions, either end users or system administrators can then connect to these shares from a client computer and install the needed software. The efficient organization of these shares can save the help desk from having to carry around a library of DVDs, and it allows you to install applications easily on many computers at once.

One of the problems in network environments is that users frequently install applications whether or not they really need them. They may stumble upon applications that are stored on common file servers and install them out of curiosity. These actions can often decrease productivity and may violate software licensing agreements. You can help avoid this by placing all of your application installation files in hidden shares (for example, `software$`).

Exercise 6.7 walks you through the process of creating a software distribution share point. In this exercise, you will prepare for software deployment by creating a directory share and placing certain types of files in this directory. To complete the steps in this exercise, you must have access to the Microsoft Office 2010 or Microsoft Office 2013 installation files (via DVD or through a network share) and have 2,000MB of free disk space. For this exercise, I used Microsoft Office 2013.

EXERCISE 6.7

Creating a Software Deployment Share

1. Using Windows Explorer, create a folder called `Software` that you can use with application sharing. Be sure that the volume on which you create this folder has at least 2,000MB of available disk space.
2. Create a folder called `Office 2013` within the `Software` folder.
3. Copy all of the installation files for Microsoft Office 2013 from the DVD or network share containing the files to the `Office 2013` folder you created in step 2. If you prefer, you can use switches to install all of the Office 2013 installation files. You can find these switches at `http://technet.microsoft.com/en-us/library/ee624360.aspx`.

4. Right-click the `Software` folder (created in step 1) and select Share. In the Choose People On Your Network To Share With dialog box, type **Everyone**, and click the Add button. Next click the Share button. When you see a message that the sharing process is complete, click Done.

Once you have created an application distribution share, it's time to publish and assign the applications. This topic is covered next.

Software Restriction Policies

One of the biggest problems that we face as IT managers is users downloading and installing software. Many software packages don't cause any issues and are completely safe. Unfortunately, many software packages do have viruses and can cause problems. This is where software restriction policies can help. Software restriction policies help to identify software and to control its ability to run on a local computer, organizational unit, domain, or site.

Software restriction policies give administrators the ability to regulate unknown or untrusted software. Software restriction policies allow you to protect your computers from unwanted software by identifying and also specifying what software packages are allowed to be installed.

When configuring software restriction policies, an administrator is able to define a default security level of Unrestricted (software is allowed) or Disallowed (software is not allowed to run) for a GPO. Administrators can make exceptions to this default security level. They can create software restriction policy rules for specific software.

To create a software policy using the Group Policy Management Console, create a new GPO. In the GPO, expand the Windows Settings for either the user or computer configuration section, expand Security, right-click Software Restriction Policy, and choose New Software Restriction Policy. Set the policy for the level of security that you need.

Using AppLocker

AppLocker is a feature in Windows 7, Windows 8, Windows Server 2012, and Windows Server 2012 R2. It is the replacement for software restriction policies. *AppLocker* allows you to configure a Denied list and an Accepted list for applications. Applications that are configured on the Denied list will not run on the system, whereas applications on the Accepted list will operate properly.

The new capabilities and extensions of the AppLocker feature help reduce administrative overhead and help administrators control how users can access and use files, such as EXE files, scripts, Windows Installer files (MSI and MSP files), and DLLs.

Group Policy Slow Link Detection

When setting up GPOs, most of us assume that the connection speeds between servers and clients are going to be fast. In today's world, it is unlikely to see slow connections between

locations, but they are still out there. Sometimes connection speeds can cause issues with the deployment of GPOs, specifically ones that are deploying software.

A setting in the Computer and User section of the GPO called *Group Policy Slow Link Detection* defines a slow connection for the purposes of applying and updating GPOs. If the data transfer rate from the domain controller providing the GPO to the computer is slower than what you have specified in this setting, the connection is considered to be a slow connection. If a connection is considered slow, the system response will vary depending on the policy. For example, if a GPO is going to deploy software and the connection is considered slow, the software may not be installed on the client computer. If you configure this option as 0, all connections are considered fast connections.

Publishing and Assigning Applications

As mentioned earlier in this section, system administrators can make software packages available to users by using publishing and assigning operations. Both of these operations allow system administrators to leverage the power of Active Directory and, specifically, GPOs to determine which applications are available to users. Additionally, OUs can provide the organization that can help group users based on their job functions and software requirements.

The general process involves creating a GPO that includes software deployment settings for users and computers and then linking this GPO to Active Directory objects.

Exercise 6.8 walks you through the steps required to publish and assign applications. In this exercise, you will create applications and assign them to specific Active Directory objects using GPOs. To complete the steps in this exercise, you must have completed Exercise 6.7.

EXERCISE 6.8

Publishing and Assigning Applications Using Group Policy

1. Open the Active Directory Users and Computers tool from the Administrative Tools program group (using the Windows key).
2. Expand the domain and create a new top-level OU called **Software**.
3. Within the Software OU, create a user named **Jane User** with a login name of **juser** (choose the defaults for all other options).
4. Exit Active Directory Users and Computers and open the Group Policy Management Console.
5. Right-click the Software OU and choose Create A GPO In This Domain And Link It Here.
6. For the name of the new GPO, type **Software Deployment**.
7. To edit the Software Deployment GPO, right-click it and choose Edit. Expand the Computer Configuration ➢ Policies ➢ Software Settings object.

8. Right-click the Software Installation item and select New ➢ Package.
9. Navigate to the Software share you created in Exercise 6.7.
10. Within the Software share, double-click the `Office 2013` folder and select the appropriate MSI file depending on the version of Office 2013 you have. Office 2013 Professional is being used in this example, so you'll see that the `OFFICEMUI.MSI` file is chosen. Click Open.
11. In the Deploy Software dialog box, choose Advanced. (Note that the Published option is unavailable because applications cannot be published to computers.) Click OK to return to the Deploy Software dialog box.
12. To examine the deployment options of this package, click the Deployment tab. Accept the default settings by clicking OK.
13. Within the Group Policy Object Editor, expand the User Configuration ➢ Software Settings object.
14. Right-click the Software Installation item and select New ➢ Package.
15. Navigate to the Software share you created in Exercise 6.7.
16. Within the Software share, double-click the `Office 2013` folder and select the appropriate MSI file. Click Open.
17. For the Software Deployment option, select Published in the Deploy Software dialog box and click OK.
18. Close the GPMC.

The overall process involved with deploying software using Active Directory is quite simple. However, you shouldn't let the intuitive graphical interface fool you—there's a lot of power under the hood of these software deployment features! Once you've properly assigned and published applications, it's time to see the effects of your work.

Applying Software Updates

The steps described in the previous section work only when you are installing a new application. However, software companies often release updates that you need to install on top of existing applications. These updates usually consist of bug fixes or other changes that are required to keep the software up-to-date. You can apply software updates in Active Directory by using the Upgrades tab of the software package Properties dialog box found in the Group Policy Object Editor.

In Exercise 6.9, you will apply a software update to an existing application. You should add the upgrade package to the GPO in the same way you added the original application in steps 8 through 12 of Exercise 6.8. You should also have completed Exercise 6.8 before attempting this exercise.

EXERCISE 6.9

Applying Software Updates

1. Open the Group Policy Management Console from the Administrative Tools program group.
2. Click the Software OU, right-click the Software Deployment GPO, and choose Edit.
3. Expand the Computer Configuration ➢ Policies ➢ Software Settings ➢ Software Installation object.
4. Right-click the software package and select Properties from the context menu to bring up the Properties dialog box.
5. Select the Upgrades tab and click the Add button.
6. Click the Current Group Policy Object (GPO) radio button in the Choose A Package From section of the dialog box or click the Browse button to select the GPO to which you want to apply the upgrade. Consult your application's documentation to see whether you should choose the Uninstall The Existing Package, Then Install The Upgrade Package radio button or the Package Can Upgrade Over The Existing Package radio button.
7. Click Cancel to close the Add Upgrade Package dialog box.
8. Click Cancel and exit the GPMC.

You should understand that not all upgrades make sense in all situations. For instance, if the Paniva 2010 files are incompatible with the Paniva 2013 application, then your Paniva 2010 users might not want you to perform the upgrade without taking additional steps to ensure that they can continue to use their files. In addition, users might have some choice about which version they use when it doesn't affect the support of the network.

Regardless of the underlying reason for allowing this flexibility, you should be aware that there are two basic types of upgrades that are available for administrators to provide to the users:

Mandatory Upgrade Forces everyone who currently has an existing version of the program to upgrade according to the GPO. Users who have never installed the program for whatever reason will be able to install only the new, upgraded version.

Nonmandatory Upgrade Allows users to choose whether they would like to upgrade. This upgrade type also allows users who do not have their application installed to choose which version they would like to use.

Verifying Software Installation

To ensure that the software installation settings you make in a GPO have taken place, you can log into the domain from a Windows 8, Windows 7, or Windows Vista computer that

is within the OU to which the software settings apply. When you log in, you will notice two changes. First the application is installed on the computer (if it was not installed already). To access the application, a user needs to click one of the icons within the Program group of the Start menu. Note also that applications are available to any of the users who log on to this machine. Second, the settings apply to any computers that are contained within the OU and to any users who log on to these computers.

If you publish an application to users, the change may not be as evident, but it is equally useful. When you log on to a Windows 8, Windows 7, or Windows Vista computer that is a member of the domain, and when you use a user account from the OU where you published the application, you will be able to install any of the published applications automatically. On a Windows 8 or Windows 7 computer, you can do this by accessing the Programs icon in Control Panel. By clicking Add New Programs, you access a display of the applications available for installation. By clicking the Add button in the Add New Programs section of the Programs dialog box, you will automatically begin the installation of the published application.

Configuring Automatic Updates in Group Policy

So far you've seen the advantages of deploying application software in a group policy. Group policies also provide a way to install operating system updates across the network for Windows 2000, XP, Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 machines using Windows Update in conjunction with Windows Server Update Service. WSUS is the newer version of SUS, and it is used on a Windows Server 2012 R2 system to update systems. As you may remember, WSUS and SUS are patch-management tools that help you deploy updates to your systems in a controlled manner.

Windows Update is available through the Microsoft website, and it is used to provide the most current files for Windows operating systems. Examples of updates include security fixes, critical updates, updated help files, and updated drivers. You can access Windows Update by clicking the Windows Update icon in the system tray.

WSUS is used to leverage the features of Windows Update within a corporate environment by downloading Windows updates to a corporate server, which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment.

Within an enterprise network that is using Active Directory, you would typically see automatic updates configured through Group Policy. Group policies are used to manage configuration and security settings via Active Directory. Group Policy is also used to specify what server a client will use for automatic updates.

If the WSUS client were part of an enterprise network that is using Active Directory, you would configure the client via a group policy.

Configuring Software Deployment Settings

In addition to the basic operations of assigning and publishing applications, you can use several other options to specify the details of how software is deployed. In the following sections, you will examine the various options that are available and their effects on the software installation process.

The Software Installation Properties Dialog Box

The most important software deployment settings are contained in the Software Installation Properties dialog box, which you can access by right-clicking the Software Installation item and selecting Properties from the context menu. The following sections describe the features contained on the various tabs of the dialog box.

Managing Package Defaults

On the Deployment tab of the Software Installation Properties dialog box, you'll be able to specify some defaults for any packages that you create within this GPO. Figure 6.10 shows the Deployment options for managing software installation settings.

FIGURE 6.10 Deployment tab of the Software Installation Properties dialog box

The following options are used for managing software installation settings:

Default Package Location This setting specifies the default file system or network location for software installation packages. This is useful if you are already using a specific share on a file server for hosting the necessary installation files.

New Packages These settings specify the default type of package assignment that will be used when you add a new package to either the user or computer settings. If you'll be assigning or publishing multiple packages, you may find it useful to set a default here. Selecting the Advanced option (see Figure 6.11) enables Group Policy to display the package's Properties dialog box each time a new package is added.

FIGURE 6.11 Advanced Deployment dialog box

Installation User Interface Options When installing an application, system administrators may or may not want end users to see all of the advanced installation options. If Basic is chosen, the user will be able to configure only the minimal settings (such as the installation location). If Maximum is chosen, all of the available installation options will be displayed. The specific installation options available will depend on the package itself.

Uninstall Applications When They Fall Out Of The Scope of Management So far, you have seen how applications can be assigned and published to users or computers. But what happens when effective GPOs change? For example, suppose User A is currently located within the Sales OU. A GPO that assigns the Microsoft Office 2013 suite of applications is linked to the Sales OU. You decide to move User A to the Engineering OU, which has no software deployment settings. Should the application be uninstalled or should it remain?

If the Uninstall Applications When They Fall Out Of The Scope of Management option is checked, applications will be removed if they are not specifically assigned or published

within GPOs. In this example, this means Office 2013 would be uninstalled for User A. If this box is left unchecked, however, the application will remain installed.

Managing File Extension Mappings

One of the potential problems associated with using many different file types is that it's difficult to keep track of which applications work with which files. For example, if you received a file with the filename extension `.abc`, you would have no idea which application you would need to view it.

Fortunately, through software deployment settings, system administrators can specify mappings for specific *filename extensions*. For example, you could specify that whenever users attempt to access a file with the extension `.vsd`, the operating system should attempt to open the file using Visio diagramming software. If Visio is not installed on the user's machine, the computer can automatically download and install it (assuming that the application has been properly advertised).

This method allows users to have applications automatically installed when they are needed. The following is an example of a sequence of events that might occur:

1. A user receives an email message that contains a PDF (`.pdf`) file attachment.
2. The computer realizes that the PDF file does not have the appropriate viewing application for this type of file installed. However, it also realizes that a filename extension mapping is available within the Active Directory software deployment settings.
3. The client computer automatically requests the PDF software package from the server, and it uses the Microsoft Windows Installer to install the application automatically.
4. The computer opens the attachment for the user.

Notice that all of these steps were carried out without any further interaction with the user.

You can manage filename extension mappings by right-clicking the Software Installation item, selecting Properties, and then clicking the File Extensions tab.

Creating Application Categories

In many network environments, the list of supported applications can include hundreds of items. For users who are looking for only one specific program, searching through a list of all of these programs can be difficult and time-consuming.

Fortunately, methods for categorizing the applications are available on your network. You can easily manage the application categories for users and computers by right-clicking the Software Installation item, selecting Properties, and then clicking the Categories tab.

Figure 6.12 shows you the categories tab of the Software Installation package. When creating categories, it is a good idea to use category names that are meaningful to users because it will make it easier for them to find the programs they're seeking.

Once the software installation categories have been created, you can view them by clicking the Programs or Programs And Features icon in Control Panel. When you click Add New Programs, you'll see that several options appear in the Category drop-down list. Now when you select the properties for a package, you will be able to assign the application to one or more of the categories.

FIGURE 6.12 The Categories tab of the Software Installation Properties dialog box

Removing Programs

As discussed in the beginning of the chapter, an important phase in the software management life cycle is the removal of applications. Fortunately, if you use the GPMC and the Windows Installer packages, the process is simple. To remove an application, you can right-click the package within the Group Policy settings and select All Tasks ➢ Remove (see Figure 6.13).

When choosing to remove a software package from a GPO, you have two options, shown here:

Immediately Uninstall The Software From Users And Computers System administrators can choose this option to ensure that an application is no longer available to users who are affected by the GPO. When this option is selected, the program will be uninstalled automatically from users and/or computers that have the package. This option might be useful, for example, if the license for a certain application has expired or if a program is no longer on the approved applications list.

Allow Users To Continue To Use The Software, But Prevent New Installations This option prevents users from making new installations of a package, but it does not remove the software if it has already been installed for users. This is a good option if the company has run out of additional licenses for the software but the existing licenses are still valid. Figure 6.14 shows these two removal options.

If you no longer require the ability to install or repair an application, you can delete it from your software distribution share point by deleting the appropriate Windows Installer package files. This will free up additional disk space for newer applications.

FIGURE 6.13 Removing a software package

FIGURE 6.14 Software removal options

Microsoft Windows Installer Settings

Several options influence the behavior of the Windows Installer; you can set them within a GPO. You can access these options by navigating to User Configuration ➢ Administrative Templates ➢ Windows Components ➢ Windows Installer (see Figure 6.15).
The options are as follows:

Always Install With Elevated Privileges This policy allows users to install applications that require elevated privileges. For example, if a user does not have the permissions necessary to modify the registry but the installation program must make registry changes, this policy will allow the process to succeed.

FIGURE 6.15 GPO settings for Windows Installer

Prevent Removable Media Source For Any Install This option disallows the installation of software using removable media (such as a CD-ROM or DVD-ROM). It is useful for ensuring that users install only approved applications.

Prohibit Rollback When this option is enabled, the Windows Installer does not store the system state information that is required to roll back the installation of an application. System administrators may choose this option to reduce the amount of temporary disk space required during installation and to increase the performance of the installation operation. However, the drawback is that the system cannot roll back to its original state if the installation fails and the application needs to be removed.

Specify The Order In Which Windows Installer Searches This setting specifies the order in which the Windows Installer will search for installation files. The options include *n* (for network shares), *m* (for searching removal media), and *u* (for searching the Internet for installation files).

With these options, system administrators can control how the Windows Installer operates for specific users who are affected by the GPO.

Troubleshooting Group Policies

Because of the wide variety of configurations that are possible when you are establishing GPOs, you should be aware of some common troubleshooting methods. These methods will help isolate problems in policy settings or GPO links.

One possible problem with GPO configuration is that logons and system startups may take a long time. This occurs especially in large environments when the Group Policy settings must be transmitted over the network and, in many cases, slow WAN links. In general, the number of GPOs should be limited because of the processing overhead and network requirements during logon. By default, GPOs are processed in a synchronous manner. This means that the processing of one GPO must be completed before another one is applied (as opposed to asynchronous processing, where they can all execute at the same time).

When a group policy gets processed on a Windows-based operating system, client-side extensions are the mechanisms that interpret the stored policy and then make the appropriate changes to the operating system environment. When an administrator is troubleshooting a given extension's application of policy, the administrator can view the configuration parameters for that extension in the operating system's registry. To view the extension in the registry, you would view the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows \CurrentVersion\Group Policy
```

The most common issue associated with Group Policy is the unexpected setting of Group Policy options. In Windows Server 2000, administrators spent countless hours analyzing inheritance hierarchy and individual settings to determine why a particular user or computer was having policy problems. For instance, say a user named wpanek complains that the Run option is missing from his Start menu. The wpanek user account is stored in the New Hampshire OU, and you've applied group policies at the OU, domain, and site levels. To determine the source of the problem, you would have to sift through each GPO manually to find the Start menu policy as well as to figure out the applicable inheritance settings.

Windows Server 2012 R2 has a handy feature called *Resultant Set of Policy (RSoP)* that displays the exact settings that actually apply to individual users, computers, OUs, domains, and sites after inheritance and filtering have taken effect. In the example just described, you could run RSoP on the wpanek account and view a single set of Group Policy settings that represent the settings that apply to that account. In addition, each setting's Properties dialog box displays the GPO from which the setting is derived as well as the order of priority, the filter status, and other useful information, as you will see a bit later.

RSoP actually runs in two modes.

Logging Mode *Logging mode* displays the actual settings that apply to users and computers, as shown in the example in the preceding paragraph.

Planning Mode *Planning mode* can be applied to users, computers, OUs, domains, and sites, and you use it before you apply any settings. As its name implies, planning mode is used to plan GPOs.

Additionally, you can run the command-line utility `gpresult.exe` to get a quick snapshot of the Group Policy settings that apply to a user and/or computer. Let's take a closer look at the two modes and the `gpresult.exe` command.

RSoP in Logging Mode

RSoP in logging mode can query policy settings only for users and computers. The easiest way to access RSoP in logging mode is through the Active Directory Users and Computers tool, although you can run it as a stand-alone MMC snap-in if you want.

To analyze the policy settings for wpanek from the earlier example, you would right-click the user icon in Active Directory Users and Computers and select All Tasks ➢ Resultant Set of Policy (Logging). The Group Policy Results Wizard appears. The wizard walks you through the steps necessary to view the RSoP for wpanek.

The Computer Selection page, shown in Figure 6.16, requires you to select a computer for which to display settings. Remember that a GPO contains both user and computer settings, so you must choose a computer to which the user is logged on in order to continue with the wizard. If the user has never logged on to a computer, then you must run RSoP in planning mode because there is no logged policy information yet for that user.

The User Selection page, shown in Figure 6.17, requires you to select a user account to analyze. Because I selected a user from the Active Directory Users and Computers tool, the username is filled in automatically. This page is most useful if you are running RSoP in MMC mode and don't have the luxury of selecting a user contextually.

FIGURE 6.16 The Computer Selection page of the Group Policy Results Wizard

FIGURE 6.17 The User Selection page of the Group Policy Results Wizard

The Summary Of Selections page, shown in Figure 6.18, summarizes your choices and provides an option for gathering extended error information. If you need to make any changes before you begin to analyze the policy settings, you should click the Back button on the Summary screen. Otherwise, click Next.

FIGURE 6.18 The Summary Of Selections page of the Group Policy Results Wizard

After the wizard is complete, you will see the window shown in Figure 6.19. This window displays only the policy settings that apply to the user and computer that you selected in the wizard. You can see these users and computers at the topmost level of the tree.

FIGURE 6.19 The User Selection page for the administrator on computer SERVER1

Any warnings or errors appear as a yellow triangle or red *X* over the applicable icon at the level where the warning or error occurred. To view more information about the warning or error, right-click the icon and select Properties, as shown in Figure 6.20.

You cannot make changes to any of the individual settings because RSoP is a diagnostic tool and not an editor, but you can get more information about settings by clicking a setting and selecting Properties from the context menu.

The Details tab of the user's Properties window, shown in Figure 6.21, displays the actual setting that applies to the user in question based on GPO inheritance.

RSoP in Planning Mode

Running RSoP in planning mode isn't much different from running RSoP in logging mode, but the RSoP Wizard asks for a bit more information than you saw earlier.

In the former example, wpanek couldn't see the Run option in the Start menu because his user account is affected by the New Hampshire GPO in the San Jose OU. As an administrator, you could plan to move his user account to the North America OU. Before doing so, you could verify his new policy settings by running RSoP in planning mode. Run the RSoP on the user wpanek under the scenario that you've already moved him from the San Jose OU to the North America OU. At this point, you haven't actually moved the user, but you can see what his settings would be if you did.

FIGURE 6.20 Details of event pertaining to the administrator account on computer SERVER1

FIGURE 6.21 The Details tab of the object's Properties window

Using the *gpresult.exe* Command

The command-line utility `gpresult.exe` is included as part of the RSoP tool. Running the command by itself without any switches returns the following Group Policy information about the local user and computer:

- The name of the domain controller from which the local machine retrieved the policy information
- The date and time at which the policies were applied
- Which policies were applied
- Which policies were filtered out
- Group membership

You can use the switches shown in Table 6.2 to get information for remote users and computers and to enable other options.

Table 6.2 is not a complete list. To see a complete list of the `gpresult.exe` command, visit Microsoft at `www.microsoft.com`.

TABLE 6.2 `gpresult` switches

Switch	Description
`/S` *`systemname`*	Generates RSoP information for a remote computer name.
`/USER` *`username`*	Generates RSoP information for a remote username.
`/x /h` *`filename`*	Generates a report in either XML (`/x`) or HTML (`/h`) format. The filename and location is specified by the *`filename`* parameter.
`/V`	Specifies verbose mode, which displays more verbose information such as user rights information.
`/Z`	Specifies an even greater level of verbose information.
`/SCOPE MACHINE`	Displays maximum information about the computer policies applied to this system.
`/SCOPE USER`	Displays maximum information about the user policies applied to this system.
`>`*`textfile.txt`*	Writes the output to a text file.

For example, to obtain information about user wpanek in a system called STELLACON, you would use the command `gpresult/S STELLACON/USERwpanek`.

Through the use of these techniques, you should be able to track down even the most elusive Group Policy problems. Remember, however, that good troubleshooting skills do not replace planning adequately and maintaining GPO settings!

Summary

In this chapter, you examined Active Directory's solution to a common headache for many systems administrators: policy settings. Specifically, I discussed topics that covered Group Policy.

I covered the fundamentals of Group Policy including its fundamental purpose. You can use Group Policy to enforce granular permissions for users in an Active Directory environment. Group policies can restrict and modify the actions allowed for users and computers within the Active Directory environment.

Certain Group Policy settings may apply to users, computers, or both. Computer settings affect all users who access the machines to which the policy applies. User settings affect users regardless of the machines to which they log on.

You learned that you can link Group Policy objects to Active Directory sites, domains, or OUs. This link determines to which objects the policies apply. GPO links can interact through inheritance and filtering to result in an effective set of policies.

The chapter covered inheritance and how GPOs filter down. I showed you how to use the Enforced option on a GPO issued from a parent and how to block a GPO from a child.

You can also use administrative templates to simplify the creation of GPOs. There are some basic default templates that come with Windows Server 2012 R2.

In addition, administrators can delegate control over GPOs in order to distribute administrative responsibilities. Delegation is an important concept because it allows for distributed administration.

You can also deploy software using GPOs. This feature can save time and increase productivity throughout the entire software management life cycle by automating software installation and removal on client computers. The Windows Installer offers a more robust method for managing installation and removal, and applications that support it can take advantage of new Active Directory features. Make sure you are comfortable using the Windows Installer.

You learned about publishing applications via Active Directory and the difference between publishing and assigning applications. You can assign some applications to users and computers so that they are always available. You can also publish them to users so that the user can install them with minimal effort when required.

You also learned how to prepare for software deployment. Before your users can take advantage of automated software installation, you must set up an installation share and provide the appropriate permissions.

The final portion of the chapter covered the Resultant Set of Policy (RSoP) tool, which you can use in logging mode or planning mode to determine exactly which set of policies applies to users, computers, OUs, domains, and sites.

Exam Essentials

Understand the purpose of Group Policy. System administrators use Group Policy to enforce granular permissions for users in an Active Directory environment.

Understand user and computer settings. Certain Group Policy settings may apply to users, computers, or both. Computer settings affect all users that access the machines to which the policy applies. User settings affect users, regardless of which machines they log on to.

Know the interactions between Group Policy objects and Active Directory. GPOs can be linked to Active Directory objects. This link determines to which objects the policies apply.

Understand filtering and inheritance interactions between GPOs. For ease of administration, GPOs can interact via inheritance and filtering. It is important to understand these interactions when you are implementing and troubleshooting Group Policy.

Know how Group Policy settings can affect script policies and network settings. You can use special sets of GPOs to manage network configuration settings.

Understand how delegation of administration can be used in an Active Directory environment. Delegation is an important concept because it allows for distributed administration.

Know how to use the Resultant Set of Policy (RSoP) tool to troubleshoot and plan Group Policy. Windows Server 2012 R2 includes the RSoP feature, which you can run in logging mode or planning mode to determine exactly which set of policies applies to users, computers, OUs, domains, and sites.

Identify common problems with the software life cycle. IT professionals face many challenges with client applications, including development, deployment, maintenance, and troubleshooting.

Understand the benefits of the Windows Installer. Using the Windows Installer is an updated way to install applications on Windows-based machines. It offers a more robust method for making the system changes required by applications, and it allows for a cleaner uninstall. Windows Installer–based applications can also take advantage of new Active Directory features.

Understand the difference between publishing and assigning applications. Some applications can be assigned to users and computers so that they are always available.

Applications can be published to users so that the user may install the application with a minimal amount of effort when it is required.

Know how to prepare for software deployment. Before your users can take advantage of automated software installation, you must set up an installation share and provide the appropriate permissions.

Know how to configure application settings using Active Directory and Group Policy. Using standard Windows Server 2012 R2 administrative tools, you can create an application policy that meets your requirements. You can use automatic, on-demand installation of applications as well as many other features.

Create application categories to simplify the list of published applications. It's important to group applications by functionality or the users to whom they apply, especially in organizations that support a large number of programs.

Review Questions

1. You are the network administrator for a large organization that uses Windows Server 2012 R2 domain controllers and DNS servers. All of your client machines currently have the Windows XP operating system. You want to be able to have client computers edit the domain-based GPOs by using the ADMX files that are located in the ADMX Central Store. How do you accomplish this task? (Choose all that apply.)
   - **A.** Upgrade your clients to Windows 8.
   - **B.** Upgrade your clients to Windows 7.
   - **C.** Add the client machines to the ADMX edit utility.
   - **D.** In the ADMX store, choose the box Allow All Client Privileges.

2. You work for an organization with a single Windows Server 2012 R2 Active Directory domain. The domain has OUs for Sales, Marketing, Admin, R&D, and Finance. You need only the users in the Finance OU to get Windows Office 2013 installed automatically onto their computers. You create a GPO named OfficeApp. What is the next step in getting all of the Finance users Office 2013?
   - **A.** Edit the GPO, and assign the Office application to the user's account. Link the GPO to the Finance OU.
   - **B.** Edit the GPO, and assign the Office application to the user's account. Link the GPO to the domain.
   - **C.** Edit the GPO, and assign the Office application to the computer account. Link the GPO to the domain.
   - **D.** Edit the GPO, and assign the Office application to the computer account. Link the GPO to the Finance OU.

3. You are hired as a consultant to the ABC Company. The owner of the company complains that she continues to have desktop wallpaper that she did not choose. When you speak with the IT team, you find out that a former employee created 20 GPOs and they have not been able to figure out which GPO is changing the owner's desktop wallpaper. How can you resolve this issue?
   - **A.** Run the RSoP utility against all forest computer accounts.
   - **B.** Run the RSoP utility against the owner's computer account.
   - **C.** Run the RSoP utility against the owner's user account.
   - **D.** Run the RSoP utility against all domain computer accounts.

4. You are the network administrator for a large organization that has multiple sites and multiple OUs. You have a site named SalesSite that is for the sales building across the street. In the domain, there is an OU for all salespeople called Sales. You set up a GPO for the SalesSite, and you need to be sure that it applies to the Sales OU. The Sales OU GPOs cannot override the SalesSite GPO. What do you do?

A. On the GPO, disable the Block Child Inheritance setting.

B. On the GPO, set the Enforce setting.

C. On the GPO, set the priorities to 1.

D. On the Sales OU, set the Inherit Parent Policy settings.

5. You are the administrator for an organization that has multiple locations. You are running Windows Server 2012 R2, and you have only one domain with multiple OUs set up for each location. One of your locations, Boston, is connected to the main location by a 256Kbps ISDN line. You configure a GPO to assign a sales application to all computers in the entire domain. You have to be sure that Boston users receive the GPO properly. What should you do?

A. Disable the Slow Link Detection setting in the GPO.

B. Link the GPO to the Boston OU.

C. Change the properties of the GPO to publish the application to the Boston OU.

D. Have the users in Boston run the `GPResult/force` command.

6. To disable GPO settings for a specific security group, which of the following permissions should you apply?

A. Deny Write

B. Allow Write

C. Enable Apply Group Policy

D. Deny Apply Group Policy

7. GPOs assigned at which of the following level(s) will override GPO settings at the domain level?

A. OU

B. Site

C. Domain

D. Both OU and site

8. A system administrator wants to ensure that only the GPOs set at the OU level affect the Group Policy settings for objects within the OU. Which option can they use to do this (assuming that all other GPO settings are the defaults)?

A. The Enforced option

B. The Block Policy Inheritance option

C. The Disable option

D. The Deny permission

9. A system administrator is planning to implement Group Policy objects in a new Windows Server 2012 R2 Active Directory environment. In order to meet the needs of the organization, he decides to implement a hierarchical system of Group Policy settings. At which of the following levels is he able to assign Group Policy settings? (Choose all that apply.)

A. Sites

B. Domains

C. Organizational units

D. Local system

10. Ann is a system administrator for a medium-sized Active Directory environment. She has determined that several new applications that will be deployed throughout the organization use registry-based settings. She would like to do the following:

- Control these registry settings using Group Policy
- Create a standard set of options for these applications and allow other system administrators to modify them using the standard Active Directory tools

Which of the following options can she use to meet these requirements? (Choose all that apply.)

A. Implement the inheritance functionality of GPOs.

B. Implement delegation of specific objects within Active Directory.

C. Implement the No Override functionality of GPOs.

D. Create administrative templates.

E. Provide administrative templates to the system administrators who are responsible for creating Group Policy for the applications.

Chapter 7

Manage Security

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configuring security policies**

- Configure User Rights Assignment
- Configure Security Options settings
- Configure Security templates
- Configure Audit Policy
- Configure Local Users and Groups
- Configure User Account Control (UAC)

✓ **Configuring Windows Firewall**

- Configure rules for multiple profiles using Group Policy
- Configure connection security rules
- Configure Windows Firewall to allow or deny applications, scopes, ports, and users
- Configure authenticated firewall exceptions
- Import and export settings

As an IT Director and Microsoft Trainer, I can explain the importance of every chapter in this book, but some chapters are more important for real-world use. This is one of them.

Setting up security so that only people who need access to resources are the ones who get access to those resources is one of the most important jobs an IT member can have. This helps protect your data from hackers and, believe it or not, your own users.

In this chapter, you will learn how to protect data on your network. I will also discuss how to protect your individual system by using Windows Firewall.

Managing Security

One of the fundamental design goals for Active Directory is to define a single, centralized repository of users and information resources. Active Directory records information about all of the users, computers, and resources on your network. Each domain acts as a logical boundary, and members of the domain (including workstations, servers, and domain controllers) share information about the objects within them.

The information stored within Active Directory determines which resources are accessible to which users. Through the use of *permissions* that are assigned to Active Directory objects, you can control all aspects of network security.

You should be sure that you have implemented appropriate access control settings for the file system, network devices, and other resources. Let's look at the various components of network security, which include working with security principals and managing security and permissions, access control lists (ACLs), User Account Control (UAC), and access control entries (ACEs).

NOTE

When you are setting up a network, you should always keep in mind that 90 percent of all hacks on a network are internal. This means internal permissions and security (as well as external security) need to be as strong as possible while still allowing users to do their jobs.

Understanding Security Principals

Security principals are Active Directory objects that are assigned *security identifiers (SIDs)*. An SID is a unique identifier that is used to manage any object to which permissions can be assigned. Security principals are assigned permissions to perform certain actions and access certain network resources.

The following basic types of Active Directory objects serve as security principals:

User Accounts User accounts identify individual users on your network by including information such as the user's name and their password. User accounts are the fundamental unit of security administration.

Groups There are two main types of groups: *security groups* and *distribution groups*. Both types can contain user accounts. System administrators use security groups to ease the management of security permissions. They use distribution groups, on the other hand, solely to send email. Distribution groups are not security principals. You'll see the details of groups in the next section.

Computer Accounts *Computer accounts* identify which client computers are members of particular domains. Because these computers participate in the Active Directory database, system administrators can manage security settings that affect the computer. They use computer accounts to determine whether a computer can join a domain and for authentication purposes. As you'll see later in this chapter, system administrators can also place restrictions on certain computer settings to increase security. These settings apply to the computer and, therefore, also apply to any user who is using it (regardless of the permissions granted to the user account).

Note that other objects, such as organizational units (OUs), do not function as security principals. What this means is that you can apply certain settings (such as Group Policy) on all of the objects within an OU; however, you cannot specifically set permissions with respect to the OU. The purpose of OUs is to organize other Active Directory objects logically based on business needs, add a needed level of control for security, and create an easier way to delegate.

You can manage security by performing the following actions with security principals:

- You can assign them permissions to access various network resources.
- You can give them user rights.
- You can track their actions through auditing (covered later in this chapter).

The major types of security principals—user accounts, groups, and computer accounts—form the basis of the Active Directory security architecture. As a system administrator, you will likely spend a portion of your time managing permissions for these objects.

It is important to understand that since a unique SID defines each security principal, deleting a security principal is an irreversible process. For example, if you delete a user account and then later re-create one with the same name, you'll need to reassign permissions and group membership settings for the new account. Once a user account is deleted, its SID is deleted.

Users and groups are two types of fundamental security principals employed for security administration. In the following sections, you'll learn how users and groups interact. You'll also learn about the different types of groups you can create.

Types of Groups

When dealing with groups, you should make the distinction between local security principals and domain security principals, as follows:

Local Users and Groups You use *local users and groups* to assign the permissions necessary to access the local machine. For example, you may assign the permissions you need to reboot a domain controller to a specific domain local group.

Domain Users and Groups *Domain users and groups*, on the other hand, are used throughout the domain. These objects are available on any of the computers within the Active Directory domain and between domains that have a trust relationship.

Here are the two main types of groups used in Active Directory:

Security Groups *Security groups* are considered security principals. They can contain user accounts, computers, or groups. To make administration simpler, system administrators usually grant permissions to groups. This allows you to change permissions easily at the Active Directory level (instead of at the level of the resource on which the permissions are assigned).

You can also place Active Directory Contact objects within security groups, but security permissions will not apply to them.

Distribution Groups Distribution groups are not considered security principals because they do not have SIDs. As mentioned earlier, they are used only for the purpose of sending email messages. You can add users to distribution groups just as you would add them to security groups. You can also place distribution groups within OUs so that they are easier to manage. You will find them useful, for example, if you need to send email messages to an entire department or business unit within Active Directory.

Understanding the differences between security and distribution groups is important in an Active Directory environment. For the most part, system administrators use security groups for the daily administration of permissions. On the other hand, system administrators who are responsible for maintaining email distribution lists generally use distribution groups to group members of departments and business units logically. (A system administrator can also email all of the users within a security group, but to do so, they would have to specify the email addresses for the accounts.)

When you are working in Windows Server 2003, Server 2008, Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 functional-level domains, you can convert security groups to or from distribution groups.

It is vital that you understand group types when you are getting ready to take the Microsoft exams. Microsoft likes to include trick questions about putting permissions on distribution groups. Remember, only security groups can have permissions assigned to them.

Group Scope

In addition to being classified by type, each group is given a specific scope. The scope of a group defines two characteristics. First, it determines the level of security that applies to

a group. Second, it determines which users can be added to the group. *Group scope* is an important concept in network environments because it ultimately defines which resources users are able to access.

The three types of group scope are as follows:

Domain Local The scope of *domain local groups* extends as far as the local domain. When you're using the Active Directory Users and Computers tool, domain local accounts apply to the computer for which you are viewing information. Domain local groups are used to assign permissions to local resources, such as files and printers. They can contain domain locals, global groups, universal groups, and user accounts.

Global The scope of *global groups* is limited to a single domain. Global groups may contain any of the users who are a part of the Active Directory domain in which the global groups reside or other global groups. Global groups are often used for managing domain security permissions based on job functions. For example, if you need to specify permissions for the Engineering department, you could create one or more global groups (such as EngineeringManagers and EngineeringDevelopers). You could then assign security permissions to each group.

Universal *Universal groups* can contain accounts or other universal groups from any domains within an Active Directory forest. Therefore, system administrators use them to manage security across domains. When you are managing multiple domains, it often helps to group global groups within universal groups. For instance, if you have an Engineering global group in the `research.stellacon.com` domain and an Engineering global group in the `asia.stellacon.com` domain, you can create a universal AllEngineers group that contains both of the global groups. Now whenever you must assign security permissions to all engineers within the organization, you need only assign permissions to the AllEngineers universal group.

For domain controllers to process authentication between domains, information about the membership of universal groups is stored in the global catalog (GC). Keep this in mind if you ever plan to place users directly into universal groups and bypass global groups because all of the users will be enumerated in the GC, which will impact size and performance.

Fortunately, universal group credentials are cached on domain controllers that universal group members use to log on. This process is called *universal group membership caching*. The domain controller obtains the cached data whenever universal group members log on, and then it is retained on the domain controller for eight hours by default. This is especially useful for smaller locations, such as branch offices, that run less expensive domain controllers. Most domain controllers at these locations cannot store a copy of the entire GC, and frequent calls to the nearest GC would require an inordinate amount of network traffic.

When you create a new group using the Active Directory Users and Computers tool, you must specify the scope of the group. Figure 7.1 shows the New Object – Group dialog box and the available options for the group scope.

Changing group scope, however, can be helpful when your security administration or business needs change. You can change group scope easily using the Active Directory Users and Computers tool. To do so, access the properties of the group. As shown in Figure 7.2, you can make a group scope change by clicking one of the options.

FIGURE 7.1 The New Object – Group dialog box

FIGURE 7.2 The Sales Security Group's Properties dialog box

Built-in Domain Local Groups

System administrators use built-in domain local groups to perform administrative functions on the local server. Because these have pre-assigned permissions and privileges, they allow system administrators to assign common management functions easily. Figure 7.3 shows the default built-in groups that are available on a Windows Server 2012 R2 domain controller.

FIGURE 7.3 Default built-in local groups

The list of built-in local groups includes some of the following:

Account Operators These users can create and modify domain user and group accounts. Members of this group are generally responsible for the daily administration of Active Directory.

Administrators By default, members of the Administrators group are given full permissions to perform any functions within the Active Directory domain and on the local computer. This means they can access all files and resources that reside on any server within the domain. As you can see, this is a powerful account.

In general, you should restrict the number of users who are included in this group because most common administration functions do not require this level of access.

Backup Operators One of the problems associated with backing up data in a secure network environment is that you need to provide a way to bypass standard file system security so that you can copy files. Although you could place users in the Administrators group, doing so usually provides more permissions than necessary. Members of the Backup Operators group can bypass standard file system security for the purpose of backup and recovery only. They cannot, however, directly access or open files within the file system.

Generally, backup software applications and data use the permissions assigned to the Backup Operators group.

Certificate Service DCOM Access Members of the Certificate Service DCOM Access group can connect to certificate authority servers in the enterprise.

Cryptographic Operators Members of the Cryptographic Operators group are authorized to perform cryptographic operations. *Cryptography* allows the use of codes to convert data, which then allows a specific recipient to read it using a key.

Guests Typically, you use the Guests group to provide access to resources that generally do not require security. For example, if you have a network share that provides files that should be made available to all network users, you can assign permissions to allow members of the Guests group to access those files.

Print Operators By default, members of the Print Operators group are given permissions to administer all of the printers within a domain. This includes common functions such as changing the priority of print jobs and deleting items from the print queue.

Replicator The Replicator group allows files to be replicated among the computers in a domain. You can add accounts used for replication-related tasks to this group to provide those accounts with the permissions they need to keep files synchronized across multiple computers.

Server Operators A common administrative task is managing server configuration. Members of the Server Operators group are granted the permissions they need to manage services, shares, and other system settings.

Users The Users built-in domain local group is used to administer security for most network accounts. Usually, you don't give this group many permissions, and you use it to apply security settings for most employees within an organization.

Windows Server 2012 R2 also includes many different default groups, which you can find in the `Users` folder. As shown in Figure 7.4, these groups are of varying scopes, including domain local, global, and universal groups. You'll see the details of these groups in the next section.

FIGURE 7.4 Contents of the default `Users` folder

Three important user accounts are created during the promotion of a domain controller, described here:

Administrator Account The Administrator account is assigned the password a system administrator provides during the promotion process, and it has full permissions to perform all actions within the domain.

Guest Account The Guest account is disabled by default. The purpose of the *Guest account* is to provide anonymous access to users who do not have an individual logon and password to use within the domain. Although the Guest account might be useful in some situations, it is generally recommended that this account be disabled to increase security.

Krbtgt, or Key Distribution Center Service, Account Only the operating system uses the *krbtgt*, or *Key Distribution Center Service*, *account* for Kerberos authentication while it is using `DCPromo.exe`. This account is disabled by default. Unlike other user accounts, the krbtgt account cannot be used to log on to the domain, and therefore it does not need to be enabled. Since only the operating system uses this account, you do not need to worry about hackers gaining access by using this account.

Predefined Global Groups

As mentioned earlier in this chapter, you use global groups to manage permissions at the domain level. Members of each of these groups can perform specific tasks related to managing Active Directory.

The following predefined global groups are installed in the `Users` folder:

Cert Publishers Certificates are used to increase security by allowing for strong authentication methods. User accounts are placed within the *Cert Publishers group* if they must publish security certificates. Generally, Active Directory security services use these accounts.

Domain Computers All of the computers that are members of the domain are generally members of the *Domain Computers group*. This includes any workstations or servers that have joined the domain, but it does not include the domain controllers.

Domain Admins Members of the *Domain Admins group* have full permissions to manage all of the Active Directory objects for this domain. This is a powerful account; therefore, you should restrict its membership only to those users who require full permissions.

Domain Controllers All of the domain controllers for a given domain are generally included within the *Domain Controllers group*.

Domain Guests Generally, by default, members of the *Domain Guests group* are given minimal permissions with respect to resources. System administrators may place user accounts in this group if they require only basic access or temporary permissions within the domain.

Domain Users The *Domain Users group* usually contains all of the user accounts for the given domain. This group is generally given basic permissions to resources that do not require higher levels of security. A common example is a public file share.

Enterprise Admins Members of the *Enterprise Admins group* are given full permissions to perform actions within the entire forest. This includes functions such as managing trust relationships and adding new domains to trees and forests.

Group Policy Creator Owners Members of the *Group Policy Creator Owners group* are able to create and modify Group Policy settings for objects within the domain. This allows them to enable security settings on OUs (and the objects they contain).

Schema Admins Members of the *Schema Admins group* are given permissions to modify the Active Directory schema. As a member of Schema Admins, you can create additional fields of information for user accounts. This is a powerful function because any changes to the schema will be propagated to all the domains and domain controllers within an Active Directory forest. Furthermore, you cannot undo changes to the schema (although you can disable some).

In addition to these groups, you can create new ones for specific services and applications that are installed on the server. Specifically, services that run on domain controllers and servers will be created as security groups with domain local scope. For example, if a domain controller is running the DNS service, the DnsAdmins and DnsUpdateProxy groups become available. In addition, there are two read-only domain controller (RODC) local groups: the Allowed RODC Password Replication and the Denied RODC Password Replication groups. Similarly, if you install the DHCP service, it automatically creates the

DHCP Users and DHCP Administrators groups. The purpose of these groups depends on the functionality of the applications being installed.

Foreign Security Principals

In environments that have more than one domain, you may need to grant permissions to users who reside in multiple domains. Generally, you manage this using Active Directory trees and forests. However, in some cases, you may want to provide resources to users who belong to domains that are not part of the forest.

Active Directory uses the concept of *foreign security principals* to allow permissions to be assigned to users who are not part of an Active Directory forest. This process is automatic and does not require the intervention of system administrators. You can then add the foreign security principals to domain local groups for which, in turn, you can grant permissions for resources within the domain. You can view a list of foreign security principals by using the Active Directory Users and Computers tool. Figure 7.5 shows the contents of the `ForeignSecurityPrincipals` folder.

FIGURE 7.5 The `ForeignSecurityPrincipals` folder

Managing Security and Permissions

Now that you understand the basic issues, terms, and Active Directory objects that pertain to security, it's time to look at how you can apply this information to secure your network resources. The general practice for managing security is to assign users to groups and then grant permissions and logon parameters to the groups so that they can access certain resources.

For management ease and to implement a hierarchical structure, you can place groups within OUs. You can also assign Group Policy settings to all of the objects contained within an OU. By using this method, you can combine the benefits of a hierarchical structure (through OUs) with the use of security principals. Figure 7.6 provides a diagram of this process.

FIGURE 7.6 An overview of security management

The primary tool you use to manage security permissions for users, groups, and computers is the Active Directory Users and Computers tool. Using this tool, you can create and manage Active Directory objects and organize them based on your business needs. Common tasks for many system administrators might include the following:

- Resetting a user's password (for example, in cases where they forget their password)
- Creating new user accounts (when, for instance, a new employee joins the company)
- Modifying group memberships based on changes in job requirements and functions
- Disabling user accounts (when, for example, users will be out of the office for long periods of time and will not require network resource access)

Once you've properly grouped your users, you need to set the actual permissions that affect the objects within Active Directory. The actual permissions available vary based on the type of object. Table 7.1 provides an example of some of the permissions that you can apply to various Active Directory objects and an explanation of what each permission does.

TABLE 7.1 Permissions of Active Directory objects

Permission	Explanation
Control Access	Changes security permissions on the object
Create Child	Creates objects within an OU (such as other OUs)
Delete Child	Deletes child objects within an OU

Delete Tree	Deletes an OU and the objects within it
List Contents	Views objects within an OU
List Object	Views a list of the objects within an OU
Read	Views properties of an object (such as a username)
Write	Modifies properties of an object

Using ACLs and ACEs

Each object in Active Directory has an *access control list (ACL)*. The ACL is a list of user accounts and groups that are allowed to access the resource. For each ACL, there is an access control entry (ACE) that defines what a user or a group can actually do with the resource. Deny permissions are always listed first. This means that if users have Deny permissions through user or group membership, they will not be allowed to access the object, even if they have explicit Allow permissions through other user or group permissions. Figure 7.7 shows an ACL for the Sales OU.

FIGURE 7.7 The ACL for an OU named Sales

The Security tab is enabled only if you selected the Advanced Features option from the View menu in the Active Directory Users and Computers tool.

Configuring User Account Control

One issue that many users have run into is as follows: When they log into their standard Windows user account and they need to make a change on their local machines or run a program that requires a higher level of security, they can't complete the task. This is where User Account Controls can help.

User Account Control (UAC) allows your domain users to log into their machines using their standard Windows user account and then execute processes that may require additional user group access.

Some applications may require additional security permissions to run successfully. These types of programs are normally referred to as *legacy applications*. Some applications, however, such as installing new software or making configuration changes, require more permissions than what is available to a standard user account. This is where UAC can help.

When an executable or program needs to function properly with more than just standard user rights, UAC can give that user's token additional user groups. This token allows the executable or program to function properly by giving the standard user account the rights to complete the task.

To configure the UAC, an administrator can go into the system's Control Panel and then User Accounts. Inside the User Accounts snap-in, choose Change User Account Control Settings.

Delegating Control of Users and Groups

A common administrative function related to the use of Active Directory involves managing users and groups. You can use OUs to group objects logically so that you can easily manage them. Once you have placed the appropriate Active Directory objects within OUs, you are ready to delegate control of these objects.

Delegation is the process by which a higher-level security administrator assigns permissions to other users. For example, if Admin A is a member of the Domain Admins group, they are able to delegate control of any OU within the domain to Admin B. You can access the Delegation Of Control Wizard through the Active Directory Users and Computers tool. You can use it to perform common delegation tasks quickly and easily. The wizard walks you through the steps of selecting the objects for which you want to perform delegation, what permission you want to allow, and which users will have those permissions.

Exercise 7.1 walks through the steps required to delegate control of OUs.

EXERCISE 7.1

Delegating Control of Active Directory Objects

1. Open the Active Directory Users and Computers tool.
2. Create a new user within the Engineering OU using the following information (use the default settings for any fields not specified):

First Name: **Robert**

Last Name: **Admin**

User Logon Name: **radmin**

Password: **P@ssw0rd**

3. Right-click the Sales OU and select Delegate Control. This starts the Delegation Of Control Wizard. Click Next.
4. To add users and groups to which you want to delegate control, click the Add button. In the Add dialog box, enter **Robert Admin** for the name of the user to add. Note that you can specify multiple users or groups using this option.
5. Click OK to add the account to the delegation list, which is shown in the Users Or Groups page. Click Next to continue.
6. On the Tasks To Delegate page, you must specify which actions you want to allow the selected user to perform within this OU. Select the Delegate The Following Common Tasks option and place a check mark next to the following options:

   Create, Delete, And Manage User Accounts

   Reset User Passwords And Force Password Change At Next Logon

   Read All User Information

   Create, Delete And Manage Groups

   Modify The Membership Of A Group
7. Click Next to continue. The wizard provides you with a summary of the selections that you have made on the Completing The Delegation Of Control Wizard page. To complete the process, click Finish to have the wizard commit the changes.

   Now when the user Robert Admin logs on (using *radmin* as his logon name), he will be able to perform common administrative functions for all the objects contained within the Sales OU.
8. When you have finished, close the Active Directory Users and Computers tool.

Understanding Dynamic Access Control

One of the advantages of Windows Server 2012 R2 is the ability to apply data governance to your file server. This will help control who has access to information and auditing. You get these advantages through the use of Dynamic Access Control (DAC). DAC allows you to identify data by using data classifications (both automatic and manual) and then to control access to these files based on these classifications.

DAC also gives administrators the ability to control file access by using a central access policy. This central access policy will also allow an administrator to set up audit access to files for reporting and forensic investigation.

DAC allows an administrator to set up Active Directory Rights Management Service (AD RMS) encryption for Microsoft Office documents. For example, you can set up encryption for any documents that contain financial information.

DAC gives an administrator the flexibility to configure file access and auditing to domain-based file servers. To do this, DAC controls claims in the authentication token, resource properties, and conditional expressions within permission and auditing entries.

Administrators have the ability to give users access to files and folders based on Active Directory attributes. For example, a user named Dana is given access to the file server share because in the user's Active Directory (department attribute) properties, the value contains the value Sales.

NOTE

For DAC to function properly, an administrator must enable Windows 8 computers and Windows Server 2012/2012 R2 file servers to support claims and compound authentication.

Using Group Policy for Security

Through the use of Group Policy settings, system administrators can assign thousands of different settings and options for users, groups, and OUs. Specifically, in relation to security, you can use many different options to control how important features, such as password policies, user rights, and account lockout settings, can be configured.

The general process for making these settings is to create a Group Policy object (GPO) with the settings that you want and then link it to an OU or other Active Directory object.

Table 7.2 lists many Group Policy settings, which are relevant to creating a secure Active Directory environment. Note that this list is not comprehensive—many other options are available through Windows Server 2012 R2 administrative tools.

TABLE 7.2 Group Policy settings used for security purposes

Setting section	Setting name	Purpose
Account Policies ➢ Password Policy	Enforce Password History	Specifies how many passwords will be remembered. This option prevents users from reusing the same passwords whenever they're changed.
Account Policies ➢ Password Policy	Minimum Password Length	Prevents users from using short, weak passwords by specifying the minimum number of characters that the password must include.

Account Policies ➢ Account Lockout Policy	Account Lockout Threshold	Specifies how many bad password attempts can be entered before the account gets locked out.
Account Policies ➢ Account Lockout Policy	Account Lockout Duration	Specifies how long an account will remain locked out after too many bad password attempts have been entered. By setting this option to a reasonable value (such as 30 minutes), you can reduce administrative overhead while still maintaining fairly strong security.
Account Policies ➢ Account Lockout Policy	Reset Account Lockout Counter After	Specifies how long the Account Lockout Threshold counter will hold failed logon attempts before resetting to 0.
Local Policies ➢ Security Options	Accounts: Rename Administrator Account	Often, when trying to gain unauthorized access to a computer, individuals attempt to guess the administrator password. One method for increasing security is to rename this account so that no password allows entry using this logon.
Local Policies ➢ Security Options	Domain Controller: Allow Server Operators To Schedule Tasks	This option specifies whether members of the built-in Server Operators group are allowed to schedule tasks on the server.
Local Policies ➢ Security Options	Interactive Logon: Do Not Display Last User Name	Increases security by not displaying the name of the last user who logged onto the system.
Local Policies ➢ Security Options	Shutdown: Allow System To Be Shut Down Without Having To Log On	Allows system administrators to perform remote shutdown operations without logging on to the server.

Implementing an Audit Policy

One of the most important aspects of controlling security in networked environments is ensuring that only authorized users are able to access specific resources. Although system administrators often spend much time managing security permissions, it is almost always possible for a security problem to occur.

Sometimes, the best way to find possible security breaches is actually to record the actions that specific users take. Then, in the case of a security breach (the unauthorized shutdown of a server, for example), system administrators can examine the log to find the cause of the problem.

The Windows Server 2012 R2 operating system and Active Directory offer you the ability to audit a wide range of actions. In the following sections, you'll see how to implement auditing for Active Directory.

Overview of Auditing

The act of *auditing* relates to recording specific actions. From a security standpoint, auditing is used to detect any possible misuse of network resources. Although auditing does not necessarily prevent resources from being misused, it does help determine when security violations have occurred (or were attempted). Furthermore, just the fact that others know that you have implemented auditing may prevent them from attempting to circumvent security.

You need to complete several steps in order to implement auditing using Windows Server 2012 R2:

1. Configure the size and storage settings for the audit logs.
2. Enable categories of events to audit.
3. Specify which objects and actions should be recorded in the audit log.

Note that there are trade-offs to implementing auditing. First, recording auditing information can consume system resources. This can decrease overall system performance and use up valuable disk space. Second, auditing many events can make the audit log impractical to view. If too much detail is provided, system administrators are unlikely to scrutinize all of the recorded events. For these reasons, you should always be sure to find a balance between the level of auditing details provided and the performance-management implications of these settings.

Implementing Auditing

Auditing is not an all-or-none type of process. As is the case with security in general, system administrators must choose specifically which objects and actions they want to audit.

The main categories for auditing include the following:

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

In this list of categories, four of the categories are related to Active Directory. Let's discuss these auditing categories in a bit more detail.

Audit Account Logon Events You enable this auditing event if you want to audit when a user authenticates with a domain controller and logs onto the domain. This event is logged in the security log on the domain controller.

Audit Account Management This auditing event is used when you want to watch what changes are being made to Active Directory accounts. For example, when another administrator creates or deletes a user account, it would be an audited event.

Audit Directory Service Access This auditing event occurs whenever a user or administrator accesses Active Directory objects. Let's say that an administrator opens Active Directory and clicks a user account; even if nothing is changed on that account, an event is logged.

Audit Logon Events Account logon events are created for domain account activity. For example, you have a user who logs on to a server so that they can access files; the act of logging onto the server creates this audit event.

Audit Object Access Audit object access allows you to audit objects within your network such as folders, files, and printers. If you suspect someone is trying to hack into an object (for example, the `finance` folder), this is the type of auditing that you would use. You still would need to enable auditing on the actual object (for example, the `finance` folder).

Audit Policy Change Audit policy change allows you to audit changes to user rights assignment policies, audit policies, or trust policies. This auditing allows you to see whether anyone changes any of the other audit policies.

Audit Privilege Use Setting the audit privilege use allows an administrator to audit each instance of a user exercising a user right. For example, if a user changes the system time on a machine, this is a user right. Logging on locally is another common user right.

To audit access to objects stored within Active Directory, you must enable the Audit Directory Service Access option. Then you must specify which objects and actions should be tracked.

Exercise 7.2 walks through the steps you must take to implement auditing of Active Directory objects on domain controllers.

EXERCISE 7.2

Enabling Auditing of Active Directory Objects

1. Open the Local Security Policy tool (located in the Administrative Tools program group).
2. Expand Local Policies ➢ Audit Policy.
3. Double-click the setting for Audit Directory Service Access.
4. In the Audit Directory Service Access Properties dialog box, place check marks next to Success and Failure. Click OK to save the settings.
5. Close the Local Security Policy tool.

Using the *Auditpol.exe* Command

There may be a time when you need to look at your actual auditing policies set on a user or a system. This is where an administrator can use the `Auditpol.exe` command. *Auditpol* allows administrators the ability not only to view an audit policy but also to set, configure, modify, restore, and even remove an audit policy. Auditpol is a command-line utility, and there are multiple switches that can be used with Auditpol. The following is the syntax used with Auditpol; Table 7.3 describes some of the switches:

```
Auditpol command [<sub-command><options>]
```

Here's an example:

```
Auditpol /get /user:wpanek /category:"Detailed Tracking" /r
```

TABLE 7.3 Auditpol commands

Command	Description
`/backup`	Allows an administrator to save the audit policy to a file
`/clear`	Allows an administrator to clear an audit policy
`/get`	Gives administrators the ability to view the current audit policy
`/list`	Allows you to view selectable policy elements
`/remove`	Removes all per-user audit policy settings and disables all system audit policy settings
`/restore`	Allows an administrator to restore an audit policy from a file that was previously created by using `auditpol /backup`
`/set`	Gives an administrator the ability to set an audit policy
`/?`	Displays help

Features of Windows Server 2012 R2 Auditing

Microsoft continues to increase the level of detail in the security auditing logs. Microsoft has also simplified the deployment and management of auditing policies. The following list includes some of the features:

Global Object Access Auditing Administrators using Windows Server 2012 R2 and Windows 8 now have the ability to define computer-wide system access control lists (SACLs). Administrators can define SACLs for either the file system or the registry. After the specified SACL is defined, the SACL is then applied automatically to every object

of that type. This can be helpful to administrators for verifying that all critical files, folders, and registry settings on a computer are protected. This is also helpful for identifying when an issue occurs with a system resource.

"Reason For Access" Reporting When an administrator is performing auditing in Windows Server 2012 R2 and Windows 8, they can now see the reason why an operation was successful or unsuccessful. Previously, they lacked the ability to see the reason why an operation succeeded or failed.

Advanced Audit Policy Settings In Windows Server 2012 R2, there are many new Advanced Audit Policy settings that can be used in place of the nine basic auditing settings. These advanced audit settings also help eliminate the unnecessary auditing activities that can make audit logs difficult to manage and decipher.

Expression-Based Audit Policies Administrators have the ability, because of Dynamic Access Control, to create targeted audit policies by using expressions based on user, computer, and resource claims. For example, an administrator has the ability to create an audit policy that tracks all Read and Write operations for files that are considered high-business impact. Expression-based audit policies can be directly created on a file or folder or created through the use of a Group Policy.

Removable Storage Device Auditing Administrators have the ability to monitor attempts to use a removable storage device on your network. If an administrator decides to implement this policy, an audit event is created every time one of your users attempts to copy, move, or save a network resource onto a removable storage device.

Configuring Windows Firewall Options

Another security aspect to look into is Windows Firewall. Before I can start talking about firewall options, you must first understand what a firewall does. A *firewall* is a software or hardware device that checks the information that is received from an outside (Internet) or external network and uses that information to determine whether the packet should be accepted or declined.

Depending on the firewall, you have the ability to check all potential remote users against Active Directory to verify that the remote user has an authorized domain account. This process is called *Active Directory account integration*.

Microsoft Windows Server 2012 R2 has a built-in firewall. The following are some of the configuration options included in the Windows Firewall Settings dialog box:

Domain Profile Tab On the Domain Profile tab, you have the ability to turn the firewall on or off by using the Firewall State drop-down menu. When setting the Firewall State option on this tab, it's for turning the firewall on or off for the domain only. When turning the firewall on, you also have the ability to block inbound and outbound connections (see Figure 7.8). Administrators also have the ability to control the Windows Firewall behavior along with setting up logging.

FIGURE 7.8 Domain Profile tab of Windows Firewall Settings

Private Profile Tab On the Private Profile tab, you have the ability to turn the firewall on or off by using the Firewall State drop-down menu. When setting the Firewall State in this tab, it's for turning the firewall on or off for the Private Profile only. When turning the firewall on, you also have the ability to block inbound and outbound connections (see Figure 7.9). Administrators also have the ability to control the Windows Firewall Private Profile behavior along with setting up logging.

FIGURE 7.9 Private Profile tab of Windows Firewall Settings

Public Profile On the Public Profile tab, you have the ability to turn the firewall on or off by using the Firewall State drop-down menu. When setting the Firewall State in this tab, it's for turning the firewall on or off for the Public Profile only. When turning the firewall on, you also have the ability to block inbound and outbound connections (see Figure 7.10). Administrators also have the ability to control the Windows Firewall Public Profile behavior along with setting up logging.

FIGURE 7.10 Public Profile tab of Windows Firewall

IPsec Settings Tab The IPsec Setting tab allows you to set up the IPsec defaults, IPsec exemptions, and IPsec tunnel authorization. The IPsec defaults button allows you to specify settings used by IPsec to establish secured connections. The IPsec exemptions allow you to set up ICMP exemptions from IPsec. Finally, you can set up IPsec tunnel authorization, which allows you to specify the users and computers that are authorized to establish an IPsec tunnel (see Figure 7.11).

Windows Server 2012 R2 takes firewalls a step further than just the normal firewall settings in Control Panel. An MMC snap-in called *Windows Firewall with Advanced Security* (see Figure 7.12) can block all incoming and outgoing connections based on its configuration.

One of the major advantages to using the Windows Firewall with Advanced Security snap-in is the ability to set firewall configurations on remote computers using group policies. Another advantage to using this MMC is the ability to set up firewalls using IPsec security. Windows Firewall with Advanced Security snap-in allows an administrator to set more in-depth rules for Microsoft Active Directory users and groups, source and destination Internet Protocol (IP) addresses, IP port numbers, ICMP settings, IPsec settings, specific types of interfaces, and services.

FIGURE 7.11 IPsec Settings tab of Windows Firewall Settings

FIGURE 7.12 Windows Firewall with Advanced Security snap-in

You can configure more advanced settings by configuring Windows Firewall with Advanced Security. To access Windows Firewall with Advanced Security, press the Windows key and choose Control Panel ➢ Large Icons View ➢ Windows Firewall, and click the Advanced Settings link.

The scope pane to the left shows that you can set up specific inbound and outbound rules, connection security rules, and monitoring rules. The central area shows an overview of the firewall's status as well as the current profile settings. Let's take a look at these in more detail.

Inbound and Outbound Rules

Inbound and outbound rules consist of many preconfigured rules that can be enabled or disabled. Obviously, inbound rules (see Figure 7.13) monitor inbound traffic, and outbound rules monitor outbound traffic. By default, many are disabled. Double-clicking a rule will bring up its Properties dialog box, as shown in Figure 7.14.

You can filter the rules to make them easier to view. Filtering can be performed based on the profile the rule affects or whether the rule is enabled or disabled or based on the rule group.

If you can't find a rule that is appropriate to your needs, you can create a new rule by right-clicking Inbound Rules or Outbound Rules in the scope pane and then selecting New Rule. The New Inbound (or Outbound) Rule Wizard will launch, and you will be asked whether you want to create a rule based on a particular program, protocol or port, predefined category, or custom settings.

FIGURE 7.13 Inbound rules

FIGURE 7.14 An inbound rule's Properties dialog box for WSUS

When setting up rules, you can also set up firewall exceptions. These exceptions allow you to work around a particular rule that you may be setting up. Firewall exceptions can be handy when an authenticated user or service needs to get around a firewall setting. These exceptions can be also set under the advanced firewall settings under the Connection Security Rules link.

Exercise 7.3 will walk you through the steps needed to create a new inbound rule that will allow only encrypted TCP traffic. In this exercise, you will have the ability to create a custom rule and then specify which authorized users and computers can connect using this rule.

EXERCISE 7.3

Configuring Windows Firewall

1. Press the Windows key and select Control Panel ➢ Large Icon View ➢ Windows Firewall.
2. Click Advanced Settings on the left side.
3. Right-click Inbound Rules and select New Rule.
4. Choose a rule type. For this exercise, choose Custom so that you can see all of the options available to you; then click Next.
5. Choose the programs or services that are affected by this rule. For this exercise, choose All Programs; then click Next.

6. Choose the protocol type as well as the local and remote port numbers that are affected by this rule. For this exercise, choose TCP and make sure All Ports is selected for both Local Port and Remote Port. Click Next to continue.
7. Choose the local and remote IP addresses that are affected by this rule. Choose Any IP Address for both local and remote; then click Next.
8. Specify whether this rule will allow the connection, allow the connection only if it is secure, or block the connection. Select the option Allow The Connection If It Is Secure; then click Next.
9. Specify whether connections should be allowed only from certain users. You can experiment with these options if you want. Then click Next to continue.
10. Specify whether connections should be allowed only from certain computers. Again, you can experiment with these options if you want. Then click Next to continue.
11. Choose those profiles that will be affected by this rule. Select one or more profiles; then click Next to continue.
12. Give your profile a name and description; then click Finish. Your custom rule will appear in the list of Inbound Rules, and the rule will be enabled.
13. Double-click your newly created rule. Notice that you can change the options you previously configured.
14. Disable the rule by right-clicking the rule and choosing Disable Rule.
15. Close Windows Firewall.

Now let's take a look at setting up Connection Security Rules through Windows Firewall with Advanced Security.

Configuring Windows Firewall with a GPO

If you wanted to configure Windows Firewall on all of your client machines, you have two options. You can either configure each machine manually or set up a GPO to configure the Windows Firewall. To set up the Windows Firewall using a GPO, configure the Computer section ➢ Windows Settings ➢ Security ➢ Windows Firewall With Advanced Security.

One of the advantages of using a GPO when configuring the Windows firewall is that you can configure multiple profiles and multiple firewall settings using the Group Policy.

Another even bigger advantage is being able to configure thousands of computers by setting just one GPO. It saves an IT administrator from going around the company from machine to machine to set up the firewall.

Import/Export Policies

One advantage of configuring Windows Firewall is the ability to export and import policy settings. For example, I set up a policy for 35 machines; I created the policy on one of the 35 machines and then exported the policy. I then imported the policy to the other

34 machines so that I did not have to re-create the policy over and over again. To export a policy, right-click Windows Firewall With Advanced Security and choose Export Policy. Choose Import Policy on the other machines to import the policy.

IPsec Policy Settings in Windows Firewall

When configuring options for Windows Firewall with Advanced Security, you have the ability to configure some IPsec policies. The three options are as follows:

IPsec Defaults Specify settings used by IPsec to establish secure connections.

IPsec Exemptions Exempting ICMP from all IPsec requirements can simplify troubleshooting of network connectivity issues.

IPsec Tunnel Authorization Specify the computers or users authorized to establish IPsec tunnel connections to this computer.

Monitoring

The Monitoring section shows detailed information about the firewall configurations for the Domain Profile, Private Profile, and Public Profile settings. These network location profiles determine which settings are enforced for private networks, public networks, and networks connected to a domain.

Real World Scenario

Firewalls

When I'm consulting, it always makes me laugh when I see small to midsize companies using Microsoft Windows Firewall and no other protection.

Microsoft Windows Firewall should be your *last* line of defense, not your only one. You need to make sure that you have good hardware firewalls that separate your network from the world.

Also watch Windows Firewall when it comes to printing. I have run into many situations where a printer that needs to talk to the operating system has issues when Windows Firewall is enabled. If this happens, make sure that the printer is allowed in the Allowed Programs section.

Summary

In this chapter, you examined server security and saw why it's one of the most important aspects of Windows Server 2012 R2. As a system administrator, Windows security is something that every administrator should be using but many don't know how it works properly.

I explained how to set up groups and group security as well as how to set up the permissions for those groups. I also covered auditing. I showed you how to set up and monitor auditing to see who has successfully, or unsuccessfully, accessed resources, machines, Active Directory, and all aspects of network security.

I finished the chapter by looking into Windows Firewall. I showed you how to configure the firewall and add exclusions and rules. I also showed you how to view and monitor the firewall results.

Exam Essentials

Understand group types and group scope. The two major types of groups are security and distribution groups, and they have different purposes. Groups can be local, global, or universal. Domain local groups are used to assign permissions to local resources, such as files and printers. The scope of global groups is limited to a single domain. Universal groups can contain users from any domains within an Active Directory forest.

Understand the purpose and permissions of built-in groups. The Active Directory environment includes several built-in local and global groups that are designed to simplify common system administration tasks. For instance, members of the Administrators group are given full permissions to perform any functions within the Active Directory domain and on the local computer.

Understand how to use Group Policy to manage security-related policies. Through the use of Group Policy settings, you can configure password and account-related options. You can also specify to which users, groups, and OUs many of the settings apply.

Understand how to use auditing. Through the use of auditing, an administrator can see who has been successfully and unsuccessfully accessing resources and Active Directory.

Understand Windows Firewall. Windows Server 2012 R2 includes Windows Firewall. Windows Firewall gives you secure access to a machine by allowing or denying which applications or users can access a system.

Review Questions

1. You are the network administrator for your organization. A new company policy has been released wherein if a user enters their password incorrectly three times within five minutes, they are locked out for 30 minutes. What three actions do you need to set to comply with this policy? (Choose all that apply.)
   - **A.** Set Account Lockout Duration to five minutes.
   - **B.** Set Account Lockout Duration to 30 minutes.
   - **C.** Set the Account Lockout Threshold setting to three invalid logon attempts.
   - **D.** Set the Account Lockout Threshold setting to 30 minutes.
   - **E.** Set the Reset Account Lockout Counter setting to five minutes.
   - **F.** Set the Reset Account Lockout Counter setting to three times.

2. You create a GPO and link it to the Sales OU. You want to monitor users in the Sales OU who connect to the file server. What type of auditing do you enable?
   - **A.** Audit Object Access
   - **B.** Audit Logon Events
   - **C.** Audit System Events
   - **D.** Audit Process Tracking

3. Alexis is a system administrator for an Active Directory environment that contains four domains. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:
   - Audit changes to User objects that are contained within a specific OU.
   - Allow a special user account called Audit to view and modify all security-related information about objects in that OU.

   Which of the following steps should Alexis take to meet these requirements? (Choose all that apply.)
   - **A.** Convert all volumes on which Active Directory information resides to NTFS.
   - **B.** Enable auditing with the Active Directory Users and Computers tool.
   - **C.** Create a new Active Directory domain and create restrictive permissions for the suspected users within this domain.
   - **D.** Reconfigure trust settings using the Active Directory Domains and Trusts tool.
   - **E.** Specify auditing options for the OU using the Active Directory Users and Computers tool.
   - **F.** Use the Delegation of Control Wizard to grant appropriate permissions to view and modify objects within the OU to the Audit user account.

4. Crystal is a system administrator for an Active Directory environment that is running in Native mode. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:
   - The accessing of certain sensitive files must be logged.
   - Modifications to certain sensitive files must be logged.
   - System administrators must be able to provide information about which users accessed sensitive files and when they were accessed.
   - All logon attempts for specific shared machines must be recorded.

   Which of the following steps should Crystal take to meet these requirements? (Choose all that apply.)

   A. Enable auditing with the Computer Management tool.
   B. Enable auditing with the Active Directory Users and Computers tool.
   C. Enable auditing with the Active Directory Domains and Trusts tool.
   D. Enable auditing with the Event Viewer tool.
   E. View the audit log using the Event Viewer tool.
   F. View auditing information using the Computer Management tool.
   G. Enable failure and success auditing settings for specific files stored on NTFS volumes.
   H. Enable failure and success auditing settings for logon events on specific computer accounts.

5. You create a GPO and link it to the Sales OU. You want to monitor users in the Sales OU who connect to the file server. What type of auditing do you enable?

   A. Audit Object Access
   B. Audit Logon Events
   C. Audit System Events
   D. Audit Process Tracking

Chapter 8

Configure TCP/IP

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure IPv4 and IPv6 addressing**

- Configure IP address options
- Configure IPv4 or IPv6 subnetting
- Configure supernetting
- Configure interoperability between IPv4 and IPv6
- Configure ISATAP
- Configure Teredo

In this chapter, I will discuss the most important protocol used in a Microsoft Windows Server 2012 R2 network: *Transmission Control Protocol/Internet Protocol (TCP/IP)*.

TCP/IP is actually two sets of protocols bundled together: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP/IP is a suite of protocols developed by the U.S. Department of Defense's Advanced Research Projects Agency in 1969.

This chapter is divided into two main topics: First I'll talk about TCP/IP version 4, and then I'll discuss TCP/IP version 6. TCP/IP version 4 is still used in Windows Server 2012 R2, and it was the primary version of TCP/IP in all previous versions of Windows. However, TCP/IP version 6 is the new release of TCP/IP, and it has been incorporated into Windows Server 2012 R2.

Understanding TCP/IP

I mentioned that TCP/IP is actually two sets of protocols bundled together: TCP and IP. These protocols sit on a four-layer TCP/IP model.

Details of the TCP/IP Model

The four layers of the TCP/IP model are as follows (see Figure 8.1):

Application Layer The *Application layer* is where the applications that use the protocol stack reside. These applications include File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP).

Transport Layer The *Transport layer* is where the two Transport layer protocols reside. These are TCP and the User Datagram Protocol (UDP). TCP is a connection-oriented protocol, and delivery is guaranteed. UDP is a connectionless protocol. This means that UDP does its best job to deliver the message, but there is no guarantee.

Internet Layer The *Internet layer* is where IP resides. *IP* is a connectionless protocol that relies on the upper layer (Transport layer) for guaranteeing delivery. *Address Resolution Protocol (ARP)* also resides on this layer. ARP turns an IP address into a Media Access Control (MAC) address. All upper and lower layers travel through the IP protocol.

Link Layer The data link protocols like Ethernet and Token Ring reside in the *Link layer*. This layer is also referred to as the *Network Access layer*.

FIGURE 8.1 TCP/IP model

How TCP/IP Layers Communicate

When an application like FTP is called upon, the application moves down the layers and TCP is retrieved. TCP then connects itself to the IP protocol and gets released onto the network through the Link layer (see Figure 8.2). This is a connection-oriented protocol because TCP is the protocol that guarantees delivery.

When an application like TFTP gets called, the application moves down the layers and UDP is retrieved. UDP then connects itself to the IP protocol and gets released onto the network through the Link layer. This is a connectionless protocol because UDP does not have guaranteed delivery.

Understanding Port Numbers

TCP and UDP rely on port numbers assigned by the *Internet Assigned Numbers Authority (IANA)* to forward packets to the appropriate application process. Port numbers are 16-bit integers that are part of a message header. They identify the application software process with which the packet should be associated. For example, let's say that a client has a copy of Internet Explorer and a copy of Mail open at the same time. Both applications are sending TCP requests across the Internet to retrieve web pages and email, respectively. How does the computer know which return packets to forward to Internet Explorer and which packets to forward to Mail?

FIGURE 8.2 TCP/IP process

When making a connection, the client chooses a source port for the communication that is usually in the range 1024–65535 (or sometimes in the range 1–65535). This source port then communicates with a destination port of 80 or 110 on the server side. Every packet destined for Internet Explorer has a source port number of 80 in the header, and every packet destined for Mail has a source port number of 110 in the header.

Table 8.1 describes the most common port numbers (you might need to know these for the exam). You can visit `www.iana.org` to get the most current and complete list of port numbers. It's good to become familiar with specific port numbers because it's a benefit to be able to determine from memory the ports that, for example, allow or block specific protocols in a firewall. Allowing only port 80, for instance, does not ensure that all web traffic will be allowed. You must also allow port 443 for certain secure web traffic.

NOTE

Simply because a port is "well known" doesn't mean that a given service must run on it. It's technically valid to run any service on any port, but doing so is usually a bad idea. For example, if you chose to run your web server on TCP port 25, clients would need to type `www.example.com:25` to reach your website from most browsers.

TABLE 8.1 Common port numbers

Port number	Description
20	FTP data
21	FTP control
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP), Web
88	Kerberos
110	Post Office Protocol v3 (POP3)
443	Secure HTTP (HTTPS)

Understanding IP Addressing

Understanding IP addressing is critical to understanding how IP works. An IP address is a numeric identifier assigned to each device on an IP network. This type of address is a logical software address that designates the device's location on the network. It isn't the physical hardware address hard-coded in the device's network interface card.

In the following sections, you will see how IP addresses are used to identify uniquely every machine on the network (MAC address).

The Hierarchical IP Addressing Scheme

An IP address consists of 32 bits of information. These bits are divided into four sections (sometimes called *octets* or *quads*) containing 1 byte (8 bits) each. There are three common methods for specifying an IP address:

- Dotted-decimal, as in 130.57.30.56
- Binary, as in 10000010.00111001.00011110.00111000
- Hexadecimal, as in 82 39 1E 38

All of these examples represent the same IP address.

The 32-bit IP address is a structured, or hierarchical, address as opposed to a flat, or nonhierarchical, address. Although IP could have used either *flat addressing* or *hierarchical addressing*, its designers elected to use the latter for a very good reason, as you will now see.

Real World Scenario

Why Hierarchical Addressing Is Used

What's the difference between flat and hierarchical addressing? A good example of a flat addressing scheme is a U.S. state driver's license number. There's no partitioning to it; the range of legal numbers isn't broken up in any meaningful way (say, by county of residence or date of issue). If this method had been used for IP addressing, every machine on the Internet would have needed a totally unique address, just as each driver's license number in a particular state is unique.

The good news about flat addressing is that it can handle a large number of addresses in 32 bits of data, namely, 4.3 billion. A 32-bit address space with two possible values for each position—either 0 (zero) or 1 (one)—gives you 2^{32} values, which equals approximately 4.3 billion.

The bad news—and the reason flat addressing isn't used in IP—relates to routing. If every address were totally unique, every router on the Internet would need to store the address of every other machine on the Internet. It would be fair to say that this would make efficient routing impossible, even if only a fraction of the possible addresses were used.

The solution to this dilemma is to use a hierarchical addressing scheme that breaks the address space into ordered chunks. Telephone numbers are a great example of this type of addressing. The first section of a U.S. telephone number, the area code, designates a very large area. The area code is followed by the prefix, which narrows the scope to a local calling area. The final segment, the customer number, zooms in on the specific connection. By looking at a number such as 603-766-xxxx, you can quickly determine that the number is located in the southern part of New Hampshire (area code 603) in the Portsmouth area (the 766 exchange).

IP Address Structure

IP addressing works the same way. Instead of the entire 32 bits being treated as a unique identifier, one part of the IP address is designated as the network address (or network ID) and the other part as a node address (or host ID), giving it a layered, hierarchical structure. Together, the IP address, the network address, and the node address uniquely identify a device within an IP network.

The network address—the first two sets of numbers in an IP address—uniquely identifies each network. Every machine on the same network shares that network address

as part of its IP address, just as the address of every house on a street shares the same street name. In the IP address 130.57.30.56, for example, 130.57 is the network address.

The node address—the second two sets of numbers—is assigned to, and uniquely identifies, each machine in a network, just as each house on the same street has a different house number. This part of the address must be unique because it identifies a particular machine—an individual, as opposed to a network. This number can also be referred to as a *host address*. In the sample IP address 130.57.30.56, the node address is .30.56.

Understanding Network Classes

The designers of the Internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of nodes, they created the Class A network. At the other extreme is the Class C network, reserved for the numerous networks with small numbers of nodes. The class of networks in between the very large and very small ones is predictably called the Class B network.

The default subdivision of an IP address into a network and node address is determined by the class designation of your network. Table 8.2 summarizes the three classes of networks, which will be described in more detail in the following sections.

TABLE 8.2 Network address classes

Class	Mask bits	Leading bit pattern	Decimal range of first octet of IP address	Assignable networks	Maximum nodes per network
A	8	0	1–126	126	16,777,214
B	16	10	128–191	16,384	65,534
C	24	110	192–223	2,097,152	254

Classless Inter-Domain Routing (CIDR), explained in detail later in this chapter, has effectively done away with these class designations. You will still hear and should still know the meaning behind the class designations of addresses because they are important to understanding IP addressing. However, when you're working with IP addressing in practice, CIDR is more important to know.

To ensure efficient routing, Internet designers defined a mandate for the leading bits section of the address for each different network class. For example, because a router knows that a Class A network address always starts with a 0, it can quickly apply the default mask, if necessary, after reading only the first bit of the address. Table 8.2 illustrates how the leading bits of a network address are defined. When considering the subnet masking between

network and host addresses, the number of bits to mask is important. For example, in a Class A network, 8 bits are masked, making the default subnet mask 255.0.0.0; in a Class C, 24 bits are masked, making the default subnet mask 255.255.255.0.

Some IP addresses are reserved for special purposes and shouldn't be assigned to nodes. Table 8.3 describes some of the reserved IP addresses. See RFC 3330 for others.

TABLE 8.3 Special network addresses

Address	Function
Entire IP address set to all 0s	Depending on the mask, this network (that is, the network or subnet of which you are currently a part) or this host on this network.
A routing table entry of all 0s with a mask of all 0s	Used as the default gateway entry. Any destination address masked by all 0s produces a match for the all 0s reference address. Because the mask has no 1s, this is the least desirable entry, but it will be used when no other match exists.
Network address 127	Reserved for loopback tests. Designates the local node, and it allows that node to send a test packet to itself without generating network traffic.
Node address of all 0s	Used when referencing a network without referring to any specific nodes on that network. Usually used in routing tables.
Node address of all 1s	Broadcast address for all nodes on the specified network, also known as a *directed broadcast*. For example, 128.2.255.255 means all nodes on the Class B network 128.2. Routing this broadcast is configurable on certain routers.
169.254.0.0 with a mask of 255.255.0.0	The "link-local" block used for autoconfiguration and communication between devices on a single link. Communication cannot occur across routers. Microsoft uses this block for Automatic Private IP Addressing (APIPA).
Entire IP address set to all 1s (same as 255.255.255.255)	Broadcast to all nodes on the current network; sometimes called a *limited broadcast* or an *all-1s broadcast*. This broadcast is not routable.
10.0.0.0/8 172.16.0.0 to 172.31.255.255 192.168.0.0/16	The private-use blocks for Classes A, B, and C. As noted in RFC 1918, the addresses in these blocks must never be allowed into the Internet, making them acceptable for simultaneous use behind NAT servers and non-Internet-connected IP networks.

In the following sections, you will look at the three network types.

Class A Networks

In a Class A network, the first byte is the network address, and the three remaining bytes are used for the node addresses. The Class A format is Network.Node.Node.Node.

For example, in the IP address 49.22.102.70, 49 is the network address, and 22.102.70 is the node address. Every machine on this particular network would have the distinctive network address of 49. Within that network, however, you could have a large number of machines.

There are 126 possible Class A network addresses. Why? The length of a Class A network address is 1 byte, and the first bit of that byte is reserved, so 7 bits in the first byte remain available for manipulation. This means that the maximum number of Class A networks is 128. (Each of the 7 bit positions that can be manipulated can be either a 0 or a 1, and this gives you a total of 2^7 positions, or 128.) But to complicate things further, it was also decided that the network address of all 0s (0000 0000) would be reserved. This means that the actual number of usable Class A network addresses is 128 minus 1, or 127. Also, 127 is a reserved number (a network address of 0 followed by all 1s [0111 1111], so you actually start with 128 addresses minus the 2 reserved, and you're left with 126 possible Class A network addresses.

Each Class A network has 3 bytes (24 bit positions) for the node address of a machine, which means that there are 2^{24}, or 16,777,216, unique combinations. Because addresses with the two patterns of all 0s and all 1s in the node bits are reserved, the actual maximum usable number of nodes for a Class A network is 2^{24} minus 2, which equals 16,777,214.

Class B Networks

In a Class B network, the first 2 bytes are assigned to the network address, and the remaining 2 bytes are used for node addresses. The format is Network.Network.Node.Node.

For example, in the IP address 130.57.30.56, the network address is 130.57, and the node address is 30.56.

The network address is 2 bytes, so there would be 2^{16} unique combinations. But the Internet designers decided that all Class B networks should start with the binary digits 10. This leaves 14 bit positions to manipulate; therefore, there are 16,384 (or 2^{14}) unique Class B networks.

This gives you an easy way to recognize Class B addresses. If the first 2 bits of the first byte can be only 10, that gives you a decimal range from 128 up to 191 in the first octet of the IP address. Remember that you can always easily recognize a Class B network by looking at its first byte, even though there are 16,384 different Class B networks. If the first octet in the address falls between 128 and 191, it is a Class B network, regardless of the value of the second octet.

A Class B network has 2 bytes to use for node addresses. This is 2^{16} minus the two patterns in the reserved-exclusive club (all 0s and all 1s in the node bits) for a total of 65,534 possible node addresses for each Class B network.

Class C Networks

The first 3 bytes of a Class C network are dedicated to the network portion of the address, with only 1 byte remaining for the node address. The format is Network.Network. Network.Node.

In the example IP address 198.21.74.102, the network address is 198.21.74, and the node address is 102.

In a Class C network, the first three bit positions are always binary 110. Three bytes, or 24 bits, minus 3 reserved positions leaves 21 positions. There are therefore 2^{21} (or 2,097,152) possible Class C networks.

The lead bit pattern of 110 equates to decimal 192 and runs through 223. Remembering our handy easy-recognition method, this means you can always spot a Class C address if the first byte is in the range 192–223, regardless of the values of the second and third bytes of the IP address.

Each unique Class C network has 1 byte to use for node addresses. This leads to 2^8, or 256, minus the two special patterns of all 0s and all 1s, for a total of 254 node addresses for each Class C network.

Class D networks, used for multicasting only, use the address range 224.0.0.0 to 239.255.255.255 and are used, as in broadcasting, as destination addresses only. Class E networks (reserved for future use at this point) cover 240.0.0.0 to 255.255.255.255. Addresses in the Class E range are considered within the experimental range.

Subnetting a Network

If an organization is large and has lots of computers or if its computers are geographically dispersed, it makes good sense to divide its colossal network into smaller ones connected by routers. These smaller networks are called *subnets*. The benefits of using subnets are as follows:

Reduced Network Traffic We all appreciate less traffic of any kind, and so do networks. Without routers, packet traffic could choke the entire network. Most traffic will stay on the local network—only packets destined for other networks will pass through the router and to another subnet. This traffic reduction also improves overall performance.

Simplified Management It's easier to identify and isolate network problems in a group of smaller networks connected together than within one gigantic one.

Understanding the Benefits of Subnetting

To understand one benefit of subnetting, consider a hotel or office building. Say that a hotel has 1,000 rooms with 75 rooms to a floor. You could start at the first room on the first floor and number it 1; then when you get to the first room on the second floor, you could number it 76 and keep going until you reach room 1,000. But someone looking for room 521 would have to guess on which floor that room is located. If you were to "subnet" the hotel, you would identify the first room on the first floor with the number 101 (1 = Floor 1 and 01 = Room 1), the first room on the second floor with 201, and so on. The guest looking for room 521 would go to the fifth floor and look for room 21.

An organization with a single network address (comparable to the hotel building mentioned in the sidebar "Understanding the Benefits of Subnetting") can have a subnet address for each individual physical network (comparable to a floor in the hotel building). Each subnet is still part of the shared network address, but it also has an additional identifier denoting its individual subnetwork number. This identifier is called a *subnet address*.

Subnetting solves several addressing problems:

- If an organization has several physical networks but only one IP network address, it can handle the situation by creating subnets.
- Because subnetting allows many physical networks to be grouped together, fewer entries in a routing table are required, notably reducing network overhead.
- These things combine collectively to yield greatly enhanced network efficiency.

The original designers of the Internet Protocol envisioned a small Internet with only tens of networks and hundreds of hosts. Their addressing scheme used a network address for each physical network. As you can imagine, this scheme and the unforeseen growth of the Internet created a few problems. The following are two examples:

Not Enough Addresses A single network address can be used to refer to multiple physical networks, but an organization can request individual network addresses for each one of its physical networks. If all of these requests were granted, there wouldn't be enough addresses to go around.

Gigantic Routing Tables If each router on the Internet needed to know about every physical network, routing tables would be impossibly huge. There would be an overwhelming amount of administrative overhead to maintain those tables, and the resulting physical overhead on the routers would be massive (CPU cycles, memory, disk space, and so on). Because routers exchange routing information with each other, an additional, related consequence is that a terrific overabundance of network traffic would result.

Although there's more than one way to approach these problems, the principal solution is the one that I'll cover in this book—subnetting. As you might guess, *subnetting* is the process of carving a single IP network into smaller logical subnetworks. This trick is achieved by subdividing the host portion of an IP address to create a subnet address. The actual subdivision is accomplished through the use of a subnet mask (covered later in the chapter).

In the following sections, you will see exactly how to calculate and apply subnetting.

Implementing Subnetting

Before you can implement subnetting, you need to determine your current requirements and plan on how best to implement your subnet scheme.

How to Determine Your Subnetting Requirements

Follow these guidelines to calculate the requirements of your subnet:

1. Determine the number of required network IDs: one for each subnet and one for each wide area network (WAN) connection.
2. Determine the number of required host IDs per subnet: one for each TCP/IP device, including, for example, computers, network printers, and router interfaces.
3. Based on these two data points, create the following:
   - One subnet mask for your entire network
   - A unique subnet ID for each physical segment
   - A range of host IDs for each unique subnet

How to Implement Subnetting

Subnetting is implemented by assigning a subnet address to each machine on a given physical network. For example, in Figure 8.3, each machine on subnet 1 has a subnet address of 1.

The default network portion of an IP address can't be altered without encroaching on another administrative domain's address space, unless you are assigned multiple consecutive classful addresses. To maximize the efficient use of the assigned address space, machines on a particular network share the same network address. In Figure 8.3, you can see that all of the Widget Inc. machines have a network address of 130.57. That principle is constant. In subnetting, it's the host address that's manipulated—the network address doesn't change. The subnet address scheme takes a part of the host address and recycles it as a subnet address. Bit positions are stolen from the host address to be used for the subnet identifier. Figure 8.4 shows how an IP address can be given a subnet address.

FIGURE 8.3 A sample subnet

FIGURE 8.4 Network vs. host addresses

Because the Widget Inc. network is a Class B network, the first two bytes specify the network address and are shared by all machines on the network, regardless of their particular subnet. Here every machine's address on the subnet must have its third byte read 0000 0001. The fourth byte, the host address, is the unique number that identifies the actual host within that subnet. Figure 8.5 illustrates how a network address and a subnet address can be used together.

FIGURE 8.5 The network address and its subnet

When implementing subnetting, you need some type of hardware installed onto the network. Most of us will just use a router. But if you do not want to purchase an expensive router, there is another way.

One way that you can implement subnetting is by using a Windows Server 2012 R2 machine with multiple NIC adapters configured with routing enabled on the server. This type of router is called a *multihomed router*. This is an inexpensive way to set up a router using a Microsoft server, but it may not be the best way. Many companies specialize in routers, and these routers offer many more features and more flexibility than a multihomed router.

How to Use Subnet Masks

For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the network address. This is accomplished by assigning each machine a subnet mask.

The network administrator creates a 32-bit subnet mask comprising 1s and 0s. The 1s in the subnet mask represent the positions in the IP address that refer to the network and subnet addresses. The 0s represent the positions that refer to the host part of the address. Figure 8.6 illustrates this combination.

In the Widget Inc. example, the first two bytes of the subnet mask are 1s because Widget's network address is a Class B address, formatted as Network.Network.Node.Node. The third byte, normally assigned as part of the host address, is now used to represent the subnet address. Hence, those bit positions are represented with 1s in the subnet mask. The fourth byte is the only part of the example that represents the host address.

FIGURE 8.6 The subnet mask revealed

The subnet mask can also be expressed using the decimal equivalents of the binary patterns. The binary pattern of 1111 1111 is the same as decimal 255. Consequently, the subnet mask in the example can be denoted in two ways, as shown in Figure 8.7.

FIGURE 8.7 Different ways to represent the same mask

Subnet mask in binary: 1111 1111. 1111 1111. 1111 1111. 0000 0000

Subnet mask in decimal: 255 . 255 . 255 . 0

(The spaces in the above example are only for illustrative purposes.
The subnet mask in decimal would actually appear as 255.255.255.0.)

Not all networks need to have subnets, and therefore they don't need to use custom subnet masks. In this case, they are said to have a *default* subnet mask. This is basically the same as saying that they don't have any subnets except for the one main subnet on which the network is running. Table 8.4 shows the default subnet masks for the different classes of networks.

TABLE 8.4 Default subnet masks

Class	Format	Default Subnet Mask
A	Network.Node.Node.Node	255.0.0.0
B	Network.Network.Node.Node	255.255.0.0
C	Network.Network.Network.Node	255.255.255.0

Once the network administrator has created the subnet mask and has assigned it to each machine, the IP software applies the subnet mask to the IP address to determine its subnet address. The word *mask* carries the implied meaning of "lens" in this case; that is, the IP software looks at its IP address through the lens of its subnet mask to see its subnet address. Figure 8.8 illustrates an IP address being viewed through a subnet mask.

FIGURE 8.8 Applying the subnet mask

In this example, the IP software learns through the subnet mask that, instead of being part of the host address, the third byte of its IP address is now going to be used as a subnet address. The IP software then looks in its IP address at the bit positions that correspond to the mask, which are 0000 0001.

The final step is for the subnet bit values to be matched up with the binary numbering convention and converted to decimal. In the Widget Inc. example, the binary-to-decimal conversion is simple, as illustrated in Figure 8.9.

FIGURE 8.9 Converting the subnet mask to decimal

By using the entire third byte of a Class B address as the subnet address, it is easy to set and determine the subnet address. For example, if Widget Inc. wants to have a subnet 6, the third byte of all machines on that subnet will be 0000 0110 (decimal 6 in binary).

Using the entire third byte of a Class B network address for the subnet allows for a fair number of available subnet addresses. One byte dedicated to the subnet provides eight bit positions. Each position can be either a 1 or a 0, so the calculation is 2^8, or 256. Thus, Widget Inc. can have up to 256 total subnetworks, each with up to 254 hosts.

Although RFC 950 prohibits the use of binary all 0s and all 1s as subnet addresses, today almost all products actually permit this usage. Microsoft's TCP/IP stack allows it, as does the software in most routers (provided you enable this feature, which sometimes is not the case by default). This gives you two additional subnets. However, you should not use a subnet of 0 (all 0s) unless all the software on your network recognizes this convention.

How to Calculate the Number of Subnets

The formulas for calculating the maximum number of subnets and the maximum number of hosts per subnet are as follows:

> 2 × number of masked bits in subnet mask = maximum number of subnets
>
> 2 × number of unmasked bits in subnet mask – 2 = maximum number of hosts per subnet

In the formulas, *masked* refers to bit positions of 1, and *unmasked* refers to bit positions of 0. The downside to using an entire byte of a node address as your subnet address is that you reduce the possible number of node addresses on each subnet. As explained earlier, without a subnet, a Class B address has 65,534 unique combinations of 1s and 0s that can be used for node addresses. The question then is why would you ever want 65,534 hosts on a single physical network?

The trade-off is acceptable to most who ask themselves this question. If you use an entire byte of the node address for a subnet, you then have only 1 byte for the host addresses, leaving only 254 possible host addresses. If any of your subnets are populated with more than 254 machines, you'll have a problem. To solve it, you would then need to shorten the subnet mask, thereby lengthening the number of host bits and increasing the number of host addresses. This gives you more available host addresses on each subnet. A side effect of this solution is that it shrinks the number of possible subnets.

Figure 8.10 shows an example of using a smaller subnet address. A company called Acme Inc. expects to need a maximum of 14 subnets. In this case, Acme does not need to take an entire byte from the host address for the subnet address. To get its 14 different subnet addresses, it needs to snatch only 4 bits from the host address ($2^4 = 16$). The host portion of the address has 12 usable bits remaining ($2^{12} – 2 = 4094$). Each of Acme's 16 subnets could then potentially have a total of 4,094 host addresses, and 4,094 machines on each subnet should be plenty.

FIGURE 8.10 An example of a smaller subnet address

Acme, Inc.

Network address: 132.8 (Class B; net.net.host.host)

Example IP address: 1000 0100. 0000 1000. 0001 0010. 0011 1100

Decimal: 132 . 8 . 18 . 60

Subnet Mask Code

1s = Positions representing network or subnet addresses
0s = Positions representing the host address

Subnet mask:

Binary: 1111 1111. 1111 1111. 1111 0000. 0000 0000

Decimal: 255 . 255 . 240 . 0

(The decimal 240 is equal to the binary 1111 0000.)

Positions relating to the subnet address

Subnet mask: 1111 1111. 1111 1111. 1111 0000. 0000 0000

IP address of a Acme machine: 1000 0100. 0000 1000. 0001 0010. 0011 1100
(Decimal: 132.8.18.60)

Bits relating to the subnet address

Binary-to-Decimal Conversions for Subnet Address

Subnet mask positions:	1	1	1	1	0	0	0	0
Position/value: ←(continue)	128	64	32	16	8	4	2	1
Third byte of IP address:	0	0	0	1	0	0	1	0
Decimal equivalent:						0 + 16 = 16		
Subnet address for this IP address:								16

An Easier Way to Apply Subnetting

Now that you have the basics of how to subnet down, you'll learn an easier way. If you have learned a different way and it works for you, stick with it. It does not matter how you get to the finish line, just as long as you get there. But if you are new to subnetting, Figure 8.11 will make it easier for you.

This chart may look intimidating, but it's really simple to use once you have done it a few times.

Remember that, on this chart, 1s equal subnets, and 0s equal hosts. If you get this confused, you will get wrong answers in the following exercises.

FIGURE 8.11 TCP/IP v4 subnetting chart

$2^{(X)}$-2=Y	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

0 = Hosts, 1 = Subnets

X (POWER)			X		Y
2^x	3	=	8	–2	6
2^x	4	=	16	–2	14
2^x	5	=	32	–2	30
2^x	6	=	64	–2	62
2^x	7	=	128	–2	126
2^x	8	=	256	–2	254
2^x	9	=	512	–2	510
2^x	10	=	1024	–2	1022
2^x	11	=	2048	–2	2046
2^x	12	=	4096	–2	4094
2^x	13	=	8192	–2	8190
2^x	14	=	16384	–2	16382
2^x	15	=	32768	–2	32766
2^x	16	=	65536	–2	65534
2^x	17	=	131072	–2	131070

Watch the Y column on the lower end of the chart. This represents the number of addresses available to you after the two reserved addresses have been removed. The following exercises provide some examples.

SUBNET MASK EXERCISE 8.1

Class C, 10 Hosts per Subnet

You have a Class C address, and you require 10 hosts per subnet.

1. Write down the following:

   255.255.255.____

   The blank is the number you need to fill in.

2. Look under the Y column and choose the first number that is larger than 10 (the number of hosts per subnet you need). You should have come up with 14.

SUBNET MASK EXERCISE 8.1 *(continued)*

3. Move across the page and look at number in the X (Power) column. The power number is 4.
4. Go to the top of the chart and look for the row with exactly four 0s (hosts). Find the number at the beginning of the row.

The number at the beginning of the row is 240. That's your answer. The subnet mask should be 255.255.255.240.

SUBNET MASK EXERCISE 8.2

Class C, 20 Hosts per Subnet

You have a Class C address, and you need 20 hosts per subnet.

1. Write down the following:

   255.255.255.___

2. Look under the Y column and find the first number that covers 20. (This should be 30.)
3. Go across to the power number (5).
4. Go to the top part of the chart and find the row with exactly five 0s from right to left.

The number at the beginning of the row is 224. Your answer should be 255.255.255.224.

SUBNET MASK EXERCISE 8.3

Class C, Five Subnets

Now you have a Class C address, and you need five subnets. Remember that subnets are represented by 1s in the chart.

1. Write down the following:

   255.255.255.___

2. Look under the Y column and find the first number that covers 5. (This should be 6.)
3. Go across to the power number. (This should be 3.)
4. Go to the top part of the chart and find out which row has exactly three 1s (remember, 1s are for subnets) from left to right.

Your answer should be 255.255.255.224.

SUBNET MASK EXERCISE 8.4

Class B, 1,500 Hosts per Subnet

This one is a bit harder. You have a Class B address, and you need 1,500 hosts per subnet. Because you have a Class B address, you need to fill in the third octet of numbers. The fourth octet contains eight 0s.

1. Write down the following:

   255.255.___.0

2. Look at the Y column and find the first number that covers 1,500. (This should be 2,046.)
3. Go across and find the power number. (This should be 11.)
4. Remember, you already have eight 0s in the last octet. So, you need only three more. Find the row with three 0s.

You should come up with an answer of 255.255.248.0. This actually breaks down to 11111111.11111111.11111000.00000000, and that's how you got the 11 zeros.

SUBNET MASK EXERCISE 8.5

Class B, 3,500 Hosts per Subnet

You have a Class B address, and you need 3,500 hosts per subnet.

1. Write down the following:

   255.255.___.0

2. Look at the Y column and find the first number that covers 3,500. (This should be 4,094.)
3. Go across and find the power number. (This should be 12.)
4. Remember, you already have eight 0s in the last octet, so you need only four more. Count for four zeros from right to left.

You should come up with an answer of 255.255.240.0. Again, this actually breaks down to 111 11111.11111111.11110000.00000000, and that's how you got the 12 zeros.

TIP

If you get a question that gives you both the hosts and the subnets, always figure out the larger number first. Then, depending on the mask you have decided to use, make sure that the lower number is also correct with that mask.

Now try some more subnet mask exercises using the data that follows:

Class B address	**Class B address**
1,000 hosts per subnet	25 subnets
Class C address	**Class B address**
45 hosts per subnet	4,000 hosts per subnet
192.168.0.0	**Class B address**
10 subnets	2,000 hosts per subnet
	25 subnets

Here are the answers. If any of your answers are wrong, follow the previous examples and try to work through them again.

Class B address	**Class B address**
1,000 hosts per subnet 255.255.252.0	25 subnets 255.255.248.0
Class C address	**Class B address**
45 hosts per subnet 255.255.255.192	4,000 hosts per subnet 255.255.240.0
192.168.0.0	**Class B address**
10 subnets 255.255.255.240	2,000 hosts per subnet
	25 subnets 255.255.248.0

Applying Subnetting the Traditional Way

Sometimes subnetting can be confusing. After all, it can be quite difficult to remember all of those numbers. You can step back a minute and take a look at the primary classes of networks and how to subnet each one. Let's start with Class C because it uses only 8 bits for the node address, so it's the easiest to calculate. In the following sections, I will explain how to subnet the various types of networks.

Subnetting Class C

If you recall, a Class C network uses the first 3 bytes (24 bits) to define the network address. This leaves you 1 byte (8 bits) with which to address hosts. So if you want to create subnets, your options are limited because of the small number of bits available.

If you break down your subnets into chunks smaller than the default Class C, then figuring out the subnet mask, network number, broadcast address, and router address can be confusing. To build a sturdy base for subnetting, study the following techniques for determining these special values for each subnet, but also learn and use the more efficient technique presented in the later section "Quickly Identifying Subnet Characteristics Using CIDR" and the earlier section "An Easier Way to Apply Subnetting." Table 8.5 summarizes

how you can break down a Class C network into one, two, four, or eight smaller subnets, and it gives you the subnet masks, network numbers, broadcast addresses, and router addresses. The first three bytes have simply been designated x.y.z. (Note that the table assumes you can use the all-0s and all-1s subnets too.)

TABLE 8.5 Setting up Class C subnets

Number of desired subnets	Subnet mask	Network number	Router address	Broadcast address	Remaining number of IP addresses
1	255.255.255.0	x.y.z.0	x.y.z.1	x.y.z.255	253
2	255.255.255.128	x.y.z.0	x.y.z.1	x.y.z.127	125
	255.255.255.128	x.y.z.128	x.y.z.129	x.y.z.255	125
4	255.255.255.192	x.y.z.0	x.y.z.1	x.y.z.63	61
	255.255.255.192	x.y.z.64	x.y.z.65	x.y.z.127	61
	255.255.255.192	x.y.z.128	x.y.z.129	x.y.z.191	61
	255.255.255.192	x.y.z.192	x.y.z.193	x.y.z.255	61
8	255.255.255.224	x.y.z.0	x.y.z.1	x.y.z.31	29
	255.255.255.224	x.y.z.32	x.y.z.33	x.y.z.63	29
	255.255.255.224	x.y.z.64	x.y.z.65	x.y.z.95	29
	255.255.255.224	x.y.z.96	x.y.z.97	x.y.z.127	29
	255.255.255.224	x.y.z.128	x.y.z.129	x.y.z.159	29
	255.255.255.224	x.y.z.160	x.y.z.161	x.y.z.191	29
	255.255.255.224	x.y.z.192	x.y.z.193	x.y.z.223	29
	255.255.255.224	x.y.z.224	x.y.z.225	x.y.z.255	29

For example, suppose you want to chop up a Class C network, 200.211.192.*x*, into two subnets. As you can see in the table, you'd use a subnet mask of 255.255.255.128 for each subnet. The first subnet would have the network number 200.211.192.0, router address 200.211.192.1, and broadcast address 200.211.192.127. You could assign IP addresses 200.211.192.2 through 200.211.192.126—that's 125 additional different IP addresses.

> **TIP** Heavily subnetting a network results in the loss of a progressively greater percentage of addresses to the network number, broadcast address, and router address.

The second subnet would have the network number 200.211.192.128, router address 200.211.192.129, and broadcast address 200.211.192.255.

Why It's Best to Use Routers That Support Subnet 0

When subnetting a Class C network using the method in Table 8.5, if you use the $2^x - 2$ calculation, the subnet 128 in the table doesn't make sense. It turns out that there's a legitimate and popular reason to do it this way, however.

- Remember that using subnet 0 is not allowed according to the RFC standards, but by using it you can subnet your Class C network with a subnet mask of 128. This uses only 1 bit, and according to your calculator $2^1 - 2 = 0$, giving you zero subnets.
- By using routers that support subnet 0, you can assign 1–126 for hosts and 129–254 for hosts, as stated in the table. This saves a bunch of addresses! If you were to stick to the method defined by the RFC standards, the best you could gain is a subnet mask of 192 (2 bits), which allows you only two subnets ($2^2 - 2 = 2$).

Determining the Subnet Numbers for a Class C Subnet

The first subnet always has a 0 in the interesting octet. In the example, it would be 200.211.192.0, the same as the original nonsubnetted network address. To determine the subnet numbers for the additional subnets, first you have to determine the incremental value:

1. Begin with the octet that has an interesting value (other than 0 or 255) in the subnet mask. Then subtract the interesting value from 256. The result is the incremental value.

   If again you use the network 200.211.192.*x* and a mask of 255.255.255.192, the example yields the following equation: 256 – 192 = 64. Thus, 64 is your incremental value in the interesting octet—the fourth octet in this case. Why the fourth octet? That's the octet with the interesting value, 192, in the mask.
2. To determine the second subnet number, add the incremental value to the 0 in the fourth octet of the first subnet.

   In the example, it would be 200.211.192.64.
3. To determine the third subnet number, add the incremental value to the interesting octet of the second subnet number.

   In the example, it would be 200.211.192.128.
4. Keep adding the incremental value in this fashion until you reach the actual subnet mask number.

For example, 0 + 64 = 64, so your second subnet is 64. And 64 + 64 is 128, so your third subnet is 128. And 128 + 64 is 192, so your fourth subnet is 192. Because 192 is the subnet mask, this is your last subnet. If you tried to add 64 again, you'd come up with 256, an unusable octet value, which is always where you end up when you've gone too far. This means your valid subnets are 0, 64, 128, and 192.

The numbers between the subnets are your valid host and broadcast addresses. For example, the following are valid hosts for two of the subnets in a Class C network with a subnet mask of 192:

- The valid hosts for subnet 64 are in the range 65–126, which gives you 62 hosts per subnet.

  (You can't use 127 as a host because that would mean your host bits would be all 1s. The all-1s format is reserved as the broadcast address for that subnet.)
- The valid hosts for subnet 128 are in the range 129–190, with a broadcast address of 191.

As you can see, this solution wastes a few addresses—six more than not subnetting at all, to be exact. In a Class C network, this should not be hard to justify. The 255.255.255.128 subnet mask is an even better solution if you need only two subnets and expect to need close to 126 host addresses per subnet.

Calculating Values for an Eight-Subnet Class C Network

What happens if you need eight subnets in your Class C network?

By using the calculation of 2^x, where x is the number of subnet bits, you would need 3 subnet bits to get eight subnets ($2^3 = 8$). What are the valid subnets, and what are the valid hosts of each subnet? Let's figure it out.

11100000 is 224 in binary, and it would be the interesting value in the fourth octet of the subnet mask. This must be the same on all workstations.

You're likely to see test questions that ask you to identify the problem with a given configuration. If a workstation has the wrong subnet mask, the router could "think" that the workstation is on a different subnet than it actually is. When that happens, the misguided router won't forward packets to the workstation in question. Similarly, if the mask is incorrectly specified in the workstation's configuration, that workstation will observe the mask and send packets to the default gateway when it shouldn't.

To figure out the valid subnets, subtract the interesting octet value from 256 (256 – 224 = 32), so 32 is your incremental value for the fourth octet. Of course, the 0 subnet is your first subnet, as always. The other subnets would be 32, 64, 96, 128, 160, 192, and 224. The valid hosts are the numbers between the subnet numbers, except the numbers that equal all 1s in the host bits. These numbers would be 31, 63, 95, 127, 159, 191, 223, and 255. Remember that using all 1s in the host bits is reserved for the broadcast address of each subnet.

The valid subnets, hosts, and broadcasts are as follows:

Subnet	Hosts	Broadcast
0	1–30	31
32	33–62	63
64	65–94	95
96	97–126	127
128	129–158	159
160	161–190	191
192	193–222	223
224	225–254	255

You can add one more bit to the subnet mask just for fun. You were using 3 bits, which gave you 224. By adding the next bit, the mask now becomes 240 (11110000).

By using 4 bits for the subnet mask, you get 14 subnets because $2^4 = 16$. This subnet mask also gives you only 4 bits for the host addresses, or $2^4 - 2 = 14$ hosts per subnet. As you can see, the number of hosts per subnet gets reduced rather quickly for each host bit that gets reallocated for subnet use.

The first valid subnet for subnet 240 is 0, as always. Because 256 – 240 = 16, your remaining subnets are then 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. Remember that the actual interesting octet value also represents the last valid subnet, so 240 is the last valid subnet number. The valid hosts are the numbers between the subnets, except for the numbers that are all 1s—the broadcast address for the subnet.

Table 8.6 shows the numbers in the interesting (fourth) octet for a Class C network with eight subnets.

TABLE 8.6 Fourth octet addresses for a Class C network with eight subnets

Subnet	Hosts	Broadcast
0	1–14	15
16	17–30	31
32	33–46	47
48	49–62	63
64	65–78	79

80	81–94	95
96	97–110	111
112	113–126	127
128	129–142	143
144	145–158	159
160	161–174	175
176	177–190	191
192	193–206	207
208	209–222	223
224	225–238	239
240	241–254	255

Subnetting Class B

Because a Class B network has 16 bits for host addresses, you have plenty of available bits to play with when figuring out a subnet mask. Remember that you have to start with the leftmost bit and work toward the right. For example, a Class B network would look like x.y.0.0, with the default mask of 255.255.0.0. Using the default mask would give you one network with 65,534 hosts.

The default mask in binary is 11111111.11111111.00000000.00000000. The 1s represent the corresponding network bits in the IP address, and the 0s represent the host bits. When you're creating a subnet mask, the leftmost bit(s) will be borrowed from the host bits (0s will be turned into 1s) to become the subnet mask. You then use the remaining bits that are still set to 0 for host addresses.

If you use only 1 bit to create a subnet mask, you have a mask of 255.255.128.0. If you use 2 bits, you have a mask of 255.255.192.0, or 11111111.11111111.11000000.00000000.

As with subnetting a Class C address, you now have three parts of the IP address: the network address, the subnet address, and the host address. You figure out the subnet mask numbers the same way as you did with a Class C network (see the previous section, "Calculating Values for an Eight-Subnet Class C Network"), but you'll end up with a lot more hosts per subnet.

There are four subnets, because $2^2 = 4$. The valid third-octet values for the subnets are 0, 64, 128, and 192 (256 – 192 = 64, so the incremental value of the third octet is 64). However, there are 14 bits (0s) left over for host addressing. This gives you 16,382 hosts per subnet ($2^{14} – 2 = 16,382$).

The valid subnets and hosts are as follows:

Subnet	Hosts	Broadcast
x.y.0.0	x.y.0.1 through x.y. 63.254	x.y.63.255
x.y.64.0	x.y.64.1 through x.y.127.254	x.y.127.255
x.y.128.0	x.y.128.1 through x.y.191.254	x.y.191.255
x.y.192.0	x.y.192.1 through x.y.255.254	x.y.255.255

You can add another bit to the subnet mask, making it 11111111.11111111.11100000.00000000, or 255.255.224.0. This gives you eight subnets ($2^3 = 8$) and 8,190 hosts. The valid subnets are 0, 32, 64, 96, 128, 160, 192, and 224 (256 – 224 = 32). The subnets, valid hosts, and broadcasts are listed here:

Subnet	Hosts	Broadcast
x.y.0.0	x.y.0.1 through x.y.31.254	x.y.31.255
x.y.32.0	x.y.32.1 through x.y.63.254	x.y.63.255
x.y.64.0	x.y.64.1 through x.y.95.254	x.y.95.255
x.y.96.0	x.y.96.1 through x.y.127.254	x.y.127.255
x.y.128.0	x.y.128.1 through x.y.159.254	x.y.159.255
x.y.160.0	x.y.160.1 through x.y.191.254	x.y.191.255
x.y.192.0	x.y.192.1 through x.y.223.254	x.y.223.255
x.y.224.0	x.y.224.1 through x.y.255.254	x.y.255.255

The following are the breakdowns for a 9-bit mask and a 14-bit mask:

- If you use 9 bits for the mask, it gives you 512 subnets (2^9). With only 7 bits for hosts, you still have 126 hosts per subnet ($2^7 – 2 = 126$). The mask looks like this:

  11111111.11111111.11111111.10000000, or 255.255.255.128

- If you use 14 bits for the subnet mask, you get 16,384 subnets (2^{14}) but only two hosts per subnet ($2^2 – 2 = 2$). The subnet mask would look like this:

  11111111.11111111.11111111.11111100, or 255.255.255.252

Real World Scenario

Subnet Mask Use in an ISP

You may be wondering why you would use a 14-bit subnet mask with a Class B address. This approach is actually very common. Let's say you have a Class B network and use a subnet mask of 255.255.255.0. You'd have 256 subnets and 254 hosts per subnet. Imagine also that you are an Internet service provider (ISP) and have a network with many WAN links, a different one between you and each customer. Typically, you'd have a direct connection between each site. Each of these links must be on its own subnet or network. There will be two hosts on these subnets—one address for each router port. If you used the mask described earlier (255.255.255.0), you would waste 252 host addresses per subnet. But by using the 255.255.255.252 subnet mask, you have more subnets available, which means more customers—each subnet with only two hosts, which is the maximum allowed on a point-to-point circuit.

You can use the 255.255.255.252 subnet mask only if you are running a routing algorithm such as Enhanced Interior Gateway Routing Protocol (EIGRP) or Open Shortest Path First (OSPF). These routing protocols allow what is called *variable-length subnet masking (VLSM)*. VLSM allows you to run the 255.255.255.252 subnet mask on your interfaces to the WANs and run 255.255.255.0 on your router interfaces in your local area network (LAN) using the same classful network address for all subnets. It works because these routing protocols transmit the subnet mask information in the update packets that they send to the other routers. Classful routing protocols, such as RIP version 1, don't transmit the subnet mask and therefore cannot employ VLSM.

Subnetting Class A

Class A networks have even more bits available than Class B and Class C networks. A default Class A network subnet mask is only 8 bits, or 255.0.0.0, giving you a whopping 24 bits for hosts to play with. Knowing which hosts and subnets are valid is a lot more complicated than it was for either Class B or Class C networks.

If you use a mask of 11111111.1111111.00000000.00000000, or 255.255.0.0, you'll have 8 bits for subnets, or 256 subnets (2^8). This leaves 16 bits for hosts, or 65,534 hosts per subnet ($2^{16} - 2 = 65534$).

If you split the 24 bits evenly between subnets and hosts, you would give each one 12 bits. The mask would look like this: 11111111.11111111.11110000.00000000, or 255.255.240.0. How many valid subnets and hosts would you have? The answer is 4,096 subnets each with 4,094 hosts ($2^{12} - 2 = 4094$).

The second octet will be somewhere between 0 and 255. However, you will need to figure out the third octet. Because the third octet has a 240 mask, you get 16

(256 – 240 = 16) as your incremental value in the third octet. The third octet must start with 0 for the first subnet, the second subnet will have 16 in the third octet, and so on. This means that some of your valid subnets are as follows (not in order):

Subnet	Hosts	Broadcast
x.0-255.0.0	x.0-255.0.1 through x.0-255.15.254	x.0-255.15.255
x.0-255.16.0	x.0-255.16.1 through x.0-255.31.254	x.0-255.31.255
x.0-255.32.0	x.0-255.32.1 through x.0-255.47.254	x.0-255.47.255
x.0-255.48.0	x.0-255.48.1 through x.0-255.63.254	x.0-255.63.255

They go on in this way for the remaining third-octet values through 224 in the subnet column.

Working with Classless Inter-Domain Routing

Microsoft uses an alternate way to write address ranges, called *Classless Inter-Domain Routing* (*CIDR*; pronounced "cider"). CIDR is a shorthand version of the subnet mask. For example, an address of 131.107.2.0 with a subnet mask of 255.255.255.0 is listed in CIDR as 131.107.2.0/24 because the subnet mask contains 24 1s. An address listed as 141.10.32.0/19 would have a subnet mask of 255.255.224.0, or 19 1s (the default subnet mask for Class B plus 3 bits). This is the nomenclature used in all Microsoft exams (see Figure 8.12).

FIGURE 8.12 Subnet mask represented by 1s

Subnet mask in binary: 1111 1111. 1111 1111. 1111 1111. 0000 0000

Subnet mask in decimal: 255 . 255 . 255 . 0

(The spaces in the above example are only for illustrative purposes.
The subnet mask in decimal would actually appear as 255.255.255.0.)

Let's say an Internet company has assigned you the following Class C address and CIDR number: 192.168.10.0/24. This represents the Class C address of 192.168.10.0 and a subnet mask of 255.255.255.0.

Again, CIDR represents the number of 1s turned on in a subnet mask. For example, a CIDR number of /16 stands for 255.255.0.0 (11111111.11111111.00000000.00000000).

The following is a list of all of the CIDR numbers (starting with a Class A default subnet mask) and their corresponding subnet masks:

CIDR	Mask	CIDR	Mask	CIDR	Mask
/8	255.0.0.0	/17	255.255.128.0	/25	255.255.255.128
/9	255.128.0.0	/18	255.255.192.0	/26	255.255.255.192
/10	255.192.0.0	/19	255.255.224.0	/27	255.255.255.224
/11	255.224.0.0	/20	255.255.240.0	/28	255.255.255.240
/12	255.240.0.0	/21	255.255.248.0	/29	255.255.255.248
/13	255.248.0.0	/22	255.255.252.0	/30	255.255.255.252
/14	255.252.0.0	/23	255.255.254.0	/31	255.255.255.254
/15	255.254.0.0	/24	255.255.255.0	/32	255.255.255.255
/16	255.255.0.0				

Quickly Identifying Subnet Characteristics Using CIDR

Given the limited time you have to dispatch questions in the structured environment of a Microsoft certification exam, every shortcut to coming up with the correct answer is a plus. The following method, using CIDR notation, can shave minutes off the time it takes you to complete a single question. Since you already understand the underlying binary technology at the heart of subnetting, you can use the following shortcuts, one for each address class, to come up with the correct answer without working in binary.

Identifying Class C Subnet Characteristics

Consider the host address 192.168.10.50/27. The following steps flesh out the details of the subnet of which this address is a member:

1. Obtain the CIDR-notation prefix length for the address by converting the dotted-decimal mask to CIDR notation.

   In this case, /27 corresponds to a mask of 255.255.255.224. Practice converting between these notations until it becomes second nature.

2. Using the closest multiple of 8 that is greater than or equal to the prefix length, compute the interesting octet (the octet that increases from one subnet to the next in increments other than 1 or 0). Divide this multiple by 8. The result is a number corresponding to the octet that is interesting.

   In this case, the next multiple of 8 greater than 27 is 32. Dividing 32 by 8 produces the number 4, pointing to the fourth octet as the interesting one.

3. To compute the incremental value in the interesting octet, subtract the prefix length from the next higher multiple of 8, which in this case is 32. The result (32 – 27) is 5. Raise 2 to the computed value ($2^5 = 32$). The result is the incremental value of the interesting octet.

4. Recall the value of the interesting octet from the original address (50 in this case). Starting with 0, increment by the incremental value until the value is exceeded. The values then are 0, 32, 64, and so on.
5. The subnet in question extends from the increment that is immediately less than or equal to the address's interesting octet value to the address immediately before the next increment. In this example, 192.168.10.50/27 belongs to the subnet 192.168.10.32, and this subnet extends to the address immediately preceding 192.168.10.64, which is its broadcast address, 192.168.10.63.

   Note that if the interesting octet is not the fourth octet, all octets after the interesting octet must be set to 0 for the subnet address.
6. The usable range of addresses for the subnet in question extends from one higher than the subnet address to one less than the broadcast address, making the range for the subnet in question 192.168.10.33 through 192.168.10.62. As you can see, 192.168.10.50/27 definitely falls within the subnet 192.168.10.32/27.

Identifying Class B Subnet Characteristics

Using the steps in the previous section, find the subnet in which the address 172.16.76.12 with a mask of 255.255.240.0 belongs.

1. The corresponding CIDR notation prefix length is /20.
2. The next multiple of 8 that is greater than 20 is 24. $24 \times 8 = 3$. Octet 3 is interesting.
3. $24 - 20 = 4$, so the incremental value is $2^4 = 16$.
4. The increments in the third octet are 0, 16, 32, 48, 64, 80, and so on.
5. The increments of 64 and 80 bracket the address's third-octet value of 76, making the subnet in question 172.16.64.0, after setting all octets after the interesting octet to 0. This subnet's broadcast address is 172.16.79.255, which comes right before the next subnet address of 172.16.80.0.
6. The usable address range then extends from 172.16.64.1 through 172.16.79.254.

Identifying Class A Subnet Characteristics

Try it one more time with 10.6.127.255/14. Combine some of the related steps if possible:

1. The prefix length is 14. The next multiple of 8 that is greater than or equal to 14 is 16. $16 \times 8 = 2$, so the second octet is interesting.
2. $16 - 14 = 2$, so the incremental value in the second octet is $2^2 = 4$.
3. The corresponding second-octet value of 6 in the address falls between the 4 and 8 increments. This means that the subnet in question is 10.4.0.0 (setting octets after the second one to 0) and its broadcast address is 10.7.255.255.
4. The usable address range is from 10.4.0.1 through 10.7.255.254.

Determining Quantities of Subnets and Hosts

The general technique described in the previous section is also useful when trying to determine the total number of subnets and hosts produced by a given mask with respect to the default mask of the class of address in question.

For example, consider the Class B address 172.16.0.0 with a subnet mask of 255.255.254.0.

This is a prefix length of 23 bits. When you subtract the default prefix length for a Class B address of 16 from 23, you get the value 7. Raising 2 to the 7th power results in the value 128, which is the number of subnets you get when you subnet a Class B address with the 255.255.254.0 mask.

Determining the number of hosts available in each of these 128 subnets is simple because you always subtract the prefix length that the subnet mask produces, 23 in this example, from the value 32, which represents the total number of bits in any IP address. The difference, 9, represents the remaining number of 0s, or host bits, in the subnet mask. Raising 2 to this value produces the total possible number of host IDs per subnet that this subnet mask allows. Remember to subtract 2 from this result to account for the subnet and broadcast addresses for each subnet. This gives you the actual number of usable host IDs per subnet. In this case, this value is $2^9 - 2 = 510$.

Repeated practice with this technique will reduce your time to obtain the desired answer to mere seconds, leaving time for the more challenging tasks in each question. You have a wealth of examples and scenarios in this chapter, as well as in the review questions, on which to try your technique and build your trust in this faster method.

Supernetting

Let's take a look at a different type of subnetting. Class B addresses give you 65,534 addresses, but let's say that you have 1,000 users. Would you really need a Class B address? Not if you use supernetting.

Supernetting allows you to have two or more blocks of contiguous subnetwork addresses. So what does that actually mean? Class C addresses give you 254 useable addresses. So if you needed 1,000 users, you could set up supernetting of 4 Class C addresses that are contiguous.

Example:
192.168.16.0
192.168.17.0
192.168.18.0
192.168.19.0

When you set up supernetting for a Class C, you would use a Class B subnet mask. When you set up supernetting for a Class B, you would use a Class A subnet mask. This allows you to use multiple classes to get a larger number of hosts without taking up an entire class.

So the subnet mask for the above example would be 255.255.252.0 or /22. The reason we used this subnet mask is because a 252 subnet mask allows for 4 subnets. Each of the above Class C numbers would equal one subnet on this network.

Understanding IPv6

Internet Protocol version 6 (IPv6) is the first major revamping of IP since RFC 791 was accepted in 1981. Yes, the operation of IP has improved, and there have been a few bells and whistles added (such as NAT, for example), but the basic structure is still being used as it was originally intended. IPv6 has actually been available to use in Microsoft operating systems since NT 4.0, but it always had to be manually enabled. Windows Vista was the first Microsoft operating system to have it enabled by default. It is also enabled by default in Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 R2, and it probably will be in all Microsoft operating systems from this point on.

TCP and UDP—as well as the IP applications, such as HTTP, FTP, SNMP, and the rest—are still being used in IPv4. So, you might ask, why change to the new version? What does IPv6 bring to your networking infrastructure? What is the structure of an IPv6 address? How is it implemented and used within Windows Server 2012 R2? I'll answer all of those questions and more in the following sections.

IPv6 History and Need

In the late 1970s, as the IP specifications were being put together, the vision of the interconnected devices was limited compared to what we actually have today. To get an idea of the growth of the Internet, take a look at Hobbes' Internet Timeline in RFC 2235 (`www.faqs.org/rfcs/rfc2235.html`). As you can see, in 1984, the number of hosts finally surpassed 1,000—two years after TCP and IP were introduced. With 32 bits of addressing available in IPv4, it handled the 1,000+ hosts just fine. And even with the number of hosts breaking the 10,000 mark in 1987 and then 100,000 in 1989, there were still plenty of IP addresses to go around. But when the number of hosts exceeded 2 million in 1992 and 3 million in 1994, concern in the industry started to build. So in 1994, a working group was formed to come up with a solution to the quickly dwindling usable address availability in the IPv4 space. Internet Protocol next generation (IPng) was started.

Have you heard of IP address depletion being a problem today? Probably not as much. When the working group realized that it could not have IPv6 standardized before the available addresses might run out, they developed and standardized *Network Address Translation (NAT)* as an interim solution. NAT, or more specifically an implementation of NAT called *Port Address Translation (PAT)*, took care of a big portion of the problem.

NAT works very well, but it does have some limitations, including issues of peer-to-peer applications with their IPv4 addresses embedded in the data, issues of end-to-end traceability, and issues of overlapping addresses when two networks merge. Because all devices in an IPv6 network will have a unique address and no network address translation will take place, the global addressing concept of IPv4 will be brought back (the address put on by the source device will stay all the way to the destination). Thus, with the new-and-improved functionality of IPv6, the drawbacks of NAT and the limitations of IPv4 will be eliminated.

New and Improved IPv6 Concepts

Several elements of the IPv4 protocol could use some enhancements. Fortunately, IPv6 incorporates those enhancements as well as new features directly into the protocol specification to provide better and additional functionality.

The following list includes new concepts and new implementations of old concepts in IPv6:

- Larger address space (128-bit vs. 32-bit).
- Autoconfiguration of Internet-accessible addresses with or without DHCP. (Without DHCP, it's called *stateless autoconfiguration*.)
- More efficient IP header (fewer fields and no checksum).
- Fixed-length IP header (the IPv4 header is variable length) with extension headers beyond the standard fixed length to provide enhancements.
- Built-in IP mobility and security. (Although available in IPv4, the IPv6 implementation is a much better implementation.)
- Built-in transition schemes to allow integration of the IPv4 and IPv6 spaces.
- ARP broadcast messages replaced with multicast request.

Here are more details about these features:

128-Bit Address Space The new 128-bit address space will provide unique addresses for the foreseeable future. Although I would like to say that we will never use up all of the addresses, history may prove me wrong. The number of unique addresses in the IPv6 space is 2^{128}, or 3.4×10^{38}, addresses. How big is that number? It's enough for toasters and refrigerators (and maybe even cars) to all have their own addresses.

As a point of reference, the nearest black hole to Earth is 1,600 light years away. If you were to stack 4mm BB pellets from here to the nearest black hole and back, you would need 1.51×10^{22} BBs. This means you could uniquely address each BB from Earth to the black hole and back and still have quite a few addresses left over.

Another way to look at it is that the IPv6 address space is big enough to provide more than 1 million addresses per square inch of the surface area of the earth (oceans included).

Autoconfiguration and Stateless Autoconfiguration Autoconfiguration is another added/improved feature of IPv6. We've used DHCP for a while to assign IP addresses to client machines. You should even remember that APIPA can be used to assign addresses automatically to Microsoft DHCP client machines in the absence of a DHCP server. The problem with APIPA is that it confines communication between machines to a local LAN (no default gateway). What if a client machine could ask whether there was a router on the LAN and what network it was on? If the client machine knew that, it could not only assign itself an address, it could also choose the appropriate network and default gateway. The stateless autoconfiguration functionality of IPv6 allows the clients to do this.

Improved IPv6 Header The IPv6 header is more efficient than the IPv4 header because it is fixed length (with extensions possible) and has only a few fields. The IPv6 header consists of a total of 40 bytes:

32 bytes Source and destination IPv6 addresses

8 bytes Version field, traffic class field, flow label field, payload length field, next header field, and hop limit field

You don't have to waste your time with a checksum validation anymore, and you don't have to include the length of the IP header (it's fixed in IPv6; the IP header is variable length in IPv4, so the length must be included as a field).

IPv6 Mobility IPv6 is only a replacement of the OSI layer 3 component, so you'll continue to use the TCP (and UDP) components as they currently exist. IPv6 addresses a TCP issue, though. Specifically, TCP is connection oriented, meaning that you establish an end-to-end communication path with sequencing and acknowledgments before you ever send any data, and then you have to acknowledge all of the pieces of data sent. You do this through a combination of an IP address, port number, and port type (socket).

If the source IP address changes, the TCP connection may be disrupted. But then how often does this happen? Well, it happens more and more often because more people are walking around with a wireless laptop or a wireless Voice over IP (VoIP) telephone. IPv6 mobility establishes a TCP connection with a home address and, when changing networks, it continues to communicate with the original endpoint from a care-of address as it changes LANs, which sends all traffic back through the home address. The handing off of network addresses does not disrupt the TCP connection state (the original TCP port number and address remain intact).

Improved Security Unlike IPv4, IPv6 has security built in. *Internet Protocol Security (IPsec)* is a component used today to authenticate and encrypt secure tunnels from a source to a destination. This can be from the client to the server or between gateways. IPv4 lets you do this by enhancing IP header functionality (basically adding a second IP header while encrypting everything behind it). In IPv6, you add this as standard functionality by using extension headers. Extension headers are inserted into the packet only if they are needed. Each header has a "next header" field, which identifies the next piece of information. The extension headers currently identified for IPv6 are Hop-By-Hop Options, Routing, Fragment, Destination Options, Authentication, and Encapsulating Security Payload. The Authentication header and the Encapsulating Security Payload header are the IPsec-specific control headers.

IPv4 to IPv6 Interoperability Several mechanisms in IPv6 make the IPv4-to-IPv6 transition easy.

- A simple dual-stack implementation where both IPv4 and IPv6 are installed and used is certainly an option. In most situations (so far), this doesn't work so well because most of us aren't connected to an IPv6 network and our Internet connection is not IPv6 even if we're using IPv6 internally. Therefore, Microsoft includes other mechanisms that can be used in several different circumstances.
- *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)* is an automatic tunneling mechanism used to connect an IPv6 network to an IPv4 address space (not using NAT). ISATAP treats the IPv4 space as one big logical link connection space.

- *6to4* is a mechanism used to transition to IPv4. This method, like ISATAP, treats the IPv4 address space as a logical link layer with each IPv6 space in transition using a 6to4 router to create endpoints using the IPv4 space as a point-to-point connection (kind of like a WAN, eh?). 6to4 implementations still do not work well through a NAT, although a 6to4 implementation using an Application layer gateway (ALG) is certainly doable.
- *Teredo* is a mechanism that allows users behind a NAT to access the IPv6 space by tunneling IPv6 packets in UDP.

Pseudo-interfaces are used in these mechanisms to create a usable interface for the operating system. Another interesting feature of IPv6 is that addresses are assigned to interfaces (or pseudo-interfaces), not simply to the end node. Your Windows Server 2012 R2 will have several unique IPv6 addresses assigned.

New Broadcast Methods IPv6 has moved away from using broadcasting. The three types of packets used in IPv6 are unicast, multicast, and anycast. IPv6 clients then must use one of these types to get the MAC address of the next Ethernet hop (default gateway). IPv6 makes use of multicasting for this along with the new functionality called *neighbor discovery*. Not only does ARP utilize new functionality, but ICMP (also a layer 3 protocol) has been redone and is now known as ICMP6. *ICMP6* is used for messaging (packet too large, time exceeded, and so on) as it was in IPv4, but now it's also used for the messaging of IPv6 mobility. ICMP6 echo request and ICMP6 echo reply are still used for ping.

IPv6 Addressing Concepts

You need to consider several concepts when using IPv6 addressing. For starters, the format of the address has changed. Three types of addresses are used in IPv6 with some predefined values within the address space. You need to get used to seeing these addresses and be able to identify their uses.

IPv6 Address Format

For the design of IPv4 addresses, you present addresses as octets or the decimal (base 10) representation of 8 bits. Four octets add up to the 32 bits required. IPv6 expands the address space to 128 bits, and the representation is for the most part shown in hexadecimal (a notation used to represent 8 bits using the values 0–9 and A–F). Figure 8.13 compares IPv4 to IPv6.

A full IPv6 address looks like this example:

2001:0DB8:0000:0000:1234:0000:A9FE:133E

You can tell the implementation of DNS will make life a lot easier even for those who like to ping the address in lieu of the name. Fortunately, DNS already has the ability to handle IPv6 addresses with the use of an AAAA record. (*A* is short for *alias*.) An A record in IPv4's addressing space is 32 bits, so an AAAA record, or four *A*s, is 128 bits. The Windows Server 2012 R2 DNS server handles the AAAA and the reverse pointer (PTR) records for IPv6.

FIGURE 8.13 IPv4/IPv6 comparison

IPv6 Address Shortcuts

There are several shortcuts for writing an IPv6 address. These are described in the following list:

- :0: stands for :0000:.
- You can omit preceding 0s in any 16-bit word. For example, :DB8: and :0DB8: are equivalent.
- :: is a variable standing for enough zeros to round out the address to 128 bits. :: can be used only once in an address.

You can use these shortcuts to represent the example address 2001:0DB8:0000:0000:1234:0000:A9FE:133E, as shown here:

- Compress :0000: into :0::

  2001:0DB8:0000:0000:1234:0:A9FE:133E

- Eliminate preceding zeros:

  2001:DB8:0000:0000:1234:0:A9FE:133E

- Use the special variable shortcut for multiple 0s:

  2001:DB8::1234:0:A9FE:133E

You now also use prefix notation or slash notation when discussing IPv6 networks. For example, the network of the previous address can be represented as 2001:DB8:0000:0000:0000:0000:0000:0000. This can also be expressed as 2001:DB8:: /32. The /32 indicates 32 bits of network, and 2001:DB8: is 32 bits of network.

IPv6 Address Assignment

So, do you subnet IPv6? The answer depends on your definition of subnetting. If you are given 32 bits of network from your ISP, you have 96 bits with which to work. If you use some of the 96 bits to route within your network infrastructure, then you are subnetting. In this context, you do subnet IPv6. However, given the huge number of bits you have available, you will no longer need to implement VLSM. For example, Microsoft has a network space of 2001:4898:: /32. That gives the administrators a space of 96 bits (2^{96} = 79,228,162,514,264,337,593,543,950,336 unique addresses using all 96 bits) with which to work.

You can let Windows Server 2012 R2 dynamically/automatically assign its IPv6 address, or you can still assign it manually (see Figure 8.14). With dynamic/automatic assignment, the IPv6 address is assigned either by a DHCPv6 server or by the Windows Server 2012 R2 machine. If no DHCPv6 server is configured, the Windows Server 2012 R2 machine can query the local LAN segment to find a router with a configured IPv6 interface. If so, the server will assign itself an address on the same IPv6 network as the router interface and set its default gateway to the router interface's IPv6 address. Figure 8.14 shows that you have the same dynamic and manual choices as you do in IPv4; however, the input values for IPv6 must conform to the new format.

FIGURE 8.14 TCP/IPv6 Properties window

To see your configured IP addresses (IPv4 and IPv6), you can still use the `ipconfig` command. For example, I have configured a static IPv4 address and an IPv6 address on my server. The IPv6 address is the same as the one used in the earlier IPv6 example address. Figure 8.15 shows the result of this command on Windows Server 2012 R2 for my server.

FIGURE 8.15 IPv6 configuration as seen from the command prompt

```
Administrator: C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel 21140-Based PCI Fast Ethernet Adapt
er (Emulated)
   Physical Address. . . . . . . . . : 00-03-FF-11-02-CD
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8::1234:0:a9fe:133e(Preferred)
   Link-local IPv6 Address . . . . . : fe80::a425:ab9d:7da4:ccba%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.200(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 2001:db8::1234:0:0:1
                                       0.0.0.0
                                       192.168.1.1
   DNS Servers . . . . . . . . . . . : ::1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

IPv6 Address Types

As stated earlier, there are three types of addresses in IPv6: anycast, unicast, and multicast. A description of each of these types of IPv6 addresses follows.

Note the absence of the broadcast type, which is included in IPv4. You can't use broadcasts in IPv6; they've been replaced with multicasts.

Anycast Addresses Anycast addresses are not really new. The concept of anycast existed in IPv4 but was not widely used. An *anycast address* is an IPv6 address assigned to multiple devices (usually different devices). When an anycast packet is sent, it is delivered to one of the devices, usually the closest one.

Unicast Addresses A *unicast packet* uniquely identifies an interface of an IPv6 device. The interface can be a virtual or pseudo-interface or a real (physical) interface.

Unicast addresses come in several types, as described in the following list:

Global Unicast Address As of this writing, the global unicast address space is defined as 2000:: /3. The 2001::/32 networks are the IPv6 addresses currently being issued to business entities. As mentioned, Microsoft has been allocated 2001:4898:: /32. A Microsoft DHCPv6 server would be set up with scopes (ranges of addresses to be assigned) within this address space. There are some special addresses and address formats that you will see in use as well. You'll find most example addresses listed as 2001:DB8:: /32; this space has been reserved for documentation. Do you remember the loopback address in IPv4, 127.0.0.1? In IPv6 the loopback address is ::1 (or 0:0:0:0:0:0:0:0001). You may also see an address with dotted-decimal used. A dual-stack Windows Server 2012 machine may also show you FE80::5EFE:192.168.1.200. This address form is used in an integration/migration model of IPv6 (or if you just can't leave the dotted-decimal era, I suppose).

Link-Local Address Link-local addresses are defined as FE80:: /10. If you refer to Figure 8.15 showing the `ipconfig` command, you will see the link-local IPv6 address as fe80::a425:ab9d:7da4:ccba. The last 8 bytes (64 bits) are random to ensure a high

probability of randomness for the link-local address. The link-local address is to be used on a single link (network segment) and should never be routed.

There is another form of the local-link IPv6 address called the *Extended User Interface 64-bit (EUI-64)* format. This is derived by using the MAC address of the physical interface and inserting an FFFE between the third and fourth bytes of the MAC. The first byte is also made 02 (this sets the universal/local or U/L bit to 1 as defined in IEEE 802 frame specification). Again looking at Figure 8.15, the EUI-64 address would take the physical (MAC) address 00-03-FF-11-02-CD and make the link-local IPv6 address FE80::0203:FFFF:FE11:02CD. (I've left the preceding zeros in the link-local IPv6 address to make it easier for you to pick out the MAC address with the FFFE inserted.)

AnonymousAddress Microsoft Server 2012 R2 uses the random address by default instead of EUI-64. The random value is called the *AnonymousAddress* in Microsoft Server 2012 R2. It can be modified to allow the use of EUI-64.

Unique Local Address The *unique local address* can be Fc00 or FD00, and it is used like the private address space of IPv4. RFC 4193 describes unique local addresses. They are not expected to be routable on the global Internet. They are used for private routing within an organization.

Multicast Address *Multicast addresses* are one-to-many communication packets. Multicast packets are identifiable by their first byte (most significant byte, leftmost byte, leftmost 2 nibbles, leftmost 8 bits, and so on). A multicast address is defined as FF00::/8.

In the second byte shown (the 00 of FF00), the second 0 is what's called the *scope*. Interface-local is 01, and link-local is 02. FF01:: is an interface-local multicast.

There are several well-known (already defined) multicast addresses. For example, if you want to send a packet to all nodes in the link-local scope, you send the packet to FF02::1 (also shown as FF02:0:0:0:0:0:0:1). The all-routers multicast address is FF02::2.

You can also use multicasting to get the logical link layer address (MAC address) of a device with which you are trying to communicate. Instead of using the ARP mechanism of IPv4, IPv6 uses the ICMPv6 neighbor solicitation (NS) and neighbor advertisement (NA) messages. The NS and NA ICMPv6 messages are all part of the new *Neighbor Discovery Protocol (NDP)*. This new ICMPv6 functionality also includes router solicitation and router advertisements as well as redirect messages (similar to the IPv4 redirect functionality). Table 8.7 outlines the IPv6 address space known prefixes and some well-known addresses.

Unicast vs. Anycast

Unicast and anycast addresses look the same and may be indistinguishable from each other; it just depends on how many devices have the same address. If only one device has a globally unique IPv6 address, it's a unicast address. If more than one device has the same address, it's an anycast address. Both unicast and anycast are considered one-to-one communication, although you could say that anycast is one-to-"one of many."

TABLE 8.7 IPv6 address space known prefixes and addresses

Address Prefix	Scope of Use
2000:: /3	Global unicast space prefix
FE80:: /10	Link-local address prefix
FC00:: /7	Unique local unicast prefix
FD00:: /8	Unique local unicast prefix
FF00:: /8	Multicast prefix
2001:DB8:: /32	Global unicast prefix used for documentation
::1	Reserved local loopback address
2001:0000: /32	Teredo prefix (discussed later in this chapter)
2002:: /16	6to4 prefix

IPv6 Integration/Migration

It's time to get into the mind-set of integrating IPv6 into your existing infrastructure with the longer goal of migrating to IPv6. In other words, this is not going to be an "OK, Friday the Internet is changing over" rollout. You have to bring about the change as a controlled implementation. It could easily take three to five years before a solid migration occurs and probably longer. I think the migration will take slightly less time than getting the world to migrate to the metric system on the overall timeline. The process of integration/migration consists of several mechanisms.

Dual Stack Simply running both IPv4 and IPv6 on the same network, utilizing the IPv4 address space for devices using only IPv4 addresses and utilizing the IPv6 address space for devices using IPv6 addresses

Tunneling Using an encapsulation scheme for transporting one address space inside another

Address Translation Using a higher-level application to change one address type (IPv4 or IPv6) to the other transparently so that end devices are unaware one address space is talking to another

I elaborate on these three mechanisms in the following sections.

IPv6 Dual Stack

The default implementation in Windows Server 2012 R2 is an enabled IPv6 configuration along with IPv4; this is dual stack. The implementation can be dual IP layer or dual TCP/IP stack. Windows Server 2012 R2 uses the dual IP layer implementation (see Figure 8.16). When an application queries a DNS server to resolve a hostname to an IP address, the DNS server may respond with an IPv4 address or an IPv6 address. If the DNS server responds with both, Windows Server 2012 R2 will prefer the IPv6 address. Windows Server 2012 R2 can use both IPv4 and IPv6 addresses as necessary for network communication. When looking at the output of the `ipconfig` command, you will see both address spaces displayed.

FIGURE 8.16 IPv6 dual IP layer diagram

IPv6 Tunneling

Windows Server 2012 R2 includes several tunneling mechanisms for tunneling IPv6 through the IPv4 address space. They include the following:

- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), which is used for unicast IPv6 communication across an IPv4 infrastructure. ISATAP is enabled by default in Windows Server 2012 R2.
- 6to4, which is used for unicast IPv6 communication across an IPv4 infrastructure.
- Teredo, which is used for unicast IPv6 communication with an IPv4 NAT implementation across an IPv4 infrastructure.

With multiple tunneling protocols available and enabled by default, you might ask, what's the difference, and why is one used over the others? They all allow you to tunnel IPv6 packets through the IPv4 address space (a really cool thing if you're trying to integrate/migrate). Here are the details of these tunneling mechanisms:

ISATAP *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)* is the automatic tunnel addressing protocol providing IPv6 addresses based on the IPv4 address of the end interface (node). The IPv6 address is automatically configured on the local device, and the

dual stack machine can use either its IPv4 or IPv6 address to communicate on the local network (within the local network infrastructure). ISATAP can use the neighbor discovery mechanism to determine the router ID and network prefix where the device is located, thus making intrasite communication possible even in a routed infrastructure.

The format of an ISATAP address is as follows:

[64bits of prefix] [32bits indicating ISATAP] [32bits IPv4 Address]

The center 32 bits indicating ISATAP are actually 0000:5EFE (when using private IPv4 addresses). The ISATAP address of the example Windows Server 2012 R2 machine using the link-local IPv6 address is FE80::5EFE:192.168.1.200. Each node participating in the ISATAP infrastructure must support ISATAP. If you're routing through an IPv4 cloud, a border router (a router transitioning from an IPv6 to IPv4 space) must support ISATAP. Windows Server 2012 R2 can be configured as a border router, and it will forward ISATAP packets. ISATAP is experimental and is defined in RFC 4214.

6to4 *6to4* specifies a procedure for IPv6 networks to communicate with each other through an IPv4 space without the IPv6 nodes having to know what's happening. The IPv6 nodes do not need to be dual stacked to make this happen. The border router is the device responsible for knowing about the IPv6-to-IPv4 transition. The IPv6 packets are encapsulated at the border router (and decapsulated at the other end or on the way back). There is an assigned prefix for the 6to4 implementation: 2002:: /16. 6to4 is defined in RFC 3056.

Teredo *Teredo* (named after a kind of shipworm that drills holes in the wood of ships) is a protocol designed to allow IPv6 addresses to be available to hosts through one or more layers of NAT. Teredo uses a process of tunneling packets through the IPv4 space using UDP. The Teredo service encapsulates the IPv6 data within a UDP segment (packet) and uses IPv4 addressing to get through the IPv4 cloud. Having a layer 4 (Transport layer) available to use as translation functionality is what gives you the ability to be behind a NAT. Teredo provides host-to-host communication and dynamic addressing for IPv6 nodes (dual stack), allowing the nodes to have access to resources in an IPv6 network and the IPv6 devices to have access to the IPv6 devices that have only connectivity to the IPv4 space (like home users who have an IPv6-enabled operating system connecting to IPv6 resources while their home ISP has only IPv4 capabilities). Teredo is defined in RFC 4380.

In Windows Server 2012 R2, an IPv4 Teredo server is identified and configured (using the `netsh` command interface). The Teredo server provides connectivity resources (address) to the Teredo client (the node that has access to the IPv4 Internet and needs access to an IPv6 network/Internet). A Teredo relay is a component used by the IPv6 router to receive traffic destined for Teredo clients and forward the traffic appropriately. The defined prefix for Teredo address is 2001:0000:: /32. Teredo does add overhead like all the other implementations discussed. It is generally accepted that you should use the simplest model available. However, in the process of integration/migration for most of us behind a NAT, Teredo will be the process to choose.

From Windows Server 2012 R2, use the `ipconfig /all` command to view the default configurations including IPv4 and IPv6. You may notice a notation that I didn't discuss, the

percent sign at the end of the IPv6 address (see Figure 8.17). The number after the percent sign is the virtual interface identifier used by Windows Server 2012 R2.

FIGURE 8.17 IPv6 interface identifier for `ipconfig` display

```
Link-local IPv6 Address . . . . . : fe80::a425:ab9d:7da4:ccba%10
```

Useful IPv6 Information Commands

You can use numerous commands to view, verify, and configure the network parameters of Windows Server 2012 R2. Specifically, you can use the `netsh` command set and the `route` command set as well as the standard `ping` and `tracert` functions.

Use the `netsh` command interface (as well as the provided dialog boxes, if you want) to examine and configure IPv6 functionality. The `netsh` command issued from the command interpreter changes into a network shell (`netsh`) where you can configure and view both IPv4 and IPv6 components.

Don't forget to use the ever-popular `route print` command to see the Windows Server 2012 R2 routing tables (IPv4 and IPv6). The other diagnostic commands are still available for IPv4 as well as IPv6. In previous versions of Microsoft operating systems, `ping` was the IPv4 command, and `ping6` was the IPv6 command. This has changed in Windows Server 2012 R2; `ping` works for both IPv4 and IPv6 to test layer 3 connectivity to remote devices. The IPv4 `tracert` command was `tracert6` for IPv6. The command is now `tracert` for both IPv4 and IPv6, and it will show you every layer 3 (IP) hop from source to destination. (This assumes that all of the administrators from here to there want you to see the hops and are not blocking ICMP. It also assumes that there are no IP tunnels, which your packets are traversing; you won't see the router hops in the tunnel either.)

Overall, the consortium of people developing the Internet and the Internet Protocol have tried to make all of the changes to communication infrastructures easy to implement. (This is a daunting task with the many vendors and various infrastructures currently in place.) The goal is not to daze and confuse administrators; it's designed to provide maximum flexibility with the greatest functionality. IPv6 is going to provide the needed layer 3 (Network layer, global addressing layer, logical addressing layer…call it what you like) functionality for the foreseeable future.

Subnetting with IPv6

Subnetting with IPv6 is a lot like subnetting with IPv4. You need to know how many bits you are going to use for the network mask to subnet it correctly.

For example, let's say you have an IPv6 prefix of 2001:DB8:BBCC:0000::/53 and you need to set up your network so that your IPv6 addressing scheme can handle 1,500 more subnets. How would you figure this out?

When determining any number of hosts or subnets, the calculation is 2 to the power (2^x). The first power number that is greater than or equal to the number you need is the power number that you add to the current network mask. Thus, in the previous question, to get

to 1,500 subnets, you would need to determine which 2^x is the first one that is greater than or equal to 1,500. If you calculate your powers correctly, 2^{11} (2^{11} = 2,048) is the first one that is greater than or equal to 1,500. So, you would add the power of 11 to the /53 in the previous address, and you would now use /64 as your network mask. Table 8.8 shows you some of the power numbers for the power of 2.

TABLE 8.8 Powers of 2

Power	Equals
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128
2^8	256
2^9	512
2^{10}	1024
2^{11}	2048
2^{12}	4096

Summary

Why TCP/IP is the primary protocol in use today is one of the important topics covered in this chapter. You also learned that the 32-bit IPv4 address is a structured and hierarchical one that is used to identify uniquely every machine on a network. You learned how to determine available IP addresses and implement subnetting. In addition, you learned how the new layer 3 IPv6 protocol is implemented, including the structure of the IPv6 address. Finally, I discussed the new functionality included in IPv6 addressing as well as several Windows Server 2012 R2 integration/migration implementations.

Exam Essentials

Understand what subnetting is and when to use it. If an organization is large and has many computers or if its computers are geographically dispersed, it's sensible to divide its large network into smaller ones connected by routers. These smaller networks are called *subnets*. Subnetting is the process of carving a single IP network into smaller, logical subnetworks.

Understand subnet masks. For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. The network administrator creates a 32-bit subnet mask consisting of 1s and 0s. The 1s in the subnet mask represent the positions that refer to the network or subnet addresses. The 0s represent the positions that refer to the host portion of the address.

Understand IPv6. Understand the structure of an IPv6 address and how it's displayed. Know the shortcuts and rules (such as for displaying 0s) for writing IPv6 addresses. Know the integration/migration components for IPv6 included in Windows Server 2012 R2, including tunneling and dual stack.

Review Questions

1. You are the network administrator for ABC Company. You have an IPv6 prefix of 2001:DB8:BBCC:0000::/53, and you need to set up your network so that your IPv6 addressing scheme can handle 1,000 more subnets. Which network mask would you use?
   - **A.** /60
   - **B.** /61
   - **C.** /62
   - **D.** /63
   - **E.** /64

2. You are the network administrator for Stellacon Corporation. Stellacon has a Windows Server 2012 R2 machine that needs to be able to communicate with all of the computers on the internal network. Stellacon has decided to add 15 new segments to its IPv6 network. How would you configure the IPv6 address so that the server can communicate with all the segments?
   - **A.** Configure the IPv6 address as fd00::2b0:e0ff:dee9:4143/8.
   - **B.** Configure the IPv6 address as fe80::2b0:e0ff:dee9:4143/32.
   - **C.** Configure the IPv6 address as ff80::2b0:e0ff:dee9:4143/64.
   - **D.** Configure the IPv6 address as fe80::2b0:e0ff:dee9:4143/64.

3. You are the network administrator for a midsize organization that has installed Windows Server 2012 R2 onto the network. You are thinking of moving all machines to Windows 8 and IPv6. You decide to set up a test environment with four subnets. What type of IPv6 addresses do you need set up?
   - **A.** Global addresses
   - **B.** Link-local addresses
   - **C.** Unique local addresses
   - **D.** Site-local addresses

4. You have a large IP-routed network using the address 137.25.0.0; it is composed of 20 subnets, with a maximum of 300 hosts on each subnet. Your company continues on a merger-and-acquisitions spree, and your manager has told you to prepare for an increase to 50 subnets with some containing more than 600 hosts. Using the existing network address, which of the following subnet masks would work for the requirement set by your manager?
   - **A.** 255.255.252.0
   - **B.** 255.255.254.0
   - **C.** 255.255.248.0
   - **D.** 255.255.240.0

5. Your company is growing dramatically via acquisitions of other companies. As the network administrator, you need to keep up with the changes because they affect the workstations, and you need to support them. When you started, there were 15 locations connected via routers, and now there are 25. As new companies are acquired, they are migrated to Windows Server 2012 R2 and brought into the same domain as another site. Management says that they are going to acquire at least 10 more companies in the next two years. The engineers have also told you that they are redesigning the company's Class B address into an IP addressing scheme that will support these requirements and that there will never be more than 1,000 network devices on any subnet. What is the appropriate subnet mask to support this network when the changes are completed?

   A. 255.255.252.0

   B. 255.255.248.0

   C. 255.255.255.0

   D. 255.255.255.128

6. You work for a small printing company that has 75 workstations. Most of them run standard office applications such as word processing, spreadsheet, and accounting programs. Fifteen of the workstations are constantly processing huge graphics files and then sending print jobs to industrial-sized laser printers. The performance of the network has always been an issue, but you have never addressed it. You have now migrated your network to Windows 8 and Windows Server 2012 R2 and have decided to take advantage of the routing capability built into Windows Server 2012 R2. You choose the appropriate server and place two NICs in the machine, but you realize that you have only one network address, 201.102.34.0, which you obtained years ago. How should you subnet this address to segment the bandwidth hogs from the rest of the network while giving everyone access to the entire network?

   A. 255.255.255.192

   B. 255.255.255.224

   C. 255.255.255.252

   D. 255.255.255.240

7. You work for Carpathian Worldwide Enterprises, which has more than 50 administrative and manufacturing locations around the world. The size of these organizations varies greatly, with the number of computers per location ranging from 15 to slightly fewer than 1,000. The sales operations use more than 1,000 facilities, each of which contains 2 to 5 computers. Carpathian is also in merger talks with another large organization. If the merger materializes as planned, you will have to accommodate another 100 manufacturing and administrative locations, each with a maximum of 600 computers, as well as 2,000 additional sales facilities. You don't have any numbers for the future growth of the company, but you are told to keep growth in mind. You decide to implement a private addressing plan for the entire organization. More than half of your routers don't support variable-length subnet masking. Which subnet masks would work for this situation? (Choose all that apply.)

   A. 255.255.224.0

   B. 255.255.240.0

   C. 255.255.248.0

   D. 255.255.252.0

   E. 255.255.254.0

8. Which of the following subnet masks are represented with the CIDR of /27?

A. 255.255.255.254

B. 255.255.255.248

C. 255.255.255.224

D. 255.255.255.240

9. You are the administrator for a Windows Server 2012 R2 network that uses DHCP. You notice that your DHCP database is getting too large, and you want to reduce the size of the database. What should you do?

A. From the folder containing the DHCP database, run `jetpack.exe dhcp.mdb temp.mdb`.

B. From the folder containing the DHCP database, run `shrinkpack.exe dhcp.mdb temp.mdb`.

C. From the folder containing the DHCP database, run `jetshrink.exe dhcp.mdb temp.mdb`.

D. From the folder containing the DHCP database, run `shrinkjet.exe dhcp.mdb temp.mdb`.

10. You ask one of your technicians to get the IPv6 address of a new Windows Server 2012 R2 machine, and she hands you a note with FE80::0203:FFFF:FE11:2CD on it. What can you tell from this address? (Choose two.)

A. This is a globally unique IPv6 address.

B. This is a link-local IPv6 address.

C. This is a multicast IPv6 address.

D. In EUI-64 format, you can see the MAC address of the node.

E. In EUI-64 format, you can see the IPv4 address of the node.

Chapter

9

Use Virtualization in Windows Server 2012

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Create and configure virtual machine settings**

- Configure dynamic memory
- Configure smart paging
- Configure Resource Metering
- Configure guest integration services
- Create and configure Generation 1 and 2 virtual machines
- Configure and use extended session mode
- Configure remoteFX

✓ **Create and configure virtual machine storage**

- Create VHDs and VHDX
- Configure differencing drives
- Modify VHDs
- Configure pass-through disks
- Manage checkpoints
- Implement a virtual Fibre Channel adapter
- Configure storage Quality of Service

✓ **Create and configure virtual networks**

- Configure Hyper-V virtual switches
- Optimize network performance
- Configure MAC addresses
- Configure network isolation
- Configure synthetic and legacy virtual network adapters
- Configure NIC teaming in virtual machines

Hyper-V is a server role in Windows Server 2012 R2 that allows you to virtualize your environment and therefore run multiple virtual operating system instances simultaneously on a physical server. This not only helps you to improve server utilization but also helps you to create a more cost-effective and dynamic system.

In this chapter, you will learn the basic concepts and features of Hyper-V that a Windows Server 2012 R2 technical specialist must know. You will also get a solid understanding of what is important in virtualization and in what areas of your work life you can use it.

Hyper-V Overview

In the following sections, I'll introduce you to Hyper-V. To begin, you'll take a look at virtualization and what types of virtualization exist. I will then discuss Hyper-V features and the Hyper-V architecture before finishing up with the Hyper-V requirements for software and hardware.

What Is Virtualization?

Virtualization is a method for abstracting physical resources from the way that they interact with other resources. For example, if you abstract the physical hardware from the operating system, you get the benefit of being able to move the operating system between different physical systems.

This is called *server virtualization*. But there are also other forms of virtualization available, such as presentation virtualization, desktop virtualization, and application virtualization. I will now briefly explain the differences between these forms of virtualization:

Server Virtualization This basically enables multiple servers to run on the same physical server. Hyper-V is a server virtualization tool that allows you to move physical machines to virtual machines and manage them on a few physical servers. Thus, you will be able to consolidate physical servers.

Presentation Virtualization When you use *presentation virtualization*, your applications run on a different computer, and only the screen information is transferred to your computer. An example of presentation virtualization is Microsoft Remote Desktop Services in Windows Server 2012 R2.

Desktop Virtualization *Desktop virtualization* provides you with a virtual machine on your desktop, comparable to server virtualization. You run your complete operating system and applications in a virtual machine so that your local physical machine just needs to run a very basic operating system. An example of this form of virtualization is Microsoft Virtual PC.

Application Virtualization *Application virtualization* helps prevent conflicts between applications on the same PC. Thus, it helps you to isolate the application running environment from the operating system installation requirements by creating application-specific copies of all shared resources. It also helps reduce application-to-application incompatibility and testing needs. An example of an application virtualization tool is Microsoft Application Virtualization (App-V).

Hyper-V Features

As a lead-in to the virtualization topic and Hyper-V, I will start with a list of key features, followed by a list of supported guest operating systems. This should provide you with a quick, high-level view of this feature before you dig deeper into the technology.

Key Features of Hyper-V

The following are the key features of Hyper-V:

New Architecture The hypervisor-based architecture, which has a 64-bit micro-kernel, provides a new array of device support as well as performance and security improvements.

Operating System Support Both 32-bit and 64-bit operating systems can run simultaneously in Hyper-V. Also, different platforms like Windows, Linux, and others are supported.

Support for Symmetric Multiprocessors Support for up to 64 processors in a virtual machine environment provides you with the ability to run applications as well as multiple virtual machines faster.

Network Load Balancing Hyper-V provides support for *Windows Network Load Balancing (NLB)* to balance the network load across virtual machines on different servers.

New Hardware Architecture Hyper-V's new architecture provides improved utilization of resources such as networking and disks.

Quick Migration Hyper-V's *quick migration* feature provides you with the functionality to run virtual machines in a clustered environment with switchover capabilities when there is a failure. Thus, you can reduce downtime and achieve higher availability of your virtual machines.

Virtual Machine Snapshot You can take snapshots of running virtual machines, which provides you with the capability to recover to any previous virtual machine snapshot state quickly and easily.

Resource Metering Hyper-V *resource metering* allows an organization to track usage within the businesses departments. It allows an organization to create a usage-based billing solution that adjusts to the provider's business model and strategy.

Scripting Using the Windows Management Instrumentation (WMI) interfaces and APIs, you can easily build custom scripts to automate processes in your virtual machines.

RemoteFX Windows Server 2012 R2 Hyper-V RemoteFX allows for an enhanced user experience for RemoteFX desktops by providing a 3D virtual adapter, intelligent codecs, and the ability to redirect USB devices in virtual machines.

Fibre Channel The virtual Fibre Channel feature allows you to connect to the Fibre Channel storage unit from within the virtual machine. *Virtual Fibre Channel* allows an administrator to use their existing Fibre Channel to support virtualized workloads. Hyper-V users have the ability to use Fibre Channel storage area networks (SANs) to virtualize the workloads that require direct access to SAN logical unit numbers (LUNs).

Enhanced Session Mode *Enhanced Session Mode* enhances the interactive session of the Virtual Machine Connection for Hyper-V administrators who want to connect to their virtual machines. It gives administrators the same functionality as a remote desktop connection when the administrator is interacting with a virtual machine.

In previous versions of Hyper-V, the virtual machine connection gave you limited functionality while you connected to the virtual machine screen, keyboard, and mouse. An administrator could use an RDP connection to get full redirection abilities, but that would require a network connection to the virtual machine host.

Enhanced Session Mode gives administrators the following benefits for local resource redirection:

- Display configuration
- Audio
- Printers
- Clipboard
- Smart cards
- Drives
- USB devices
- Supported Plug and Play devices

Shared Virtual Hard Disk Windows Server 2012 R2 Hyper-V has a new feature called Shared Virtual Hard Disk. *Shared Virtual Hard Disk* allows an administrator to cluster virtual machines by using shared virtual hard disk (VHDX) files.

Shared virtual hard disks allow an administrator to build a high availability infrastructure, which is important if you are setting up either a private cloud deployment or a cloud-hosted environment for managing large workloads. Shared virtual hard disks allow two or more virtual machines to access the same virtual hard disk (VHDX) file.

Automatic Virtual Machine Activation (AVMA) *Automatic Virtual Machine Activation (AVMA)* is a new feature that allows administrators to install virtual machines on a properly activated Windows Server 2012 R2 system without the need to manage individual

product keys for each virtual machine. When using AVMA, virtual machines get bound to the licensed Hyper-V server as soon as the virtual machine starts.

Network Isolation One nice feature of using Microsoft Hyper-V network virtualization is the ability of Hyper-V to keep virtual networks isolated from the physical network infrastructure of the hosted system. Because administrators can set up Hyper-V software–defined virtualization policies, you are no longer limited by the IP address assignment or VLAN isolation requirements of the physical network. Hyper-V allows for built-in network isolation to keep the virtual network separated from the virtual network.

Dynamic Memory *Dynamic Memory* is a feature of Hyper-V that allows it to balance memory automatically among running virtual machines. Dynamic Memory allows Hyper-V to adjust the amount of memory available to the virtual machines in response to the needs of the virtual machines. It is currently available for Hyper-V in Windows Server 2012 R2.

Supported Guest Operating Systems

The following guest operating systems have been successfully tested on Hyper-V and are hypervisor-aware. Table 9.1 shows all of the guest server operating systems and the maximum number of virtual processors. Table 9.2 shows all of the guest client operating systems and the maximum number of virtual processors.

TABLE 9.1 Hyper-V guest server operating systems

Guest Operating System (Server)	Maximum Number of Virtual Processors
Windows Server 2012 and Server 2012 R2	64
Windows Server 2008 R2 with Service Pack 1 (SP1)	64
Windows Server 2008 R2	64
Windows Server 2008 with Service Pack 2 (SP2)	8
Windows Home Server 2011	4
Windows Small Business Server 2011	Essentials edition: 2 Standard edition: 4
Windows Server 2003 R2 with Service Pack 2 (SP2)	2
Windows Server 2003 with Service Pack 2 (SP2)	2

TABLE 9.1 Hyper-V guest server operating systems *(continued)*

Guest Operating System (Server)	Maximum Number of Virtual Processors
Red Hat Enterprise Linux 5.7 and 5.8	64
Red Hat Enterprise Linux 6.0–6.3	64
SUSE Linux Enterprise Server 11 SP2	64
Open SUSE 12.1	64
Ubuntu 12.04	64

TABLE 9.2 Hyper-V guest client operating systems

Guest Operating System (Client)	Maximum Number of Virtual Processors
Windows 8	32
Windows 7 with Service Pack 1 (SP1)	4
Windows 7	4
Windows Vista with Service Pack 2 (SP2)	2
Windows XP with Service Pack 3 (SP3)	2
Windows XP x64 Edition with Service Pack 2 (SP2)	2
CentOS 5.7 and 5.8	64
CentOS 6.0–6.3	64
Red Hat Enterprise Linux 5.7 and 5.8	64
Red Hat Enterprise Linux 6.0–6.3	64
SUSE Linux Enterprise Server 11 SP2	64
Open SUSE 12.1	64
Ubuntu 12.04	64

The list of supported guest operating systems may always be extended. Please check the official Microsoft Hyper-V site to obtain a current list of supported operating systems: `www.microsoft.com/virtualization`.

Hyper-V Architecture

This section will provide you with an overview of the Hyper-V architecture (see Figure 9.1). I'll explain the differences between a hypervisor-aware and a non-hypervisor-aware child partition.

FIGURE 9.1 Hyper-V architecture

As you can see, Hyper-V is based on the new microkernel architecture. Hyper-V provides a virtualization layer called a *hypervisor* that runs directly on the system hardware. You can see that the hypervisor is similar to what the kernel is to Windows. It is a software layer responsible for the interaction with the core hardware and works in conjunction with an optimized instance of Windows Server 2012 R2 that allows running multiple operating systems on a physical server simultaneously. The Hyper-V architecture consists of the hypervisor and parent and child partitions.

The Windows Server 2012 R2 operating system runs in the parent partition, and it delivers the WMI provider for scripting as well as the VM service.

Virtual machines each run in their own child partitions. Child partitions do not have direct access to hardware resources; instead, they have a virtual view of the resources, which are called *virtual devices*.

If you're running a hypervisor-aware operating system like Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 in your virtual machine, any request to the virtual devices is redirected via the high-speed bus to the devices in the parent partition, which will manage the requests.

By default, only Windows Server 2008 R2, Server 2012, and Server 2012 R2 are hypervisor-aware operating systems. Once you install Hyper-V Integration Components on an operating system other than Windows Server 2008 R2 and newer, it will be hypervisor-aware. Microsoft provides a hypervisor adapter to make Linux hypervisor aware.

Non-hypervisor-aware operating systems (for example, Windows NT 4.0) use an emulator to communicate with the Windows hypervisor, which is slower than molasses in the winter.

Hyper-V Requirements

The following sections will describe the hardware and software requirements for installing the Hyper-V server role. It is important to understand these requirements for obtaining your software license as well as for planning for server hardware. When you understand the requirements, you can design and configure a Hyper-V solution that will meet the needs of your applications.

Hardware Requirements

In addition to the basic hardware requirements for Windows Server 2012 R2, there are requirements for running the Hyper-V server role on your Windows server. They are listed in Table 9.3.

TABLE 9.3 Hardware requirements for Hyper-V

Requirement Area	Definition
CPU	x64-compatible processor with Intel VT or AMD-V technology enabled. Hardware Data Execution Prevention (DEP), specifically Intel XD bit (execute disable bit) or AMD NX bit (no execute bit), must be available and enabled. Minimum: 1.4GHz. Recommended: 2GHz or faster.
Memory	Minimum: 1GB RAM. Recommended: 2GB RAM or greater. (Additional RAM is required for each running guest operating system.) Maximum: 1TB.
Hard disk	Minimum: 8GB. Recommended: 20GB or greater. (Additional disk space needed for each guest operating system.)

The Add Roles Wizard in Server Manager additionally verifies the hardware requirements. A good starting point is to check your hardware against the Microsoft hardware list to make sure that Windows Server 2012 R2 supports your hardware. If you try to install the Hyper-V server role on a computer that does not meet the CPU requirements, you'll get a warning window that looks like Figure 9.2.

FIGURE 9.2 Warning window that Hyper-V cannot be installed

Software Requirements

To use virtualization in Windows Server 2012 R2, you need to consider the basic software requirements for Hyper-V. Hyper-V runs only on the following editions of the Windows Server 2012 R2 operating system:

- Windows Server 2012 R2 Standard edition
- Windows Server 2012 R2 Datacenter edition
- Microsoft Hyper-V Server 2012 R2 edition

Hyper-V Installation and Configuration

The following sections explain how to install the Hyper-V role using Server Manager in Windows Server 2012 R2 Full installation mode or the command line mode in Windows Server 2012 R2 Server Core. We will then take a look at Hyper-V as part of Server Manager before discussing how to use the Hyper-V Manager. Finally, we will look at the Hyper-V server settings and then cover two important areas for Hyper-V: virtual networks and virtual hard disks.

Install the Hyper-V Role

Now it's time to see how to install the Hyper-V server role on the two installation options of Windows Server 2012 R2, namely, a Full installation and a Server Core installation.

Installing Hyper-V in Full Installation Mode

You can install the Hyper-V server role on any Windows Server 2012 R2 installation for which the Full option was chosen. In addition, the server must meet both the hardware and software requirements. The installation process is simple, as Exercise 9.1 demonstrates.

EXERCISE 9.1

Installing Hyper-V in Full Installation Mode

1. Open Server Manager.
2. In Server Manager, choose option 2, Add Roles And Features.
3. At the Select Installation Type page, choose the role-based or feature-based installation. Click Next.
4. On the Select Destination Server screen, choose Select A Server From The Server Pool and choose the server to which you want to add this role. Click Next.
5. On the Select Server Roles screen, click the check box next to Hyper-V. When the Add Features dialog box appears, click the Add Features button. Then click Next.

6. At the Select Features screen, click Next.
7. At the Hyper-V introduction screen, click Next.
8. At the Create Virtual Switches screen, choose your adapter and click Next.

9. At the Virtual Machine Migration screen, click Next. You want to use migration only if you have multiple Hyper-V servers. Since we will have only one for this exercise, just skip this screen.
10. At the Default Stores screen, accept the defaults and click Next.
11. At the Confirmation screen, click the Install button.
12. After the installation is complete, click the Close button.
13. Restart your server.

Installing Hyper-V in Server Core

The Server Core installation option is introduced in Windows Server 2012 R2. It creates an operating system installation without a GUI shell. You can either manage the server remotely from another system or use the Server Core's command-line interface.

This installation option provides the following benefits:

- Reduces attack surface (because fewer applications are running on the server)
- Reduces maintenance and management (because only the required options are installed)
- Requires less disk space and produces less processor utilization
- Provides a minimal parent partition
- Reduces system resources required by the operating system as well as the attack surface

By using Hyper-V on a Server Core installation, you can fundamentally improve availability because the attack surface is reduced and the downtime required for installing patches is optimized. It will thus be more secure and reliable with less management.

To install Hyper-V for a Windows Server 2012 R2 installation, you must execute the following command in the command-line interface:

```
Dism /online /enable-feature /featurename:Microsoft-Hyper-V
```

Hyper-V in Server Manager

As with all of the other Windows Server 2012 R2 roles, the Hyper-V role neatly integrates into Server Manager. Server Manager filters the information just for the specific role and thus displays only the required information. As you can see in Figure 9.3, the Hyper-V Summary page shows related event log entries, the state of the system services for Hyper-V, and useful resources and support.

FIGURE 9.3 Hyper-V in Server Manager

Using Hyper-V Manager

Hyper-V Manager is the central management console to configure your server and create and manage your virtual machines, virtual networks, and virtual hard disks. Unlike Virtual Server 2005, where you managed all virtual machines through a web interface, Hyper-V Manager is managed through a Microsoft Management Console (MMC) snap-in. You can access it either in Server Manager or by using Administrative Tools ➢ Hyper-V Manager. Figure 9.4 shows how Hyper-V Manager looks once you start it.

FIGURE 9.4 Hyper-V Manager

Hyper-V Manager is available for the following operating systems:

- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2008
- Windows 8
- Windows 7
- Windows Vista with Service Pack 1 (SP1)

Hyper-V Manager is installed on a Windows Server 2012 R2 machine only when you install Hyper-V on it. On Windows Server 2008/2008 R2, Server 2003, Windows Vista, Windows 7, or Windows 8, you will need to install the Hyper-V Manager MMC.

You can use Hyper-V Manager to connect to any Full or Server Core installation remotely. Besides Hyper-V Manager, you can use the WMI interface for scripting Hyper-V.

Configure Hyper-V Settings

In this section, you will get an overview of the available Hyper-V settings for the server. You configure all server-side default configuration settings like default locations of your configuration files or the release key. You can open the Hyper-V Settings page (see Figure 9.5) in Hyper-V Manager by clicking Hyper-V Settings in the Actions pane.

FIGURE 9.5 Hyper-V Settings

The Hyper-V Settings page includes the following settings:

Virtual Hard Disks Specifies the default location of your virtual hard disk files (`.vhd` and `.vdhx`).

Virtual Machines Specifies the default location of your virtual machine configuration files. It includes the Virtual Machine XML configuration files (part of the `Virtual Machines` folder) as well as related snapshots (part of the `Snapshot` folder).

Physical GPUs This feature allows for graphical processing unit (GPU) accelerated video within a virtual machine. The GPU will allow you to support 3D GPU accelerated graphics.

NUMA Spanning An administrator can configure Hyper-V to allow virtual machines to span nonuniform memory architecture (NUMA) nodes. When the physical computer has NUMA nodes, this setting provides virtual machines with additional computing resources. Spanning NUMA nodes can help you run more virtual machines at the same time. However, using NUMA can decrease overall performance.

Live Migrations *Live migration* allows a Hyper-V administrator to relocate running virtual machines easily from one node of the failover cluster to another node in the same cluster. Live Migration is explained in more detail later in this chapter.

Storage Migrations *Storage Migration* allows an administrator to move their virtual machine storage from one location to another. This setting allows you to specify how many storage migrations can be performed at the same time on this system.

Replication Configuration This setting allows you to configure this computer as a Replica Server to another Hyper-V server. Hyper-V Replica allows administrators to replicate their Hyper-V virtual machines from one Hyper-V host at a primary site to another Hyper-V host at the Replica site.

Each node of the failover cluster that is involved in Replica must have the Hyper-V server role installed. One of the servers in the Hyper-V replication needs to be set up as a Replica Broker to allow the replication to work properly.

Keyboard Defines how to use Windows key combinations. Options are Physical Computer, Virtual Machine, and Virtual Machine Only When Running Full Screen.

Mouse Release Key Specifies the key combination to release the mouse in your virtual machine. Options are Ctrl+Alt+left arrow, Ctrl+Alt+right arrow, Ctrl+Alt+space, and Ctrl+Alt+Shift.

Reset Check Boxes Resets any check boxes that hide pages and messages when checked. This will bring any window up again on which you checked the Do Not Show This Window Again check box.

Manage Virtual Switches

A *virtual network* provides the virtual links between nodes in either a virtual or physical network. Virtual networking in Hyper-V is provided in a secure and dynamic way because you can granularly define virtual network switches for their required usage. For example, you can define a private or internal virtual network if you don't want to allow your virtual machines to send packages to the physical network.

To allow your virtual machines to communicate with each other, you need virtual networks. Just like normal networks, virtual networks exist only on the host computer and allow you to configure how virtual machines communicate with each other, with the host, and with the network or the Internet. You manage virtual networks in Hyper-V using Virtual Switch Manager, as shown in Figure 9.6.

FIGURE 9.6 Virtual Network Manager

Using *Virtual Switch Manager*, you can create, manage, and delete virtual switches. You can define the network type as external, internal only, or private.

External Any virtual machine connected to this virtual switch can access the physical network. You would use this option if you want to allow your virtual machines to access, for example, other servers on the network or the Internet. This option is used in production environments where your clients connect directly to the virtual machines.

Internal This option allows virtual machines to communicate with each other as well as the host system but not with the physical network. When you create an internal network, it also creates a local area connection in Network Connections that allows the host machine to communicate with the virtual machines. You can use this if you want to separate your host's network from your virtual networks.

Private When you use this option, virtual machines can communicate with each other but not with the host system or the physical network; thus, no network packets are hitting the wire. You can use this to define internal virtual networks for test environments or labs, for example.

On the external and internal-only virtual networks, you also can enable virtual LAN (VLAN) identification. You can use VLANs to partition your network into multiple subnets using a VLAN ID. When you enable virtual LAN identification, the NIC that is

connected to the switch will never see packets tagged with VLAN IDs. Instead, all packets traveling from the NIC to the switch will be tagged with the access mode VLAN ID as they leave the switch port. All packets traveling from the switch port to the NIC will have their VLAN tags removed. You can use this if you are already logically segmenting your physical machines and also use it for your virtual ones.

Exercise 9.2 explains how to create an internal-only virtual switch.

EXERCISE 9.2

Creating an Internal Virtual Network

1. Click the Windows Key ➢ Administrative Tools ➢ Hyper-V Manager.
2. In Hyper-V Manager, in the Actions pane, choose Virtual Switch Manager.
3. On the Virtual Switch page, select Private and click the Create Virtual Switch button.
4. On the New Virtual Switch page, enter **Private Virtual Network** in the Name field.
5. Click OK.

When you create the internal virtual switch, a network device is created in Network Connections, as shown in Figure 9.7.

FIGURE 9.7 Virtual network card

This is also the case when you create an external virtual network because it will replace the physical network card of the host machine to give the parent partition a virtual network card that is also used in the child partitions.

Unlike with Virtual Server 2005, Hyper-V binds the virtual network service to a physical network adapter only when an external virtual network is created. The benefit of this is that the performance is better if you do not use the external virtual network option. The downside, however, is that there will be a network disruption when you create or delete an external virtual network.

Communication between the virtual machine and the local host computer is not configured automatically. Once you install a virtual machine, you need to make sure that the TCP/IP settings are in agreement with the settings you define in the virtual network card. Start with a ping from your host machine to the virtual machines to verify that communication is working.

Managing Virtual Hard Disks

In addition to virtual networks, you need to manage virtual hard disks that you attach to your virtual machines. A virtual hard disk in Hyper-V, apart from a pass-through disk, is a VHD or VHDX file that basically simulates a hard drive on your virtual machine.

The following sections will first show you what types of virtual hard disks are available and then show you how to create them. You will also learn about what options are available to manage virtual hard disks.

Types of Hard Disks

Depending on how you want to use the disk, Hyper-V offers various types, as described in Table 9.4.

TABLE 9.4 Virtual hard disks in Hyper-V

Type of disk	Description	When to use it
Dynamically expanding	This disk starts with a small VHD file and expands it on demand once an installation takes place. It can grow to the maximum size you defined during creation. You can use this type of disk to clone a local hard drive during creation.	This option is effective when you don't know the exact space needed on the disk and when you want to preserve hard disk space on the host machine. Unfortunately, it is the slowest disk type.

Fixed size	The size of the VHD file is fixed to the size specified when the disk is created. This option is faster than a dynamically expanding disk. However, a fixed-size disk uses up the maximum defined space immediately. This type is ideal for cloning a local hard drive.	A fixed-size disk provides faster access than dynamically expanding or differencing disks, but it is slower than a physical disk.
Differencing	This type of disk is associated in a parent-child relationship with another disk. The differencing disk is the child, and the associated virtual disk is the parent. Differencing disks include only the differences to the parent disk. By using this type, you can save a lot of disk space in similar virtual machines. This option is suitable if you have multiple virtual machines with similar operating systems.	Differencing disks are most commonly found in test environments and should not be used in production environments.
Physical (or pass-through disk)	The virtual machine receives direct pass-through access to the physical disk for exclusive use. This type provides the highest performance of all disk types and thus should be used for production servers where performance is the top priority. The drive is not available for other guest systems.	This type is used in high-end datacenters to provide optimum performance for VMs. It's also used in failover cluster environments.

Creating Virtual Hard Disks

To help you gain practice in creating virtual hard disks, the following three exercises will teach you how to create a differencing hard disk, how to clone an existing disk by creating a new disk, and how to configure a physical or pass-through disk to your virtual machine. First, in Exercise 9.3, you will learn how to create a differencing virtual hard disk.

EXERCISE 9.3

Creating a Differencing Hard Disk

1. Open Hyper-V Manager.
2. In Hyper-V Manager, on the Actions pane, choose New ➢ Hard Disk.
3. In the New Virtual Hard Disk Wizard, click Next on the Before You Begin page.

EXERCISE 9.3 *(continued)*

4. At the Choose Disk Format screen, choose VHDX and click Next. The size of your VHDs depends on which format you choose. If you're going to have a VHD larger than 2,040GB, use VHDX. If your VHD is less than 2,040GB, then you should use VHD.
5. On the Choose Disk Type page, select Fixed Size and click Next.
6. On the Specify Name And Location page, enter the new name of the child disk (for example, **newvirtualharddisk.vhd**). You can also modify the default location of the new VHD file if you want. Click Next to continue.
7. Next, on the Configure Disk page, you need to specify the size of the VHD file. Choose a size based on your hard disk and then click Next to continue. I used 60GB as our test size.
8. On the Completing The New Virtual Hard Disk Wizard page, verify that all settings are correct and click Finish to create the hard disk.

The process to add a physical or pass-through disk to a virtual machine is quite different. For this, first you need to create the virtual machine, and then you open the virtual machine settings to configure the physical disk. If you want to add a physical disk to a virtual machine, the physical disk must be set as Offline in Disk Management, as shown in Figure 9.8.

FIGURE 9.8 In Disk Management, you can set disks as Offline.

To access Disk Management, click the Windows key, choose Administrative Tools ➢ Computer Management, expand Storage in the left pane, and click Disk Management.

You cannot share a physical disk among multiple virtual machines or with the host system.

Physical or pass-through disks might not be that important if your use of virtualization is based on test environments, but they become crucial when you need to plan for highly available virtual datacenters. This is especially true if you consider using failover clusters to provide the Quick Migration feature, which is when you should consider matching one logical unit number (LUN) from your enterprise storage system or storage area network (SAN) as one physical disk. This provides you with the optimum performance you need in such an environment.

Managing Virtual Hard Disks

Hyper-V also provides two tools to manage virtual hard disks: Inspect Disk and Edit Disk. These tools are available on the Actions pane in Hyper-V Manager.

Inspect Disk This provides you with information about the virtual hard disk. It shows you not only the type of the disk but also information such as the maximum size for dynamically expanding disks and the parent VHD for differencing disks.

Edit Disk This provides you with the Edit Virtual Hard Disk Wizard, which you can use to compact, convert, expand, merge, or reconnect hard disks. Figure 9.9 shows you the wizard's options when you select a dynamically expanding disk.

FIGURE 9.9 The Edit Virtual Hard Disk Wizard

Table 9.5 provides you with an overview of what you can do with the wizard.

TABLE 9.5 Edit Disk overview

Action	Description
Compact	Reduces the size of a dynamically expanding or differencing disk by removing blank space from deleted files.
Convert	Converts a dynamically expanding disk to a fixed disk or vice versa.
Expand	Increases the storage capacity of a dynamically expanding disk or a fixed virtual hard disk.
Merge	Merges the changes from a differencing disk into either the parent disk or another disk (applies to differencing disks only!).
Reconnect	If a differencing disk no longer finds its referring parent disk, this option can reconnect the parent to the disk.

Generation 1 vs. Generation 2 VHDs

Previous versions of Hyper-V had some pretty major drawbacks. One big drawback was that Hyper-V could not boot a virtual machine from a virtual hard drive that was SCSI. Believe it or not, SCSI controllers were not even recognized by Hyper-V unless you installed the Integration Services component.

Another issue that the previous versions of Hyper-V had was the inability to copy files from the Hyper-V host to the virtual machines without the use of a network connection in the virtual machine. The older versions of Hyper-V, prior to Windows Server 2012 R2, are now considered generation 1 versions. Why is it so important to know which generations of Hyper-V you should use or need to use?

Hyper-V generations help determine what functionality and what virtual hardware you can use in your virtual machine. Windows Server 2012 R2 Hyper-V now supports two different virtual machine generations: generation 1 and generation 2.

As already explained, previous versions of Hyper-V are considered generation 1, and this provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

Generation 2 is now included with Windows Server 2012 R2, and it provides new functionality on the virtual machines including secure boot (which is enabled by default), the ability to boot from a SCSI virtual hard disk or boot from a SCSI virtual DVD, the ability to use a standard network adapter to PXE boot, and Unified Extensible Firmware

Interface (UEFI) firmware support. Generation 2 now gives you the ability to support UEFI firmware instead of BIOS-based firmware.

So when you create VHDs in Windows Server 2012 R2, one of your choices will be the ability to create the VHDs as a generation 1 or generation 2 VHD. If you need the ability to have your VHDs run on older versions of Hyper-V, make them a generation 1 VHD. If they are going to run only on Windows Server 2012 R2, make your VHDs generation 2 and take advantage of all the new features and functionality.

Configuring Virtual Machines

The following sections cover the topics of creating and managing virtual machines as well as how to back up and restore virtual machines using features such as Import and Export and Snapshot. You'll also briefly look at Hyper-V's Live Migration feature.

Creating and Managing Virtual Machines

It is important to learn how to create a virtual machine, how to change its configuration, and how to delete it. You will take a look at the Virtual Machine Connection tool and install the Hyper-V Integration Components onto a virtual machine.

Virtual Machines

Virtual machines define the child partitions in which you run operating system instances. Each virtual machine is separate and can communicate with the others only by using a virtual network. You can assign hard drives, virtual networks, DVD drives, and other system components to it. A virtual machine is similar to an existing physical server, but it no longer runs on dedicated hardware—it shares the hardware of the host system with the other virtual machines that run on the host.

Exercise 9.4 shows you how to create a new virtual machine.

EXERCISE 9.4

Creating a New Virtual Machine

1. Open Hyper-V Manager.
2. In Hyper-V Manager, on the Actions pane, choose New ➢ Virtual Machine.
3. In the New Virtual Machine Wizard, click Next on the Before You Begin page.
4. On the Specify Name And Location page, give your virtual machine a name and change the default location of the virtual machine configuration files. Click Next to continue.

EXERCISE 9.4 *(continued)*

5. On the Assign Memory page, define how much of your host computer's memory you want to assign to this virtual machine. Remember that once your virtual machine uses up all of your physical memory, it will start swapping to disk, thus reducing the performance of all virtual machines. Click Next to continue.
6. On the Configure Networking page, select the virtual network that you previously configured using Virtual Network Manager. Click Next to continue.
7. On the next page, you configure your virtual hard disk. You can create a new virtual hard disk, select an existing disk, or choose to attach the hard disk later. Be aware that you can create only a dynamically expanding virtual disk on this page; you cannot create a differencing, physical, or fixed virtual hard disk there. However, if you created the virtual hard disk already, you can, of course, select it. Click Next to continue.
8. On the Installation Options page, you can select how you want to install your operating system. You have the option to install an operating system later, install the operating system from a boot CD/DVD-ROM where you can select a physical device or an image file (ISO file), install an operating system from a floppy disk image (VFD file, or a virtual boot floppy disk), or install an operating system from a network-based installation server. The last option will install a legacy network adapter to your virtual machine so that you can boot from the network adapter. Select Install An Operating System Later and then click Next.
9. On the Completing The New Virtual Machine Wizard summary page, verify that all settings are correct. You also have the option to start the virtual machine immediately after creation. Click Next to create the virtual machine.
10. Repeat this process and create a few more virtual machines.
11. If you want to install an operating system on one of the VMs, start the VM, load a Windows Server 2012 R2 installation disk into the DVD drive, and then, under the Media menu, choose DVD and Capture. Then just do a normal install.

After completing Exercise 9.4, you will have a virtual machine available in Hyper-V Manager. Initially, the state of the virtual machine will be Off. Virtual machines can have the following states: Off, Starting, Running, Paused, and Saved. You can change the state of a virtual machine in the Virtual Machines pane by right-clicking the virtual machine's name, as shown in Figure 9.10, or by using the Virtual Machine Connection window.

Here is a list of some of the state options (when the VM is running) available for a virtual machine:

Start Turn on the virtual machine. This is similar to pressing the power button when the machine is turned off. This option is available when your virtual machine is Off or in Saved state.

Turn Off Turn off the virtual machine. This is similar to pressing the power-off button on the computer. This option is available when your virtual machine is in Running, Saved, or Paused state.

FIGURE 9.10 Options available when right-clicking a virtual machine

Shut Down This option shuts down your operating system. You need to have the Hyper-V Integration Components installed on the operating system; otherwise, Hyper-V will not be able to shut down the system.

Save The virtual machine is saved to disk in its current state. This option is available when your virtual machine is in Running or Paused state.

Pause Pause the current virtual machine, but do not save the state to disk. You can use this option to release processor utilization quickly from this virtual machine to the host system.

Reset Reset the virtual machine. This is like pressing the reset button on your computer. You will lose the current state and any unsaved data in the virtual machine. This option is available when your virtual machine is in Running or Paused state.

Resume When your virtual machine is paused, you can resume it and bring it online again.

Changing Configuration on an Existing Virtual Machine

To change the configuration settings on an existing virtual machine, you right-click your virtual machine's name in the Virtual Machines pane in Hyper-V Manager and choose Settings. You can change settings such as memory allocation and hard drive configuration. All items that you can configure are described in the following list:

Add Hardware Add devices to your virtual machine, namely, a SCSI controller, a network adapter, or a legacy network adapter. A legacy network adapter is required if you want to perform a network-based installation of an operating system.

BIOS This is the replacement of the virtual machine's BIOS. Because you can no longer enter the BIOS during startup, you need to configure it with this setting. You can turn Num Lock on or off and change the basic startup order of the devices.

Memory Change the amount of random access memory (RAM) allocated to the virtual machine.

Processor Change the number of logical processors this virtual machine can use and define resource control to balance resources among virtual machines by using a relative weight.

IDE Controller Add/change and remove devices from the IDE controller. You can have hard drives or DVD drives as devices. Every IDE controller can have up to two devices attached, and by default, you have two IDE controllers available.

Hard Drive Select a controller to attach to this device as well as to specify the media to use with your virtual hard disk. The available options are Virtual Hard Disk File (with additional buttons labeled New, Edit, Inspect, and Browse that are explained in the virtual hard disk section) and Physical Hard Disk. You can also remove the device here.

DVD Drive Select a controller to attach to this device and specify the media to use with your virtual CD/DVD drive. The available options are None, Image File (ISO Image), and Physical CD/DVD Drive Connected To The Host Computer. You also can remove the device here.

SCSI Controller Configure all hard drives that are connected to the SCSI controller. You can add up to 63 hard drives to each SCSI controller, and you can have multiple SCSI controllers available.

Network Adapter Specify the configuration of the network adapter or remove it. You can also configure the virtual network and MAC address for each adapter and enable virtual LAN identification.

COM1 and COM2 Configure the virtual COM port to communicate with the physical computer through a named pipe. You have COM1 and COM2 available.

Diskette Specify a virtual floppy disk file to use.

Name Edit the name of the virtual machine and provide some notes about it.

Integration Services Define what integration services are available to your virtual machine. Options are Operating System Shutdown, Time Synchronization, Data Exchange, Heartbeat, and Backup (Volume Snapshot).

Snapshot File Location Define the default file location of your snapshot files.

Smart Paging File Location This area allows you to set up a paging file for your virtual machine.

Windows Server 2012 R2 has a Hyper-V feature called *Smart Paging*. If you have a virtual machine that has a smaller amount of memory than what it needs for startup memory, when the virtual machine gets restarted, Hyper-V then needs additional memory to restart

the virtual machine. Smart Paging is used to bridge the memory gap between minimum memory and startup memory. This allows your virtual machines to restart properly.

Automatic Start Define what this virtual machine will do when the physical computer starts. Options are Nothing, Automatically Start If The Service Was Running, and Always Start This Virtual Machine. You also can define a start delay here.

Automatic Stop Define what this virtual machine will do when the physical computer shuts down. Options are Save State, Turn Off, and Shut Down.

Please be aware that only some settings can be changed when the virtual machine's state is Running. It is best practice to shut down the virtual machine before you modify any setting.

Deleting Virtual Machines

You can also delete virtual machines using Hyper-V Manager. This deletes all of the configuration files, as shown in Figure 9.11.

FIGURE 9.11 Delete Virtual Machine warning window

Make sure you manually delete any virtual disks that were part of the virtual machines to free up disk space. Virtual disks are *not* deleted when you delete a virtual machine.

Virtual Machine Connection

Similar to the Virtual Machine Remote Control (VMRC) client that was available with Virtual Server 2005 R2 and previous versions, Hyper-V comes with Virtual Machine Connection to connect to virtual machines that run on a local or remote server.

You can use it to log onto the virtual machine and use your computer's mouse and keyboard to interact with the virtual machine. You can open Virtual Machine Connection in Hyper-V Manager by double-clicking a virtual machine or by right-clicking a virtual machine and selecting Connect. If your virtual machine is turned off, you might see a window similar to the one in Figure 9.12.

FIGURE 9.12 Virtual Machine Connection window when the machine is turned off

Virtual Machine Connection not only provides you with functionality similar to that of Hyper-V Manager, such as being able to change the state of a virtual machine, but it also provides you with additional features that are especially useful when you want to work with a virtual machine.

File Access Settings or Exit Virtual Machine Connection Change the state of a virtual machine and create or revert a snapshot. Additionally, you have the options to send Ctrl+Alt+Delete to your virtual machine and Insert Integration Services Setup Disk.

Context-Sensitive Buttons Provide Quick Access to Key Features These buttons are available under the menu bar to provide you with fast access to the most important features, as you can see in Figure 9.13. It shows the connection of a running VM, but the VM has not had an operating system installed yet, so the figure shows the Windows Setup screen.

NIC Teaming

NIC Teaming, also known as load balancing and failover (LBFO), gives an administrator the ability to allow multiple network adapters on a system to be placed into a team. Independent hardware vendors (IHVs) have required NIC Teaming, but until Windows Server 2012, NIC Teaming was *not* part of the Windows Server operating system.

To be able to use NIC Teaming, the computer system must have at least one Ethernet adapter. If you want to provide fault protection, an administrator must have a minimum of two Ethernet adapters. One advantage of Windows Server 2012 R2 is that an administrator can set up 32 network adapters in a NIC team.

FIGURE 9.13 Virtual Machine Connection window showing a running Windows Server 2012 virtual machine

NIC Teaming is a common practice when setting up virtualization. This is one way that you can have load balancing with Hyper-V.

NIC Teaming gives an administrator the ability to allow a virtual machine to use virtual network adapters in Hyper-V. The advantage of using NIC Teaming in Hyper-V is that the administrator can use NIC Teaming to connect to more than one Hyper-V switch. This allows Hyper-V still to have connectivity even if the network adapter under the Hyper-V switch gets disconnected.

An administrator can configure NIC Teaming in either Server Manager or PowerShell.

Storage Quality of Service

Windows Server 2012 R2 Hyper-V includes a new feature called *Storage Quality of Service (QoS)*. Storage QoS allows a Hyper-V administrator to manage how virtual machines access storage throughput for virtual hard disks.

Storage QoS gives an administrator the ability to guarantee that the storage throughput of a single VHD cannot adversely affect the performance of another VHD on the same host. It does this by giving administrators the ability to specify the maximum and minimum I/O loads based on I/O operations per second (IOPS) for each virtual disk in your virtual machines.

To configure Storage QoS, you would set the maximum IOPS values (or limits) and set the minimum values (or reserves) on virtual hard disks for virtual machines.

If you are using shared virtual hard disks, Storage QoS will not be available.

Installing Hyper-V Integration Components

Hyper-V *Integration Components*, also called *Integration Services*, are required to make your guest operating system hypervisor-aware. Similar to the VM Additions that were part of Microsoft Virtual Server 2005, these components improve the performance of the guest operating system once they are installed. From an architectural perspective, virtual devices are redirected directly via the VMBus; thus, quicker access to resources and devices is provided.

If you do not install the Hyper-V Integration Components, the guest operating system uses emulation to communicate with the host's devices, which of course makes the guest operating system slower.

Exercise 9.5 shows you how to install Hyper-V Integration Components on one of your virtual machines running Windows Server 2012.

EXERCISE 9.5

Installing Hyper-V Integration Components

1. Open Hyper-V Manager.
2. In Hyper-V Manager, in the Virtual Machines pane, right-click the virtual machine on which you want to install Hyper-V Integration Components and click Start.
3. Right-click the virtual machine again and click Connect. Meanwhile, your virtual machine should already be booting.
4. If you need to log into the operating system of your virtual machine, you should do so.
5. Once the Windows Desktop appears, you need to select Insert Integration Services Setup Disk from the Actions menu of your Virtual Machine Connection window.
6. Once the Hyper-V Integration Components are installed, you are asked to perform a reboot.

After the reboot, Hyper-V Integration Components are installed on your operating system, and you will be able to use them.

Summary

Virtualization is quickly becoming a hot topic in information technology. The potential for consolidation is tremendous, and thus it will become more and more important.

After reading this chapter, you should have a good understanding of the Hyper-V architecture and what is required to install Hyper-V.

The section about installation and configuration covered various basic aspects of configuring the virtualization environment. You learned about the different types of virtual networks that are available, the options for installing the Hyper-V role, and the various types of virtual hard disks that you can use to optimize virtualization for your specific scenario.

You also learned how to configure virtual machines using the Hyper-V environment and how to create your own virtual datacenter on top of your Hyper-V machines. I showed you how to create and manage virtual machines, how to use Virtual Machine Connection to control a virtual machine remotely, and how to install Hyper-V Integration Components. You also learned how to export and import virtual machines as well as how to do snapshots of your virtual machine.

If you have never worked with virtualization software before, the information in this chapter may have been completely new to you. You should now be well prepared to try Hyper-V in your own environment.

Exam Essentials

Understand Hyper-V's architecture. When you have a good understanding of Hyper-V's architecture, especially when an operating system in a virtual machine is hypervisor aware versus non-hypervisor aware, you have a solid understanding of what is important from an architectural perspective.

You should know about the Hyper-V Integration Components and how they change the behavior of a virtual machine. Also know for which operating systems the integration components are available.

Know Hyper-V's requirements and how to install it. Know the hardware and software requirements as well as how to install Hyper-V. Hyper-V requires an x64-based processor and Data Execution Protection (DEP). Hardware-assisted virtualization must be enabled—don't forget this! Also remember that you can install Hyper-V two ways: using Server Manager or using the command line in Server Core.

Understand virtual networks and virtual hard disks. Virtual networks and hard disks are the two most tested topics. You definitely should know the types of virtual networks available (that is, external, internal only, and private virtual network) as well as all types of virtual hard disks (namely, dynamically expanding, fixed size, differential, and physical or

pass-through). You should be able to apply the correct one when needed. Don't forget the Edit Virtual Hard Disk Wizard, which is also a good source for questions in the exam.

Know how to create and manage virtual machines. You should be able to explain how to create a virtual machine, what options are available to install an operating system in a virtual machine, and how to install the Hyper-V Integration Components on a virtual machine. Don't forget about the virtual machine states and the virtual machine settings!

Understand how to back up and restore virtual machines. Have a good understanding of the concept of exporting and importing virtual machines, how snapshots work, and what lies behind a quick migration. Understand how you can export a virtual machine, what you should consider when moving it to a new host machine, and what happens after importing it to the import folder. The same applies to snapshots: You need to know what options you have available and what each option will do. Especially recognize the difference between applying and reverting a snapshot.

Review Questions

1. On which of the following x64 editions of Windows Server 2012 R2 does Hyper-V run? (Choose all that apply.)
   - **A.** Windows Server 2012 R2 Web Edition
   - **B.** Windows Server 2012 R2 Standard Edition
   - **C.** Windows Server 2012 R2 Itanium Edition
   - **D.** Windows Server 2012 R2 Datacenter Edition

2. You want to build a test environment based on virtual machines on a single Windows Server 2012 R2 machine, but you also want to make sure that the virtual machines communicate only with each other. What type of virtual network do you need to configure?
   - **A.** External
   - **B.** Internal only
   - **C.** Private virtual machine network
   - **D.** Public virtual machine network

3. Andy wants to change the memory of a virtual machine that is currently powered up. What does he need to do?
   - **A.** Shut down the virtual machine, use the virtual machine's settings to change the memory, and start it again.
   - **B.** Use the virtual machine's settings to change the memory.
   - **C.** Pause the virtual machine, use the virtual machine's settings to change the memory, and resume it.
   - **D.** Save the virtual machine, use the virtual machine's settings to change the memory, and resume it.

4. You want to make sure that the hard disk space for your virtual machines is occupied only when needed. What type of virtual hard disk would you recommend?
   - **A.** Dynamically expanding disk
   - **B.** Fixed-size disk
   - **C.** Differencing disk
   - **D.** Physical or pass-through disk

5. How do you add a physical disk to a virtual machine?
   - **A.** Use the Virtual Hard Disk Wizard.
   - **B.** Use the Edit Virtual Hard Disk Wizard.
   - **C.** Use the virtual machine's settings.
   - **D.** Use the New Virtual Machine Wizard.

6. Rich bought a new server with an Itanium IA-64 processor, 4GB RAM, and a SAN that provides 1TB hard disk space. After installing Windows Server 2012 R2 for Itanium-based systems, he wants to install Hyper-V on this server. Can Hyper-V be installed on this system?
   - **A.** Yes
   - **B.** No

7. What are the minimum CPU requirements for running Hyper-V on a machine? (Choose all that apply.)
   - **A.** An x64-based processor (Intel or AMD).
   - **B.** Hardware Data Execution Protection (DEP) must be enabled.
   - **C.** Hardware-assisted virtualization must be enabled.
   - **D.** The processor must at least have a dual core.

8. What is the command to install Hyper-V on a Windows Server 2008 machine that was installed in Server Core?
   - **A.** `start /w ocsetup Hyper-V`
   - **B.** `start /w ocsetup microsoft-hyper-v`
   - **C.** `start /w ocsetup Microsoft-Hyper-V`
   - **D.** `start /w ocsetup hyper-v`

9. On what operating systems can you install the Hyper-V Manager MMC? (Choose all that apply.)
   - **A.** Windows Server 2008 R2
   - **B.** Windows Server 2003
   - **C.** Windows XP SP3
   - **D.** Windows 7, Windows 8

10. What statement is correct for an external virtual network?
    - **A.** The virtual machines can communicate with each other and with the host machine.
    - **B.** The virtual machines can communicate with each other only.
    - **C.** The virtual machines can communicate with each other, with the host machine, and with an external network.
    - **D.** The virtual machines cannot communicate with each other.

Exam 70-411: Administering Windows Server 2012 R2

PART II

CHAPTER 10 ■ Manage and Maintain Servers

CHAPTER 11 ■ Manage File Services

CHAPTER 12 ■ Configure DNS

CHAPTER 13 ■ Configure Routing and Remote Access

CHAPTER 14 ■ Configure a Network Policy Server Infrastructure

CHAPTER 15 ■ Configure and Manage Active Directory

CHAPTER 16 ■ Configure and Manage Group Policy

Chapter 10

Manage and Maintain Servers

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Deploy and manage server images**

- Install the Windows Deployment Services (WDS) role
- Configure and manage boot, install, and discover images
- Update images with patches, hotfixes, and drivers
- Install features for offline images
- Configure driver groups and packages

✓ **Implement patch management**

- Install and configure the Windows Server Update Services (WSUS) role
- Configure group policies for updates

✓ **Configure client-side targeting**

- Configure WSUS synchronization
- Configure WSUS groups
- Manage patch management in mixed environments

✓ **Monitor servers**

- Configure Data Collector Sets (DCS)
- Configure alerts
- Monitor real-time performance
- Monitor virtual machines (vms)
- Monitor events
- Configure event subscriptions
- Configure network monitoring
- Schedule performance monitoring

We have already discussed how to set up clients on a network and how to keep their systems running on that network. In this chapter, we will start the Windows Deployment Services. We will then turn the discussion to keeping your systems updated using Windows Server Update Services (WSUS).

Another important task of an IT team is to keep the network up and running quickly and efficiently. Keeping your network running at its peak performance is one way to make sure your end users continue to use the network and its resources without problems or interruptions. Remember, everyone has clients—salespeople have theirs, accountants have theirs, and so do we as system administrators. Our clients are the end users, and it's our job to make sure that our clients can do their jobs.

When you are working with servers, it is important you make sure that your system's information is safely backed up. Backups become useful when you lose data because of system failures, file corruptions, or accidental modifications of information. As consultants, we can tell you from experience that backups are among the most important tasks that an IT person performs daily.

Sometimes, performance optimization can feel like a luxury, especially if you can't get your domain controllers to the point where they are actually performing the services for which you intended them, such as servicing printers or allowing users to share and work on files. The Windows Server 2012 R2 operating system has been specifically designed to provide high-availability services solely intended to keep your mission-critical applications and data accessible, even in times of disaster. Occasionally, however, you might experience intermittent server crashes on one or more of the domain controllers or other computers in your environment.

The most common cause of such problems is a hardware configuration issue. Poorly written device drivers and unsupported hardware can cause problems with system stability. Failed hardware components (such as system memory) may do so as well. Memory chips can be faulty, electrostatic discharge can ruin them, and other hardware issues can occur. No matter what, a problem with your memory chip spells disaster for your server.

Third-party hardware vendors usually provide utility programs with their computers that can be used for performing hardware diagnostics on machines to help you find problems. These utilities are a good first step in resolving intermittent server crashes. When these utility programs are used in combination with the troubleshooting tips provided in this and other chapters of this book, you should be able to pinpoint most network-related problems that might occur.

In this chapter, I'll cover the tools and methods used for measuring performance and troubleshooting failures in Windows Server 2012 R2. Before you dive into the technical details, however, you should thoroughly understand what you're trying to accomplish and how you'll meet this goal.

Knowing How to Locate and Isolate Problems

In a book such as this, it would be almost impossible to cover everything that could go wrong with your Windows Server 2012 R2 system. This book covers many of the most common issues that you might come across, but almost anything is possible. Make sure you focus on the methodology used and the steps required to locate and isolate a problem—even if you are not 100 percent sure about the cause of the problem. Use online resources to help you locate and troubleshoot the problem, but don't believe everything you read (some things that are posted online can be wrong or misleading). Test your changes in a lab environment, and try to read multiple sources. Always use Microsoft Support (`http://support.microsoft.com/`) as one of your sources because this site is most likely the right source for information. You won't be able to find and fix everything, but knowing where to find critical information that will help you in your efforts never hurts. One of the tools that many of us in the industry use is *Microsoft TechNet*. The full version of TechNet (a paid subscription) is a resource that will help you find and fix many real-world issues.

Using Windows Deployment Services

In this section, you will look at how to install and configure *Windows Deployment Services (WDS)*. WDS is a utility that allows an administrator to deploy an operating system remotely. The client machine that is receiving the operating system needs to use a set of disks (WDS client disks) that will automatically initiate a network card, connect to the WDS server, and download the operating system.

WDS allows an IT administrator to install a Windows operating system without using a CD or DVD installation disc. Using WDS allows you to deploy the operating system through a network installation. WDS can deploy Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Microsoft Windows 2012, and Microsoft Windows Server 2012 R2.

The following are some of the advantages of using WDS for automated installation:

- You can remotely install Windows 7 or Windows 8.
- The procedure simplifies management of the server image by allowing you to access Windows 7 or Windows 8 distribution files from a distribution server.
- You can quickly recover the operating system in the event of a computer failure.

Here are the basic steps of the WDS process from a PXE-enabled WDS client:

1. The WDS client initiates a special boot process through the PXE network adapter (and the computer's BIOS configured for a network boot). On a PXE client, the user presses F12 to start the PXE boot process and to indicate that they want to perform a WDS installation.
2. A list of available Windows PE boot images is displayed. The user should select the appropriate Windows PE boot image from the boot menu.

3. The Windows Welcome screen is displayed. The user should click the Next button.
4. The WDS user is prompted to enter credentials for accessing and installing images from the WDS server.
5. A list of available operating system images is displayed. The user should select the appropriate image file to install.
6. The WDS user is prompted to enter the product key for the selected image.
7. The Partition And Configure The Disk screen is displayed. This screen provides the ability to install a mass storage device driver, if needed, by pressing F6.
8. The image copy process is initiated, and the selected image is copied to the WDS client computer.

The following sections describe how to set up the WDS server and the WDS clients and how to install Windows 7 or Windows 8 through WDS.

Windows Server 2012 R2 WDS Functionality

Windows Server 2012 R2 allows you to use many new and improved features of WDS. Table 10.1 shows some of the highpoints of what WDS can do when installed onto a Windows Server 2012 or Windows Server 2012 R2 system.

Preparing the WDS Server

With the WDS server, you can manage and distribute Windows 7 or Windows 8 operating system images to WDS client computers. The WDS server contains any files necessary for PXE booting, Windows PE boot images, and the Windows 7 or Windows 8 images to be deployed.

The following steps for preparing the WDS server are discussed in the upcoming sections:

1. Make sure that the server meets the requirements for running WDS.
2. Install WDS.
3. Configure and start WDS.
4. Configure the WDS server to respond to client computers (if this was not configured when WDS was installed).

For WDS to work, the server on which you will install WDS must meet the requirements for WDS and be able to access the required network services.

WDS Server Requirements

WDS needs some services and requirements installed before it will work properly:

- Active Directory Domain Services must be present for WDS to function properly. The WDS server must be a domain controller or a member of the Active Directory domain.
- At least one partition on the server must be formatted as NTFS.
- The operating system must be Windows Server 2003, Windows Server 2008/2008 R2, Windows Server 2012, or Windows Server 2012 R2.

TABLE 10.1 WDS functionality with Windows Server 2012 R2

Feature	Description
OS deployed using WDS	Windows XP, Windows Server 2003, Windows Vista SP1, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows 8, Windows 8.1, Windows Server 2012 R2.
Image types deployed	`.wim` and `.vhd` images are both supported. `.vhd` images can now be managed via the WDS management snap-in in addition to the command line. Also, `.vhdx` files, the new file format available since Windows Server 2012, are supported directly and over multicast.
Boot environment	Windows PE.
Administration options	MMC snap-in and WDSUTIL. Windows PowerShell cmdlets added in Windows Server 2012 R2.
Multicasting	IPv6 and DHCPv6 support for TFTP and multicasting along with improved multicast deployments.
Driver provisioning	Drivers are automatically detected and installed. Because of this, duplicate driver packages are prevented from being installed into the driver store.
PowerShell cmdlet scripting	Supported on Windows Server 2012 R2 only.

Network Services

Besides the server requirements, some networking requirements need to be installed for WDS. The following network services must be running on the WDS server or be accessible to the WDS server from another network server:

- TCP/IP installed and configured.
- A DHCP server, which is used to assign DHCP addresses to WDS clients. (Make sure your DHCP scope has enough addresses to accommodate all of the WDS clients that will need IP addresses.)
- A DNS server, which is used to locate the Active Directory controller.
- Active Directory, which is used to locate WDS servers and WDS clients as well as authorize WDS clients and manage WDS configuration settings and client installation options.

Installing the WDS Server Components

You can configure WDS on a Windows Server 2003/2008/2008 R2, Windows Server 2012, or Windows Server 2012 R2 computer by using the Windows Deployment Services Configuration Wizard or by using the WDSUTIL command-line utility. Table 10.2 describes the WDSUTIL command-line options.

TABLE 10.2 WDSUTIL command-line options

WDSUTIL option	Description
`/initialize-server`	Initializes the configuration of the WDS server
`/uninitialized -server`	Undoes any changes made during the initialization of the WDS server
`/add`	Adds images and devices to the WDS server
`/convert-ripimage`	Converts Remote Installation Preparation (RIPrep) images to WIM images
`/remove`	Removes images from the server
`/set`	Sets information in images, image groups, WDS servers, and WDS devices
`/get`	Gets information from images, image groups, WDS servers, and WDS devices
`/new`	Creates new capture images or discover images
`/copy- image`	Copies images from the image store
`/export-image`	Exports to WIM files images contained within the image store
`/start`	Starts WDS services
`/stop`	Stops WDS services
`/disable`	Disables WDS services
`/enable`	Enables WDS services
`/approve-autoadddevices`	Approves Auto-Add devices
`/reject-autoadddevices`	Rejects Auto-Add devices
`/delete-autoadddevices`	Deletes records from the Auto-Add database
`/update`	Uses a known good resource to update a server resource

The first step in setting up WDS to deploy operating systems to the clients is to install the WDS role. You do this by using Server Manager.

One of the advantages of using the Windows deployment server is that WDS can work with Windows image (`.wim`) files. Windows image files can be created through the use of the Windows Sysprep utility.

One component to which you need to pay attention when using the Windows deployment server is *Preboot Execution Environment (PXE)* network devices. PXE boot devices are network interface cards (NICs) that can talk to a network without the need for an operating system. PXE boot NIC adapters are network adapters that have a set of preboot commands within the boot firmware.

This is important when using WDS because PXE boot adapters connect to a WDS server and request the data needed to load the operating system remotely. Remember, most of these machines for which you are using WDS do not have an operating system on the computer. You need NIC adapters that can connect to a network without the need for an operating system for WDS to work properly.

For the same reason, you must set up DHCP to accept PXE machines. Those machines need a valid TCP/IP address so that they can connect to the WDS server.

Installing the WDS Services Using PowerShell

As we have stated multiple times throughout this book, we will show you how to do many of these tasks using the Windows PowerShell commands. Table 10.3 describes many of the WDS cmdlets that you can use in Windows Server 2012 R2.

NOTE

This table comes directly from Microsoft TechNet at `http://technet.microsoft.com/library/dn283416.aspx`.

TABLE 10.3 WDSUTIL command-line options

Cmdlet	Description
`Add-WdsDriverPackage`	Adds an existing driver package to a driver group or injects it into a boot image
`Approve-WdsClient`	Approves clients
`Copy-WdsInstallImage`	Copies install images within an image group
`Deny-WdsClient`	Denies approval for clients
`Disable-WdsBootImage`	Disables a boot image

TABLE 10.3 WDSUTIL command-line options *(continued)*

Cmdlet	Description
`Disable-WdsDriverPackage`	Disables a driver package in the Windows Deployment Services driver store
`Disable-WdsInstallImage`	Disables an install image
`Disconnect-WdsMulticastClient`	Disconnects a multicast client from a transmission or namespace
`Enable-WdsBootImage`	Enables a boot image
`Enable-WdsDriverPackage`	Enables a driver package in the Windows Deployment Services driver store
`Enable-WdsInstallImage`	Enables an install image
`Export-WdsBootImage`	Exports an existing boot image from an image store
`Export-WdsInstallImage`	Exports an existing install image from an image store
`Get-WdsBootImage`	Gets properties of boot images from the image store
`Get-WdsClient`	Gets client devices from the pending device database, or pre-staged devices from Active Directory or the standalone server device database.
`Get-WdsDriverPackage`	Gets properties of driver packages from the Windows Deployment Services driver store
`Get-WdsInstallImage`	Gets properties of install images from an image store
`Get-WdsInstallImageGroup`	Gets properties of install image groups
`Get-WdsMulticastClient`	Gets a list of clients connected to a multicast transmission or namespace
`Import-WdsBootImage`	Imports a boot image to the image store
`Import-WdsDriverPackage`	Imports a driver package into the Windows Deployment Services driver store
`Import-WdsInstallImage`	Imports an install image to an image store
`New-WdsClient`	Creates a prestaged client

`New-WdsInstallImageGroup`	Creates an install image group
`Remove-WdsBootImage`	Removes a boot image from the image store
`Remove-WdsClient`	Removes a prestaged client from AD DS or the stand-alone server device database or clears the Pending Devices database
`Remove-WdsDriverPackage`	Removes a driver package from a driver group or removes it from all driver groups and deletes it
`Remove-WdsInstallImage`	Removes an install image from an image store
`Remove-WdsInstallImageGroup`	Removes an install image group
`Set-WdsBootImage`	Modifies settings of a boot image
`Set-WdsClient`	Modifies a prestaged client device
`Set-WdsInstallImage`	Modifies the properties of an install image
`Set-WdsInstallImageGroup`	Modifies the name and access permissions of an install image group

Preparing the WDS Client

The WDS client is the computer on which Windows 7 or Windows 8 will be installed. WDS clients rely on PXE technology, which allows the client computer to remotely boot and connect to a WDS server.

To act as a WDS client, the computer must meet all of the hardware requirements for Windows 7 or Windows 8 and have a PXE-capable network adapter installed. In addition, a WDS server must be present on the network. Furthermore, the user account used to install the image must be a member of the Domain Users group in Active Directory.

After the WDS server has been installed and configured, you can install Windows 7 or Windows 8 on a WDS client that uses a PXE-compliant network card.

To install Windows 7 or Windows 8 on the WDS client, follow these steps:

1. Start the computer. When prompted, press F12 for a network service boot. The Windows PE appears.
2. The Windows Welcome screen appears. Click the Next button to start the installation process.
3. Enter the username and password of an account that has permissions to access and install images from the WDS server.

4. A list of available operating system images stored on the WDS server appears. Select the image to install and click Next.
5. Enter the product key for the selected Windows 7 or Windows 8 image and click Next.
6. The Partition And Configure The Disk screen appears. Select the desired disk-partitioning options or click OK to use the default options.
7. Click Next to initiate the image-copying process. The Windows Setup process will begin after the image is copied to the WDS client computer.

Configuring Windows Server Update Services

To keep your Windows operating systems up-to-date and secure, you can use Windows Update, Automatic Updates, WSUS, and the Microsoft Baseline Security Analyzer.

Windows Update This utility attaches to the Microsoft website through a user-initiated process, and it allows Windows users to update their operating systems by downloading updated files (critical and noncritical software updates).

Automatic Updates This utility extends the functionality of Windows Update by automating the process of updating critical files. With Automatic Updates, you can specify whether you want updates to be downloaded and installed automatically or whether you just want to be notified when updates are available.

Windows Server Update Services (WSUS) This utility is used to deploy a limited version of Windows Update to a corporate server, which in turn provides the Windows updates to client computers within the corporate network. This allows clients that are limited to what they can access through a firewall to be able to keep their Windows operating systems up-to-date.

Microsoft Baseline Security Analyzer (MBSA) You can download this utility from the Microsoft website to ensure you have the most current security updates.

In the following sections, you will learn how to use these tools.

Windows Update

Windows Update is available through the Microsoft website, and it is used to provide the most current files for Windows operating systems. Examples of updates include security fixes, critical updates, updated help files, and updated drivers.

You can download Windows Update through the Help And Support page on the Microsoft website. Once it's installed, click the Scan For Updates link on the Welcome To Windows Update screen to search for new updates.

The results of the Windows Update search will be displayed on the left side of the Windows Update screen. You will see the following options:

Pick Updates To Install This lists what updates are available for your computer, and it includes the following categories:

- Critical Updates And Service Packs
- Windows Server 2012 R2 Family
- Driver Updates

Review And Install Updates This allows you to view all of the updates that you have selected to install, and it installs the updates.

View Installation History This allows you to track all of the updates that you have applied to your server.

Personalize Windows Update This customizes what you see when you use Windows Update.

Get Help And Support This displays help and support information about Windows Update.

Sometimes the updates that are installed require the computer to be restarted before they can take effect. In this event, Windows Update uses a technology called *chained installation*. With chained installation, all updates that require a computer restart are applied before the computer is restarted. This eliminates the need to restart the computer more than once.

The information that is collected by Windows Update includes the operating system and version number, the Internet Explorer version, the software version information for any software that can be updated through Windows Update, the Plug and Play ID numbers for installed hardware, and the region and language settings. Windows Update will also collect the product ID and product key to confirm that you are running a licensed copy of Windows, but this information is retained only during the Windows Update session and it is not stored. No personal information that can be used to identify users of the Windows Update service is collected.

Windows Automatic Updates

The *Automatic Updates* application extends the functionality of Windows Update by automating the update process. With Automatic Updates, Windows Server 2012 R2 recognizes when you have an Internet connection and will automatically search for any updates for your computer from the Windows Update website.

If any updates are identified, they will be downloaded using *Background Intelligent Transfer Services (BITS)*. BITS is a bandwidth-throttling technology that allows downloads

to occur using idle bandwidth only. This means that downloading automatic updates will not interfere with any other Internet traffic.

If Automatic Updates detects any updates for your computer, you will see an update icon in the notification area of the taskbar.

> **NOTE** To configure Automatic Updates, you must have local administrative rights to the computer on which Automatic Updates is being configured. Requiring administrative rights prevents users from specifying that critical security updates not be installed. In addition, Microsoft must digitally sign any updates that are downloaded.

You configure Automatic Updates by selecting Start ➢ Control Panel ➢ Windows Update. You will see the Check For Updates button shown in Figure 10.1.

FIGURE 10.1 Windows Update control panel

You enable Automatic Updates by clicking the Change Settings link. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates (see Figure 10.2).

FIGURE 10.2 Change Settings window of the Windows Update control panel

Using Windows Server Update Services

Windows Server Update Services (WSUS), formerly known as Software Update Services (SUS), is used to leverage the features of Windows Update within a corporate environment. WSUS downloads Windows updates to a corporate server, which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment. WSUS is designed to work in medium-sized corporate networks that are not using System Center Essentials 2012 R2.

Advantages of Using WSUS

Using WSUS has many advantages:

- It allows an internal server within a private intranet to act as a virtual Windows Update server.
- Administrators have selective control over what updates are posted and deployed from the public Windows Update site. No updates are deployed to client computers unless an administrator first approves them.

- Administrators can control the synchronization of updates from the public Windows Update site to the WSUS server either manually or automatically.
- Administrators can configure Automatic Updates on client computers to access the local WSUS server as opposed to the public Windows Update site.
- WSUS checks each update to verify that Microsoft has digitally signed it. Any updates that are not digitally signed are discarded.
- Administrators can selectively specify whether clients can access updated files from the intranet or from Microsoft's public Windows Update site, which is used to support remote clients.
- Administrators can deploy updates to clients in multiple languages.
- Administrators can configure client-side targeting to help client machines get updates. Client-side targeting allows your organization's computers to automatically add themselves to the computer groups that were created in the WSUS console.
- Administrators can configure a WSUS statistics server to log update access, which allows them to track which clients have installed updates. The WSUS server and the WSUS statistics server can coexist on the same computer.
- Administrators can manage WSUS servers remotely using HTTP or HTTPS if their web browser is Internet Explorer 6.0 or newer.

WSUS Server Requirements

To act as a WSUS server, the server must meet the following requirements:

- It must be running Windows 2000 Server with Service Pack 4 or newer, Windows Server 2003 SP1 or greater, Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- It must have all of the most current security patches applied.
- It must be running Internet Information Services (IIS) 6.0 or newer.
- It must be connected to the network.
- It must have an NTFS partition with 100MB free disk space to install the WSUS server software, and it must have 6GB of free space to store all of the update files.
- It must use BITS version 2.0.
- It must use Microsoft Management Console 3.0.
- It must use Microsoft Report Viewer Redistributable 2008.

If your WSUS server meets the following system requirements, it can support up to 15,000 WSUS clients:

- Pentium III 700MHz processor
- 512MB of RAM

Installing the WSUS Server

WSUS should run on a dedicated server, meaning that the server will not run any other applications except IIS, which is required. Microsoft recommends that you install a clean or new version of Windows Server 2003 SP1 or newer, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 and apply any service packs or security-related patches.

Exercise 10.1 walks you through the installation process for WSUS.

EXERCISE 10.1

Installing a WSUS Server

1. Choose Server Manager by clicking the Server Manager icon on the taskbar.
2. Click option number 2, Add Roles And Features.
3. Choose role-based or featured-based installation and click Next.
4. Choose your server and click Next.
5. Choose Windows Server Update Service. Click the Add Features button when the dialog box appears. Then click Next.
6. At the Select features screen, just click Next.
7. At the Windows Server Update Services screen, click Next.
8. At the Select Role Services screen, make sure that WID Database and WSUS Services are both checked. Click Next.

EXERCISE 10.1 *(continued)*

9. At the Content Location Selection screen, uncheck the box Store Updates In The Following Location and click Next. When you uncheck this box, updates are not stored locally. They are downloaded from Microsoft only once they are approved. This will help save hard drive space.

10. At the Confirmation screen, click the Install button.

11. The installation will begin, and you will see the progress. Once the installation is complete, click Close.

12. In Server Manager, click the WSUS link on the left side. Then click the More link next to Configuration Required For Windows Server Update Services.

13. At the All Servers Task Details And Notifications screen, click the Launch Post-Installation Tasks link.

14. The installation process will automatically continue. Once it is finished, you will see Complete under Stage. Close the All Servers Task Details And Notifications screen.

15. Close Server Manager.

16. If a WSUS Configure Options box appears, just close it. You will set options in the next exercise.

Configuring a WSUS Server

Configuring a WSUS machine is a straightforward process. The easiest way to do it is to use the WSUS Server Configuration Wizard. This wizard walks you through the WSUS setup process, and it makes it easy to configure WSUS. When in the WSUS snap-in, you can configure different options.

Update Source And Proxy Server This option allows you to configure whether this WSUS server synchronizes either from Microsoft Update or from another WSUS server on your network.

Products And Classifications This option allows you to select the products for which you want to get updates and the type of updates that you want to receive.

Update Files And Languages This option allows you to choose whether to download update files and where to store these update files. This option also allows you to choose which update languages you want downloaded.

Automatic Approvals This option allows you to specify how to approve installation of updates automatically for selected groups and how to approve revisions to existing updates.

Synchronization Schedule This option allows you to configure how and when you synchronize your updates. Administrators can choose to synchronize manually or to set up a schedule for daily automatic synchronization.

Computers This option allows you to set computers to groups or use Group Policy or registry settings on the computer to receive updates.

Server Cleanup Wizard This option allows you to clean out old computers, updates, and update files from your server.

Reporting Rollup This option allows you to choose whether to have replica downstream servers roll up computer and update status to this WSUS server.

Email Notifications This option allows you to set up email notifications for WSUS. You can be notified when new updates are synchronized, or you can get email status reports. This option also allows you to set up the email server's information on your WSUS server.

Microsoft Update Improvement Program This option allows you to choose whether you want to participate in the Microsoft Update Improvement program. When you choose to participate in this program, your WSUS server will automatically send information to Microsoft about the quality of your updates. This following information is included:

- How many computers are in the organization
- How many computers successfully installed each update
- How many computers failed to install each update

Personalization This option allows you to personalize the way that information is displayed for this server. This option also allows you to set up a to-do list for WSUS.

WSUS Server Configuration Wizard This option allows you to set up many of the preceding options by just using this one setup wizard.

In Exercise 10.2, you will learn how to set up some of the WSUS server options. To complete this exercise, you need to have an Internet connection that can communicate with Microsoft.

EXERCISE 10.2

Setting WSUS Server Options

1. Open the Windows Server Update Services snap-in from Administrative Tools by pressing the Windows key on the keyboard and then choosing Administrative Tools. The Windows Server Update Services snap-in will be at the bottom of the list alphabetically.

2. On the left side, click the name of your server. Then, in the middle section under To Do, click the Options link.

EXERCISE 10.2 *(continued)*

3. A WSUS Server Configuration Wizard appears at the bottom of the options list. Click this link.
4. Click Next at the Before You Begin screen.
5. At the Join Microsoft Update Improvement Program screen, uncheck the Yes box and click Next.
6. At the Choose Upstream Server screen, choose Synchronize From Microsoft Update and click Next.
7. Fill in the information at the Specify Proxy Server screen if you need to use a proxy server. If you do not need a proxy server, just click Next.
8. At the Connect To Upstream Server screen, click the Start Connecting button. This step can take a few minutes depending on your connection speed. Once it's finished connecting, click Next.

9. At the Choose Products screen, scroll down and choose the products for which you want to receive updates. Then click Next.

10. At the Choose Classifications screen, choose the classifications of updates you would like and click Next.

11. The Set Sync Schedule screen will appear next. At this screen, you can choose whether you want manual or automatic synchronizations. For this exercise, choose Synchronize Manually and click Next.

12. At the Finish screen, you can click Begin Initial Synchronization and click Finish. Be advised, this initial sync can take some time to finish. So if you don't have time to complete it now, you can always synchronize later.

13. Close WSUS.

Testing and Approving Updates

The administrator should test and approve updates before they are deployed to WSUS clients. The testing should be done on a test machine that is not used for daily tasks.

To approve updates, from the welcome screen, click Updates on the site's toolbar. Make your settings on the Updates page that appears.

Viewing the Synchronization Log

To view the synchronization log, click the Reports button on the site's toolbar from the welcome screen. The Reports page will appear. Click Synchronization Results to view the results.

Configuring a Disconnected Network

You have the ability to use WSUS on a disconnected network. To do so, you download the updates to the Internet-connected WSUS server. After the download is complete, you can export the updates and then import the updates to the disconnected network.

WSUS Client Requirements

WSUS clients run a special version of Automatic Updates that is designed to support WSUS. The following enhancements to Automatic Updates are included:

- Clients can receive updates from a WSUS server as opposed to the public Microsoft Windows Update site.
- The administrator can schedule when the downloading of updated files will occur.
- Clients can be configured via Group Policy or through editing the registry.
- Updates can occur when an administrative account or nonadministrative account is logged on.

The following client platforms are the only ones that WSUS currently supports:

- Windows XP Home Edition (with Service Pack 3)
- Windows XP Professional (with Service Pack 3)
- Windows Server 2003 (SP1 or newer)
- Windows Vista (all platforms)
- Windows 7 (all platforms)
- Windows 8 (all platforms)
- Windows Server 2008 and 2008 R2 (all platforms)
- Windows Server 2012 R2 (all platforms)

Configuring the WSUS Clients

You can configure WSUS clients in two ways. The method you use depends on whether you use Active Directory in your network.

In a nonenterprise network (not running Active Directory), you would configure Automatic Updates through the Control Panel using the same process that was defined in the section "Windows Automatic Updates" earlier in this chapter. Each client's registry would then be edited to reflect the location of the server providing the automatic updates.

Within an enterprise network, using Active Directory, you would typically see Automatic Updates configured through Group Policy. Group Policy is used to manage configuration and security settings via Active Directory. Group Policy is also used to specify what server a client will use for Automatic Updates. If Automatic Updates is configured through Group Policy, the user will not be able to change Automatic Updates settings by choosing Control Panel ➢ System (for XP) or Windows Update (for Windows 8, Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2).

Configuring a Client in a Non–Active Directory Network

The easiest way to configure the client to use Automatic Updates is through the control panel. However, you can also configure Automatic Updates through the registry. The registry is a database of all your server settings. You can access it by choosing Start ➢ Run and typing **`regedit`** in the Run dialog box. Automatic Updates settings are defined through `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU`.

Table 10.4 lists some of the registry options that you can configure for Automatic Updates.

TABLE 10.4 Selected registry keys and values for Automatic Updates

Registry key	Options for values
`NoAutoUpdate`	0: Automatic Updates are enabled (default).
	1: Automatic Updates are disabled.
	2: Notify of download and installation.
	3: Autodownload and notify of installation.
	4: Autodownload and schedule installation.
	5: Automatic Updates is required, but end users can configure.
`ScheduledInstallDay`	1: Sunday.
	2: Monday.
	3: Tuesday.
	4: Wednesday.
	5: Thursday.
	6: Friday.
	7: Saturday.
`UseWUServer`	0: Use public Microsoft Windows Update site.
	1: Use server specified in `WUServer` entry.

To specify what server will be used as the Windows Update server, you edit two registry keys, which are found here:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate
```

- The `WUServer` key sets the Windows Update server using the server's HTTP name—for example, `http://intranetSUS`.
- The `WUStatusServer` key sets the Windows Update intranet WSUS statistics server by using the server's HTTP name—for example, `http://intranetSUS`.

Configuring a Client in an Active Directory Network

If the WSUS client is part of an enterprise network using Active Directory, you would configure the client via Group Policy. In Exercise 10.3, we will walk you through the steps needed to configure the Group Policy object (GPO) for WSUS clients. The *Group Policy Management Console (GPMC)* needs to be installed to complete this exercise. If you don't have the GPMC installed, you can install it using the Server Manager utility.

EXERCISE 10.3

Configuring a GPO for WSUS

1. Open the GPMC by pressing the Windows key and selecting Administrative Tools ➢ Group Policy Management.
2. Expand the forest, domains, and your domain name. Under your domain name, click Default Domain Policy. Right-click and choose Edit.
3. Under the Computer Configuration section, expand Policies ➢ Administrative Templates ➢ Windows Components ➢ Windows Update.
4. In the right pane, double-click the Configure Automatic Updates option. The Configure Automatic Updates Properties dialog box appears. Click the Enabled button. Then, in the drop-down list, choose Auto Download And Notify For Install. Click OK.
5. Double-click Specify Intranet Microsoft Update Service Location Properties. This setting allows you to specify the server from which the clients will get the updates. Click Enabled. In the two server name boxes, enter **//servername** (the name of the server on which you installed WSUS in Exercise 10.1). Click OK.
6. To configure the rescheduling of automatic updates, double-click Reschedule Automatic Updates Scheduled Installations. You can enable and schedule the amount of time that Automatic Updates waits after system startup before it attempts to proceed with a scheduled installation that was previously missed. Click Enabled. Enter **10** in the Startup (Minutes) box. Click OK.
7. To configure auto-restart for scheduled Automatic Updates installations, double-click No Auto-Restart For Scheduled Automatic Updates Installations. When you enable this option, the computer is not required to restart after an update. Enable this option and click OK.
8. Close the GPMC.

Configuring Client-Side Targeting

Administrators can use a GPO to enable client-side targeting. Client machines can be automatically added into the proper computer group once the client computer connects to the WSUS server. Client-side targeting can be a very useful tool when an administrator has multiple client computers and the administrator needs to automate the process of assigning those computers to computer groups.

Administrators can enable client-side targeting on the WSUS server by clicking the Use Group Policy or registry settings on client computers option on the Computers Options page.

1. On the WSUS console toolbar, click Options and then click Computer Options.
2. In Computer Options, choose one of the following options:
   - If an administrator wants to create groups and assign computers through the WSUS console (server-side targeting), click Use The Move Computers Task In Windows Server Update Services.
   - If an administrator wants to create groups and assign computers by using Group Policy settings on the client computer (client-side targeting), click Use Group Policy Or Registry Settings On Computers.
3. Under Tasks, click the Save Settings button and then click OK.

Overview of Windows Server 2012 R2 Performance Monitoring

The first step in any performance optimization strategy is to measure performance accurately and consistently. The insight that you'll gain from monitoring factors such as network and system utilization will be extremely useful when you measure the effects of any changes.

The overall performance monitoring process usually involves the following steps:

1. Establish a baseline of current performance.
2. Identify the bottlenecks.
3. Plan for and implement changes.
4. Measure the effects of the changes.
5. Repeat the process based on business needs.

Note that the performance optimization process is never really finished because you can always try to gain more performance from your system by modifying settings and applying other well-known tweaks. Before you get discouraged, realize that you'll reach some level of performance that you and your network and system users consider acceptable and that it's not worth the additional effort it will take to optimize performance any further. Also note that as your network and system load increases (more users or users doing more), so

too will the need to reiterate this process. By continuing to monitor, measure, and optimize, you will keep ahead of the pack and keep your end users happy.

Now that you have an idea of the overall process, let's focus on how changes should be made. It's important to keep in mind the following ideas when monitoring performance:

Plan Changes Carefully Here's a rule of thumb that you should always try to follow: An hour of planning can save a week of work. When you are working in an easy-to-use GUI-based operating system like Windows Server 2012 R2, it's tempting to remove a check mark here or there and then retest the performance. You should resist the urge to do this because some changes can cause large decreases in performance or can impact functionality. Before you make haphazard changes (especially on production servers), take the time to learn about, plan for, and test your changes. Plan for outages and testing accordingly.

Utilize a Test Environment Test in a test lab that simulates a production environment. Do not make changes on production environments without first giving warning. Ideally, change production environments in off-hours when fewer network and system users will be affected. Making haphazard changes in a production environment can cause serious problems. These problems will likely outweigh any benefits that you may receive from making performance tweaks.

Make Only One Change at a Time The golden rule of scientific experiments is that you should always keep track of as many variables as possible. When the topic is server optimization, this roughly translates into making only one change at a time.

One of the problems with making multiple system changes is that although you may have improved overall performance, it's hard to determine exactly *which* change created the positive effects. It's also possible, for example, that changing one parameter increased performance greatly while changing another decreased it only slightly. Although the overall result was an increase in performance, you should identify the second, performance-reducing option so that the same mistake is not made again. To reduce the chance of obtaining misleading results, always try to make only one change at a time.

The main reason to make one change at a time, however, is that if you do make a mistake or create an unexpected issue, you can easily "back out" of the change. If you make two or three changes at the same time and are not sure which one created the problem, you will have to undo all of the changes and then make one alteration at a time to find the problem. If you make only one change at a time and follow that methodology every time, you won't find yourself in this situation.

WARNING

It's important to remember that many changes (such as registry changes) take place immediately; they do not need to be applied explicitly. Once the change is made, it's live. Be careful to plan your changes wisely.

Ensure Consistency in Measurements When you are monitoring performance, consistency is extremely important. You should strive to have repeatable and accurate measurements. Controlling variables, such as system load at various times during the day, can help.

Assume, for instance, that you want to measure the number of transactions that you can simulate on the accounting database server within an hour. The results would be widely different if you ran the test during the month-end accounting close than if you ran the test on a Sunday morning. By running the same tests when the server is under a relatively static load, you will be able to get more accurate measurements.

Maintain a Performance History In the introduction to this chapter, I mentioned that the performance optimization cycle is a continuous improvement process. Because many changes may be made over time, it is important to keep track of the changes that have been made and the results you have experienced. Documenting this knowledge will help solve similar problems if they arise. I understand that many IT professionals do not like to document, but documentation can make life much easier in the long run.

As you can see, you need to keep a lot of factors in mind when optimizing performance. Although this might seem like a lot to digest and remember, do not fear. As a system administrator, you will learn some of the rules you need to know to keep your system running optimally. Fortunately, the tools included with Windows Server 2012 R2 can help you organize the process and take measurements. Now that you have a good overview of the process, let's move on to look at the tools that can be used to set it in motion.

Using Windows Server 2012 R2 Performance Tools

Because performance monitoring and optimization are vital functions in network environments of any size, Windows Server 2012 R2 includes several performance-related tools.

Introducing Performance Monitor

The first and most useful tool is the Windows Server 2012 R2 *Performance Monitor*, which was designed to allow users and system administrators to monitor performance statistics for various operating system parameters. Specifically, you can collect, store, and analyze information about CPU, memory, disk, and network resources using this tool, and these are only a handful of the things that you can monitor. By collecting and analyzing performance values, system administrators can identify many potential problems.

You can use the Performance Monitor in the following ways:

Performance Monitor ActiveX Control The Windows Server 2012 R2 Performance Monitor is an ActiveX control that you can place within other applications. Examples of applications that can host the Performance Monitor control include web browsers and client programs such as Microsoft Word or Microsoft Excel. This functionality can make it easy for applications developers and system administrators to incorporate the Performance Monitor into their own tools and applications.

Performance Monitor MMC For more common performance monitoring functions, you'll want to use the built-in Microsoft Management Console (MMC) version of the Performance Monitor.

System Stability Index The *System Stability Index* is a numerical value from 1 (least stable) to 10 (most stable) that represents the stability of your network. Performance Monitor calculates and creates the System Stability Index. You can view a graph of this index value. The graph can help a network administrator identify when the network started encountering problems. The System Stability Index also offers side-by-side comparisons. An administrator can view when system changes occurred (installing applications, devices, or drivers) and when system problems started to occur. This way, you can determine whether any system changes caused the problems that you are encountering.

Data Collector Sets Windows Server 2012 R2 Performance Monitor includes the Data Collector Set. This tool works with performance logs, telling Performance Monitor where the logs are stored and when the log needs to run. The Data Collector Sets also define the credentials used to run the set.

To access the Performance Monitor MMC, you open Administrative Tools and then choose Performance Monitor. This launches the Performance MMC and loads and initializes Performance Monitor with a handful of default counters.

You can choose from many different methods of monitoring performance when you are using Performance Monitor. A couple of examples are listed here:

- You can look at a snapshot of current activity for a few of the most important counters. This allows you to find areas of potential bottlenecks and monitor the load on your servers at a certain point in time.
- You can save information to a log file for historical reporting and later analysis. This type of information is useful, for example, if you want to compare the load on your servers from three months ago to the current load.

You'll get to take a closer look at this method and many others as you examine Performance Monitor in more detail.

In the following sections, you'll learn about the basics of working with the Windows Server 2012 R2 Performance Monitor and other performance tools. Then you'll apply these tools and techniques when you monitor the performance of your network.

Your Performance Monitor grows as your system grows, and whenever you add services to Windows Server 2012 R2 (such as installing Exchange Server 2010), you also add to what you can monitor. You should make sure that, as you install services, you take a look at what it is you can monitor.

Deciding What to Monitor

The first step in monitoring performance is to decide *what* you want to monitor. In Windows Server 2012 R2, the operating system and related services include hundreds of performance

statistics that you can track easily. For example, you may want to monitor IPsec by monitoring connection security rules. This is just one of many items that can be monitored. All performance statistics fall into three main categories that you can choose to measure:

Performance Objects A *performance object* within Performance Monitor is a collection of various performance statistics that you can monitor. Performance objects are based on various areas of system resources. For example, there are performance objects for the processor and memory as well as for specific services such as web services.

Counters *Counters* are the actual parameters measured by Performance Monitor. They are specific items that are grouped within performance objects. For example, within the Processor performance object, there is a counter for % Processor Time. This counter displays one type of detailed information about the Processor performance object (specifically, the amount of total CPU time all of the processes on the system are using). Another set of counters you can use will allow you to monitor print servers.

Instances Some counters will have instances. An *instance* further identifies which performance parameter the counter is measuring. A simple example is a server with two CPUs. If you decide you want to monitor processor usage (using the Processor performance object)—specifically, utilization (the % Total Utilization counter)—you must still specify *which* CPU(s) you want to measure. In this example, you would have the choice of monitoring either of the two CPUs or a total value for both (using the Total instance).

To specify which performance objects, counters, and instances you want to monitor, you add them to Performance Monitor using the Add Counters dialog box. Figure 10.3 shows the various options that are available when you add new counters to monitor using Performance Monitor.

FIGURE 10.3 Adding a new Performance Monitor counter

The items that you will be able to monitor will be based on your hardware and software configuration. For example, if you have not installed and configured the IIS, the options available within the Web Server performance object will not be available. Or, if you have multiple network adapters or CPUs in the server, you will have the option of viewing each instance separately or as part of the total value.

Viewing Performance Information The Windows Server 2012 R2 Performance Monitor was designed to show information in a clear and easy-to-understand format. Performance objects, counters, and instances may be displayed in each of three views. This flexibility allows system administrators to define quickly and easily the information they want to see once and then choose how it will be displayed based on specific needs. Most likely, you will use only one view, but it's helpful to know what other views are available depending on what it is you are trying to assess.

You can use the following main views to review statistics and information on performance:

Graph View The *Graph view* is the default display that is presented when you first access the Windows Server 2012 R2 Performance Monitor. The chart displays values using the vertical axis and displays time using the horizontal axis. This view is useful if you want to display values over a period of time or see the changes in these values over that time period. Each point that is plotted on the graph is based on an average value calculated during the sample interval for the measurement being made. For example, you may notice overall CPU utilization starting at a low value at the beginning of the chart and then becoming much higher during later measurements. This indicates that the server has become busier (specifically, with CPU-intensive processes). Figure 10.4 provides an example of the Graph view.

FIGURE 10.4 Viewing information in Performance Monitor Graph view

Histogram View The *Histogram view* shows performance statistics and information using a set of relative bar charts. This view is useful if you want to see a snapshot of the latest value for a given counter. For example, if you were interested in viewing a snapshot of current system performance statistics during each refresh interval, the length of each of the bars in the display would give you a visual representation of each value. It would also allow you to compare measurements visually relative to each other. You can set the histogram to display an average measurement as well as minimum and maximum thresholds. Figure 10.5 shows a typical Histogram view.

FIGURE 10.5 Viewing information in Performance Monitor Histogram view

Report View Like the Histogram view, the *Report view* shows performance statistics based on the latest measurement. You can see an average measurement as well as minimum and maximum thresholds. This view is most useful for determining exact values because it provides information in numeric terms, whereas the Chart and Histogram views provide information graphically. Figure 10.6 provides an example of the type of information you'll see in the Report view.

Managing Performance Monitor Properties

You can specify additional settings for viewing performance information within the properties of Performance Monitor. You can access these options by clicking the Properties button

FIGURE 10.6 Viewing information in Performance Monitor Report view

in the taskbar or by right-clicking the Performance Monitor display and selecting Properties. You can change these additional settings by using the following tabs:

General Tab On the General tab (shown in Figure 10.7), you can specify several options that relate to Performance Monitor views:

FIGURE 10.7 General tab of the Performance Monitor Properties dialog box

- You can enable or disable legends (which display information about the various counters), the value bar, and the toolbar.
- For the Report and Histogram views, you can choose which type of information is displayed. The options are Default, Current, Minimum, Maximum, and Average. What you see with each of these options depends on the type of data being collected. These options are not available for the Graph view because the Graph view displays an average value over a period of time (the sample interval).
- You can also choose the graph elements. By default, the display will be set to update every second. If you want to update less often, you should increase the number of seconds between updates.

Source Tab On the Source tab (shown in Figure 10.8), you can specify the source for the performance information you want to view. Options include current activity (the default setting) or data from a log file. If you choose to analyze information from a log file, you can also specify the time range for which you want to view statistics. We'll cover these selections in the next section.

FIGURE 10.8 Source tab of the Performance Monitor Properties dialog box

Data Tab The Data tab (shown in Figure 10.9) lists the counters that have been added to the Performance Monitor display. These counters apply to the Chart, Histogram, and Report views. Using this interface, you can also add or remove any of the counters and change the properties, such as the width, style, and color of the line and the scale used for display.

Graph Tab On the Graph tab (shown in Figure 10.10), you can specify certain options that will allow you to customize the display of Performance Monitor views. First you can

FIGURE 10.9 The Data tab of the Performance Monitor Properties dialog box

specify what type of view you want to see (Line, Histogram, or Report). Then you can add a title for the graph, specify a label for the vertical axis, choose to display grids, and specify the vertical scale range.

FIGURE 10.10 The Graph tab of the Performance Monitor Properties dialog box

Appearance Tab Using the Appearance tab (see Figure 10.11), you can specify the colors for the areas of the display, such as the background and foreground. You can also specify the fonts that are used to display counter values in Performance Monitor views. You can

FIGURE 10.11 The Appearance tab of the Performance Monitor Properties dialog box

change settings to find a suitable balance between readability and the amount of information shown on one screen. Finally, you can set up the properties for a border.

Now that you have an idea of the types of information Performance Monitor tracks and how this data is displayed, you'll take a look at another feature—saving and analyzing performance data.

Saving and Analyzing Data with Performance Logs and Alerts

One of the most important aspects of monitoring performance is that it should be done over a given period of time (referred to as a *baseline*). So far, I have shown you how you can use Performance Monitor to view statistics in real time. I have, however, also alluded to using Performance Monitor to save data for later analysis. Now let's take a look at how you can do this.

When viewing information in Performance Monitor, you have two main options with respect to the data on display:

View Current Activity When you first open the Performance icon from the Administrative Tools folder, the default option is to view data obtained from current system information. This method of viewing measures and displays various real-time statistics on the system's performance.

View Log File Data This option allows you to view information that was previously saved to a log file. Although the performance objects, counters, and instances may appear to be the same as those viewed using the View Current Activity option, the information itself was actually captured at a previous point in time and stored into a log file.

Log files for the View Log File Data option are created in the Performance Logs And Alerts section of the Windows Server 2012 R2 Performance tool.

Three items allow you to customize how the data is collected in the log files:

Counter Logs *Counter logs* record performance statistics based on the various performance objects, counters, and instances available in Performance Monitor. The values are updated based on a time interval setting and are saved to a file for later analysis.

Circular Logging In *circular logging*, the data that is stored within a file is overwritten as new data is entered into the log. This is a useful method of logging if you want to record information only for a certain time frame (for example, the past four hours). Circular logging also conserves disk space by ensuring that the performance log file will not continue to grow over certain limits.

Linear Logging In *linear logging*, data is never deleted from the log files, and new information is added to the end of the log file. The result is a log file that continually grows. The benefit is that all historical information is retained.

Now that you have an idea of the types of functions that are supported by the Windows Server 2012 R2 Performance tools, you can learn how you can apply this information to the task at hand—monitoring and troubleshooting your Windows network.

Real World Scenario

Real-World Performance Monitoring

In our daily jobs as system engineers and administrators, we come across systems that are in need of our help...and may even ask for it. You, of course, check your Event Viewer and Performance Monitor and perform other tasks that help you troubleshoot. But what is really the most common problem that occurs? From my experience, I'd say that you suffer performance problems many times if your Windows Server 2012 R2 operating system is installed on a subpar system. Either the server hardware isn't enterprise class or the minimum hardware requirements weren't addressed. Most production servers suffer from slow response times, lagging, and so on, because money wasn't spent where it should have been in the first place—on the server's hardware requirements.

Using Other Performance-Monitoring Tools

Performance Monitor allows you to monitor different parameters of the Windows Server 2012 R2 operating system and associated services and applications. However, you can also use three other tools to monitor performance in Windows Server 2012 R2. They are Network Monitor, Task Manager, and Event Viewer. All three of these tools are useful for monitoring different areas of overall system performance and for examining details related to specific system events. In the following sections, you'll take a quick look at these tools and how you can best use them.

The Network Monitor

Although Performance Monitor is a great tool for viewing overall network performance statistics, it isn't equipped for packet-level analysis and doesn't give you much insight into what types of network traffic are traveling on the wire. That's where the Network Monitor tool comes in. *Network Monitor* has two main components: the Network Monitor Agent and the Network Monitor tool.

The Network Monitor Agent is available for use with Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. The agent allows you to track network packets. When you install the Network Monitor Agent, you will also be able to access the Network Segment System Monitor counter.

On Windows Server 2012 R2 computers, you'll see the Network Monitor icon appear in the Administrative Tools program group. You can use the Network Monitor tool to capture data as it travels on your network.

> **NOTE** A version of Network Monitor is available for free with Windows Server 2012 R2. The full version of Network Monitor is available at Microsoft's download server. For more information, see `www.microsoft.com/downloads/`.

Once you have captured the data of interest, you can save it to a capture file or further analyze it using Microsoft Message Analyzer. Experienced network and system administrators can use this information to determine how applications are communicating and the types of data that are being passed via the network.

> **NOTE** For the exam, you don't need to understand the detailed information that Network Monitor displays, but you should be aware of the types of information that you can view and when you should use Network Monitor.

Task Manager

Performance Monitor is designed to allow you to keep track of specific aspects of system performance over time. But what do you do if you want to get a quick snapshot of what the local system is doing? Creating a System Monitor chart, adding counters, and choosing a view is overkill. Fortunately, the Windows Server 2012 R2 Task Manager has been designed to provide a quick overview of important system performance statistics without requiring any configuration. Better yet, it's always readily available.

You can easily access Task Manager in several ways:

- Right-click the Windows taskbar and then click Task Manager.
- Press Ctrl+Alt+Del and then select Task Manager.
- Press Ctrl+Shift+Esc.

Each of these methods allows you to access a snapshot of the current system performance quickly.

Once you access Task Manager, you will see the following five tabs:

Processes Tab The Processes tab shows you all of the processes that are currently running on the local computer. By default, you'll be able to view how much CPU time and memory a particular process is using. By clicking any of the columns, you can quickly sort by the data values in that particular column. This is useful, for example, if you want to find out which processes are using the most memory on your server.

By accessing the performance objects in the View menu, you can add columns to the Processes tab. Figure 10.12 shows a list of the current processes running on a Windows Server 2012 R2 computer.

FIGURE 10.12 Viewing process statistics and information using Task Manager

Performance Tab One of the problems with using Performance Monitor to get a quick snapshot of system performance is that you have to add counters to a chart. Most system administrators are too busy to take the time to do this when all they need is basic CPU and memory information. That's where the Performance tab of Task Manager comes in. Using the Performance tab, you can view details about how memory is allocated on the computer and how much of the CPU is utilized (see Figure 10.13).

FIGURE 10.13 Viewing CPU and memory performance information using Task Manager

Users Tab The Users tab (see Figure 10.14) lists the currently active user accounts. This is particularly helpful if you want to see who is online and quickly log off or disconnect users. You can also send a console message to any remote user in the list by clicking the Send Message button. (The button is grayed out in Figure 10.14 because you cannot send a message to yourself. If you select a different user, the button will be available.)

FIGURE 10.14 Viewing user information using Task Manager

Details Tab The Details tab (see Figure 10.15) shows you what applications are currently running on the system. From this location, you can stop an application from running by right-clicking the application and choosing Stop. You also have the ability to set your affinity level here. By setting the affinity, you can choose which applications will use which processors on your system.

FIGURE 10.15 Viewing applications that are currently running using Task Manager

Services Tab The Services tab (see Figure 10.16) shows you what services are currently running on the system. From this location, you can stop a service from running by right-clicking the service and choosing Stop. The Open Services link launches the Services MMC.

These tabs can be different on Windows Client machines. For example, Windows 7 has six tabs, not five, and Windows 8 has seven tabs.

As you can see, Task Manager is useful for providing important information about the system quickly. Once you get used to using Task Manager, you won't be able to get by without it!

FIGURE 10.16 Viewing services information using Task Manager

Name	PID	Description	Status	Group
WSusCertServer		WSUS Certificate Server	Stopped	
WsusService	4048	WSUS Service	Running	
wmiApSrv		WMI Performance Adapter	Stopped	
WLMS	816	Windows Licensing Monitoring S...	Running	
WIDWriter	1960	Windows Internal Database VSS ...	Running	
VSS		Volume Shadow Copy	Stopped	
vds	2868	Virtual Disk	Running	
VaultSvc	500	Credential Manager	Running	
UI0Detect		Interactive Services Detection	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	1384	Print Spooler	Running	
SNMPTRAP		SNMP Trap	Stopped	
SamSs	500	Security Accounts Manager	Running	
RSoPProv		Resultant Set of Policy Provider	Stopped	
RpcLocator		Remote Procedure Call (RPC) Lo...	Stopped	
PerfHost		Performance Counter DLL Host	Stopped	
NtFrs		File Replication	Stopped	
NTDS	500	Active Directory Domain Services	Running	
NetTcpPortSharing	1820	Net.Tcp Port Sharing Service	Running	
NetTcpActivator	1820	Net.Tcp Listener Adapter	Running	
Netlogon	500	Netlogon	Running	
MSSQL$MICROSOFT##WID	2128	Windows Internal Database	Running	

Make sure that you use Task Manager and familiarize yourself with all that it can do; you can end processes that have become intermittent, kill applications that may hang the system, view NIC performance, and so on. In addition, you can access this tool quickly to get an idea of what could be causing you problems. Event Viewer, Network Monitor, and Performance Monitor are all great tools for getting granular information on potential problems.

Event Viewer

Event Viewer is also useful for monitoring network information. Specifically, you can use the logs to view any information, warnings, or alerts related to the proper functioning of the network. You can access Event Viewer by selecting Administrative Tools ➢ Event Viewer. Clicking any of the items in the left pane displays the various events that have been logged for each item. Figure 10.17 shows the contents of the Directory Service log.

Each event is preceded by a blue *i* icon. That icon designates that these events are informational and do not indicate problems with the network. Rather, they record benign events such as Active Directory startup or a domain controller finding a global catalog server.

FIGURE 10.17 Event Viewer

A yellow warning icon or a red error icon, both of which are shown in Figure 10.18, indicate problematic or potentially problematic events. Warnings usually indicate a problem that wouldn't prevent a service from running but might cause undesired effects with the service in question. For example, I was configuring a site with some fictional domain controllers and IP addresses. My local domain controller's IP address wasn't associated with any of the sites, and Event Viewer generated a warning. In this case, the local domain controller could still function as a domain controller, but the site configuration could produce undesirable results.

Error events almost always indicate a failed service, application, or function. For instance, if the dynamic registration of a DNS client fails, Event Viewer will generate an error. As you can see, errors are more severe than warnings because, in this case, the DNS client cannot participate in DNS at all.

Double-clicking any event opens the Event Properties dialog box, as shown in Figure 10.19, which displays a detailed description of the event.

Event Viewer can display thousands of different events, so it would be impossible to list them all here. The important points of which you should be aware are the following:

- Information events are always benign.
- Warnings indicate noncritical problems.
- Errors indicate show-stopping events.

FIGURE 10.18 Information, errors, and warnings in Event Viewer

FIGURE 10.19 An Event Properties dialog box

Let's discuss some of the logs and the ways you can view data:

Applications and Services The *applications and services logs* are part of Event Viewer where applications (for example, Exchange) and services (DNS) log their events. DFS events would be logged in this part of Event Viewer. An important log in this section is the DNS Server log (see Figure 10.20). This is where all of your DNS events get stored.

FIGURE 10.20 The applications and services DNS Server log

Custom Views *Custom views* allow you to filter events (see Figure 10.21) to create your own customized look. You can filter events by event level (critical, error, warning, and so

FIGURE 10.21 Create Custom View dialog box

on), by logs, and by source. You also have the ability to view events occurring within a specific timeframe. This allows you to look only at the events that are important to you.

Subscriptions *Subscriptions* allow a user to receive alerts about events that you predefine. In the Subscription Properties dialog box (see Figure 10.22), you can define what type of events you want notifications about and the notification method. The Subscriptions section is an advanced alerting service to help you watch for events.

FIGURE 10.22 Subscription Properties dialog box

Microsoft Baseline Security Analyzer

The *Microsoft Baseline Security Analyzer (MBSA)* is a security assessment utility that you can download from the Microsoft website at the following location:

`www.microsoft.com/en-us/download/details.aspx?id=19892`

The filename of the download is `mbsasetup.msi`. It verifies whether your computer has the latest security updates and whether any common security violation configurations have been applied to your computer. MBSA can scan the following programs and operating systems:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7

- Windows 8
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- IIS 5 or newer
- Internet Explorer, versions 6.0 and newer
- SQL Server 7 or newer
- Microsoft Office 2000 or newer
- Windows Media Player, versions 6.4 and newer

To use MBSA, the computer must meet the following requirements:

- It must be running Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- It must be running Internet Explorer 5.01 or newer.
- It must have an XML parser installed for full functionality.
- It must have the Workstation and Server services enabled.
- It must have Client for Microsoft Networks installed.

Using the GUI Version of MBSA

Once you have installed MBSA, you can access it by using the Windows key and choosing Microsoft Baseline Security Analyzer or by opening the command prompt and executing `mbsa.exe`. This opens the Baseline Security Analyzer utility. You can select from Scan A Computer, Scan More Than One Computer, and View Existing Security Reports.

When you click Scan A Computer, the Pick A Computer To Scan dialog box appears. You can specify that you want to scan a computer based on a computer name or IP address. You can also specify the name of the security report that will be generated.

The following are options for the security scan:

- Check For Windows Vulnerabilities
- Check For Weak Passwords
- Check For IIS Vulnerabilities
- Check For SQL Vulnerabilities
- Check For Security Updates

If you use the Check For Security Updates option and are using WSUS, you can specify the name of the WSUS server that should be checked for the security updates.

Once you have made your selections, click Start Scan. When the scan is complete, the security report will be automatically displayed. If you have scanned multiple computers, you can sort the security reports based on issue name or score (worst first or best first).

Using the MBSA Command-Line Utility *mbsacli.exe*

After Microsoft Baseline Security Analyzer has been installed, you can use the command-line utility `mbsacli.exe`. Enter **`mbsacli.exe/hf`** and then customize the command execution with any of the options defined in Table 10.5.

TABLE 10.5 `mbsacli.exe /hf` command-line options

Option	Description
`-h` *`host name[, host name, . . .]`*	Scans the specified host. You can specify that you want to scan multiple host computers by separating the hostnames with commas.
`-fh` *`filename`*	Scans the NetBIOS name of each computer that is to be scanned, and it saves the information as text within a file specified by *`filename`*.
`-i` *`xxxx.xxxx.xxxx.xxxx [, xxxx.xxxx.xxxx.xxxx, . . .]`*	Scans a computer based on the specified IP address. You can scan multiple computers by IP address by separating the IP addresses with commas.
`-fip` *`filename`*	Looks in the text file specified by *`filename`* for IP addresses and scans the computers with those IP addresses. The file can have up to a maximum of 256 IP addresses.
`-d` *`domainname`*	Scans the specified domain.
`-n`	Scans all of the computers on the local network.

Simple Network Management Protocol

The *Simple Network Management Protocol (SNMP)* is a TCP/IP protocol monitor. The SNMP service creates trap messages that are then sent to a trap destination. One way you might use SNMP is to trap messages that don't contain an appropriate hostname for a particular service.

When you set up SNMP, you set up communities. *Communities* are groupings of computers that help monitor each other.

Windows Server 2012 R2 includes SNMP with the operating system. To install the service, you must use Server Manager. In Exercise 10.4, you will walk through the process of installing the SNMP service.

EXERCISE 10.4

Installing SNMP

1. Open Server Manager by clicking the Server Manager icon on the taskbar.
2. Click option number 2, Add Roles And Features.
3. Choose role-based or feature-based installation and click Next.
4. Choose your server and click Next.
5. Click Next at the Select Server Roles screen.
6. When the Select Features window appears, click the SNMP Services check box. If an ADD Features dialog box appears, click the Add Features button. Click Next.
7. The Confirm Installation page appears. Click Install.
8. Click Close. Exit the Server Manager application.

Now that you have installed the SNMP service, you have to set up your community so that you can start trapping messages. As stated earlier, communities are a grouping of computers to help monitor each other. After you have created the initial community, you can add other computer systems to the community.

In Exercise 10.5, you will walk through the steps to set up the SNMP service and also set up your first community name. To complete this exercise, you must have completed Exercise 10.4.

EXERCISE 10.5

Configuring SNMP

1. Open Computer Management by pressing the keyboard's Windows Key and selecting Administrative Tools ➢ Computer Management.
2. Expand Services And Applications. Click Services. In the right pane, double-click SNMP Service.
3. The SNMP Service Properties window will open. Click the Traps tab. In the Community Name box, enter **Community1**. Click the Add To List button.

4. Click the General tab. Click the Start button to start the service. Click OK.
5. Close Computer Management.

Summary

This chapter began with a discussion of WSUS and what Windows Update can do for your network. You learned why you would want to use a WSUS server instead of having clients manually connect to the Internet to receive their updates.

The chapter also covered file server and print server optimization and reliability, including many tools that can help you monitor and manage your systems and the basics of troubleshooting the network in times of disaster.

Monitoring performance on servers is imperative to rooting out any issues that may affect your network. If your systems are not running at their best, your end users may experience issues such as latency, or worse, you may experience corruption in your network data. Either way, it's important to know how to monitor the performance of your servers. You also looked at ways system administrators can optimize the operations of servers to ensure that end users experience adequate performance.

You also examined how to use the various performance-related tools that are included with Windows Server 2012 R2. Tools such as Performance Monitor, Task Manager, Network Monitor, and Event Viewer can help you diagnose and troubleshoot system performance issues. These tools will help you find typical problems related to memory, disk space, and any other hardware-related issues you may experience. Knowing how to use tools to troubleshoot and test your systems is imperative, not only to passing the exam but also

to performing your duties at work. To have a smoothly running network environment, it is vital that you understand the issues related to the reliability and performance of your network servers and domain controllers.

Exam Essentials

Understand WSUS. Windows Server Update Services is one way to have your end users receive important updates from Microsoft. WSUS gives administrators the ability to download, test, and approve updates before they get released onto the network.

Understand the methodology behind troubleshooting performance. By following a set of steps that involves making measurements and finding bottlenecks, you can systematically troubleshoot performance problems.

Be familiar with the features and capabilities of the Windows Server 2012 R2 Performance Monitor tool for troubleshooting performance problems. The Performance Monitor administrative tool is a powerful method for collecting data about all areas of system performance. Through the use of performance objects, counters, and instances, you can choose to collect and record only the data of interest and use this information for pinpointing performance problems.

Know the importance of common performance counters. Several important performance-related counters deal with general system performance. Know the importance of monitoring memory, print server, CPU, and network usage on a busy server.

Understand the role of other troubleshooting tools. Windows Task Manager, Network Monitor, SNMP, Baseline Security Analyzer, and Event Viewer can all be used to diagnose and troubleshoot configuration- and performance-related issues.

Understand how to troubleshoot common sources of server reliability problems. Windows Server 2012 R2 has been designed to be a stable, robust, and reliable operating system. Should you experience intermittent failures, you should know how to troubleshoot device drivers and buggy system-level software.

Review Questions

1. You need to stop an application from running in Task Manager. Which tab would you use to stop an application from running?
   - **A.** Performance
   - **B.** Users
   - **C.** Options
   - **D.** Details

2. You are the network administrator for a Fortune 500 company. You are responsible for all client computers at the central campus. You want to make sure that all of the client computers are secure. You decide to use MBSA to scan your client computers for possible security violations. You want to use the command-line version of MBSA to scan your computers based on IP address. Which of the following commands should you use?
   - **A.** `mdsacli.exe /hf -i` *`xxxx.xxxx.xxxx.xxxx`*
   - **B.** `mdsacli.exe /ip` *`xxxx.xxxx.xxxx.xxxx`*
   - **C.** `mbsa.exe /hf -ip` *`xxxx.xxxx.xxxx.xxxx`*
   - **D.** `mbsa.exe /ip` *`xxxx.xxxx.xxxx.xxxx`*

3. You are the network administrator for a Fortune 500 company. You are responsible for all client computers at the central campus. You want to make sure that all of the client computers have the most current software installed for their operating systems, including software in the categories Critical Updates and Service Packs, Windows Server 2012 R2 Family, and Driver Updates. You want to automate the process as much as possible, and you want the client computers to download the updates from a central server that you are managing. You decide to use Windows Server Update Services. The WSUS server software has been installed on a server called *WSUSServer*. You want to test the WSUS server before you set up group policies within the domain. You install Windows 8. Which of the following registry entries needs to be made for the client to specify that the client should use WSUSServer for Windows Update? (Choose all that apply.)
   - **A.** Use `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer` and specify 0 data.
   - **B.** Use `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer` and specify 1 for data.
   - **C.** Use `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\WUServer` and specify `http://WSUSServer`.
   - **D.** Use `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\WUServer` and specify `WSUSServer`.
   - **E.** Use `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\WUServer` and specify `http://WSUSServer`.
   - **F.** Use `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\WUServer` and specify `WSUSServer`.

4. You are the administrator of a new Windows Server 2012 R2 machine. You need to install WSUS. From where do you install WSUS?
   - **A.** Add/Remove Programs
   - **B.** Programs
   - **C.** Server Manager
   - **D.** Administrative Tools

5. You are a network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2012 R2. Windows Server Update Services (WSUS) is installed on two servers, SERVERA and SERVERB. SERVERA receives software updates from Microsoft Windows Update servers. You manually synchronized SERVERB with the Windows Update servers, and now you need to complete the WSUS configuration on SERVERB. Which of the following is *not* a step that you might take to complete the configuration of WSUS on SERVERB?
   - **A.** Approve the current updates.
   - **B.** Set SERVERB to receive updates from SERVERA and automatically synchronize with approved updates on SERVERA.
   - **C.** Set SERVERB to draw updates automatically from whichever sources that SERVERA is set to draw from.
   - **D.** Set SERVERB to receive daily updates automatically at a given time.

6. You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2012 R2. All client computers run Windows 7. The company has 16 mobile sales representatives who are all members of the Power Users local group on their computers. From 6 p.m. until 7 a.m., the sales representatives' laptops are usually turned off and disconnected from the corporate network. The mobile sales representatives' computers must receive software updates every day with minimal user interaction. While verifying the recent updates on one of the laptops, you notice that the updates from the Windows Update servers were not applied. On the Automatic Updates tab of the System Properties dialog box of the mobile computer, what should you do to make sure that software updates are applied to the computer? (Choose three.)
   - **A.** Set the scheduled time to every day at 12 a.m.
   - **B.** Select the option Automatically Download The Updates, And Install Them On The Schedule That I Specify.
   - **C.** Select the option Notify Me Before Downloading Any Updates And Notify Me Again Before Installing Them On My Computer.
   - **D.** Select the Keep My Computer Up To Date check box.
   - **E.** Select the option Download The Updates Automatically And Notify Me When They Are Ready To Be Installed.
   - **F.** Set the scheduled time to every day at 12 p.m.

7. You are responsible for managing several Windows Server 2012 R2 domain controller computers in your environment. Recently, a single hard disk on one of these machines failed, and the Active Directory database was lost. You want to perform the following tasks:
   - Determine which partitions on the server are still accessible.
   - Restore as much of the system configuration (including the Active Directory database) as possible.

   Which of the following could be used to help meet these requirements?

   A. Event Viewer

   B. Performance Monitor

   C. A hard disk from another server that is not configured as a domain controller

   D. A valid system state backup from the server

8. You have been hired as a consultant to research a network-related problem at a small organization. The environment supports many custom-developed applications that are not well documented. A manager suspects that some computers on the network are generating excessive traffic and bogging down the network. You want to do the following:
   - Determine which computers are causing the problems.
   - Record and examine network packets that are coming to/from specific machines.
   - View data related only to specific types of network packets.

   What tool should you use to accomplish all of the requirements?

   A. Task Manager

   B. Performance Monitor

   C. Event Viewer

   D. Network Monitor

9. You need to install Microsoft Baseline Security Analyzer. How do you need to do the install?

   A. Download MBSA from Microsoft's website.

   B. Install from Server Manager.

   C. Use Add/Remove Programs.

   D. Install from Programs.

10. While setting up WSUS, you need to configure the server from which you will be getting your Microsoft updates. Under which option would you set this up?

   A. Products And Classifications

   B. Update Files and Languages

   C. Update Source And Proxy Server

   D. Synchronization Schedule

Chapter

11

Manage File Services

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure Distributed File System (DFS)**

- Install and configure DFS namespaces
- Configure DFS Replication Targets
- Configure Replication Scheduling
- Configure Remote Differential Compression settings
- Configure staging
- Configure fault tolerance
- Clone a DFS database
- Recover DFS databases
- Optimize DFS replication

✓ **Configure File Server Resource Manager (FSRM)**

- Install the FSRM role service
- Configure quotas
- Configure file screens
- Configure reports
- Configure file management tasks

✓ **Configure file and disk encryption**

- Configure Bitlocker encryption
- Configure the Network Unlock feature
- Configure Bitlocker policies
- Configure the EFS recovery agent
- Manage EFS and Bitlocker certificates including backup and restore

✓ **Configure advanced audit policies**

- Implement auditing using Group Policy and AuditPol.exe
- Create expression-based
- Create removable device audit policies

In this chapter, I will show you how to set up one of the more important server types: a file server. File servers are important because you need storage allocation where you can store files on your server.

Microsoft Windows Server 2012 R2 is used for all the server types in this chapter. Although other operating systems can be used, this chapter refers only to Windows Server 2012 R2.

Configuring File Server Resource Manager

As an administrator, when you need to control and manage the amount and type of data stored on your servers, Microsoft delivers the tools to help you do just that. The *File Server Resource Manager (FSRM)* is a suite of tools that allows an administrator to place quotas on folders or volumes, filter file types, and create detailed storage reports. These tools allow an administrator to properly plan and implement policies on data as needed.

FSRM Features

Many of the advantages of using FSRM come from all of the included features, which allow administrators to manage the data that is stored on their file servers. Some of the advantages included with FSRM are as follows:

Configure File Management Tasks FSRM allows an administrator to apply a policy or action to data files. Some of the actions that can be performed include the ability to encrypt files or run a custom command.

Configure Quotas Quotas give an administrator the ability to limit how much disk space a user can use on a file server. Administrators have the ability to limit space to an entire volume or to specific folders.

File Classification Infrastructure Administrators can set file classifications and then manage the data more effectively by using these classifications. Classifying files, and then setting policies to those classifications, allows an administrator to set policies on those classifications. These policies include restricting file access, file encryption, and file expirations.

Configure File Screens Administrators can set file screening on a server and limit the types of files that are being stored on that server. For example, an administrator can set a file screen on a server so that any file ending in `.bmp` gets rejected.

Configure Reports Administrators can create reports that show them how data is classified and accessed. They also have the ability to see which users are trying to save unauthorized file extensions.

Installing the FSRM Role Service

Installing FSRM is easy when using either Server Manager or PowerShell. To install using Server Manager, you go into Add Roles And Features and choose File And Storage Services ➢ File Services ➢ File Server Resource Manager. To install FSRM using PowerShell, you use the following command:

```
Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools
```

Configuring FSRM using the Windows GUI version is straightforward, but setting up FSRM using PowerShell is a bit more challenging. Table 11.1 describes some of the PowerShell commands for FSRM.

TABLE 11.1 PowerShell commands for FSRM

PowerShell cmdlet	Description
`Get-FsrmAutoQuota`	Gets auto-apply quotas on a server
`Get-FsrmClassification`	Gets the status of the running file classification
`Get-FsrmClassificationRule`	Gets classification rules
`Get-FsrmFileGroup`	Gets file groups
`Get-FsrmFileScreen`	Gets file screens
`Get-FsrmFileScreenException`	Gets file screen exceptions
`Get-FsrmQuota`	Gets quotas on the server
`Get-FsrmSetting`	Gets the current FSRM settings
`Get-FsrmStorageReport`	Gets storage reports
`New-FsrmAutoQuota`	Creates an auto-apply quota
`New-FsrmFileGroup`	Creates a file group
`New-FsrmFileScreen`	Creates a file screen

TABLE 11.1 PowerShell commands for FSRM *(continued)*

PowerShell cmdlet	Description
`New-FsrmQuota`	Creates an FSRM quota
`New-FsrmQuotaTemplate`	Creates a quota template
`Remove-FsrmClassificationRule`	Removes classification rules
`Remove-FsrmFileScreen`	Removes a file screen
`Remove-FsrmQuota`	Removes an FSRM quota from the server
`Set-FsrmFileScreen`	Changes the configuration settings of a file screen
`Set-FsrmQuota`	Changes the configuration settings for an FSRM quota

Configure File and Disk Encryption

Hardware and software encryption are some of the most important actions you can take as an administrator. You must make sure that if anyone steals hardware from your company or from your server rooms that the data they are stealing is secured and cannot be used. This is where BitLocker can help.

Using BitLocker Drive Encryption

To prevent individuals from stealing your computer and viewing personal and sensitive data found on your hard disk, some editions of Windows come with a new feature called *BitLocker Drive Encryption*. BitLocker encrypts the entire system drive. New files added to this drive are encrypted automatically, and files moved from this drive to another drive or computers are decrypted automatically.

Only Windows 7 Enterprise, Windows 7 Ultimate, Windows 8 Pro, Windows 8 Enterprise, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 include BitLocker Drive Encryption, and only the operating system drive (usually `C:`) or internal hard drives can be encrypted with BitLocker. Files on other types of drives must be encrypted using BitLocker To Go. BitLocker To Go allows you to put BitLocker on removable media such as external hard disks or USB drives.

BitLocker uses a *Trusted Platform Module (TPM)* version 1.2 or newer to store the security key. A TPM is a chip that is found in newer computers. If you do not have a computer with a TPM, you can store the key on a removable USB drive. The USB drive will be required each time you start the computer so that the system drive can be decrypted.

If the TPM discovers a potential security risk, such as a disk error or changes made to the BIOS, hardware, system files, or startup components, the system drive will not be

unlocked until you enter the 48-digit BitLocker recovery password or use a USB drive with a recovery key as a recovery agent.

BitLocker must be set up either within the Local Group Policy editor or through the BitLocker icon in the control panel. One advantage of using BitLocker is that you can prevent any unencrypted data from being copied onto a removable disk, thus protecting the computer.

BitLocker Recovery Password

The BitLocker recovery password is important. Do not lose it, or you may not be able to unlock the drive. Even if you do not have a TPM, be sure to keep your recovery password in case your USB drive becomes lost or corrupted.

BitLocker requires that you have a hard disk with at least two partitions, both formatted with NTFS. One partition will be the system partition that will be encrypted. The other partition will be the active partition that is used to start the computer. This partition will remain unencrypted.

Features of BitLocker

As with any version of Windows, Microsoft continues to improve on the technologies used in Windows Server 2012 R2 and Windows 8. The following sections cover some of the features of BitLocker.

BitLocker Provisioning

In previous versions of BitLocker (Windows Vista and Windows 7), BitLocker provisioning (system and data volumes) was completed during the postinstallation of the BitLocker utility. BitLocker provisioning was done through either the command-line interface (CLI) or the control panel. In the Windows 8/Windows Server 2012 R2 version of BitLocker, an administrator can choose to provision BitLocker before the operating system is even installed.

Administrators have the ability to enable BitLocker prior to the operating system deployment from the Windows Preinstallation Environment (WinPE). BitLocker is applied to the formatted volume, and BitLocker encrypts the volume prior to running the Windows setup process.

If an administrator wants to check the status of BitLocker on a particular volume, the administrator can view the status of the drive either in the BitLocker control panel applet or in Windows Explorer.

Used Disk Space–Only Encryption

Windows 7 BitLocker requires that all data and free space on the drive must be encrypted. Because of this requirement, the encryption process can take a long time on larger volumes.

In Windows 8 BitLocker, administrators have the ability to encrypt either the entire volume or just the space being used. When you choose the Used Disk Space Only option, only the section of the drive that contains data will be encrypted. Because of this, encryption is completed much faster.

Standard User PIN and Password Change

One issue that BitLocker has had in the past is that you need to be an administrator to configure BitLocker on operating system drives. This could become an issue in a large organization because deploying TPM + PIN to a large number of computers can be challenging.

Even with the new operating system changes, administrative privileges are still needed to configure BitLocker, but now your users have the ability to change the BitLocker PIN for the operating system or change the password on the data volumes.

When a user gets to choose their own PIN and password, they normally choose something that has meaning to them and something that is easy to remember. That is a good and bad thing at the same time. It's a good thing because when your users choose their own PIN and password, they normally don't need to write it down—they just know it. It's a bad thing because if anyone knows the user well, they can have an easier time figuring out the person's PIN and password. Even when you allow your users to choose their own PIN and password, make sure you set a GPO to require password complexity.

Network Unlock

One of the new features of BitLocker is called Network Unlock. *Network Unlock* allows administrators to easily manage desktop and servers that are configured to use BitLocker. Network Unlock allows an administrator to configure BitLocker to automatically unlock an encrypted hard drive during a system reboot when that hard drive is connected to their trusted corporate environment. For this to function properly on a machine, there has to be a DHCP driver implementation in the system's firmware.

If your operating system volume is also protected by the TPM + PIN protection, the administrator has to be sure to enter the PIN at the time of the reboot. This protection can actually make using Network Unlock more difficult to use, but they can be used in combination.

Support for Encrypted Hard Drives for Windows

One of the new advantages of using BitLocker is *Full Volume Encryption (FVE)*. BitLocker provides built-in encryption for Windows data files and Windows operating system files. The advantage of this type of encryption is that encrypted hard drives that use *Full Disk Encryption (FDE)* get each block of the physical disk space encrypted. Because each physical block gets encrypted, it offers much better encryption. The only downside to this is that because each physical block is encrypted, it degrades the hard drive speed somewhat. So, as an administrator, you have to decide whether you want better speed or better security on your hard disk.

Windows 7 and 2008 R2 vs. Windows 8 and 2012 R2

The real question is what's the difference between Windows 7/Windows 2008 R2 and Windows 8/Windows Server 2012 R2? Table 11.2 shows you many of the common features and how they work then and now.

TABLE 11.2 BitLocker then and now

Feature	Windows 7/Server 2008 R2	Windows 8/Server 2012 R2
Resetting the BitLocker PIN or password	The user's privileges must be set to an administrator if you want to reset the BitLocker PIN on an operating system drive and the password on a fixed or removable data drive.	Standard users now have the ability to reset the BitLocker PIN and password on operating system drives, fixed data drives, and removable data drives.
Disk encryption	When BitLocker is enabled, the entire disk is encrypted.	When BitLocker is enabled, users have the ability to choose whether to encrypt the entire disk or only the used space on the disk.
Hardware-encrypted drive support	Not supported.	If the Windows logo hard drive comes preencrypted from the manufacturer, BitLocker is supported.
Unlocking using a network-based key to provide dual-factor authentication	Not available.	If a computer is rebooted on a trusted corporate wired-network key protector, then this feature allows a key to unlock and skip the PIN entry.
Protection for clusters	Not available.	Windows Server 2012 R2 BitLocker includes the ability to support cluster-shared volumes and failover clusters as long as they are running in a domain that was established by a Windows Server 2012 R2 domain controller with the Kerberos Key Distribution Center Service enabled.
Linking a BitLocker key protector to an Active Directory account	Not available.	BitLocker allows a user, group, or computer account in Active Directory to be tied to a key protector. This key protector allows protected data volumes to be unlocked.

In Exercise 11.1, you will enable BitLocker on the Windows Server 2012 R2 system.

EXERCISE 11.1

Enabling BitLocker in Windows Server 2012 R2

1. Open Server Manager by selecting the Server Manager icon or running `servermanager.exe`.
2. Select Add Roles And Features from the dashboard.
3. Select Next at the Before you begin pane (if shown).
4. Select Role-based or feature-based installation and select Next to continue.
5. Select the Select a server from the server pool option and click Next.
6. At the Select Server Roles screen, click Next.
7. At the Select features screen, click the BitLocker Drive Encryption check box. When the Add Roles and Features dialog box appears, click the Add Features button. Then click Next.

8. Select the Install button on the Confirmation pane of the Add Roles And Features Wizard to begin BitLocker feature installation. The BitLocker feature requires a restart to complete. Selecting the Restart The Destination Server Automatically If Required option in the Confirmation pane will force a restart of the computer after installation is complete.
9. If the Restart The Destination Server Automatically If Required check box is not selected, the Results pane of the Add Roles And Features Wizard will display the success or failure of the BitLocker feature installation. If required, a notification of additional action necessary to complete the feature installation, such as the restart of the computer, will be displayed in the results text.

You also can install BitLocker by using the Windows PowerShell utility. To install BitLocker, use the following PowerShell commands:

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools
-Restart
```

Using EFS Drive Encryption

If you have been in the computer industry long enough, you may remember the days when only servers used NTFS. Years ago, most client systems used FAT or FAT32, but NTFS had some key benefits over FAT/FAT32. The main advantages were NTFS security, quotas, compression, and encryption. Encryption is available on a system because you are using a file structure (for example, NTFS) that allows encryption. Windows Server 2012 R2 NTFS allows administrators to use these four advantages including encryption.

Encrypting File System (EFS) allows a user or administrator to secure files or folders by using encryption. Encryption employs the user's security identification (SID) number to secure the file or folder. Encryption is the strongest protection that Windows provides to help you keep your information secure. Some key features of EFS are as follows:

- Encrypting is simple; just select a check box in the file or folder's properties to turn it on.
- You have control over who can read the files.
- Files are encrypted when you close them but are automatically ready to use when you open them.
- If you change your mind about encrypting a file, clear the check box in the file's properties.

To implement encryption, open the Advanced Attributes dialog box for a folder and check the Encrypt Contents To Secure Data box.

If files are encrypted using EFS and an administrator has to unencrypt the files, there are two ways to do this. You can log in using the user's account (the account that encrypted the files) and unencrypt the files using the Cipher command. Alternatively, you can become a recovery agent and manually unencrypt the files.

If you use EFS, it's best not to delete users immediately when they leave a company. Administrators have the ability to recover encrypted files, but it is much easier to gain access to the user's encrypted files by logging in as the user who left the company and unchecking the encryption box.

Using the Cipher Command

The Cipher command is useful when it comes to EFS. Cipher is a command-line utility that allows you to change and/or configure EFS. When it comes to using the Cipher command, you should be aware of a few things:

- Administrators can decrypt files by running `Cipher.exe` in the Command Prompt window (advanced users).
- Administrators can use Cipher to modify an EFS-encrypted file.
- Administrators can use Cipher to import EFS certificates and keys.
- Administrators can also use Cipher to back up EFS certificates and keys.

Let's take a look at some of the different switches that you can use with Cipher. Table 11.3 describes many of the different Cipher switches you can use. This table comes from Microsoft's TechNet site. Microsoft continues to add and improve switches, so make sure you check Microsoft's website to see whether there are any changes.

TABLE 11.3 Using the cipher switches

Cipher switch	Description
`/e`	This switch allows an administrator to encrypt specified folders. With this folder encrypted, any files added to this folder will automatically be encrypted.
`/d`	This switch allows an administrator to decrypt specified folders.
`/s: dir`	By using this switch, the operation you are running will be performed in the specified folder and all subfolders.
`/i`	By default, when an error occurs, Cipher automatically halts. By using this switch, Cipher will continue to operate even after errors occur.
`/f`	The force switch (`/f`) will encrypt or decrypt all of the specified objects, even if the files have been modified by using encryption previously. Cipher, by default, does not touch files that have been encrypted or decrypted previously.

/q	This switch shows you a report about the most critical information of the EFS object.
/h	Normally, system or hidden files are not touched by encryption. By using this switch, you can display files with hidden or system attributes.
/k	This switch will create a new file encryption key based on the user currently running the Cipher command.
/?	This shows the Cipher help command.

Configuring Distributed File System

One problem that network administrators have is deciding how to share folders and communicating to end users how to find the shares. For example, if you share a folder called `Stellacon Documents` on server A, how do you make sure your users will find the folder and the files within it? The users have to know the server name and the share name. This can be a huge problem if you have hundreds of shares on multiple servers. If you want to have multiple copies of the folder called `Stellacon Documents` for fault tolerance and load balancing, the problem becomes even more complicated.

Distributed File System (DFS) in Windows Server 2012 R2 offers a simplified way for users to access geographically dispersed files. DFS allows you to set up a tree structure of virtual directories that allows users to connect to shared folders throughout the entire network.

Administrators have the ability to take shared folders that are located on different servers and transparently connect them to one or more DFS namespaces—virtual trees of shared folders throughout an organization. The advantage of using DFS is that if one of the folders becomes unavailable, DFS has failover capability that will allow your users to connect to the data on a different server.

Administrators can use the DFS tools to choose which shared folders will appear in the namespace and also to decide how the names of these shared folders will show up in the virtual tree listing.

Advantages of DFS

One of the advantages of DFS is that when a user views this virtual tree, the shared folders appear to be located on a single machine. These are some of the other advantages of DFS:

Simplified Data Migration DFS gives you the ability to move data from one location to another without the user needing to know the physical location of the data. Because the users do not need to know the physical location of the shared data, administrators can simply move data from one location to another.

Security Integration Administrators do not need to configure additional security for the DFS shared folders. The shared folders use the NTFS and shared folder permissions that an administrator has already assigned when the share was set up.

Access-Based Enumeration (ABE) This DFS feature (disabled by default) displays only the files and folders that a user has permissions to access. If a user does not have access to a folder, Windows hides the folder from the user's DFS view. This feature is not active if the user is viewing the files and folders locally.

Types of DFS

The following are types of DFS:

DFS Replication Administrators have the ability to manage replication scheduling and bandwidth throttling using the DFS management console. Replication is the process of sharing data between multiple machines. As explained earlier in the section, replicated shared folders allow you to balance the load and have fault tolerance. DFS also has read-only replication folders.

DFS Namespace The DFS Namespace service is the virtual tree listing in the DFS server. An administrator can set up multiple namespaces on the DFS, allowing for multiple virtual trees within DFS. The DFS Namespace service was once known as *Distributed File System* in Windows 2000 Server and Windows Server 2003 (in case you still use Server 2003).

In Exercise 11.2, you will install the DFS Namespace service on the file server. You need to start the installation using the Server Manager MMC.

EXERCISE 11.2

Installing the DFS Namespace Service

1. Open Server Manager by selecting the Server Manager icon or running `servermanager.exe`.
2. Select Add Roles And Features from the dashboard.
3. Select Next at the Before You Begin pane (if shown).
4. Select Role-Based or Feature-Based installation and select Next to continue.
5. Select the Select A Server From The Server Pool option and click Next.
6. At the Select Server Roles screen, expand File And Storage Services and check the DFS Namespace and DFS Replication check boxes. Then click Next. If a dialog box appears, click the Add Features button.
7. At the Select Features screen, click Next.
8. At the Confirmation screen, click the Install button.
9. After the installation is complete, click the Close button.
10. Close Server Manager.

Once you have installed DFS, it's time to learn how to manage DFS with the DFS Management MMC. The DFS Management console (see Figure 11.1) gives you one place to do all of your DFS configurations. The DFS Management console allows you to set up DFS Replication and DFS Namespace. Another task you can do in the DFS Management console is to add a folder target—a folder that you add to the DFS namespace (the virtual tree) for all your users to share.

FIGURE 11.1 DFS Management console

What's New in Windows Server 2012 R2

As with any new version of an operation system, Microsoft is trying to make each version of Windows Server better than the previous ones. This is also true with DFS. Microsoft has added many new features to DFS, and the following are just some of the major changes of Windows Server 2012 R2 DFS.

Windows PowerShell Module for DFS Replication

Windows PowerShell cmdlets for DFS replication modules can help administrators perform the majority of their DFS replication tasks. Administrators can use Windows PowerShell cmdlets to perform common administrative tasks such as creating, modifying, and removing DFS replication settings by using Window PowerShell scripts.

One of the nice new advantages of using Windows PowerShell for DFS is the ability to clone DFS replication databases and also to have the ability to restore those DFS databases in the event of an issue or crash.

Administrators have the ability to manage DFS management and replication through the use of the DNS Management and DFS Replication command-line utilities. Administrators who use the command-line tools are not doing anything incorrectly, but it is an inefficient way to do these tasks as well as being extremely time-consuming.

Administrators can use Windows PowerShell instead of command-line utilities and run hundreds of scripted commands, thus making their jobs easier and more efficient.

For an administrator who wants to use the Windows PowerShell cmdlets, the computer system installed with the DFS Management tools must be running Windows Server 2012 R2 or Windows 8.1 or newer. The DFS Management tools are part of the Remote Server Administration tools.

DFS Replication Windows Management Infrastructure Provider

In this book, I have spoken many times about using Windows Remote Management (WinRM) and how WinRM can help you administer a server remotely.

Introduced to Windows Server 2012 R2, the Windows Management Infrastructure (referred to as WMI v2) allows an administrator, using a properly configured firewall, to provide functionality and which provides programmatic access to manage DFS Replication.

Database Cloning

For the first time ever in DFS, Windows Server 2012 R2 includes a new DFS database cloning function. This new feature allows administrators to accelerate replication when creating folders, servers, or recovery systems.

Administrators will now have the ability to extract the DFS database from a single DFS server and then clone that database to multiple DFS servers.

Administrators can use PowerShell and the `Export-DfsrClone` cmdlet to export the volume that contains the DFS database and configuration `.xml` file settings. When executing this PowerShell cmdlet, a trigger is engaged that exports the DFS service, and the system will not proceed until the service is completed. Administrators would then use the PowerShell cmdlet `Import-DfsrClone` to import the data to a specific volume. The service will then validate that the replication was transferred completely.

Recovering a DFS Database

Windows Server 2012 R2 DFS database recovery is a feature that allows DFS to detect a corrupted database, thus allowing DFS to rebuild the database automatically and continue with normal operations of DFS replication. One advantage to this is that when DFS detects and fixes a corrupt database, it does so with no file conflicts.

Prior to this new feature, if a DFS database were determined to be corrupt, DFS Replication would delete the database and start again with an initial nonauthoritative sync process. This would cause newer file versions to be overwritten by older data causing real data loss.

DFS in Windows Server 2012 R2 uses local files and an update sequence number (USN) to fix a corrupt database, allowing for no loss of data.

Optimizing DFS

Windows Server 2012 R2 DFS allows an administrator to configure variable file staging sizes on individual DFS servers. This allows an administrator to set a minimum file size for a file to stage. This increases the staging size of files, and that in turn increases the performance of the replication.

Prior to Windows Server 2012 R2, DFS Replication used a hard-coded 256KB file size to determine staging requirements. If a file size were larger than 256KB, that file would be staged before it replicated. The more file staging that you have, the longer replication takes on a DFS system.

Remote Differential Compression

One issue that can arise occurs when files are changed. There has to be some mechanism that helps files stay accurate. That's where the *Remote Differential Compression (RDC)* feature comes into play. RDC is a group of application programming interfaces (APIs) that programs can use to determine whether files have changed. Once RDC determines that there has been a change, RDC then helps to detect which portions of the files contain the changes. RDC has the ability to detect insertions, removals, and rearrangements of data in files. This feature becomes helpful with limited-bandwidth networks when they replicate changes.

To install the RDC feature, use Server Manager and then run the Add Features Wizard, or type the following command at an elevated command prompt:

```
Servermanagercmd -Install Rdc
```

Implementing an Audit Policy

One of the most important aspects of controlling security in networked environments is ensuring that only authorized users are able to access specific resources. Although system administrators often spend much time managing security permissions, it is almost always possible for a security problem to occur.

Sometimes the best way to find possible security breaches is actually to record the actions that specific users take. Then, in the case of a security breach (the unauthorized shutdown of a server, for example), system administrators can examine the log to find the cause of the problem.

The Windows Server 2012 R2 operating system and Active Directory offer you the ability to audit a wide range of actions. In the following sections, you'll see how to implement auditing for Active Directory.

Overview of Auditing

The act of *auditing* relates to recording specific actions. From a security standpoint, auditing is used to detect any possible misuse of network resources. Although auditing does not necessarily prevent resources from being misused, it does help determine when security violations have occurred (or were attempted). Furthermore, just the fact that others know that you have implemented auditing may prevent them from attempting to circumvent security.

You need to complete several steps in order to implement auditing using Windows Server 2012 R2:

1. Configure the size and storage settings for the audit logs.
2. Enable categories of events to audit.
3. Specify which objects and actions should be recorded in the audit log.

Note that there are trade-offs to implementing auditing. First, recording auditing information can consume system resources. This can decrease overall system performance and use up valuable disk space. Second, auditing many events can make the audit log impractical to view. If too much detail is provided, system administrators are unlikely to scrutinize all of the recorded events. For these reasons, you should always be sure to find a balance between the level of auditing detail provided and the performance-management implications of these settings.

Implementing Auditing

Auditing is not an all-or-none type of process. As is the case with security in general, system administrators must choose specifically which objects and actions they want to audit.

The main categories for auditing include the following:

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

In this list of categories, many of the categories are related to Active Directory. Let's discuss these auditing categories in more detail.

Audit Account Logon Events You enable this auditing event if you want to audit when a user authenticates with a domain controller and logs onto the domain. This event is logged in the security log on the domain controller.

Audit Account Management This auditing event is used when you want to watch what changes are being made to Active Directory accounts. For example, when another administrator creates or deletes a user account, it would be an audited event.

Audit Directory Service Access This auditing event occurs whenever a user or administrator accesses Active Directory objects. Let's say an administrator opens Active Directory and clicks a user account; even if nothing is changed on that account, an event is logged.

Audit Logon Events Account logon events are created for domain account activity. For example, you have a user who logs on to a server so that they can access files; the act of logging onto the server creates this audit event.

Audit Object Access Audit object access allows you to audit objects within your network such as folders, files, and printers. If you suspect someone is trying to hack into an object (for example, the `finance` folder), this is the type of auditing that you would use. You still would need to enable auditing on the actual object (for example, the `finance` folder).

Audit Policy Change Audit policy change allows you to audit changes to user rights assignment policies, audit policies, or trust policies. This auditing allows you to see whether anyone changes any of the other audit policies.

Audit Privilege Use Setting the audit privilege use allows an administrator to audit each instance of a user exercising a user right. For example, if a user changes the system time on a machine, this is a user right. Log on locally is another common user right.

To audit access to objects stored within Active Directory, you must enable the Audit Directory Service Access option. Then you must specify which objects and actions should be tracked.

Exercise 11.3 walks through the steps you must take to implement auditing of Active Directory objects on domain controllers.

EXERCISE 11.3

Enabling Auditing of Active Directory Objects

1. Open the Local Security Policy tool (located in the Administrative Tools program group).
2. Expand Local Policies ➢ Audit Policy.
3. Double-click the setting for Audit Directory Service Access.
4. In the Audit Directory Service Access Properties dialog box, place check marks next to Success and Failure. Click OK to save the settings.
5. Close the Local Security Policy tool.

Viewing Auditing Information

One of the most important aspects of auditing is regularly monitoring the audit logs. If this step is ignored, as it often is in poorly managed environments, the act of auditing is useless. Fortunately, Windows Server 2012 R2 includes the *Event Viewer* tool, which allows system administrators to view audited events quickly and easily. Using the filtering capabilities of Event Viewer, they can find specific events of interest.

Exercise 11.4 walks you through the steps that you must take to generate some auditing events and to examine the data collected for these actions. In this exercise, you will perform some actions that will be audited, and then you will view the information recorded within the audit logs. To complete this exercise, you must first have completed the steps in Exercise 11.1 and Exercise 11.3.

EXERCISE 11.4

Generating and Viewing Audit Logs

1. Open the Active Directory Users and Computers tool.
2. Within the Engineering OU, right-click any user account and select Properties.
3. On the user's Properties dialog box, add the middle initial *A* for this user account and specify **Software Developer** in the Description box. Click OK to save the changes.
4. Within the Engineering OU, right-click the Robert Admin user account and select Properties.
5. In the Robert Properties dialog box, add the description **Engineering IT Admin** and click OK.
6. Close the Active Directory Users and Computers tool.
7. Open the Event Viewer tool from the Administrative Tools program group. Select the Security item under Windows Logs. You will see a list of audited events categorized under Directory Service Access. Note that you can obtain more details about a specific item by double-clicking it.
8. When you have finished viewing the security log, close the Event Viewer tool.

Using the *Auditpol.exe* Command

There may be a time when you need to look at your actual auditing policies set on a user or a system. This is where an administrator can use the `Auditpol.exe` command. *Auditpol* gives administrators the ability not only to view an audit policy but it also allows an administrator to set, configure, modify, restore, and even remove an audit policy. Auditpol is a command-line utility, and there are multiple switches that can be used with Auditpol. The following is the syntax used with Auditpol.

```
Auditpol command [<sub-command><options>]
```

Here's an example of using the command:

```
Auditpol /get /user:wpanek /category:"Detailed Tracking" /r
```

Table 11.4 describes some of the switches.

TABLE 11.4 Auditpol commands

Command	Description
/backup	Allows an administrator to save the audit policy to a file
/clear	Allows an administrator to clear an audit policy
/get	Gives administrators the ability to view the current audit policy
/list	Allows you to view selectable policy elements
/remove	Removes all per-user audit policy settings and disables all system audit policy settings
/restore	Allows an administrator to restore an audit policy from a file that was previously created using `auditpol /backup`
/set	Gives an administrator the ability to set an audit policy
/?	Displays help

Windows Server 2012 R2 Auditing Features

Auditing in Windows Server 2012 R2 and Windows 8 has been enhanced in many ways. Microsoft has increased the level of detail in the security auditing logs. Microsoft has also simplified the deployment and management of auditing policies. The following list includes some of the major enhancements:

Global Object Access Auditing Administrators using Windows Server 2012 R2 and Windows 8 now have the ability to define computer-wide system access control lists (SACLs). Administrators can define SACLs for either the file system or the registry. After the specified SACL is defined, the SACL is then applied automatically to every single object of that type. This can be helpful to administrators in verifying that all critical files, folders, and registry settings on a computer are protected. This is also helpful for identifying when an issue occurs with a system resource.

"Reason for Access" Reporting When an administrator is performing auditing in Windows Server 2012 R2 and Windows 8, they can now see the reason why an operation

was successful or unsuccessful. Previously, they lacked the ability to see the reason why an operation succeeded or failed.

Advanced Audit Policy Settings In Windows Server 2012 R2, there are hundreds of Advanced Audit Policy settings that can be used in place of the nine basic auditing settings. These advanced audit settings also help eliminate the unnecessary auditing activities that can make audit logs difficult to manage and decipher.

Expression-Based Audit Policies Administrators have the ability, because of Dynamic Access Control, to create targeted audit policies by using expressions based on user, computer, and resource claims. For example, an administrator has the ability to create an audit policy that tracks all Read and Write operations for files that are considered high-business impact. Expression-based audit policies can be directly created on a file or folder or created through the use of a Group Policy.

Removable Storage Device Auditing Administrators have the ability to monitor attempts to use a removable storage device on your network. If an administrator decides to implement this policy, an audit event is created every time one of your users attempts to copy, move, or save a network resource onto a removable storage device.

Making Active Directory Objects Available to Users

If you have been reading this book from the start, then this section will be familiar. But if you started this book with only exam 70-411 in mind, then you are about to learn how to make resources available to your users through the use of Active Directory.

With Active Directory, a system administrator can control which objects users can see. The act of making an Active Directory object available is known as *publishing*. The two main publishable objects are Printer objects and Shared Folder objects.

The general process for creating server shares and shared printers has remained unchanged from previous versions of Windows. You create the various objects (printers or file system folders) and then enable them for sharing.

To make these resources available via Active Directory, however, there's an additional step; you must publish the resources. Once an object has been published in Active Directory, clients will be able to find it.

When you publish objects in Active Directory, you should know the server name and share name of the resource. This information, however, doesn't matter to your users. A system administrator can change the resource to which an object points without having to reconfigure or even notify clients. For example, if you move a share from one server to another, all you need to do is update the Shared Folder object's properties to point to the new location. Active Directory clients still refer to the resource with the same path and name that they used previously.

Exercise 11.5 will walk you through the steps required for sharing and publishing a folder for use on your network.

EXERCISE 11.5

Creating and Publishing a Shared Network Folder

1. Create a new folder in the root directory of your `C:` partition and name it **`Test Share`**.
2. Right-click the `Test Share` folder and choose Share With ➢ Specific People.
3. In the File Sharing dialog box, enter the names of users with whom you want to share this folder. In the upper box, enter **Everyone** and then click Add. Note that Everyone appears in the lower box. Click in the Permission Level column next to Everyone and choose Read/Write from the drop-down menu. Then click Share.
4. You see a message that your folder has been shared. Click Done.
5. Open the Active Directory Users and Computers tool. Expand the current domain and right-click RD OU. Select New ➢ Shared Folder.
6. In the New Object – Shared Folder dialog box, type **`Shared Folder Test`** for the name of the folder. Then type the UNC path to the share (for example, **`\\serverA\Test Share`**). Click OK to create the share.

TIP

One of the main benefits of having all of your resource information in Active Directory is that you can easily find the information you're seeking using the Find dialog box. When setting up objects in Active Directory, I recommend that you always enter as much information as possible for the objects you are creating. The extra effort will pay off when your users start doing searches for these objects. The more information you enter, the more that will be available for users to search to find the appropriate resource they need.

Configuring Offline Folders

If you have been in this industry long enough, you have seen a major change in end-user computers. Years ago, only a few select users had laptops. They were big and bulky, and they weighed almost as much as today's desktop computers.

The pendulum has swung in the opposite direction. It probably seems like every one of your end users now has a laptop. As an IT administrator, this gives you a whole new set of challenges and problems to address. One challenge that you have to address is how users can work on files while outside of the office. If you have a user who wants to work at home, how do you give them the files they need to get their work done? The answer is *offline folders*. These folders contain data that can be worked on by users while outside the office. An IT administrator can set up offline folders through the use of *Group Policy objects (GPOs)*.

When you decide to make folders available for offline use, these folders need to synchronize with the laptops so that all of the data matches between both systems. As an administrator, one decision that you will need to make is when the offline folders will be synchronized.

You can set up any combination of these three synchronization options in the GPO:

- When you select Synchronize All Offline Files Before Logging Off, offline folders are synchronized when the user logs off the network.
- When you select Synchronize All Offline Files When Logging On, offline folders are synchronized when the user logs on to the network.
- When you select Synchronize Offline Files Before Suspend, offline folders are synchronized before the user does a system suspend.

In Exercise 11.6, you will configure offline folder options by using a GPO. This exercise uses the Group Policy Management Console (GPMC). If your GPMC is not installed, use the Server Manager MMC (under Features) to install it.

EXERCISE 11.6

Configuring Offline Folder Options

1. Open the Group Policy Management Console.
2. In the left pane, expand your forest and then your domain. Under your domain name, there should be a default domain policy.
3. Right-click the default domain policy and choose Edit.
4. In the User Configuration section, expand Policies ➢ Administrative Templates ➢ Network and then click Offline Files.
5. Right-click Synchronize All Offline Files Before Logging Off and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.
6. Right-click Synchronize All Offline Files When Logging On and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.
7. Right-click Synchronize Offline Files Before Suspend and choose Edit. The GPO setting dialog box appears. Choose the Enabled option. In the Action drop-down box, make sure Quick is selected. Click OK.
8. Close the GPMC.

Now that you have set up a GPO for synchronization, it's time to share a folder for offline usage. In Exercise 11.7, you will set up a folder for offline access. You must complete Exercise 11.5 before doing this exercise.

EXERCISE 11.7

Configuring a Shared Network Folder for Offline Access

1. Right-click the `Test Share` folder you created in Exercise 11.5 and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button.
3. When the Advanced Sharing dialog box appears, click the Caching button.
4. When the Offline Settings dialog box appears, choose the All Files And Programs That Users Open From The Shares Will Be Automatically Available Offline option. Click OK.
5. Click OK twice more to close the Properties dialog box.

Summary

This chapter took you through the use of many server tools and utilities such as DFS, BitLocker, and auditing. Distributed File System allows an administrator to set up a tree structure of virtual directories that allow users to connect to a shared folder anywhere throughout the entire network. You also looked at the new changes that have taken place with DFS in Windows Server 2012 R2.

You also learned about EFS and how to use Cipher to modify or configure EFS in a command window. Cipher is the best way to change encrypted directories and files.

This chapter also covered auditing. You looked at what needs to be audited if you are watching Active Directory and its objects. You looked at Auditpol and many of the switches that you would use when configuring Auditpol.

Finally, you learned how to publish share folders to Active Directory. By doing this, your users can search Active Directory to find resources they are looking for.

Exam Essentials

Know How to Configure DFS Distributed File System in Windows Server 2012 R2 offers a simplified way for users to access geographically dispersed files. The DFS Namespace service allows you to set up a tree structure of virtual directories that lets users connect to shared folders throughout the entire network.

Understand EFS and Cipher Users can encrypt their directories and files by using EFS. Understand how Cipher can help an administrator configure or modify an EFS object while in the command prompt.

Understand the Purpose and Function of Auditing Auditing helps determine the cause of security violations and helps troubleshoot permissions-related problems.

Review Questions

1. The company for which you work has a multilevel administrative team that is segmented by departments and locations. There are four major locations, and you are in the Northeast group. You have been assigned to the administrative group that is responsible for creating and maintaining network shares for files and printers in your region. The last place you worked was a large Windows Server 2008 network, where you had a much wider range of responsibilities. You are excited about the chance to learn more about Windows Server 2012 R2.

   For your first task, you have been given a list of file and printer shares that need to be created for the users in your region. You ask how to create them in Windows Server 2012 R2, and you are told that the process of creating a share is the same as with Windows Server 2008. You create the shares and use `NETUSE` to test them. Everything appears to work fine, so you send a message that the shares are available. The next day, you start receiving calls from users who say they cannot see any of resources you created. What is the most likely reason for the calls from the users?

   A. You forgot to enable NetBIOS for the shares.

   B. You need to force replication for the shares to appear in the directory.

   C. You need to publish the shares in the directory.

   D. The shares will appear within the normal replication period.

2. You want to publish a printer to Active Directory. Where would you click in order to accomplish this task?

   A. The Sharing tab

   B. The Advanced tab

   C. The Device Settings tab

   D. The Printing Preferences button

3. Isabel is a system administrator for an Active Directory environment that is running in Native mode. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:

   - The accessing of certain sensitive files must be logged.
   - Modifications to certain sensitive files must be logged.
   - System administrators must be able to provide information about which users accessed sensitive files and when they were accessed.
   - All logon attempts for specific shared machines must be recorded.

   Which of the following steps should Isabel take to meet these requirements? (Choose all that apply.)

   A. Enable auditing with the Computer Management tool.

   B. Enable auditing with the Active Directory Users and Computers tool.

   C. Enable auditing with the Active Directory Domains and Trusts tool.

   D. Enable auditing with the Event Viewer tool.

E. View the audit log using the Event Viewer tool.

F. View auditing information using the Computer Management tool.

G. Enable failure and success auditing settings for specific files stored on NTFS volumes.

H. Enable failure and success auditing settings for logon events on specific computer accounts.

4. You are the network administrator for a midsize coffee bean distributor. Your company's network has four Windows 2012 servers, and all of the clients are running either Windows 8 or Windows 7. Most of your end users use laptops to do their work, and many of them work away from the office. What should you configure to help them work on documents when away from the office?

A. Online file access

B. Offline file access

C. Share permissions

D. NTFS permissions

5. Your company has decided to implement an external hard drive. The company IT manager before you always used FAT32 as the system partition. Your company wants to know whether it should move to NTFS. Which of the following are some advantages of NTFS? (Choose all that apply.)

A. Security

B. Quotas

C. Compression

D. Encryption

6. You are the administrator for a large organization that uses Windows Server 2012 R2. You have been asked by your manager to help protect his folders on his Windows 7 NTFS machine. Your manager wants to make sure he is the only person that can open his files. How do you protect his files?

A. Use EFS.

B. Use CDMA.

C. Use FAT32 Security.

D. Use the `Convert:FAT32/Encrypt` command.

7. You are the administrator of your network, which consists of two Windows Server 2012 R2 systems. One of the servers is a domain controller, and the other server is a file server for data storage. The hard drive of the file server is starting to fill up. You do not have the ability to install another hard drive, so you decide to limit the amount of space everyone gets on the hard drive. What do you need to implement to solve your problem?

A. Disk spacing

B. Disk quotas

C. Disk hardening

D. Disk limitations

8. You are the administrator for a large communications company. Your company uses Windows Server 2012 R2, and your user's files are encrypted using EFS. What command-line command would you use to change or modify the EFS files?
   - **A.** Convert
   - **B.** Cipher
   - **C.** Gopher
   - **D.** Encrypt

9. You are the administrator for a large organization. You have multiple Windows Server 2012 R2 systems that all contain files that need to be shared for all users. The files and folders constantly move among servers, and users are having a hard time finding files they need. What can you implement to help your users out?
   - **A.** Encrypting File System (EFS)
   - **B.** Distributed File System (DFS)
   - **C.** Shared File System (SFS)
   - **D.** Published File System (PFS)

10. You have been hired by a small company to implement new Windows Server 2012 R2 systems. The company wants you to set up a server for users' home folder locations. What type of server would you be setting up?
   - **A.** PDC server
   - **B.** Web server
   - **C.** Exchange server
   - **D.** File server

Chapter

12

Configure DNS

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure DNS zones**

- Configure primary and secondary zones
- Configure stub zones
- Configure conditional forwards
- Configure zone and conditional forward storage in Active Directory
- Configure zone delegation
- Configure zone transfer settings
- Configure notify settings

✓ **Configure DNS records**

- Create and configure DNS Resource Records (RR) including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records
- Configure zone scavenging
- Configure record options including time to live (TTL) and weight
- Configure round robin
- Configure secure dynamic updates

If you have been reading this book from cover to cover, then this chapter is going to look very familiar. DNS is covered heavily on both the 70-410 and 70-411 exams. I am repeating much of the same stuff from Chapter 2, "Configure Network Services," but if you are reading just Part 2 of this book to take exam 70-411, then I will cover everything that can be tested on that exam. If you have read Chapter 2, then this will be a great review, with a little extra material thrown in for exam 70-411.

The Domain Name System (DNS) is one of the most important networking services that you can put on your network, and it's also one of the key topics that you'll need to understand if you plan to take any of the Microsoft Windows Server 2012 R2 exams.

By the end of this chapter, you should have a deeper understanding of how DNS works, how to set it up properly, how to configure DNS, proper management of the DNS server, and how to troubleshoot DNS issues quickly and easily in Microsoft Windows Server 2012 R2.

Introducing DNS

The *Domain Name System (DNS)* is a service that allows you to resolve a hostname to an Internet Protocol (IP) address. One of the inherent complexities of operating in networked environments is working with multiple protocols and network addresses. Owing largely to the tremendous rise in the popularity of the Internet, however, most environments have transitioned to use *Transmission Control Protocol/Internet Protocol (TCP/IP)* as their primary networking protocol. Microsoft is no exception when it comes to supporting TCP/IP in its workstation and server products. All current versions of Microsoft's operating systems support TCP/IP, as do most other modern operating systems.

An easy way to understand DNS is to think about making a telephone call. If you wanted to call Microsoft and did not know the phone number, you could call information, tell the operator the name (Microsoft), and get the telephone number. You would then make the call. Now think about trying to connect to Server1. You don't know the TCP/IP number (the computer's telephone number), so your computer asks DNS (information) for the number of Server1. DNS returns the number, and your system makes the connection (call). DNS is your network's 411, or information, and it returns the TCP/IP data for your network.

TCP/IP is actually a collection of different technologies (protocols and services) that allow computers to function together on a single, large, and heterogeneous network. Some of the major advantages of this protocol include widespread support for hardware, software, and network devices; reliance on a system of standards; and scalability. TCP

handles tasks such as sequenced acknowledgments. IP involves many jobs, such as logical subnet assignment and routing.

The Form of an IP Address

To understand DNS, you must first understand how TCP/IP addresses are formed. Because DNS is strictly on a network to support TCP/IP, understanding the basics of TCP/IP is extremely important.

Microsoft exams cover TCP/IP. The TCP/IP material is covered in Chapter 8, "Configure TCP/IP."

An *IP address* is a logical number that uniquely identifies a computer on a TCP/IP network. TCP/IP allows a computer packet to reach the correct host. Windows Server 2012 R2 works with two versions of TCP/IP: IPv4 and IPv6. An IPv4 address takes the form of four octets (eight binary bits), each of which is represented by a decimal number between 0 and 255. The four numbers are separated by decimal points. For example, all of the following are valid IP addresses:

- 128.45.23.17
- 230.212.43.100
- 10.1.1.1

The dotted decimal notation was created to make it easier for users to deal with IP addresses, but this idea did not go far enough. As a result, another abstraction layer was developed, which used names to represent the dotted decimal notation—the domain name. For example, the IP address 11000000 10101000 00000001 00010101 maps to 192.168.1.21, which in turn might map to `server1.company.org`, which is how the computer's address is usually presented to the user or application.

As stated earlier, IPv4 addresses are made up of octets, or the decimal (base 10) representation of 8 bits. It takes four octets to add up to the 32 bits required. IPv6 expands the address space to 128 bits. The address is usually represented in hexadecimal notation as follows:

```
2001:0DB8:0000:0000:1234:0000:A9FE:133E
```

You can tell that the implementation of DNS would make life a lot easier for everyone; even those of us who like to use alphanumeric values. (For example, some of us enjoy pinging the address in lieu of the name.) Fortunately, DNS already has the ability to handle IPv6 addresses using an AAAA record. An A record in IPv4's addressing space is 32 bits, and an AAAA record (4 *A*s) in IPv6's is 128 bits.

Nowadays, most computer users are quite familiar with navigating to DNS-based resources, such as `www.microsoft.com`. To resolve these "friendly" names to TCP/IP addresses that the network stack can use, you need a method for mapping them. Originally, ASCII flat files (often called *HOSTS files*, as shown in Figure 12.1) were used for this

FIGURE 12.1 HOSTS file

purpose. In some cases, they are still used today in small networks, and they can be useful in helping to troubleshoot name resolution problems.

As the number of machines and network devices grew, it became unwieldy for administrators to manage all of the manual updates required to enter new mappings to a master HOSTS file and distribute it. Clearly, a better system was needed.

As you can see from the sample HOSTS file in Figure 12.1, you can conduct a quick test of the email server's name resolution as follows:

1. Open the HOSTS file: `C:\Windows\Systems32\drivers\etc`.
2. Add the IP-address-to-hostname mapping.
3. Try to ping the server using the hostname to verify that you can reach it using an easy-to-remember name.

Following these steps should drive home the concept of DNS for you because you can see it working to make your life easier. Now you don't have to remember 10.0.0.10; you only need to remember `exchange03`. However, you can also see how this method can become unwieldy if you have many hosts that want to use easy-to-remember names instead of IP addresses to locate resources on your network.

When dealing with large networks, users and network administrators must be able to locate the resources they require with minimal searching. Users don't care about the actual physical or logical network address of the machine; they just want to be able to connect to it using a simple name that they can remember.

From a network administrator's standpoint, however, each machine must have its own logical address that makes it part of the network on which it resides. Therefore, some scalable and easy-to-manage method for resolving a machine's logical name to an IP address and then to a domain name is required. DNS was created just for this purpose.

DNS is a hierarchically distributed database. In other words, its layers are arranged in a definite order, and its data is distributed across a wide range of machines, each of which can exert control over a portion of the database. DNS is a standard set of protocols that defines the following:

- A mechanism for querying and updating address information in the database
- A mechanism for replicating the information in the database among servers
- A schema of the database

DNS is defined by a number of requests for comments (RFCs), though primarily by RFC 1034 and RFC 1035.

DNS was originally developed in the early days of the Internet (called ARPAnet at the time) when it was a small network created by the Department of Defense for research purposes. Before DNS, computer names, or hostnames, were manually entered into a HOSTS file located on a centrally administered server. Each site that needed to resolve hostnames outside of its organization had to download this file. As the number of computers on the Internet grew, so did the size of this HOSTS file—and along with it the problems of its management. The need for a new system that would offer features such as scalability, decentralized administration, and support for various data types became more and more obvious. DNS, introduced in 1984, became this new system.

With DNS, the hostnames reside in a database that can be distributed among multiple servers, decreasing the load on any one server and providing the ability to administer this naming system on a per-partition basis. DNS supports hierarchical names and allows for the registration of various data types in addition to the hostname-to-IP-address mapping used in HOSTS files. Database performance is ensured through its distributed nature as well as through caching.

The DNS distributed database establishes an inverted logical tree structure called the *domain namespace*. Each node, or domain, in that space has a unique name. At the top of the tree is the root. This may not sound quite right, which is why the DNS hierarchical model is described as being an inverted tree, with the root at the top. The root is represented by the null set: `""`. When written, the root node is represented by a single dot (`.`).

Each node in the DNS can branch out to any number of nodes below it. For example, below the root node are a number of other nodes, commonly referred to as *top-level domains (TLDs)*. These are the familiar `.com`, `.net`, `.org`, `.gov`, `.edu`, and other such names. Table 12.1 lists some of these TLDs.

TABLE 12.1 Common top-level DNS domains

Domain name	Type of organization
com	Commercial (for example, stellacon.com for Stellacon Training Corporation)
edu	Educational (for example, gatech.edu for the Georgia Institute of Technology)
gov	Government (for example, whitehouse.gov for the White House in Washington, D.C.)
int	International organizations (for example, nato.int for NATO); this top-level domain is fairly rare
mil	Military organizations (for example, usmc.mil for the Marine Corps); there is a separate set of root name servers for this domain
net	Networking organizations and Internet providers (for example, hiwaay.net for HiWAAY Information Systems); many commercial organizations have registered names under this domain too
org	Noncommercial organizations (for example, fidonet.org for FidoNet)
au	Australia
uk	United Kingdom
ca	Canada
us	United States
jp	Japan

Each of these nodes then branches out into another set of domains, and they combine to form what we refer to as *domain names*, such as microsoft.com. A domain name identifies the domain's position in the logical DNS hierarchy in relation to its parent domain by separating each branch of the tree with a dot. Figure 12.2 shows a few of the top-level domains, where the Microsoft domain fits, and a host called Tigger within the microsoft.com domain. If someone wanted to contact that host, they would use the *fully qualified domain name (FQDN)*, tigger.microsoft.com.

An FQDN includes the trailing dot (.) to indicate the root node, but it's commonly left off in practice.

As previously stated, one of the strengths of DNS is the ability to delegate control over portions of the DNS namespace to multiple organizations. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) assigns the control over TLDs

FIGURE 12.2 The DNS hierarchy

to one or more organizations. In turn, those organizations delegate portions of the DNS namespace to other organizations. For example, when you register a domain name, let's call it `example.com`, you control the DNS for the portion of the DNS namespace within `example.com`. The registrar controlling the `.com` TLD has delegated control over the `example.com` node in the DNS tree. No other node can be named `example` directly below the `.com` within the DNS database.

Within the portion of the domain namespace that you control (`example.com`), you could create host and other records (more on these later). You could also further subdivide `example.com` and delegate control over those divisions to other organizations or departments. These divisions are called *subdomains*. For example, you might create subdomains named for the cities in which the company has branch offices and then delegate control over those subdomains to the branch offices. The subdomains might be named `losangeles.example.com`, `chicago.example.com`, `portsmouth.example.com`, and so on.

Each domain (or delegated subdomain) is associated with DNS name servers. In other words, for every node in the DNS, one or more servers can give an authoritative answer to queries about that domain. At the root of the domain namespace are the root servers, which I'll cover later in the chapter.

NOTE

Domain names and hostnames must contain only characters `a` to `z`, `A` to `Z`, `0` to `9`, and `-` (hyphen). Other common and useful characters, such as the `&` (ampersand), `/` (slash), `.` (period), and `_` (underscore) characters, are not allowed. This is in conflict with NetBIOS's naming restrictions. However, you'll find that Windows Server 2012 R2 is smart enough to take a NetBIOS name, like `Server_1`, and turn it into a legal DNS name, like `server1.example.com`.

DNS servers work together to resolve hierarchical names. If a server already has information about a name, it simply fulfills the query for the client. Otherwise, it queries other DNS servers for the appropriate information. The system works well because it distributes the authority over separate parts of the DNS structure to specific servers. A DNS zone is a portion of the DNS namespace over which a specific DNS server has authority. (DNS zone types are discussed in detail later in this chapter.)

There is an important distinction to make between DNS zones and Active Directory (AD) domains. Although both use hierarchical names and require name resolution, DNS zones do not map directly to AD domains.

Within a given DNS zone, resource records (RRs) contain the hosts and other database information that make up the data for the zone. For example, an RR might contain the host entry for `www.example.com`, pointing it to the IP address 192.168.1.10.

Understanding Servers, Clients, and Resolvers

You will need to know a few terms and concepts in order to manage a DNS server. Understanding these terms will make it easier to understand how the Windows Server 2012 R2 DNS server works:

DNS Server Any computer providing domain name services is a *DNS name server*. No matter where the server resides in the DNS namespace, it's still a DNS name server. For example, 13 root name servers at the top of the DNS tree are responsible for delegating the TLDs. The *root servers* provide referrals to name servers for the TLDs, which in turn provide referrals to an authoritative name server for a given domain.

The Berkeley Internet Name Domain (BIND) was originally the only software available for running the root servers on the Internet. However, a few years ago the organizations responsible for the root servers undertook an effort to diversify the software running on these important machines. Today, root servers run multiple types of name server software. BIND is still primarily on Unix-based machines, and it is also the most popular for Internet providers. None of the root servers run Windows DNS.

Any DNS server implementation supporting Service Location Resource Records (see RFC 2782) and Dynamic Updates (RFC 2136) is sufficient to provide the name service for any operating system running Windows 2003 software and newer.

DNS Client A *DNS client* is any machine that issues queries to a DNS server. The client hostname may or may not be registered in a DNS database. Clients issue DNS requests through processes called *resolvers*. You'll sometimes see the terms *client* and *resolver* used synonymously.

Resolver *Resolvers* are software processes, sometimes implemented in software libraries, which handle the actual process of finding the answers to queries for DNS data. The resolver is also built into many larger pieces of software so that external libraries don't have to be called to make and process DNS queries. Resolvers can be what you'd consider client computers or other DNS servers attempting to resolve an answer on behalf of a client (for example, Internet Explorer).

Query A *query* is a request for information sent to a DNS server. Three types of queries can be made to a DNS server: recursive, inverse, and iterative. I'll discuss the differences between these query types in the section "DNS Queries" a bit later in the chapter.

Understanding the DNS Process

To help you understand the DNS process, I will start by covering the differences between Dynamic DNS and Non-Dynamic DNS. During this discussion, you will learn how Dynamic DNS populates the DNS database. You'll also see how to implement security for Dynamic DNS. I will then talk about the workings of different types of DNS queries. Finally, I will discuss caching and time to live (TTL). You'll learn how to determine the best setting for your organization.

Dynamic DNS and Non-Dynamic DNS

To understand Dynamic DNS and Non-Dynamic DNS, you must go back in time (here is where the TV screen always used to get wavy). Many years ago when we all worked on NT 3.51 and NT 4.0, most networks used Windows Internet Name Service (WINS) to do their TCP/IP name resolution. Windows versions 95/98 and NT 4.0 Professional were all built on the idea of using WINS. This worked out well for administrators because WINS was dynamic (which meant that once it was installed, it automatically built its own database). Back then, there was no such thing as Dynamic DNS; administrators had to enter DNS records into the server manually. This is important to know even today. If you have clients still running any of these older operating systems (95/98 or NT 4), these clients cannot use Dynamic DNS.

Now let's move forward in time to the release of Windows Server 2000. Microsoft announced that DNS was going to be the name resolution method of choice. Many administrators (me included) did not look forward to the switch. Because there was no such thing as Dynamic DNS, most administrators had nightmares about manually entering records. However, luckily for us, when Microsoft released Windows Server 2000, DNS had the ability to operate dynamically. Now when you're setting up Windows Server 2012 R2 DNS, you can choose what type of dynamic update you would like to use, if any. Let's talk about why you would want to choose one over the other.

The *Dynamic DNS (DDNS) standard*, described in RFC 2136, allows DNS clients to update information in the DNS database files. For example, a Windows Server 2012 R2 DHCP server can automatically tell a DDNS server which IP addresses it has assigned to what machines. Windows 2000, 2003, 2008, XP Pro, Vista, Windows 7, and Windows 8 DHCP clients can do this too. For security reasons, however, it's better to let the DHCP

server do it. The result: IP addresses and DNS records stay in sync so that you can use DNS and DHCP together seamlessly. Because DDNS is a proposed Internet standard, you can even use the Windows Server 2012 R2 DDNS-aware parts with Unix/Linux-based DNS servers.

Non-Dynamic DNS (NDDNS) does not automatically populate the DNS database. The client systems do not have the ability to update to DNS. If you decide to use Non-Dynamic DNS, an administrator will need to populate the DNS database manually. Non-Dynamic DNS is a reasonable choice if your organization is small-to-midsize and you do not want extra network traffic (clients updating to the DNS server) or if you need to enter the computer's TCP/IP information manually because of strict security measures.

Dynamic DNS has the ability to be secure, and the chances are slim that a rogue system (a computer that does not belong in your DNS database) could update to a secure DNS server. Nevertheless, some organizations have to follow stricter security measures and are not allowed to have dynamic updates.

The major downside to entering records into DNS manually occurs when the organization is using the *Dynamic Host Configuration Protocol (DHCP)*. When using DHCP, it is possible for users to end up with different TCP/IP addresses every day. This means that an administrator has to update DNS manually each day to keep it accurate.

If you choose to allow Dynamic DNS, you need to decide how you want to set it up. When setting up dynamic updates on your DNS server, you have three choices (see Figure 12.3).

FIGURE 12.3 Setting the Dynamic Updates option

None This means your DNS server is Non-Dynamic.

Nonsecure and Secure This means that any machine (even if it does not have a domain account) can register with DNS. Using this setting could allow rogue systems to enter records into your DNS server.

Secure Only This means that only machines with accounts in Active Directory can register with DNS. Before DNS registers any account in its database, it checks Active Directory to make sure that account is an authorized domain computer.

How Dynamic DNS Populates the DNS Database

TCP/IP is the protocol used for network communications on a Microsoft Windows Server 2012 R2 network. Users have two ways to receive a TCP/IP number:

- Static (administrators manually enter the TCP/IP information)
- Dynamic (using DHCP)

When an administrator sets up TCP/IP, DNS can also be configured.

Once a client gets the address of the DNS server, if that client is allowed to update with DNS, the client sends a registration to DNS or requests DHCP to send the registration. DNS then does one of two things, depending on which Dynamic Updates option is specified:

- Check with Active Directory to see if that computer has an account (Secure Only updates) and, if it does, enter the record into the database.
- Enter the record into its database (nonsecure and secure updates).

What if you have clients that cannot update DNS? Well, there is a solution—DHCP. In the DNS tab of the IPv4 Properties window, check the option labeled "Dynamically update DNS A and PTR records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)," which is shown in Figure 12.4.

FIGURE 12.4 DHCP settings for DNS

DHCP, along with Dynamic DNS clients, allows an organization to update its DNS database dynamically without the time and effort of having an administrator manually enter DNS records.

DNS Queries

As stated earlier, a client can make three types of queries to a DNS server: recursive, inverse, and iterative. Remember that the client of a DNS server can be a resolver (what you'd normally call a client) or another DNS server.

Iterative Queries

Iterative queries are the easiest to understand: A client asks the DNS server for an answer, and the server returns the best answer. This information likely comes from the server's cache. The server never sends out an additional query in response to an iterative query. If the server doesn't know the answer, it may direct the client to another server through a referral.

Recursive Queries

In a *recursive query*, the client sends a query to a name server, asking it to respond either with the requested answer or with an error message. The error states one of two things:

- The server can't come up with the right answer.
- The domain name doesn't exist.

In a recursive query, the name server isn't allowed to just refer the client to some other name server. Most resolvers use recursive queries. In addition, if your DNS server uses a forwarder, the requests sent by your server to the forwarder will be recursive queries.

Figure 12.5 shows an example of both recursive and iterative queries. In this example, a client within the Microsoft Corporation is querying its DNS server for the IP address for `www.whitehouse.gov`.

FIGURE 12.5 A sample DNS query

Here's what happens to resolve the request:

1. The resolver sends a recursive DNS query to its local DNS server asking for the IP address of `www.whitehouse.gov`. The local name server is responsible for resolving the name, and it cannot refer the resolver to another name server.
2. The local name server checks its zones, and it finds no zones corresponding to the requested domain name.
3. The root name server has authority for the root domain and will reply with the IP address of a name server for the `.gov` top-level domain.
4. The local name server sends an iterative query for `www.whitehouse.gov` to the Gov name server.
5. The Gov name server replies with the IP address of the name server servicing the `whitehouse.gov` domain.
6. The local name server sends an iterative query for `www.whitehouse.gov` to the `whitehouse.gov` name server.
7. The `whitehouse.gov` name server replies with the IP address corresponding to `www.whitehouse.gov`.
8. The local name server sends the IP address of `www.whitehouse.gov` back to the original resolver.

Inverse Queries

Inverse queries use pointer (PTR) records. Instead of supplying a name and then asking for an IP address, the client first provides the IP address and then asks for the name. Because there's no direct correlation in the DNS namespace between a domain name and its associated IP address, this search would be fruitless without the use of the `in-addr.arpa` domain. Nodes in the `in-addr.arpa` domain are named after the numbers in the dotted-octet representation of IP addresses. However, because IP addresses get more specific from left to right and domain names get less specific from left to right, the order of IP address octets must be reversed when building the `in-addr.arpa` tree. With this arrangement, administration of the lower limbs of the DNS `in-addr.arpa` tree can be given to companies as they are assigned their Class A, B, or C subnet address or delegated even further down thanks to variable-length subnet masking (VLSM).

Once the domain tree is built into the DNS database, a special PTR record is added to associate the IP addresses with the corresponding hostnames. In other words, to find a hostname for the IP address 206.131.234.1, the resolver would query the DNS server for a PTR record for `1.234.131.206.in-addr.arpa`. If this IP address is outside the local domain, the DNS server will start at the root and sequentially resolve the domain nodes until arriving at `234.131.206.in-addr.arpa`, which would contain the PTR record for the desired host.

Caching and Time to Live

When a name server is processing a recursive query, it may be required to send out several queries to find the definitive answer. Name servers, acting as resolvers, are allowed to cache

all of the received information during this process; each record contains information called *time to live (TTL)*. The TTL specifies how long the record will be held in the local cache until it must be resolved again. If a query comes in that can be satisfied by this cached data, the TTL that's returned with it equals the current amount of time left before the data is flushed.

There is also a negative cache TTL. The *negative cache TTL* is used when an authoritative server responds to a query indicating that the record queried doesn't exist, and it indicates the amount of time that this negative answer may be held. Negative caching is quite helpful in preventing repeated queries for names that don't exist.

The administrator for the DNS zone sets TTL values for the entire zone. The value can be the same across the zone, or the administrator can set a separate TTL for each RR within the zone. Client resolvers also have data caches and honor the TTL value so that they know when to flush.

Choosing Appropriate TTL Values

For zones that you administer, you can choose the TTL values for the entire zone, for negative caching, and for individual records. Choosing an appropriate TTL depends on a number of factors, including the following:

- Amount of change you anticipate for the records within the zone
- Amount of time that you can withstand an outage that might require changing an IP address
- Amount of traffic that you believe the DNS server can handle

Resolvers query the name server every time the TTL expires for a given record. A low TTL, say 60 seconds, can burden the name server, especially for popular DNS records. (DNS queries aren't particularly intensive for a server to handle, but they can add up quickly if you mistakenly use 60 seconds instead of 600 seconds for the TTL on a popular record.) Set a low TTL only when you need to respond quickly to a changing environment.

A high TTL, say 604,800 seconds (that's one week), means that if you need to make a change to the DNS record, clients might not see the change for up to a week. This consideration is especially important when making changes to the network, and it's one that's all too frequently overlooked. I can't count the number of times I've worked with clients who have recently made a DNS change to a new IP for their email or website only to ask why it's not working for some clients. The answer can be found in the TTL value. If the record is being cached, then the only thing that can solve their problem is time.

You should choose a TTL that's appropriate for your environment. Take the following factors into account:

- The amount of time that you can afford to be offline if you need to make a change to a DNS record that's being cached
- The amount of load that a low TTL will cause on the DNS server

In addition, you should plan well ahead of any major infrastructure changes and change the TTL to a lower value to lessen the effect of the downtime by reducing the amount of time that the record(s) can be cached.

Introducing DNS Database Zones

As mentioned earlier in this chapter, a DNS zone is a portion of the DNS namespace over which a specific DNS server has authority. Within a given DNS zone, there are resource records that define the hosts and other types of information that make up the database for the zone. You can choose from several different zone types. Understanding the characteristics of each will help you choose which is right for your organization.

The DNS zones discussed in this book are all Microsoft Windows Server 2012/2012 R2 zones. Non-Windows (for example, Unix) systems set up their DNS zones differently.

In the following sections, I will discuss the different zone types and their characteristics.

Understanding Primary Zones

When you're learning about zone types, things can get a bit confusing. But it's really not difficult to understand how they work and why you would want to choose one type of zone over another. Zones are databases that store records. By choosing one zone type over another, you are basically just choosing how the database works and how it will be stored on the server.

The primary zone is responsible for maintaining all of the records for the DNS zone. It contains the primary copy of the DNS database. All record updates occur on the primary zone. You will want to create and add primary zones whenever you create a new DNS domain.

There are two types of primary zones:

- Primary zone
- Primary zone with Active Directory Integration (Active Directory DNS)

From this point forward, I refer to a primary zone with Active Directory Integration as an *Active Directory DNS*. When I use only the term *primary zone,* Active Directory is not included.

To install DNS as a primary zone, first you must install DNS using the Server Manager MMC. Once DNS is installed and running, you create a new zone and specify it as a primary zone.

The process of installing DNS and its zones will be discussed later in this chapter. In addition, there will be step-by-step exercises to walk you through how to install these components.

Primary zones have advantages and disadvantages. Knowing the characteristics of a primary zone will help you decide when you need the zone and when it fits into your organization.

Local Database

Primary DNS zones get stored locally in a file (with the suffix `.dns`) on the server. This allows you to store a primary zone on a domain controller or a member server. In addition, by loading DNS onto a member server, you can help a small organization conserve resources. Such an organization may not have the resources to load DNS on an Active Directory domain controller.

Unfortunately, the local database has many disadvantages:

Lack of Fault Tolerance Think of a primary zone as a contact list on your smartphone. All of the contacts in the list are the records in your database. The problem is that if you lose your phone or the phone breaks, you lose your contact list. Until your phone gets fixed or you swap out your phone card, the contacts are unavailable.

It works the same way with a primary zone. If the server goes down or you lose the hard drive, DNS records on that machine are unreachable. An administrator can install a secondary zone (explained later in the next section), and that provides temporary fault tolerance. Unfortunately, if the primary zone is down for an extended period of time, the secondary server's information will no longer be valid.

Additional Network Traffic Let's imagine that you are looking for a contact number for John Smith. John Smith is not listed in your cell phone directory, but he is listed in your partner's cell phone. You have to contact your partner to get the listing. You cannot directly access your partner's cell contacts.

When a resolver sends a request to DNS to get the TCP/IP address for Jsmith (in this case Jsmith is a computer name) and the DNS server does not have an answer, it does not have the ability to check the other server's database directly to get an answer. Thus, it forwards the request to another DNS. When DNS servers are replicating zone databases with other DNS servers, this causes additional network traffic.

No Security Staying with the cell phone example, let's say that you call your partner looking for John Smith's phone number. When your partner gives you the phone number over your wireless phone, someone with a scanner can pick up your conversation. Unfortunately, wireless telephone calls are not very secure.

Now a resolver asks a primary zone for the Jsmith TCP/IP address. If someone on the network has a packet sniffer, they can steal the information in the DNS packets being sent over the network. The packets are not secure unless you implement some form of secondary security. Also, the DNS server has the ability to be dynamic. A primary zone accepts all updates from DNS servers. You cannot set it to accept secure updates only.

Understanding Secondary Zones

In Windows Server 2012 R2 DNS, you have the ability to use secondary DNS zones. Secondary zones are noneditable copies of the DNS database. You use them for *load balancing* (also referred to as *load sharing*), which is a way of managing network overloads on a single server. A secondary zone gets its database from a primary zone.

A *secondary zone* contains a database with all of the same information as the primary zone, and it can be used to resolve DNS requests. Secondary zones have the following advantages:

- A secondary zone provides fault tolerance, so if the primary zone server becomes unavailable, name resolution can still occur using the secondary zone server.
- Secondary DNS servers can also increase network performance by offloading some of the traffic that would otherwise go to the primary server.

Secondary servers are often placed within the parts of an organization that have high-speed network access. This prevents DNS queries from having to run across slow wide area network (WAN) connections. For example, if there are two remote offices within the `stellacon.com` organization, you may want to place a secondary DNS server in each remote office. This way, when clients require name resolution, they will contact the nearest server for this IP address information, thus preventing unnecessary WAN traffic.

Having too many secondary zone servers can actually cause an increase in network traffic because of replication (especially if DNS changes are fairly frequent). Therefore, you should always weigh the benefits and drawbacks and properly plan for secondary zone servers.

Configure Zone Delegation

One advantage of DNS is the ability of turning a namespace into one or more zones. These zones can be replicated to each other or other DNS servers. As an administrator, you must decide when you want to break your DNS into multiple zones. When considering this option, there are a few things to think about:

- You want the management of your DNS namespace to be delegated by another location or department in your organization.

- You want to load-balance your traffic among multiple servers by turning a large zone into many smaller zones. This will help improve performance and create redundancy among your DNS servers.
- You have remote offices opening up, and you want to expand your DNS namespace.

To create a new zone delegation, you would complete the following steps:

1. Open the DNS console.
2. In the console tree, right-click the applicable subdomain and then click New Delegation.
3. Follow the instructions provided in the New Delegation Wizard to finish creating the newly delegated domain.

Understanding Active Directory Integrated DNS

Windows Server 2000 introduced *Active Directory Integrated DNS* to the world. This zone type was unique, and it was a separate choice during setup. In Windows Server 2003, this zone type became an add-on to a primary zone. In Windows Server 2012 R2, it works the same way. After choosing to set up a primary zone, you check the box Store The Zone In Active Directory (see Figure 12.6).

FIGURE 12.6 Setting up an Active Directory Integrated zone

Disadvantages of Active Directory Integrated DNS

The main disadvantage of Active Directory Integrated DNS is that it has to reside on a domain controller because the DNS database is stored in Active Directory. As a result, you cannot load this zone type on a member server, and small organizations might not have the resources to set up a dedicated domain controller.

Advantages of Active Directory Integrated DNS

The advantages of using an Active Directory Integrated DNS zone well outweigh the disadvantages just discussed. The following are some of the major advantages to an Active Directory Integrated zone:

Full Fault Tolerance Think of an Active Directory Integrated zone as a database on your server that stores contact information for all your clients. If you need to retrieve John Smith's phone number, as long as it was entered, you can look it up on the software.

If John Smith's phone number was stored only on your computer and your computer stopped working, no one could access John Smith's phone number. But since John Smith's phone number is stored in a database to which everyone has access, if your computer stops working, other users can still retrieve John Smith's phone number.

An Active Directory Integrated zone works the same way. Since the DNS database is stored in Active Directory, all Active Directory DNS servers can have access to the same data. If one server goes down or you lose a hard drive, all other Active Directory DNS servers can still retrieve DNS records.

No Additional Network Traffic As previously discussed, an Active Directory Integrated zone is stored in Active Directory. Since all records are now stored in Active Directory, when a resolver needs a TCP/IP address for Jsmith, any Active Directory DNS server can access Jsmith's address and respond to the resolver.

When you choose an Active Directory Integrated zone, DNS zone data can be replicated automatically to other DNS servers during the normal Active Directory replication process.

DNS Security An Active Directory Integrated zone has a few security advantages over a primary zone:

- An Active Directory Integrated zone can use secure dynamic updates.
- As explained earlier, the Dynamic DNS standard allows secure-only updates or dynamic updates, not both.
- If you choose secure updates, then only machines with accounts in Active Directory can register with DNS. Before DNS registers any account in its database, it checks Active Directory to make sure that it is an authorized domain computer.
- An Active Directory Integrated zone stores and replicates its database through Active Directory replication. Because of this, the data gets encrypted as it is sent from one DNS server to another.

Background Zone Loading Background zone loading (discussed in more detail later in this chapter) allows an Active Directory Integrated DNS zone to load in the background. As a result, a DNS server can service client requests while the zone is still loading into memory.

Understanding Stub Zones

Stub zones work a lot like secondary zones—the database is a noneditable copy of a primary zone. The difference is that the stub zone's database contains only the information

necessary (three record types) to identify the authoritative DNS servers for a zone (see Figure 12.7). You should not use stub zones to replace secondary zones, nor should you use them for redundancy and load balancing.

FIGURE 12.7 DNS stub zone type

NOTE

Stub zone databases contain only three record types: name server (NS), start of authority (SOA), and glue host (A) records. Understanding these records will help you on the Microsoft certification exams. Microsoft asks many questions about stub zones on all DNS-related exams.

When to Use Stub Zones

Stub zones become particularly useful in a couple of different scenarios. Consider what happens when two large companies merge: `example.com` and `example.net`. In most cases, the DNS zone information from both companies must be available to every employee. You could set up a new zone on each side that acts as a secondary for the other side's primary zone, but administrators tend to be very protective of their DNS databases and probably wouldn't agree to this plan.

A better solution is to add to each side a stub zone that points to the primary server on the other side. When a client in `example.com` (which you help administer) makes a request for a name in `example.net`, the stub zone on the `example.com` DNS server would send the client to the primary DNS server for `example.net` without actually resolving the name. At this point, it would be up to `example.net`'s primary server to resolve the name.

An added benefit is that, even if the administrators over at `example.net` change their configuration, you won't have to do anything because the changes will automatically replicate to the stub zone, just as they would for a secondary server.

Stub zones can also be useful when you administer two domains across a slow connection. Let's change the previous example a bit and assume that you have full control over `example.com` and `example.net` but they connect through a 56Kbps line. In this case, you wouldn't necessarily mind using secondary zones because you personally administer the entire network. However, it could get messy to replicate an entire zone file across that slow line. Instead, stub zones would refer clients to the appropriate primary server at the other site.

GlobalName Zones

Earlier in this chapter, I talked about organizations using WINS to resolve NetBIOS names (also referred to as *computer names*) to TCP/IP addresses. Even today, many organizations still use WINS along with DNS for name resolution. Unfortunately, WINS is slowly becoming obsolete.

To help organizations move forward with an all-DNS network, Microsoft Windows Server 2012 R2 DNS supports *GlobalName zones*. These use single-label names (DNS names that do not contain a suffix such as `.com`, `.net`, and so on). GlobalName zones are not intended to support peer-to-peer networks and workstation name resolution, and they don't support dynamic DNS updates.

GlobalName zones are designed to be used with servers. Because GlobalName zones are not dynamic, an administrator has to enter the records into the zone database manually. In most organizations, the servers have static TCP/IP addresses, and this works well with the GlobalName zone design. GlobalName zones are usually used to map single-label CNAME (alias) resource records to an FQDN.

Zone Transfers and Replication

DNS is such an important part of the network that you should not just use a single DNS server. With a single DNS server, you also have a single point of failure and, in fact, many domain registrars encourage the use of more than two name servers for a domain. Secondary servers or multiple primary Active Directory Integrated servers play an integral role in providing DNS information for an entire domain.

As previously stated, secondary DNS servers receive their zone databases through zone transfers. When you configure a secondary server for the first time, you must specify the primary server that is authoritative for the zone and will send the zone transfer. The primary server must also permit the secondary server to request the zone transfer.

Zone transfers occur in one of two ways: *full zone transfers (AXFR)* and *incremental zone transfers (IXFR)*.

When a new secondary server is configured for the first time, it receives a full zone transfer from the primary DNS server. The full zone transfer contains all of the information in the DNS database. Some DNS implementations always receive full zone transfers.

After the secondary server receives its first full zone transfer, subsequent zone transfers are incremental. The primary name server compares its zone version number with that of the secondary server, and it sends only the changes that have been made in the interim. This significantly reduces network traffic generated by zone transfers.

The secondary server typically initiates zone transfers when the refresh interval time for the zone expires or when the secondary or stub server boots. Alternatively, you can configure notify lists on the primary server that send a message to the secondary or stub servers whenever any changes to the zone database occur.

When you consider your DNS strategy, you must carefully consider the layout of your network. If you have a single domain with offices in separate cities, you want to reduce the number of zone transfers across the potentially slow or expensive WAN links, although this is becoming less of a concern because of continuous increases in bandwidth.

Active Directory Integrated zones do away with traditional zone transfers altogether. Instead, they replicate across Active Directory with all of the other AD information. This replication is secure and encrypted because it uses the Active Directory security.

How DNS Notify Works

Windows Server 2012 R2 supports DNS Notify. *DNS Notify* is a mechanism that allows the process of initiating notifications to secondary servers when zone changes occur (RFC 1996). DNS Notify uses a push mechanism for communicating to a select set of secondary zone servers when their zone information is updated. (DNS Notify does not allow you to configure a notify list for a stub zone.)

After being notified of the changes, secondary servers can then start a pull zone transfer and update their local copies of the database.

Many different mechanisms use the push/pull relationship. Normally, one object pushes information to another, and the second object pulls the information from the first. Most applications push replication on a change value and pull it on a time value. For example, a system can push replication after 10 updates, or it can be pulled every 30 minutes.

To configure the DNS Notify process, you create a list of secondary servers to notify. List the IP address of the server in the primary master's Notify dialog box (see Figure 12.8). The Notify dialog box is located under the Zone Transfers tab, which is located in the zone Properties dialog box (see Figure 12.9).

FIGURE 12.8 DNS Notify dialog box

FIGURE 12.9 DNS Zone Transfers tab

Configuring Stub Zone Transfers with Zone Replication

In the preceding section, I talked about how to configure secondary server zone transfers. What if you wanted to configure settings for stub zone transfers? This is where zone replication scope comes in.

Only Active Directory–integrated primary and stub zones can configure their replication scope. Secondary servers do not have this ability.

You can configure zone replication scope configurations in two ways. An administrator can set configuration options through the DNS snap-in or through a command-line tool called `DNSCmd`.

To configure zone replication scope through the DNS snap-in, follow these steps:

1. Click Start ➢ Administrative Tools ➢ DNS.
2. Right-click the zone that you want to set up.
3. Choose Properties.
4. In the Properties dialog box, click the Change button next to Replication (see Figure 12.10).

FIGURE 12.10 DNS zone replication scope

5. Choose the replication scope that fits your organization.

Advantages of DNS in Windows Server 2012 R2

DNS in Microsoft Windows Server 2012 R2 has some great advantages over many other versions of Microsoft DNS. Here are some of the improvements of DNS in Windows Server 2012 R2 (some of these became available in Windows Server 2008):

- Background zone loading
- Support for TCP/IP version 6 (IPv6)
- Read-only domain controllers
- GlobalName zone
- DNS socket pools
- DNS cache locking
- DNS Security Extensions (DNSSEC)
- DNS devolution
- Record weighting
- Netmask ordering
- DnsUpdateProxy group

Background Zone Loading

If an organization had to restart a DNS server with an extremely large Active Directory Integrated DNS zones database in the past, DNS had a common problem with an Active Directory Integrated DNS zone. After the DNS restart, it could take hours for DNS data to be retrieved from Active Directory. During this time, the DNS server was unable to service any client requests.

Microsoft Windows Server 2008 DNS addressed this problem by implementing background zone loading, and Windows Server 2012 R2 has taken it a step further. As the DNS restarts, the Active Directory zone data populates the database in the background. This allows the DNS server to service client requests for data from other zones almost immediately after a restart.

Background zone loading accomplishes this task by loading the DNS zone using separate threads. This allows a DNS server to service requests while still loading the rest of the zone. If a client sends a request to the DNS server for a computer that has not yet loaded into memory, the DNS server retrieves the data from Active Directory and updates the record.

Support for IPv6 Addresses

Over the past few years, the Internet has starting running into a problem that was not foreseen when it was first created—it started running out of TCP/IP addresses. As you probably know, when the Internet was created, it was used for government and academic purposes only. Then, seemingly overnight, it grew to be the information superhighway. Nowadays, asking someone for their email address is almost more common as asking for their phone number.

Version 4 (IPv4) was the common version of TCP/IP. The release of TCP/IP version 6 (IPv6) has solved the lack-of-IP-addresses problem. IPv4 addresses are 32 bits long, but IPv6 addresses are 128 bits in length. The longer lengths allow for a much greater number of globally unique TCP/IP addresses.

Microsoft Windows Server 2012 R2 DNS has built-in support to accommodate both IPv4 and IPv6 address records (DNS records are explained later in this chapter). DHCP can also issue IPv6 addresses, which lets administrators allow DHCP to register the client with DNS, or the IPv6 client can register their address with the DNS server.

Support for Read-Only Domain Controllers

Windows Server 2008 introduced a new type of domain controller called the *read-only domain controller (RODC)*. This is a full copy of the Active Directory database without the ability to write to Active Directory. The RODC gives an organization the ability to install a domain controller in a location (onsite or offsite) where security is a concern.

Microsoft Windows Server 2012 R2 DNS has implemented a type of zone to help support an RODC. A primary read-only zone allows a DNS server to receive a copy of the application partition (including ForestDNSZones and DomainDNSZones) that DNS uses. This allows DNS to support an RODC because DNS now has a full copy of all DNS zones stored in Active Directory.

A primary, read-only zone is just what it says—a read-only zone; so to make any changes to it, you have to change the primary zones located on the Active Directory Integrated DNS server.

DNS Socket Pools

If your server is running Windows Server 2012 R2, you will be able to take advantage of DNS socket pools. *DNS socket pools* allow source port randomization to protect against DNS cache-poisoning attacks.

If you choose to use source port randomization, when the DNS service starts, the DNS server will randomly pick a source port from a pool of available sockets. This is an advantage because instead of DNS using a well-known source port when issuing queries, the DNS server uses a random port selected from the socket pool. This helps guard against attacks because a hacker must correctly access the source port of the DNS query. The socket pool is automatically enabled in DNS with the default settings.

When using the DNS socket pool, the default size of the DNS socket pool is 2,500. When configuring the socket pool, you have the ability to choose a size value from 0 to 10,000. The larger the value, the greater the protection you will have against DNS spoofing attacks. If you decide to configure your socket pool size with a zero value, only a single socket for remote DNS queries will be used.

DNS Cache Locking

Windows Server 2012 R2 *DNS cache locking* allows cached DNS records to remain safe for the duration of the record's time to live (TTL) value. This means that the cached DNS records cannot be overwritten or changed. Because of this new DNS feature, it's tougher for hackers to perform cache-poisoning attacks against your DNS server.

DNS administrators can set how long a record will remain safe in cache. The configuration is based on a percent value. For example, if you set your cache locking value to 50 percent, then the cached records cannot be overwritten until half of the TTL has been reached. DNS cache locking is set to 100 percent by default. This means that the cached records never get overwritten.

DNS Security Extensions

One major issue that you must always look at is keeping your DNS safe. Think about it: DNS is a database of computer names and IP addresses. As a hacker, if I control DNS, I can control your company. In organizations that do not support extra security like IPsec, DNS security is even more important. This is where *Domain Name System Security Extensions (DNSSEC)* can help.

Windows Server 2012 R2 can use a suite of extensions that will help add security to DNS, and that suite is called DNSSEC, which was introduced in Windows Server 2008 R2. The DNSSEC protocol allows your DNS servers to be secure by validating DNS responses. DNSSEC secures your DNS resource records by accompanying the records with a digital signature.

To allow your DNS resource records to receive digital signatures, DNSSEC is applied to your DNS server by a procedure called *zone signing*. This process begins when a DNS resolver initiates a DNS query for a resource record in a signed DNS zone. When a response is returned, a digital signature (RRSIG) accompanies the response, and this allows the response to be verified. If the verification is successful, then the DNS resolver knows that the data has not been modified or tampered with in any way.

Once you implement a zone with DNSSEC, all of the records that are contained within that zone get individually signed. Since all of the records in the zone get individually signed, this gives administrators the ability to add, modify, or delete records without re-signing the entire zone. The only requirement is to re-sign any updated records.

Trust Anchors

Trust anchors are an important part of the DNSSEC process because trust anchors allow the DNS servers to validate the DNSKEY resource records. *Trust anchors* are preconfigured public keys that are linked to a DNS zone. For a DNS server to perform validation, one or more trust anchors must be configured. If you are running an Active Directory Integrated zone, trust anchors can be stored in the Active Directory Domain Services directory partition of the forest. If you decide to store the trust anchors in the directory partition, then all DNS servers that reside on a domain controller get a copy of this trust anchor. On DNS servers that reside on stand-alone servers, trust anchors are stored in a file called `TrustAnchors.dns`.

If your servers are running Windows Server 2012 R2, then you can view trust anchors in the DNS Manager Console tree in the Trust Points container. You can also use Windows PowerShell or `Dnscmd.exe` to view trust anchors. Windows PowerShell is the recommended

command-line method for viewing trust anchors. The following line is a PowerShell command to view the trust anchors for `Contoso.com`:

```
get-dnsservertrustanchor sec.contoso.com
```

DNSSEC Clients

Windows 7, Windows 8, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2 are all DNS clients that receive a response to a DNS query, examine the response, and then evaluate whether the response has been validated by a DNS server. The DNS client itself is nonvalidating, and the DNS client relies on the local DNS server to indicate that validation was successful. If the server doesn't perform validation, then the DNS client service can be configured to return no results.

DNS Devolution

Using *DNS devolution*, if a client computer is a member of a child namespace, the client computer will be able to access resources in the parent namespace without the need to explicitly provide the fully qualified domain name of the resource. DNS devolution removes the leftmost label of the namespace to get to the parent suffix. DNS devolution allows the DNS resolver to create the new FQDNs. DNS devolution works by appending the single-label, unqualified domain name with the parent suffix of the primary DNS suffix name.

Record Weighting

Weighting DNS records will allow an administrator to place a value on DNS SRV records. Clients will then randomly choose SRV records proportional to the weight value assigned.

Netmask Ordering

If round robin is enabled, when a client requests name resolution, the first address entered in the database is returned to the resolver, and it is then sent to the end of the list. The next time a client attempts to resolve the name, the DNS server returns the second name in the database (which is now the first name) and then sends it to the end of the list, and so on. Round robin is enabled by default.

Netmask ordering is a part of the round robin process. When an administrator configures netmask ordering, the DNS server will detect the subnet of the querying client. The DNS server will then return a host address available for the same subnet. Netmask ordering is enabled through the DNS Manager console on the Advanced tab of the server Properties dialog box.

DnsUpdateProxy Group

As mentioned previously, the DHCP server can be configured to register host (A) and pointer (PTR) resource records dynamically on behalf of DHCP clients. Because of this, the DNS server can end up with stale resources. To help solve this issue, an administrator can use the built-in security group called *DnsUpdateProxy*.

To use the DnsUpdateProxy group, an administrator must first create a dedicated user account and configure the DHCP servers with its credentials. This will protect against the creation of unsecured records. Also, when you create the dedicated user account, members of the DnsUpdateProxy group will be able to register records in zones that allow only secured dynamic updates. Multiple DHCP servers can use the same credentials of one dedicated user account.

Now that you have learned about some of the new features of Windows Server 2012 R2 DNS, let's take a look at some of the DNS record types.

Introducing DNS Record Types

No matter where your zone information is stored, you can rest assured that it contains a variety of DNS information. Although the DNS snap-in makes it unlikely that you'll ever need to edit these files by hand, it's good to know exactly what data is contained there.

As stated previously, zone files consist of a number of resource records. You need to know about several types of resource records to manage your DNS servers effectively. They are discussed in the following sections.

Part of the resource record is its class. *Classes* define the type of network for the resource record. There are three classes: Internet, Chaosnet, and Hesoid. By far, the Internet class is the most popular. In fact, it's doubtful that you'll see either Chaosnet or Hesoid classes in the wild.

NOTE

The following are some of the more important resource records in a DNS database. For a complete listing of records in a Microsoft DNS database, visit Microsoft's website at `http://technet.microsoft.com/en-us/library/cc758321(v=WS.10).aspx`.

Start of Authority (SOA) Records

The first record in a database file is the *start of authority (SOA) record*. The SOA defines the general parameters for the DNS zone, including the identity of the authoritative server for the zone.

The SOA appears in the following format:

```
@ IN SOA primary_mastercontact_e-mailserial_number
refresh_timeretry_timeexpiration_timetime_to_live
```

Here is a sample SOA from the domain `example.com`:

```
@ IN SOA win2k3r2.example.com. hostmaster.example.com. (
                        5            ; serial number
                        900          ; refresh
                        600          ; retry
                        86400        ; expire
                        3600       ) ; default TTL
```

Table 12.2 lists the attributes stored in the SOA record.

TABLE 12.2 The SOA record structure

Field	Meaning
Current zone	The current zone for the SOA. This can be represented by an `@` symbol to indicate the current zone or by naming the zone itself. In the example, the current zone is `example.com`. The trailing dot (`.com.`) indicates the zone's place relative to the root of the DNS.
Class	This will almost always be the letters *IN* for the Internet class.
Type of record	The type of record follows. In this case, it's SOA.
Primary master	The primary master for the zone on which this file is maintained.
Contact email	The Internet email address for the person responsible for this domain's database file. There is no `@` symbol in this contact email address because `@` is a special character in zone files. The contact email address is separated by a single dot (`.`). So, the email address of `root@example.com` would be represented by `root.example.com` in a zone file.
Serial number	This is the "version number" of this database file. It increases each time the database file is changed.
Refresh time	The amount of time (in seconds) that a secondary server will wait between checks to its master server to see whether the database file has changed and a zone transfer should be requested.
Retry time	The amount of time (in seconds) that a secondary server will wait before retrying a failed zone transfer.
Expiration time	The amount of time (in seconds) that a secondary server will spend trying to download a zone. Once this time limit expires, the old zone information will be discarded.
Time to live	The amount of time (in seconds) that another DNS server is allowed to cache any resource records from this database file. This is the value that is sent out with all query responses from this zone file when the individual resource record doesn't contain an overriding value.

Name Server Records

Name server (NS) records list the name servers for a domain. This record allows other name servers to look up names in your domain. A zone file may contain more than one name server record. The format of these records is simple:

```
example.com.    IN      NS      Hostname.example.com
```

Table 12.3 explains the attributes stored in the NS record.

TABLE 12.3 The NS record structure

Field	Meaning
Name	The domain that will be serviced by this name server. In this case I used `example.com`.
AddressClass	Internet (IN)
RecordType	Name server (NS)
Name Server Name	The FQDN of the server responsible for the domain

Any domain name in the database file that is not terminated with a period will have the root domain appended to the end. For example, an entry that just has the name *sales* will be expanded by adding the root domain to the end, whereas the entry `sales.example.com.` won't be expanded.

Host Record

A *host record* (also called an *A record* for IPv4 and *AAAA record* for IPv6) is used to associate statically a host's name to its IP addresses. The format is pretty simple:

```
host_nameoptional_TTL IN  A  IP_Address
```

Here's an example from my DNS database:

```
www  IN  A  192.168.0.204
SMTP IN  A  192.168.3.144
```

The A or AAAA record ties a hostname (which is part of an FQDN) to a specific IP address. This makes these records suitable for use when you have devices with statically assigned IP addresses. In this case, you create these records manually using the DNS snap-in. As it turns out, if you enable DDNS, your DHCP server can create these for you. This automatic creation is what enables DDNS to work.

Notice that an optional TTL field is available for each resource record in the DNS. This value is used to set a TTL that is different from the default TTL for the domain. For example, if you wanted a 60-second TTL for the www A or AAAA record, it would look like this:

```
www 60 IN  A  192.168.0.204
```

Alias Record

Closely related to the host record is the *alias record*, or *canonical name (CNAME) record*. The syntax of an alias record is as follows:

aliasoptional_TTL `IN CNAME` *hostname*

Aliases are used to point more than one DNS record toward a host for which an A record already exists. For example, if the hostname of your web server was actually `chaos`, you would likely have an A record such as this:

```
chaos IN A 192.168.1.10
```

Then you could make an alias or CNAME for the record so that `www.example.com` would point to `chaos`:

```
www IN CNAME chaos.example.com.
```

Note the trailing dot (`.`) on the end of the CNAME record. This means the root domain is not appended to the entry.

Pointer Record

A or AAAA records are probably the most visible component of the DNS database because Internet users depend on them to turn FQDNs like `www.microsoft.com` into the IP addresses that browsers and other components require to find Internet resources. However, the host record has a lesser-known but still important twin: the *pointer (PTR) record*. The format of a PTR record appears as follows:

`reversed_address.in-addr.arpa. optional_TTL IN PTR targeted_domain_name`

The A or AAAA record maps a hostname to an IP address, and the PTR record does just the opposite—mapping an IP address to a hostname through the use of the `in-addr.arpa` zone.

The PTR record is necessary because IP addresses begin with the least-specific portion first (the network) and end with the most-specific portion (the host), whereas hostnames begin with the most-specific portion at the beginning and the least-specific portion at the end.

Consider the example 192.168.1.10 with a subnet mask 255.255.255.0. The portion 192.168.1 defines the network and the final .10 defines the host, or the most-specific portion of the address. DNS is just the opposite: The hostname `www.example.com.` defines the most-specific portion, `www`, at the beginning and then traverses the DNS tree to the least-specific part, the dot (`.`), at the root of the tree.

Reverse DNS records, therefore, need to be represented in this most-specific-to-least-specific manner. The PTR record for mapping 192.168.1.10 to `www.example.com` would look like this:

```
10.1.168.192.in-addr.arpa. IN PTR www.example.com.
```

Now a DNS query for that record can follow the logical DNS hierarchy from the root of the DNS tree all the way to the most-specific portion.

Mail Exchanger Record

The *mail exchanger (MX) record* is used to specify which servers accept mail for this domain. Each MX record contains two parameters—a preference and a mail server, as shown in the following example:

```
domain IN MX preference mailserver_host
```

The MX record uses the preference value to specify which server should be used if more than one MX record is present. The preference value is a number. The lower the number, the more preferred the server. Here's an example:

```
example.com.    IN  MX  0  mail.example.com.
example.com.    IN  MX  10 backupmail.example.com.
```

In the example, `mail.example.com` is the default mail server for the domain. If that server goes down for any reason, the `backupmail.example.com` mail server is used by emailers.

Service Record

Windows Server 2012 R2 depends on some other services, like the Lightweight Directory Access Protocol (LDAP) and Kerberos. Using a service record, which is another type of DNS record, a Windows 2000, XP, Vista, Windows 7, or Windows 8 client can query DNS servers for the location of a domain controller. This makes it much easier (for both the client and the administrator) to manage and distribute logon traffic in large-scale networks. For this approach to work, Microsoft has to have some way to register the presence of a service in DNS. Enter the service (SRV) record.

Service (SRV) records tie together the location of a service (like a domain controller) with information about how to contact the service. SRV records provide seven items of information. Let's review an example to help clarify this powerful concept. (Table 12.4 explains the fields in the following example.)

```
ldap.tcp.example.com.  86400 IN SRV  10  100  389  hsv.example.com
ldap.tcp.example.com.  86400 IN SRV  20  100  389  msy.example.com
```

TABLE 12.4 The SRV record structure

Field	Meaning
Domain name	Domain for which this record is valid (`ldap.tcp.example.com.`).
TTL	Time to live (86,400 seconds).
Class	This field is always `IN`, which stands for Internet.
Record type	Type of record (`SRV`).
Priority	Specifies a preference, similar to the Preference field in an MX record. The SRV record with the lowest priority is used first (`10`).
Weight	Service records with equal priority are chosen according to their weight (`100`).
Port number	The port where the server is listening for this service (`389`).
Target	The FQDN of the host computer (`hsv.example.com` and `msy.example.com`).

NOTE

You can define other types of service records. If your applications support them, they can query DNS to find the services they need.

Configuring DNS

In the following sections, you'll begin to learn about the actual DNS server. You will start by installing DNS. Then I will talk about different zone configuration options and what they mean. Finally, you'll complete an exercise that covers configuring Dynamic DNS, delegating zones, and manually entering records.

Installing DNS

If you have been reading this book since Chapter 1, then this exercise was done in Chapter 2. If you started reading this book with Part 2, then this chapter will show you how to install DNS. If DNS is already installed onto your server, you can skip this exercise. But if you have not installed DNS, let's start by installing DNS. Installing DNS is an important part of running a network. Exercise 12.1 walks you through the installation of a DNS server.

If you are using a Dynamic TCP/IP address, please change your TCP/IP number to static. If you are unsure how to assign your server a static TCP/IP address, please refer to Chapter 2.

EXERCISE 12.1

Installing and Configuring the DNS Service

1. Open Server Manager.
2. On the Server Manager dashboard, click the Add Roles And Features link.

3. If a Before You Begin screen appears, click Next.
4. On the Selection type page, choose Role-Based Or Feature-Based Installation and click Next.
5. Click the Select A Server From The Server Pool radio button and choose the server under the Server Pool section. Click Next.

EXERCISE 12.1 *(continued)*

6. Click the DNS Server Item in the Server Role list. If a pop-up window appears telling you that you need to add additional features, click the Add Features button. Click Next to continue.

7. On the Add Features page, just click Next.
8. Click Next on the DNS Server information screen.
9. On the Confirm Installation screen, choose the Restart The Destination Server Automatically If Required check box and then click the Install button.
10. At the Installation progress screen, click Close after the DNS server is installed.
11. Close Server Manager.

Load Balancing with Round Robin

Like other DNS implementations, the Windows Server 2012 R2 implementation of DNS supports load balancing through the use of round robin. Load balancing distributes the network load among multiple network hosts if they are available. You set up round-robin load balancing by creating multiple resource records with the same hostname but different IP addresses for multiple computers. Depending on the options that you select, the DNS server responds with the addresses of one of the host computers.

If round robin is enabled, when a client requests name resolution, the first address entered in the database is returned to the resolver and is then sent to the end of the list. The next time a client attempts to resolve the name, the DNS server returns the second name in the database (which is now the first name) and then sends it to the end of the list, and so on. Round robin is enabled by default.

Configuring a Caching-Only Server

Although all DNS name servers cache queries that they have resolved, caching-only servers are DNS name servers that only perform queries, cache the answers, and return the results. They are not authoritative for any domains, and the information that they contain is limited to what has been cached while resolving queries. Accordingly, they don't have any zone files, and they don't participate in zone transfers. When a caching-only server is first started, it has no information in its cache; the cache is gradually built over time.

Caching-only servers are easy to configure. After installing the DNS service, simply make sure the root hints are configured properly.

1. Right-click your DNS server and choose the Properties command.
2. When the Properties dialog box appears, switch to the Root Hints tab (see Figure 12.11).
3. If your server is connected to the Internet, you should see a list of root hints for the root servers maintained by ICANN and the Internet Assigned Numbers Authority (IANA). If not, click the Add button to add root hints as defined in the `cache.dns` file.

FIGURE 12.11 The Root Hints tab of the DNS server's Properties dialog box

You can obtain current cache·dns files on the Internet by using a search engine. Just search for *cache.dns* and download one. (I always try to get cache·dns files from a university or a company that manages domain names.)

Setting Zone Properties

There are six tabs on the Properties dialog box for a forward or reverse lookup zone. You only use the Security tab to control who can change properties and to make dynamic updates to records on that zone. The other tabs are discussed in the following sections.

Secondary zones don't have a Security tab, and their SOA tab shows you the contents of the master SOA record, which you can't change.

General Tab

The General tab includes the following:

- The Status indicator and the associated Pause button let you see and control whether this zone can be used to answer queries. When the zone is running, the server can use it to answer client queries; when it's paused, the server won't answer any queries it gets for that particular zone.
- The Type indicator and its Change button allow you to select the zone type. The options are Standard Primary, Standard Secondary, and AD-Integrated. (See "Introducing DNS Database Zones" earlier in this chapter.) As you change the type, the controls you see

below the horizontal dividing line change too. For primary zones, you'll see a field that lets you select the zone filename; for secondary zones, you'll get controls that allow you to specify the IP addresses of the primary servers. But the most interesting controls are the ones you see for AD Integrated zones. When you change to the AD Integrated zones, you have the ability to make the dynamic zones Secure Only.

- The Replication indicator and its Change button allow you to change the replication scope if the zone is stored in Active Directory. You can choose to replicate the zone data to any of the following:
  - All DNS servers in the Active Directory forest
  - All DNS servers in a specified domain
  - All domain controllers in the Active Directory domain (required if you use Windows 2000 domain controllers in your domain)
  - All domain controllers specified in the replication scope of the application directory partition
- The Dynamic Updates field gives you a way to specify whether you want to support Dynamic DNS updates from compatible DHCP servers. As you learned earlier in the section "Dynamic DNS and Non-Dynamic DNS," the DHCP server or DHCP client must know about and support Dynamic DNS in order to use it, but the DNS server has to participate too. You can turn dynamic updates on or off, or you can require that updates be secured.

Start Of Authority (SOA) Tab

The following options in the Start Of Authority (SOA) tab, shown in Figure 12.12, control the contents of the SOA record for this zone.

FIGURE 12.12 The Start Of Authority (SOA) tab of the zone Properties dialog box

- The Serial Number field indicates which version of the SOA record the server currently holds. Every time you change another field, you should increment the serial number so that other servers will notice the change and get a copy of the updated record.
- The Primary Server and Responsible Person fields indicate the location of the primary name server for this zone and the email address of the administrator responsible for the maintenance of this zone, respectively. The standard username for this is hostmaster.
- The Refresh Interval field controls how often any secondary zones of this zone must contact the primary zone server and get any changes that have been posted since the last update.
- The Retry Interval field controls how long secondary servers will wait after a zone transfer fails before they try again. They'll keep trying at the interval you specify (which should be shorter than the refresh interval) until they eventually succeed in transferring zone data.
- The Expires After field tells the secondary servers when to throw away zone data. The default of 1 day (24 hours) means that a secondary server that hasn't gotten an update in 24 hours will delete its local copy of the zone data.
- The Minimum (Default) TTL field sets the default TTL for all RRs created in the zone. You can assign specific TTLs to individual records if you want.
- The TTL For This Record field controls the TTL for the SOA record itself.

Name Servers Tab

The *name server (NS) record* for a zone indicates which name servers are authoritative for the zone. That normally means the zone primary server and any secondary servers you've configured for the zone. (Remember, secondary servers are authoritative read-only copies of the zone.) You edit the NS record for a zone using the Name Servers tab (see Figure 12.13).

FIGURE 12.13 The Name Servers tab of the zone Properties dialog box

The tab shows you which servers are currently listed, and you use the Add, Edit, and Remove buttons to specify which name servers you want included in the zone's NS record.

WINS Tab

The WINS tab allows you to control whether this zone uses WINS forward lookups or not. These lookups pass on queries that DNS can't resolve to WINS for action. This is a useful setup if you're still using WINS on your network. You must explicitly turn this option on with the Use WINS Forward Lookup check box in the WINS tab for a particular zone.

Zone Transfers Tab

Zone transfers are necessary and useful because they're the mechanism used to propagate zone data between primary and secondary servers. For primary servers (whether AD Integrated or not), you can specify whether your servers will allow zone transfers and, if so, to whom.

You can use the following controls on the Zone Transfers tab to configure these settings per zone:

- The Allow Zone Transfers check box controls whether the server answers zone transfer requests for this zone at all—when it's not checked, no zone data is transferred. The Allow Zone Transfers selections are as follows:
  - To Any Server allows any server anywhere on the Internet to request a copy of your zone data.
  - Only To Servers Listed On The Name Servers Tab (the default) limits transfers to servers you specify. This is a more secure setting than To Any Server because it limits transfers to other servers for the same zone.
  - Only To The Following Servers allows you to specify exactly which servers are allowed to request zone transfers. This list can be larger or smaller than the list specified on the Name Servers tab.
- The Notify button is for setting up automatic notification triggers that are sent to secondary servers for this zone. Those triggers signal the secondary servers that changes have occurred on the primary server so that the secondary servers can request updates sooner than their normally scheduled interval. The options in the Notify dialog box are similar to those in the Zone Transfers tab. You can enable automatic notification and then choose either Servers Listed On The Name Servers Tab or The Following Servers.

Configuring Zones for Dynamic Updates

In Exercise 12.2, you will create and then modify the properties of a forward lookup zone. In addition, you'll configure the zone to allow dynamic updates.

EXERCISE 12.2

Configuring a Zone for Dynamic Updates

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Click the DNS server to expand it and then click the Forward Lookup Zones folder. Right-click the Forward Lookup Zones folder and choose New Zone.

3. At the New Zone Welcome screen, click Next.
4. At the Zone Type screen, choose the Primary Zone option. If your DNS server is also a domain controller, do not check the box to store the zone in Active Directory. Click Next when you are ready.

5. Enter a new zone name in the Zone Name field and click Next. (I used my last name—`Panek.com`.)
6. Leave the default zone filename and click Next.
7. Select the Do Not Allow Dynamic Updates radio button and click Next.
8. Click Finish to end the wizard.
9. Right-click the zone you just created and choose the Properties command.
10. Click the down arrow next to Dynamic Updates. Notice that there are only two options (None and Nonsecure And Secure). The Secure Only option is not available because you are not using Active Directory Integrated. Make sure Nonsecure And Secure is chosen.

11. Click OK to close the Properties box.
12. Close the DNS management snap-in.
13. Close the Server Manager snap-in.

Delegating Zones for DNS

DNS provides the ability to divide the namespace into one or more zones, which can then be stored, distributed, and replicated to other DNS servers. When deciding whether to divide your DNS namespace to make additional zones, consider the following reasons to use additional zones:

- A need to delegate management of part of your DNS namespace to another location or department within your organization

- A need to divide one large zone into smaller zones for distributing traffic loads among multiple servers, for improving DNS name-resolution performance, or for creating a more fault-tolerant DNS environment
- A need to extend the namespace by adding numerous subdomains at once, such as to accommodate the opening of a new branch or site

Each newly delegated zone requires a primary DNS server just as a regular DNS zone does. When delegating zones within your namespace, be aware that for each new zone you create, you need to place delegation records in other zones that point to the authoritative DNS servers for the new zone. This is necessary both to transfer authority and to provide correct referral to other DNS servers and clients of the new servers being made authoritative for the new zone.

In Exercise 12.3, you'll create a delegated subdomain of the domain you created in Exercise 12.2. Note that the name of the server to which you want to delegate the subdomain must be stored in an A or CNAME record in the parent domain.

EXERCISE 12.3

Creating a Delegated DNS Zone

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Expand the DNS server and locate the zone you created in Exercise 12.2.
3. Right-click the zone and choose the New Delegation command.
4. The New Delegation Wizard appears. Click Next to dismiss the initial wizard page.
5. Enter **`ns1`** (or whatever other name you like) in the Delegated Domain field of the Delegated Domain Name page. This is the name of the domain for which you want to delegate authority to another DNS server. It should be a subdomain of the primary domain (for example, to delegate authority for `farmington.example.net`, you'd enter **`farmington`** in the Delegated Domain field). Click Next to complete this step.
6. When the Name Servers page appears, click the Add button to add the names and IP addresses of the servers that will be hosting the newly delegated zone. For the purpose of this exercise, enter the server name you used in Exercise 12.2. Click the Resolve button to resolve this domain name's IP address automatically into the IP address field. Click OK when you are finished. Click Next to continue with the wizard.
7. Click the Finish button. The New Delegation Wizard disappears, and you'll see the new zone you just created appear beneath the zone you selected in step 3. The newly delegated zone's folder icon is drawn in gray to indicate that control of the zone is delegated.

DNS Forwarding

If a DNS server does not have an answer to a DNS request, it may be necessary to send that request to another DNS server. This is called *DNS forwarding*. You need to understand the two main types of forwarding:

External Forwarding When a DNS server forwards an external DNS request to a DNS server outside of your organization, this is considered *external forwarding*. For example, a resolver requests the host `www.microsoft.com`. Most likely, your internal DNS server is not going to have Microsoft's web address in its DNS database. So, your DNS server is going to send the request to an external DNS (most likely your ISP).

Conditional Forwarding *Conditional forwarding* is a lot like external forwarding except that you are going to forward requests to specific DNS servers based on a condition. Usually this is an excellent setup for internal DNS resolution. For example, let's say that you have two companies, `stellacon.com` and `stellatest.com`. If a request comes in for `Stellacon.com`, it gets forwarded to the Stellacon DNS server, and any requests for `Stellatest.com` will get forwarded to the Stellatest DNS server. Requests are forwarded to a specific DNS server depending on the condition that an administrator sets up.

Manually Creating DNS Records

From time to time you may find it necessary to add resource records manually to your Windows Server 2012 R2 DNS servers. Although Dynamic DNS frees you from the need to fiddle with A and PTR records for clients and other such entries, you still have to create other resource types (including MX records, required for the proper flow of SMTP email) manually. You can manually create A, PTR, MX, SRV, and many other record types.

There are only two important things to remember for manually creating DNS records:

- You must right-click the zone and choose either the New Record command or the Other New Records command.
- You must know how to fill in the fields of whatever record type you're using.

  For example, to create an MX record, you need three pieces of information (the domain, the mail server, and the priority). To create an SRV record, however, you need several more pieces of information.

In Exercise 12.4, you will manually create an MX record for a mailtest server in the zone you created in Exercise 12.2.

EXERCISE 12.4

Manually Creating DNS RRs

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.

EXERCISE 12.4 *(continued)*

2. Expand your DNS server, right-click its zone, and choose New Host (A record).

3. Enter **`mailtest`** in the Name field. Enter a TCP/IP number in the IP Address field. (You can use any number for this exercise, for example, 192.168.1.254.) Click the Add Host button.
4. A dialog box appears stating that the host record was created successfully. Click OK. Click Done.
5. Right-click your zone name and choose New Mail Exchanger (MX).
6. Enter **`mailtest`** in the Host Or Child Domain field and enter **`mailtest.yourDomain.com`** (or whatever domain name you used in Exercise 12.2) in the Fully-Qualified Domain Name (FQDN) Of Mail Server field and then click OK. Notice that the new record is already visible.
7. Next create an alias (or CNAME) record to point to the mail server. (It is assumed that you already have an A record for `mailtest` in your zone.) Right-click your zone and choose New Alias (CNAME).
8. Type **`mail`** into the Alias Name field.
9. Type **`mailtest.yourDomain.com`** into the Fully-Qualified Domain Name (FQDN) For Target Host field.
10. Click the OK button.
11. Close the DNS management snap-in.

DNS Aging and Scavenging

When using dynamic updates, computers (or DHCP) will register a resource record with DNS. These records get removed when a computer is shut down properly. A major problem in the industry is that laptops are frequently removed from the network without a proper shutdown. Therefore, their resource records continue to live in the DNS database.

Windows Server 2012 R2 DNS supports two features called *DNS aging* and *DNS scavenging*. These features are used to clean up and remove stale resource records. DNS zone or DNS server aging and scavenging flag old resource records that have not been updated in a certain amount of time (determined by the scavenging interval). These stale records will be scavenged at the next cleanup interval. DNS uses time stamps on the resource records to determine how long they have been listed in the DNS database.

Monitoring and Troubleshooting DNS

Now that you have set up and configured your DNS name server and created some resource records, you will want to confirm that it is resolving and replying to client DNS requests. A couple of tools allow you to do some basic monitoring and managing. Once you are able to monitor DNS, you'll want to start troubleshooting.

The simplest test is to use the `ping` command to make sure that the server is alive. A more thorough test would be to use `nslookup` to verify that you can actually resolve addresses for items on your DNS server.

In the following sections, you'll look at some of these monitoring and management tools and how to troubleshoot DNS.

Monitoring DNS with the DNS Snap-In

You can use the DNS snap-in to do some basic server testing and monitoring. More important, you use the snap-in to monitor and set logging options. On the Event Logging tab of the server's Properties dialog box (see Figure 12.14), you can pick which events you want logged. The more events you select, the more logging information you'll get. This is useful when you're trying to track what's happening with your servers, but it can result in a very large log file if you're not careful.

FIGURE 12.14 The Event Logging tab of the server's Properties dialog box

The Monitoring tab (see Figure 12.15) gives you some testing tools. When the check box labeled A Simple Query Against This DNS Server is checked, a test is performed that asks for a single record from the local DNS server. It's useful for verifying that the service is running and listening to queries, but not much else. When the check box labeled A Recursive Query To Other DNS Servers is checked, the test is more sophisticated—a recursive query checks whether forwarding is working okay. The Test Now button and the Perform Automatic Testing At The Following Interval check box allow you to run these tests now or later as you require.

FIGURE 12.15 The Monitoring tab of the server's Properties dialog box

Another tab in the server's properties that allows you to monitor the activity of the DNS server is the Debug Logging tab. The Debug Logging tab allows you to monitor all outbound and inbound DNS traffic, packet content, packet type, and which transport protocol (TCP or UDP) that you want to monitor on the DNS server.

If the simple query fails, check that the local server contains the zone `1.0.0.127.in-addr.arpa`. If the recursive query fails, check that your root hints are correct and that your root servers are running.

In Exercise 12.5, you will enable logging, use the DNS MMC to test the DNS server, and view the contents of the DNS log.

EXERCISE 12.5

Simple DNS Testing

1. Open the DNS management snap-in by selecting Server Manager. Once in Server Manager, click DNS on the left side. In the Servers window (center screen), right-click your server name and choose DNS Manager.
2. Right-click the DNS server name on the top left and select Properties.
3. Switch to the Debug Logging tab, check all the debug logging options except Filter Packets By IP Address and enter a full path and filename in the File Path And Name field. Click the Apply button.

4. Switch to the Monitoring tab and check both A Simple Query Against This DNS Server and A Recursive Query To Other DNS Servers.
5. Click the Test Now button several times and then click OK.
6. Press the Windows key on the keyboard (left side between the Ctrl and Alt keys) and then choose Computer. Navigate to the folder that you specified in step 3 and use WordPad or Notepad to view the contents of the log file.

Troubleshooting DNS

When troubleshooting DNS problems, ask yourself the following basic questions:

- What application is failing? What works? What doesn't work?

- Is the problem basic IP connectivity, or is it name resolution? If the problem is name resolution, does the failing application use NetBIOS names, DNS names, or hostnames?
- How are the things that do and don't work related?
- Have the things that don't work ever worked on this computer or network? If so, what has changed since they last worked?

Windows Server 2012 R2 provides several useful tools, discussed in the following sections, which can help you answer these questions:

- `Nslookup` is used to perform DNS queries and to examine the contents of zone files on local and remote servers.
- `DNSLint` is a command-line utility used for troubleshooting many common DNS issues.
- `Ipconfig` allows you to perform the following tasks:
  - View DNS client settings
  - Display and flush the resolver cache
  - Force a dynamic update client to register its DNS records
- The DNS log file monitors certain DNS server events and logs them for your edification.

Using *Nslookup*

`Nslookup` is a standard command-line tool provided in most DNS server implementations, including Windows Server 2012 R2. Windows Server 2012 R2 gives you the ability to launch `nslookup` from the DNS snap-in.

When `nslookup` is launched from the DNS snap-in, a command prompt window opens automatically. You enter `nslookup` commands in this window.

`Nslookup` offers you the ability to perform query testing of DNS servers and to obtain detailed responses at the command prompt. This information can be useful for diagnosing and solving name resolution problems, for verifying that resource records are added or updated correctly in a zone, and for debugging other server-related problems. You can do a number of useful things with `nslookup`:

- Use it in noninteractive mode to look up a single piece of data
- Enter interactive mode and use the debug feature
- Perform the following from within interactive mode:
  - Set options for your query
  - Look up a name
  - Look up records in a zone

- Perform zone transfers
- Exit nslookup

When you are entering queries, it is generally a good idea to enter FQDNs so that you can control what name is submitted to the server. However, if you want to know which suffixes are added to unqualified names before they are submitted to the server, you can enter **nslookup** in debug mode and then enter an unqualified name.

Using *Nslookup* on the Command Line

To use nslookup in plain-old command-line mode, enter the following in the command prompt window:

```
nslookup DNS_name_or_IP_address server_IP_address
```

This command will look up a DNS name or address using a server at the IP address you specify.

Using *Nslookup* in Interactive Mode

Nslookup is a lot more useful in interactive mode because you can enter several commands in sequence. Entering **nslookup** by itself (without specifying a query or server) puts it in interactive mode, where it will stay until you type **exit** and press Enter. Before that point, you can look up lots of useful stuff. The following are some of the tasks that you can perform with nslookup in interactive mode:

Setting Options with the set Command While in interactive mode, you can use the set command to configure how the resolver will carry out queries. Table 12.5 shows a few of the options available with set.

TABLE 12.5 Command-line options available with the set command

Option	Purpose
set all	Shows all the options available.
set d2	Puts nslookup in debug mode so that you can examine the query and response packets between the resolver and the server.
set domain=*domain name*	Tells the resolver what domain name to append for unqualified queries.
set timeout=*timeout*	Tells the resolver how long to keep trying to contact the server. This option is useful for slow links where queries frequently time out and the wait time must be lengthened.
set type=*record type*	Tells the resolver which type of resource records to search for (for example, A, PTR, or SRV). If you want the resolver to query for all types of resource records, type **settype=all**.

Looking Up a Name While in interactive mode, you can look up a name just by typing it: **`stellacon.com`**. In this example, `stellacon` is the owner name for the record for which you are searching, and `.com` is the server that you want to query.

You can use the wildcard character (`*`) in your query. For example, if you want to look for all resource records that have *k* as the first letter, just type **`k*`** as your query.

Looking Up a Record Type If you want to query a particular type of record (for instance, an MX record), use the `set type` command. The command `set type=mx` tells `nslookup` that you're interested only in seeing MX records that meet your search criteria.

Listing the Contents of a Domain To get a list of the contents of an entire domain, use the `ls` command. To find all the hosts in your domain, you'd type **`set type=a`** and then type **`ls -t yourdomain.com`**.

Troubleshooting Zone Transfers You can simulate zone transfers by using the `ls` command with the `-d` switch. This can help you determine whether the server you are querying allows zone transfers to your computer. To do this, type the following: **`ls -d domain_name`**.

Nslookup Responses and Error Messages

A successful `nslookup` response looks like this:

```
Server: Name_of_DNS_server
Address: IP_address_of_DNS_server
Response_data
```

`Nslookup` might also return an error message. Some common messages are listed in Table 12.6.

TABLE 12.6 Common `nslookup` error messages

Error message	Meaning

`DNS request timed out.`
`Timeout was x seconds.`
`*** Can't find server name for address IP_Address: Timed out`
`*** Default servers are not available`
`Default Server: Unknown`
`Address: IP_address_of_DNS_server`
	The resolver did not locate a PTR resource record (containing the hostname) for the server IP address you specified. `Nslookup` can still query the DNS server, and the DNS server can still answer queries.

`*** Request to Server timed-out`	A request was not fulfilled in the allotted time. This might happen, for example, if the DNS service was not running on the DNS server that is authoritative for the name.

`*** Server can't find` *`Name_or_IP_address_queried_for`*`: No response from server`	The server is not receiving requests on User Datagram Protocol (UDP) port 53.
`*** Server can't find` *`Name_or_IP_address_queried_for:`* `Non-existent domain`	The DNS server was unable to find the name or IP address in the authoritative domain. The authoritative domain might be on the remote DNS server or on another DNS server that this DNS server is unable to reach.
`*** Server can't find` *`Name_or_IP_address_queried_for`*`: Server failed`	The DNS server is running, but it is not working properly. For example, it might include a corrupted packet, or the zone in which you are querying for a record might be paused. However, this message can also be returned if the client queries for a host in a domain for which the DNS server is not authoritative. You will also receive the error if the DNS server cannot contact its root servers, it is not connected to the Internet, or it has no root hints.

In Exercise 12.6, you'll get some hands-on practice with the `nslookup` tool.

EXERCISE 12.6

Using the `nslookup` Command

1. Press the Windows key on the keyboard and then choose Computer. Navigate to the `C:\Windows\System32` folder and double-click `CMD.exe`. (When you get to this file, you can right-click the file and choose Send To Desktop. The shortcut will then always be available on the desktop.)
2. Type **`nslookup`** and press the Enter key. (For the rest of the exercise, use the Enter key to terminate each command.)
3. Try looking up a well-known address: Type **`www.microsoft.com`**.
4. Try looking up a nonexistent host: Type **`www.example.ccccc`**. Notice that your server indicates that it can't find the address and times out. This is normal behavior.
5. Type **`Exit`** at the prompt. Type **`Exit`** again to leave the command prompt.

Using *DNSLint*

Microsoft Windows Server 2012 R2 DNS can use the `DNSLint` command-line utility to help diagnose some common DNS name-resolution issues and to help diagnose potential problems of incorrect delegation. You need to download `DNSLint` from the Microsoft Download Center.

`DNSLint` uses three main functions to verify DNS records and to generate a report in HTML:

`dnslint /d` This function helps diagnose the reasons for "lame delegation" and other related DNS problems.

`dnslint /ql` This function helps verify a user-defined set of DNS records on multiple DNS servers.

`dnslint /ad` This function helps verify DNS records pertaining to Active Directory replication.

Here is the syntax for `DNSLint`:

```
dnslint /d domain_name | /ad [LDAP_IP_address] | /ql input_file
[/c [smtp,pop,imap]] [/no_open] [/r report_name]
[/t] [/test_tcp] [/s DNS_IP_address] [/v] [/y]
```

The following are some sample queries:

```
dnslint /d stellacon.com
dnslint /ad /s 192.168.36.201
dnslint /ql dns_server.txt
dnslint /ql autocreate
dnslint /v /d stellacon.com
dnslint /r newfile /d stellacon.com
dnslint /y /d stellacon.com
dnslint /no_open /d stellacon.com
```

Table 12.7 explains the command options.

TABLE 12.7 **`DNSLint`** command options

Command option	Meaning
/d	Domain name that is being tested.
/ad	Resolves DNS records that are used for Active Directory forest replication.
/s	TCP/IP address of host.

/ql	Requests DNS query tests from a list. This switch sends DNS queries specified in an input file.
/v	Turns on verbose mode.
/r *filename*	Allows you to create a report file.
/y	Overwrites an existing report file without being prompted.
/no_open	Prevents a report from opening automatically.

Using *Ipconfig*

You can use the command-line tool `ipconfig` to view your DNS client settings, to view and reset cached information used locally for resolving DNS name queries, and to register the resource records for a dynamic update client. If you use the `ipconfig` command with no parameters, it displays DNS information for each adapter, including the domain name and DNS servers used for that adapter. Table 12.8 shows some command-line options available with `ipconfig`.

TABLE 12.8 Command-line options available for the **`ipconfig`** command

Command	What it does
`ipconfig /all`	Displays additional information about DNS, including the FQDN and the DNS suffix search list.
`ipconfig /flushdns`	Flushes and resets the DNS resolver cache. For more information about this option, see the section "Configuring DNS" earlier in this chapter.
`ipconfig /displaydns`	Displays the contents of the DNS resolver cache. For more information about this option, see "Configuring DNS" earlier in this chapter.
`ipconfig /registerdns`	Refreshes all DHCP leases and registers any related DNS names. This option is available only on Windows 2000 and newer computers that run the DHCP client service.

NOTE

You should know and be comfortable with the `ipconfig` commands related to DNS for the exam.

Using *DNSCmd*

DNSCmd allows you to display and change the properties of DNS servers, zones, and resource records through the use of command-line commands. The DNSCmd utility allows you to modify, create, and delete resource records and/or zones manually, and it allows you to force replication between two DNS servers.

Table 12.9 lists some of the DNSCmd commands and their explanations.

TABLE 12.9 DNSCmd command-line options

Command	Explanation
dnscmd /clearcache	Clears the DNS server cache
dnscmd /config	Resets DNS server or zone configuration
dnscmd /createdirectorypartition	Creates a DNS application directory partition
dnscmd /deletedirectorypartition	Deletes a DNS application directory partition
dnscmd /enumrecords	Shows the resource records in a zone
dnscmd /exportsettings	Creates a text file of all server configuration information
dnscmd /info	Displays server information
dnscmd /recordadd	Adds a resource record to a zone
dnscmd /recorddelete	Deletes a resource record from a zone
dnscmd /zoneadd	Creates a new DNS zone
dnscmd /zonedelete	Deletes a DNS zone
dnscmd /zoneexport	Creates a text file of all resource records in the zone
dnscmd /zoneinfo	Displays zone information
dnscmd /zonerefresh	Forces replication of the master zone to the secondary zone

Using the DNS Log File

You can configure the DNS server to create a log file that records the following information:

- Queries
- Notification messages from other servers
- Dynamic updates
- Content of the question section for DNS query messages
- Content of the answer section for DNS query messages
- Number of queries this server sends
- Number of queries this server has received
- Number of DNS requests received over a UDP port
- Number of DNS requests received over a TCP port
- Number of full packets sent by the server
- Number of packets written through by the server and back to the zone

The DNS log appears in `systemroot\System32\dns\Dns.log`. Because the log is in RTF format, you must use WordPad or Word to view it.

Once the log file reaches the maximum size, Windows Server 2012 R2 writes over the beginning of the file. You can change the maximum size of the log. If you increase the size value, data persists for a longer time period, but the log file consumes more disk space. If you decrease the value, the log file uses less disk space, but the data persists for a shorter time period.

Do not leave DNS logging turned on during normal operation because it sucks up both processing and hard disk resources. Enable it only when diagnosing and solving DNS problems.

Troubleshooting the *.(root)* Zone

The *DNS root zone* is the top-level DNS zone in the DNS hierarchy. Windows Server 2012 R2-based DNS servers will build a `.(root)` zone when a connection to the Internet can't be found.

Because of this, the `.(root)` zone may prevent access to the Internet. The DNS forwarding option and DNS root hints will not be configurable. If you want your DNS to work as a DNS forwarder or you want to use root hints, you must remove the `.(root)` zone.

Issues with Non-Microsoft DNS Servers

Another troubleshooting problem that you may run into is working with both Microsoft DNS servers and non-Microsoft DNS servers. One of the most common non-Microsoft DNS servers is the Unix-based BIND DNS server.

If you need to complete a zone transfer from Microsoft DNS to a BIND DNS server, you need to enable BIND Secondaries on the Microsoft DNS server (see Figure 12.16).

FIGURE 12.16 Enabling BIND Secondaries

If you need to enable Bind Secondaries, complete the following steps:

1. Open DNS management.
2. Right-click the server name and choose Properties.
3. Click the Advanced tab.
4. Check the Enable BIND Secondaries box.
5. Click OK.

Integrating Dynamic DNS and IPv4 DHCP

DHCP integration with Dynamic DNS is a simple concept but powerful in action. By setting up this integration, you can pass addresses to DHCP clients while still maintaining the integrity of your DNS services.

The DNS server can be updated in two ways. One way is for the DHCP client to tell the DNS server its address. Another way is for the DHCP server to tell the DNS server when it registers a new client.

Neither of these updates will take place, however, unless you configure the DNS server to use Dynamic DNS. You can make this change in two ways:

- If you change it at the scope level, it will apply only to the scope.
- If you change it at the server level, it will apply to all scopes and superscopes served by the server.

Which of these options you choose depends on how widely you want to support Dynamic DNS; most of the sites I visit have enabled DNS updates at the server level.

To update the settings at either the server or scope level, you need to open the scope or server properties by right-clicking the appropriate object and choosing Properties. The DNS tab of the Properties dialog box includes the following options:

Enable DNS Dynamic Updates According To The Settings Below This check box controls whether this DHCP server will attempt to register lease information with a DNS server. It must be checked to enable Dynamic DNS.

Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients This radio button (which is on by default) tells the DHCP server to register the update only if the DHCP client asks for DNS registration. When this button is active, DHCP clients that aren't hip to DDNS won't have their DNS records updated. However, Windows 2000, XP, Vista, Windows 7, Windows 8, Server 2003, Server 2008/2008 R2, and Server 2012/2012 R2 DHCP clients are smart enough to ask for the updates.

Always Dynamically Update DNS A And PTR Records This radio button forces the DHCP server to register any client to which it issues a lease. This setting may add DNS registrations for DHCP-enabled devices that don't really need them, such as print servers. However, it allows other clients (such as Mac OS, Windows NT, and Linux machines) to have their DNS information automatically updated.

Discard A And PTR Records When Lease Is Deleted This check box has a long name but a simple function. When a DHCP lease expires, what should happen to the DNS registration? Obviously, it would be nice if the DNS record associated with a lease vanished when the lease expired. When this check box is checked (as it is by default), that's exactly what happens. If you uncheck this box, your DNS will contain entries for expired leases that are no longer valid. When a particular IP address is reissued on a new lease, the DNS will be updated, but in between leases you'll have incorrect data in your DNS—something that's always best to avoid.

Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates This check box lets you handle these older clients graciously by making the updates using a separate mechanism.

In Exercise 12.7, you will enable a scope to participate in Dynamic DNS updates.

EXERCISE 12.7

Enabling DHCP-DNS Integration

1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Right-click the IPv4 item, and select Properties.
3. The Server Properties dialog box appears. Click the DNS tab.

EXERCISE 12.7 *(continued)*

4. Verify that the check box labeled Enable DNS Dynamic Updates According To The Settings Below is checked, and verify that the radio button labeled Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients is selected.
5. Verify that the check box labeled Discard A And PTR Records When Lease Is Deleted is checked. If not, then check it.
6. Click the OK button to apply your changes and close the Server Properties dialog box.

Summary

DNS was designed to be a robust, scalable, and high-performance system for resolving friendly names to TCP/IP host addresses. This chapter presented an overview of the basics of DNS and how DNS names are generated. You then looked at the many new features available in the Microsoft Windows Server 2012 R2 version of DNS, and you learned how to install, configure, and manage the necessary services. Microsoft's DNS is based on a widely accepted set of industry standards. Because of this, Microsoft's DNS can work with both Windows- and non-Windows-based networks.

Exam Essentials

Understand the purpose of DNS. DNS is a standard set of protocols that defines a mechanism for querying and updating address information in the database, a mechanism for replicating the information in the database among servers, and a schema of the database.

Understand the different parts of the DNS database. The SOA record defines the general parameters for the DNS zone, including who is the authoritative server. NS records list the name servers for a domain; they allow other name servers to look up names in your domain. A host record (also called an address record or an A record) statically associates a host's name with its IP addresses. Pointer records (PTRs) map an IP address to a hostname, making it possible to do reverse lookups. Alias records allow you to use more than one name to point to a single host. The MX record tells you which servers can accept mail bound for a domain. SRV records tie together the location of a service (like a domain controller) with information about how to contact the service.

Know how DNS resolves names. With iterative queries, a client asks the DNS server for an answer, and the client, or resolver, returns the best kind of answer it has. In a recursive query, the client sends a query to one name server, asking it to respond either with the requested answer or with an error. The error states either that the server can't come up with

the right answer or that the domain name doesn't exist. With inverse queries, instead of supplying a name and then asking for an IP address, the client first provides the IP address and then asks for the name.

Understand the differences among DNS servers, clients, and resolvers. Any computer providing domain name services is a DNS server. A DNS client is any machine issuing queries to a DNS server. A resolver handles the process of mapping a symbolic name to an actual network address.

Know how to install and configure DNS. DNS can be installed before, during, or after installing the Active Directory service. When you install the DNS server, the DNS snap-in is installed too. Configuring a DNS server ranges from easy to difficult, depending on what you're trying to make it do. In the simplest configuration, for a caching-only server, you don't have to do anything except to make sure that the server's root hints are set correctly. You can also configure a root server, a normal forward lookup server, and a reverse lookup server.

Know how to create new forward and reverse lookup zones. You can use the New Zone Wizard to create a new forward or reverse lookup zone. The process is basically the same for both types, but the specific steps and wizard pages differ somewhat. The wizard walks you through the steps, such as specifying a name for the zone (in the case of forward lookup zones) or the network ID portion of the network that the zone covers (in the case of reverse lookup zones).

Know how to configure zones for dynamic updates. The DNS service allows dynamic updates to be enabled or disabled on a per-zone basis at each server. This is easily done in the DNS snap-in.

Know how to delegate zones for DNS. DNS provides the ability to divide the namespace into one or more zones; these can then be stored, distributed, and replicated to other DNS servers. When delegating zones within your namespace, be aware that for each new zone you create, you need delegation records in other zones that point to the authoritative DNS servers for the new zone.

Understand the tools that are available for monitoring and troubleshooting DNS. You can use the DNS snap-in to do some basic server testing and monitoring. More important, you use the snap-in to monitor and set logging options. Windows Server 2012 R2 automatically logs DNS events in the event log under a distinct DNS server heading. `Nslookup` offers the ability to perform query testing of DNS servers and to obtain detailed responses at the command prompt. You can use the command-line tool `ipconfig` to view your DNS client settings, to view and reset cached information used locally for resolving DNS name queries, and to register the resource records for a dynamic update client. Finally, you can configure the DNS server to create a log file that records queries, notification messages, dynamic updates, and various other DNS information.

Review Questions

1. You are the network administrator for the ABC Company. Your network consists of two DNS servers named *DNS1* and *DNS2*. The users who are configured to use DNS2 complain because they are unable to connect to Internet websites. The following table shows the configuration of both servers:

DNS1	DNS2
`_msdcs.abc.comabc.com`	`.(root)_msdcs.abc.comabc.com`

   The users who are connected to DNS2 need to be able to access the Internet. What needs to be done?

   A. Build a new Active Directory Integrated zone on DNS2.

   B. Delete the `.(root)` zone from DNS2 and configure conditional forwarding on DNS2.

   C. Delete the current `cache.dns` file.

   D. Update your `cache.dns` file and root hints.

2. You are the network administrator for a large company that has one main site and one branch office. Your company has a single Active Directory forest, `ABC.com`. You have a single domain controller (ServerA) in the main site that has the DNS role installed. ServerA is configured as a primary DNS zone. You have decided to place a domain controller (ServerB) in the remote site and implement the DNS role on that server. You want to configure DNS so that if the WAN link fails, users in both sites can still update records and resolve any DNS queries. How should you configure the DNS servers?

   A. Configure ServerB as a secondary DNS server. Set replication to occur every 5 minutes.

   B. Configure ServerB as a stub zone.

   C. Configure ServerB as an Active Directory Integrated zone and convert ServerA to an Active Directory Integrated zone.

   D. Convert ServerA to an Active Directory Integrated zone and configure ServerB as a secondary zone.

3. You are the network administrator for a midsize computer company. You have a single Active Directory forest, and your DNS servers are configured as Active Directory Integrated zones. When you look at the DNS records in Active Directory, you notice that there are many records for computers that do not exist on your domain. You want to make sure that only domain computers register with your DNS servers. What should you do to resolve this issue?

   A. Set dynamic updates to None.

   B. Set dynamic updates to Nonsecure And Secure.

   C. Set dynamic updates to Domain Users Only.

   D. Set dynamic updates to Secure Only.

4. Your company consists of a single Active Directory forest. You have a Windows Server 2012 R2 domain controller that also has the DNS role installed. You also have a Unix-based DNS server at the same location. You need to configure your Windows DNS server to allow zone transfers to the Unix-based DNS server. What should you do?
   - **A.** Enable BIND Secondaries.
   - **B.** Configure the Unix machine as a stub zone.
   - **C.** Convert the DNS server to Active Directory Integrated.
   - **D.** Configure the Microsoft DNS server to forward all requests to the Unix DNS server.

5. You are the network administrator for Stellacon Corporation. Stellacon has two trees in its Active Directory forest, `stellacon.com` and `abc.com`. Company policy does not allow DNS zone transfers between the two trees. You need to make sure that when anyone in `abc.com` tries to access the `stellacon.com` domain, all names are resolved from the `stellacon.com` DNS server. What should you do?
   - **A.** Create a new secondary zone in `abc.com` for `stellacon.com`.
   - **B.** Configure conditional forwarding on the `abc.com` DNS server for `stellacon.com`.
   - **C.** Create a new secondary zone in `stellacon.com` for `abc.com`.
   - **D.** Configure conditional forwarding on the `stellacon.com` DNS server for `abc.com`.

6. You are the network administrator for your organization. A new company policy states that all inbound DNS queries need to be recorded. What can you do to verify that the IT department is compliant with this new policy?
   - **A.** Enable Server Auditing – Object Access.
   - **B.** Enable DNS debug logging.
   - **C.** Enable server database query logging.
   - **D.** Enable DNS Auditing – Object Access.

7. You are the network administrator for a small company with two DNS servers: DNS1 and DNS2. Both DNS servers reside on domain controllers. DNS1 is set up as a standard primary zone, and DNS2 is set up as a secondary zone. A new security policy was written stating that all DNS zone transfers must be encrypted. How can you implement the new security policy?
   - **A.** Enable the Secure Only setting on DNS1.
   - **B.** Enable the Secure Only setting on DNS2.
   - **C.** Configure Secure Only on the Zone Transfers tab for both servers.
   - **D.** Delete the secondary zone on DNS2. Convert both DNS servers to use Active Directory Integrated zones.

8. You are responsible for DNS in your organization. You look at the DNS database and see a large number of older records on the server. These records are no longer valid. What should you do?
   - **A.** In the zone properties, enable Zone Aging and Scavenging.
   - **B.** In the server properties, enable Zone Aging and Scavenging.
   - **C.** Manually delete all of the old records.
   - **D.** Set Dynamic Updates to None.

9. Your IT team has been informed by the compliance team that they need copies of the DNS Active Directory Integrated zones for security reasons. You need to give the Compliance department a copy of the DNS zone. How should you accomplish this goal?
   - **A.** Run **`dnscmd /zonecopy`**.
   - **B.** Run **`dnscmd /zoneinfo`**.
   - **C.** Run **`dnscmd /zoneexport`**.
   - **D.** Run **`dnscmd /zonefile`**.

10. You are the network administrator for a Windows Server 2012 R2 network. You have multiple remote locations connected to your main office by slow satellite links. You want to install DNS into these offices so that clients can locate authoritative DNS servers in the main location. What type of DNS servers should be installed in the remote locations?
    - **A.** Primary DNS zones
    - **B.** Secondary DNS zones
    - **C.** Active Directory Integrated zones
    - **D.** Stub zones

Chapter 13

Configure Routing and Remote Access

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure VPN and routing**

- Install and configure the Remote Access role
- Implement Network Address Translation (NAT)
- Configure VPN settings
- Configure remote dial-in settings for users
- Configure routing
- Configure Web Application proxy in passthrough mode

✓ **Configure DirectAccess**

- Implement server requirements
- Implement client configuration
- Configure DNS for DirectAccess
- Configure certificates for DirectAccess

Now that you understand how routing works, it's time to discuss how clients connect using remote access. *Routing and Remote Access Services (RRAS)* includes some security features necessary to provide remote access effectively. For example, you'll probably want the ability to restrict user dial-up access by group membership, time of day, or other factors. You'll also need a way to specify the various callback, authentication, and encryption options that the protocols support.

In this chapter, you'll learn about *virtual private networks (VPNs)*, which provide remote access to private networks across public connections. That is, using the Internet, clients can dial in to an Internet service provider (ISP) and connect to your private network. The main benefit of VPNs is reduced cost because it means that long-distance calls are unnecessary. VPNs are becoming more popular because of the increased popularity of high-speed Internet connections, such as cable and digital subscriber line (DSL) connections.

Many of the features included in Windows Server 2012 R2 are simply carried over from Windows Server 2008, with a few minor additions. This is the case with the Routing and Remote Access console.

Before I can get into the details of what these features do and how to configure them to provide remote access for your network, you need to understand some of the terms and concepts specific to RRAS. That's where you'll begin in this chapter, and then you'll move on to learning about the features and configuration settings that you need to understand to meet the exam objectives.

Overview of Dial-Up Networking

LANs provide relatively high-speed connectivity to attached machines, but where does that leave those of us who work from home, who travel, or who need to access data on a remote computer? Until wireless access is available worldwide, we have the option of using dial-up networking in which the client computer uses a modem to dial in and connect to a remote server. Once the connection is established, a variety of protocols and services make it possible for us to view web pages, transfer files and email, and do pretty much anything we could do with a hardwired LAN connection, albeit at a reduced speed.

In the following sections, you will learn more about what dial-up networking does and how it works by examining the specific technologies and protocols associated with remote access.

What DUN Does

At this point in the book, you should understand that Windows Server 2012 R2 network protocols are actually implemented as drivers. These drivers normally work with hardware network interfaces to get data from point A to point B. How do dial-up connections fit in? Many people may read this and say, "Who still uses dial-up?" Well, as a person who lives in New Hampshire, I can tell you that we still have many areas that can't get broadband or even satellite access.

Think back to the OSI model. Each layer has a function, and each layer serves as an intermediary between the layer above it and the one below it. By substituting one driver for another at some level in the stack, you can dramatically change how things work. That's exactly what the Windows Server 2012 R2's *Dial-Up Networking (DUN)* subsystem does. It makes the dial-up connection appear to be just another network adapter.

The DUN driver takes care of the task of making a slow asynchronous modem appear to work just like a fast LAN interface. Applications and services that use TCP/IP on your DUN connection never know the difference. In fact, you can configure Windows Server 2012 R2 to use your primary connection first and then to pass traffic over a secondary connection (such as a dial-up link) if the primary connection is down. This does not affect the applications with which you're working (except that they might run more slowly).

On the server side, DUN allows you to host one or more network users who dial into your Windows Server 2012 R2 machine. Windows XP Professional, Windows Vista, Windows 7, and Windows 8 all allow up to 10 concurrent dial-up connections, and Windows Server 2012 R2 allows up to 255. (Be aware that by the time you allow 255 concurrent connections, you'll probably be overloading your server.)

Depending on how you configure the DUN server, users who dial in can see the whole network or only specific resources on the server. You also get to control who can log on, when they can log on, and what they can do once they've logged on. As far as Windows Server 2012 R2 is concerned, a user connected via DUN is no different from one using resources over your LAN, so all the access controls and permissions you apply remain in force for DUN users.

How DUN Works

A lot of pieces are required to complete a dial-up call successfully from your computer to a server at another physical location. Understanding what these pieces are, how they work, and what they do for you is important. The following sections will cover the DUN infrastructure, how the *Point-to-Point Protocol (PPP)* helps with this connection, the relationship between PPP and the network protocols, and how multilink can be used to increase the speed and efficiency of your remote connections.

The DUN Infrastructure

This section covers the physical layer that underlies voice and data calls. Most of the following material will be familiar to anyone who has ever used a modem, but you should still understand the details you may not have considered before.

Plain Old Telephone Service

Plain Old Telephone Service (POTS) connections offer a theoretical maximum speed of 56Kbps; in practice, many users routinely get connections at 51Kbps or 52Kbps.

The word *modem* is actually short for *modulator-demodulator*. The original Bell System modems took digital data and modulated it into screechy analog audio tones suitable for use on regular phone lines. Because phone lines are purposely designed to pass only the low end of the audible frequency range that most can hear, the amount of data was limited. However, in the early 1990s, an engineer discovered that you could communicate much faster when the path between the sender and receiver was all digital.

An all-digital path doesn't have any analog components that induce signal loss, so it preserves the original signal quality faithfully. This in turn makes it possible to put more information into the original signal. As it happens, phone companies nationwide were in the process of making major upgrades to replace their analog equipment with newer and better digital equivalents. These upgrades made it possible for people in most areas to get almost 56Kbps speeds without changing any of the wiring in their homes or offices. The connection between the house and the phone office was still analog, but the connections between phone offices were digital, ensuring high-quality connections.

Integrated Services Digital Network

In the mid-1970s, *Integrated Services Digital Network (ISDN)* was designed. At the time, no one had any idea that you'd be able to get 56Kbps speeds out of an ordinary phone line. ISDN speeds of up to 128Kbps over a single pair of copper wires seemed pretty revolutionary. In addition, ISDN had features such as call forwarding, caller ID, and multiple directory numbers (so you could have more than one number, perhaps with different ringing patterns, associated with a single line).

Unfortunately, ISDN requires an all-digital signal path. It also requires special equipment on both ends of the connection. The phone companies were slow to promote ISDN as a faster alternative to regular dial-up service, so customers avoided it.

ISDN still has some advantages, though. Because it's all digital, call setup times are much shorter than they are for analog modems—it takes only about half a second to establish a new ISDN call. Modern ISDN adapters and ISDN-capable routers can seamlessly stitch together multiple ISDN channels to deliver bandwidth in 64Kbps increments. Because you can use ISDN lines for regular analog voice, data, and fax traffic, you can make a single ISDN act like two voice lines, a single 128Kbps data line, or a 64Kbps data line plus a voice line.

NOTE

ISDN is quickly being replaced by faster broadband services such as DSL and cable modems. In fact, you should resort to ISDN only if these other solutions are not available in your area. Note that DSL (a misnomer because they are all digital) and cable modems do not use PPP (discussed later), so they are technically not considered dial-up connections.

Other Connection Methods

Any other on-demand connection that's established using the Point-to-Point Protocol can be thought of as a dial-up connection, and Windows Server 2012 R2 doesn't make any distinction between POTS, ISDN, and other dial-ups—they're all treated identically.

Connecting with PPP

The Point-to-Point Protocol enables any two devices to establish a TCP/IP connection over a serial link. That usually means a dial-up modem connection, but it could just as easily be a direct serial cable connection, an infrared connection, or any other type of serial connection. When one machine dials another, the machine that initiates the connection is referred to as a *client*, and the machine that receives the call is referred to as a *server*—even though PPP itself makes no such distinction.

PPP negotiation involves three phases that are required to establish a remote access connection. Actually, at least six distinct protocols run on top of PPP. Understanding what they do helps to make the actual PPP negotiation process clearer. These protocols are as follows:

The Link Control Protocol The *Link Control Protocol (LCP)* handles the details of establishing and configuring the lowest-level PPP link. In that regard, you can think of LCP as if it were almost part of the Physical layer. When one PPP device calls another, the devices use LCP to agree that they want to establish a PPP connection.

The Challenge Handshake Authentication Protocol *The Challenge Handshake Authentication Protocol (CHAP)*—as well as MS-CHAPv2 and PAP—allow the client to authenticate itself to the server. This authentication functions much like a regular network logon; once the client presents its logon credentials, the server can figure out what access to grant.

The Callback Control Protocol The *Callback Control Protocol (CBCP)* is used to negotiate whether a callback is required, whether it's permitted, and when it happens. Once the client has authenticated itself, the server can decide whether it should hang up and call the client back. The client can also request a callback at a number it provides. Although this isn't as secure as having the server place a call to a predetermined number, it provides some additional flexibility. If a callback occurs, the connection is reestablished and reauthenticated, but the CBCP stage is skipped.

The Compression Control Protocol The *Compression Control Protocol (CCP)* allows the two sides of the connection to determine what kind of compression, if any, they want to use on the network data. Because PPP traffic actually consists of wrapped-up IP datagrams and because IP datagram headers tend to be fairly compressible, negotiating effective compression can significantly improve overall PPP throughput.

The IP Control Protocol At this point in the call, the two sides have agreed to authentication, compression, and a callback. They haven't yet agreed on what IP parameters to use for the connection. These parameters, which include the maximum packet size to be sent over the link (the *maximum transmission unit*, or *MTU*), have a great

impact on the overall link performance, so the client and server use the *IP Control Protocol (IPCP)* to negotiate them based on the traffic they expect to be passed.

The Internet Protocol Once the IPCP negotiation has been completed, each end has complete knowledge of how to communicate with its peer. That knowledge allows the two sides to begin exchanging Internet Protocol (IP) datagrams over the link, just as they would over a standard LAN connection.

The Relationship Between PPP and Network Protocols

Usually, when you hear about network communication, you hear about using TCP/IP on a hardwired LAN. How does this protocol fit in with PPP? In the case of TCP/IP, that's an easy question to answer: The client routes all (or some) of its outgoing TCP/IP traffic to its PPP peer, which can then inspect the IP datagrams it gets back from the PPP stack to analyze and route them properly.

Windows Server 2012 R2 supports only TCP/IP, so consider what has to happen when a client using AppleTalk needs to connect via dial-up. Because the server will not use those other protocols, it will drop the call or cause the client to warn its user (that's what Windows Server 2012 R2 does). After the other PPP setup steps are finished, the client and server can wrap other types of network traffic inside an IP datagram. This process, called *encapsulation*, allows the client to take a packet with some kind of private content, wrap it inside an IP datagram, and send it to the server. The server, in turn, processes the IP datagram, routing real datagrams normally and handling any encapsulated packets with the appropriate protocol. At that point, the client can communicate with the server without knowing that its non-TCP/IP packets are being encapsulated in any way—that detail is hidden deep in the layers of the OSI model.

Understanding the Benefits of Multilink

Many parts of the world don't have high-speed broadband access yet. In fact, many places don't have ISDN or even phone lines that support 56Kbps modems. The *multilink extensions* to the Point-to-Point Protocol provide a way to take several independent PPP connections and make them look like one line so that they act as a single connection.

For example, if you use two phone lines and modems to place a two-line multilink call to your ISP, instead of getting the usual 48Kbps connection, you would end up with an apparent bandwidth of 96Kbps. The multilink PPP software on your Windows Server 2012 R2 machine and on the ISP's router takes care of stringing all of the packets together to make this process seamless. Windows Server 2012's RRAS supports multilink PPP for inbound and outbound calls.

The primary drawback to multilink calls is that they take up more than one phone line apiece.

Overview of Virtual Private Networks

Private networks offer superior security. You own the wires, so you have control over what they're used for, who can use them, and what kind of data passes over them. However, they're not very flexible because they require you to configure and manage costly leased lines between remote locations. To make things worse, most private networks face a dilemma: Implementing enough capacity to handle peak loads almost guarantees that much of that capacity will remain idle much of the time, even though it still has to be paid for.

One way to work around this problem is to maintain private dial-up services. Such services allow, for example, a field rep in Chicago to dial into the home office in Boston. But dial-ups are expensive, and they have the same excess capacity problem as truly private networks. As an added detriment, someone has to pay long-distance or toll-free number charges.

Virtual private networks (VPNs) offer a solution. You get the security of a true private network with the flexibility, ubiquity, and low cost of the Internet. In the following sections, I will cover VPNs, including what they are used for and how they work (in general and with Windows Server 2012).

What VPNs Do

At any time, two parties can create a connection over the Internet. The idea behind a VPN is that you can use these connections to let two parties establish an *encrypted tunnel* between them using the Internet as a transportation medium. The VPN software on each end takes care of encrypting the VPN packets as they go; when the packets leave one end of the tunnel, their payloads are encrypted and encapsulated inside regular IP packets that cause them to be delivered to the remote machine. Figure 13.1 shows one way to conceptualize this process.

FIGURE 13.1 Drilling a tunnel through the Internet

As an example, let's say you're in the field at a client site. As long as you're somewhere that your ISP serves, you can dial into the client's local point of presence and get connected to the Internet. At that point, you can open a VPN connection back to the servers at your office and do whatever you could do when sitting in front of a regular desktop machine.

VPNs and Windows Server 2012 R2

Windows Server 2012 R2 includes support for Microsoft's proprietary *Point-to-Point Tunneling Protocol* and Layer 2 Tunneling Protocol. *Layer 2 Tunneling Protocol (L2TP)* provides a more generic tunneling mechanism than PPTP, and when combined with IPsec, L2TP also allows you to establish VPNs using a wide range of Microsoft or non-Microsoft hardware and software products, including routers and access devices from companies such as Cisco, Red Creek, and Nortel.

Windows Server 2012 R2's VPN support includes the following worthwhile features:

- You can set up account lockout policies for dial-up and VPN users. This capacity has existed for network and console users for some time.
- The *Extensible Authentication Protocol (EAP)* allows Microsoft or third parties to write modules that implement new authentication methods and retrofit them to servers. One example is the EAP-TLS module, which implements access control based on smart cards and certificates for VPN and dial-up users.

How you enable VPN support on your Windows Server 2012 R2 machine depends on whether you're using a server or a client (Windows XP, Windows Vista, Windows 7, Windows 8, and so on).

Client configuration is easy. Just install the Dial-Up Networking service and then use the Make New Connection Wizard to create a new VPN connection. On the server side, you'll need to install and configure RRAS and then enable it to accept incoming VPN connections.

How VPNs Work

The VPN client assumes that the VPN server is already connected to the Internet in some way. Here's how the VPN connection process works:

1. The client establishes a connection to the Internet. Dial-up networking or any other connection method can be used for this connection. The client must be able to send packets to the Internet.
2. The client sends a VPN connection request to the server. The exact format of the request varies, depending on whether the VPN is using PPTP, L2TP, or SSTP.
3. The client authenticates itself to the server. Again, the exact process varies according to the VPN protocol in use. If the client can't provide valid credentials, the connection is terminated.

4. The client and server negotiate parameters for the VPN session. This negotiation allows the two ends to agree on an encryption algorithm and strength.
5. The client and server go through the PPP negotiation process because both L2TP and PPTP depend on the lower-level PPP.

Because the contents of data passed around in step 2 and step 3 vary according to the tunneling protocol in use, I'll explain the differences. First, though, you should understand encapsulation and how VPNs use it to wrap one kind of data inside another.

An Encapsulation Primer

Most of yesterday's networks could carry only one kind of data. Each network vendor had its own protocol, and most of the time there was no way to intermingle data using different protocols on the same line. Over time, vendors began to find ways to allow a single network to carry many different types of traffic, resulting in the current assortment of traffic types found on most large networks. However, the Internet works only with IP, which is why it's called *Internet Protocol*. If you need to send other types of traffic, such as AppleTalk, across the Internet, you can encapsulate it within IP.

How does encapsulation work? Software at each level of the OSI model has to see header information to figure out where a packet is coming from and where it's going. However, the payload contents aren't important to most of those components, and the payload is what's encapsulated. By fabricating the right kind of header and prepending it for whatever you want in the payload, you can route foreign traffic types through IP networks with no trouble.

VPNs depend on encapsulation because their security method depends on being able to keep the payload information encrypted. The following steps demonstrate what happens to a typical packet as it goes from being a regular IP datagram to a PPTP packet (see Figure 13.2).

FIGURE 13.2 The encapsulation process

1. An application creates a block of data bound for a remote host. In this case, it's a web browser.
2. The client-side IP stack takes the application's data and turns it into an IP packet, first by adding a TCP header and then by adding an IP header. This is called the *IP datagram* because it contains all of the necessary addressing information to be delivered by IP.
3. The client is connected via PPP, so it adds a PPP header to the IP datagram. This PPP+IP combination is called a *PPP frame*.
4. If you are using PPP instead of a VPN protocol, the packet goes across the PPP link without further modification. When you are using a VPN (as in this example), the next step is for the VPN to encrypt the PPP frame, turning it into unreadable information to be transported over the Internet.
5. A *Generic Routing Encapsulation (GRE) header* is combined with the encrypted payload. GRE really is generic; in this case, the protocol ID field in the GRE header says that this is an encapsulated PPTP packet.
6. Now that there is a tag to tell you what's in the payload, the PPTP stack can add an IP header (specifying the destination address of the VPN server) and a PPP header.
7. Now the packet can be sent out over your PPP connection. The IP header specifies that it should be routed to the VPN server.
8. When the packet arrives at the VPN server, the server reverses steps 1 through 6 to extract the payload.

Encapsulation allows the use of VPN data inside ordinary-looking IP datagrams, which is part of what makes VPNs so powerful—you don't have to change any of your applications, routers, or network components (unless they have to be configured to recognize and pass GRE packets).

PPTP Tunneling

PPTP is a pretty straightforward protocol. It works by encapsulating packets using the mechanism described in the previous section, "An Encapsulation Primer," and performs encryption (step 4) using the *Microsoft Point-to-Point Encryption (MPPE) algorithm*. The encryption keys used to encrypt the packets are generated dynamically for each connection; in fact, the keys can be changed periodically during the connection.

When the client and server have successfully established a PPTP tunnel, the authorization process begins. This process is an exchange of credentials that allows the server to decide whether the client is permitted to connect:

1. The server sends a challenge message to the client.
2. The client answers with an encrypted response.
3. The server checks the response to see whether the answer is right. The challenge-response process allows the server to determine which account is trying to make a connection.

4. The server determines whether the user account is authorized to make a connection.
5. If the account is authorized, the server accepts the inbound connection; any access controls or remote access restrictions still apply.

L2TP/IPsec Tunneling

L2TP is much more flexible than PPTP, but it's also more complicated. It was designed to be a general-purpose tunneling protocol not limited to VPN use.

L2TP itself doesn't offer any kind of security. When you use L2TP, you're setting up an unencrypted, unauthenticated tunnel. Using L2TP by itself over the Internet, therefore, would be dangerous because anyone who wanted to could read your traffic.

The overall flow of an L2TP/IPsec tunnel session looks a little different from that of a PPTP session because IPsec security is different. Here's how the L2TP/IPsec combination works:

1. The client and server establish an IPsec security association using the ISAKMP and Oakley protocols. At this point, the two machines have an encrypted channel between them.
2. The client builds a new L2TP tunnel to the server. Because this happens after the channel has been encrypted, there's no security risk.
3. The server sends an authentication challenge to the client.
4. The client encrypts its answer to the challenge and returns it to the server.
5. The server checks the challenge response to see whether it's valid; if so, the server can determine which account is connecting. At this point, the server can accept the inbound connection, subject to whatever access policies you've put in place.

Note that steps 3 through 5 mirror the steps described for PPTP tunneling. This is because the authorization process is a function of the remote access server, not the VPN stack. All the VPN does is to provide a secure communications channel, and something else has to decide who gets to use it.

SSTP Tunneling

The *Secure Sockets Tunneling Protocol (SSTS)* is a secure way to make a VPN connection using the Secure Sockets Layer v.3 (SSL) port 443. The following steps show how SSTP operates and functions:

1. The client connects to the server through the Internet using port 443.
2. During the TCP session, SSL negotiation takes place.
3. During the SSL authentication phase, the client machine receives the server certificate.
4. The client machine will send HTTPS requests on top of the encrypted SSL session.
5. The client machine will then also send SSTP control packets on top of the HTTPS session.
6. PPP negotiation now takes place on both ends of the connection.
7. After PPP is finished, both ends are ready to send IP packets to each other.

Configuring Your Remote Access Server

Most of the configuration necessary for a remote access server happens at the server level. You use the server's Properties dialog box to control whether the server allows remote connections, what protocols and options it supports, and so forth. Because all of the protocols are carried via PPP, you can set some generic PPP options as well. I will cover these options in the following sections. You also have to configure settings for your users, which you'll read about in the next section, and you will install and configure the Remote Access role for the server in the first exercise.

Configuring PPP Options

You can use the PPP tab of the RRAS server's Properties dialog box (see Figure 13.3) to control the PPP layer options available to clients that call in. The settings you specify here control whether the related PPP options are available to clients; you can use remote access policies to control whether individual connections can use them.

FIGURE 13.3 The PPP tab of the RRAS server's Properties dialog box

This tab has four check boxes:

- The Multilink Connections check box, which is selected by default, controls whether the server will allow clients to establish multilink connections when they call in.

- The Dynamic Bandwidth Control Using BAP Or BACP check box determines whether clients and servers are allowed to add or remove links dynamically during a multilink session. If you enable this feature, you can throttle the amount of available bandwidth up or down on demand. It's available only when the Multilink Connections check box is selected. (BAP stands for Bandwidth Allocation Protocol, and BACP stands for Bandwidth Allocation Control Protocol.)
- The Link Control Protocol (LCP) is used to establish a PPP link and negotiate its settings. A variety of LCP extensions are defined in various RFCs; these extensions allow a client and server to agree dynamically about which protocols are being passed back and forth, among other things. The Link Control Protocol (LCP) Extensions check box controls whether these extensions are available. Windows 9*x*, NT, 2000, Vista, XP, Windows 7, and Windows 8 clients depend on the LCP extensions, so you should leave this check box selected.
- The Software Compression check box controls whether RRAS will allow a remote client to use the Compression Control Protocol (CCP) to compress PPP traffic. In some cases, hardware compression at the modem level is more efficient, but not everyone has a compression-capable modem. You should leave this check box selected as well.

Configuring IP-Based Connections

TCP/IP is far and away the most commonly used remote access protocol; coincidentally, it's also the most configurable of the protocols that Windows Server 2012 R2 supports. Both of these facts are reflected in the IPv4 and IPv6 tabs of the server's Properties dialog box. Figure 13.4 shows the IPv4 tab.

FIGURE 13.4 The IPv4 tab of the RRAS server's Properties dialog box

The controls on the IPv4 tab do the following:

- The Enable IPv4 Forwarding check box controls whether RRAS will route IPv4 packets between the remote client and other interfaces on your RRAS server. When this box is checked, as it is by default, remote clients' packets can go to the RRAS server or to any other host to which the RRAS server has a route. To allow clients to access resources on the RRAS server only, uncheck this box.
- The IP Address Assignment control group lets you specify how you want remote clients to get their IP addresses. The default settings here depend on what you told the RRAS Setup Wizard during setup:
  - If you want to use a DHCP server on your network as the source of IP addresses for remote clients, select the Dynamic Host Configuration Protocol (DHCP) radio button and make sure that you have the DHCP relay agent installed and running.
  - If you'd rather use static address allocation, select the Static Address Pool radio button. Then, in the list below, specify which IP address ranges you want issued to clients.
  - The Enable Broadcast Name Resolution option allows remote clients to resolve TCP/IP names without the use of a WINS or DNS server. This feature is enabled by default, and it is new for Windows Server 2012.

Figure 13.5 shows the IPv6 tab of the RRAS server's Properties dialog box.
The controls on the IPv6 tab do the following:

FIGURE 13.5 The IPv6 tab of the RRAS Server's Properties dialog box

- The Enable IPv6 Forwarding check box controls whether RRAS will route IPv6 packets between the remote client and other interfaces on your RRAS server. When this box is checked, as it is by default, remote clients' packets can go to the RRAS server

or to any other host to which the RRAS server has a route. To allow clients to access resources on the RRAS server only, uncheck this box.

- The Enable Default Route Advertisement check box (enabled by default) makes the *Border Gateway Protocol (BGP)* routing protocol available. BGP can exchange routing information between Windows Server 2012 R2 routers. When this box is checked, your Windows Server 2012 R2 router can announce its route to other routers.
- On the IPv6 tab, you can also set up your IPv6 prefix assignment (assigning IPv6 prefixes were discussed in Chapter 9).

In Exercise 13.1, I will show you how to install and configure the Remote Access role onto your server. Just like many of our installations, you will use Server Manager to install the Remote Access role. This role also installs the DirectAccess role onto your server.

EXERCISE 13.1

Installing the Remote Access Role

1. Open Server Manager.
2. On the Server Manager dashboard, click the Add Roles And Features link (number 2).
3. If a Before You Begin screen appears, click Next.
4. On the Selection type page, choose a role-based or feature-based installation and click Next.
5. Click the top radio button, Select A Server From The Server Pool, and choose the server in the Server Pool section. Click Next.
6. On the Select Server Roles screen, click the Remote Access check box. If a pop-up window appears telling you that you need to add features, click the Add Features button. Click Next.

EXERCISE 13.1 *(continued)*

7. On the Add Features page, click Next.
8. On the Remote Access page, click Next.
9. On the Select role services page, choose the first two check boxes: DirectAccess and VPN (RAS) and Routing. If a pop-up window appears telling you that you need to add additional features, click the Add Features button. Click Next.
10. At the Web Server Role (IIS) page, click Next.
11. At the Select Role Services page, click Next.
12. At the Confirmation screen, click the Install button.
13. Open the Routing and Remote Access MMC in Administrative Tools.
14. Right-click your server name and choose Configure And Enable Routing And Remote Access.
15. At the Welcome Screen, click Next.
16. Choose the Custom Configuration radio button. Click Next.
17. Choose VPN access. Click Next.
18. Click Finish at the Completing screen.
19. Click the Start Service button.

Understanding a VPN

Conventional dial-up access works well, but as you saw earlier, it can be expensive to implement, painful to manage, and extremely slow by today's standards. VPNs offer a way around these problems by providing low initial and ongoing costs, easy management, and excellent speeds (depending on your connection). Windows Server 2012's RRAS component includes two complete VPN implementations: one using Microsoft's PPTP and one using a combination of the Internet-standard IPsec protocol and L2TP or SSTP.

The basic process of setting up a VPN is simple, but you need to think some things through before plunging ahead. Getting the VPN installation right may require small hardware or networking changes plus proper configuration of the VPN service. You will look at this process in the following sections.

How VPN Works

A VPN sits between your internal network and the Internet, accepting connections from clients in the outside world. In Figure 13.6, clients 1 and 2 are using different ISPs

(probably because they're at different physical locations). For example, a packet from client 1 goes from its computer to its ISP and then through some route, unknown to you, that eventually delivers it to the VPN server, which transforms it into a packet suitable for use on the internal network.

Imagine a line around the internal network, and think of it as a security boundary. In general, you'll want your VPN server to be outside any firewalls or network security measures that you have in place. The most common configuration is to use two NICs: one connects to the Internet, and the other connects either to the private network or to an

FIGURE 13.6 VPNs provide private connections between clients and servers across the Internet

intermediate network that itself connects to the private network. Of course, you can use any type of Internet connection you want for the VPN server, such as cable modem, DSL, T1, satellite, or whatever.

The point behind giving the VPN its own network adapter is that your VPN clients need a public IP address to which they can connect, and you probably don't want them calling directly into your internal network. That also means that things will be easiest for your VPN users if the IP address for your VPN server's external interface is statically assigned so that it won't be changing on them when they least expect it.

Enabling RRAS as a VPN

If you're already using RRAS for IP routing or remote access, you can enable it as a VPN server without reinstalling.

The General tab of the server's Properties dialog box allows you to specify whether your RRAS server is a router, a remote access server, or both. The first step in converting your existing RRAS server to handle VPN traffic is to make sure that the IPv4 Remote Access Server or IPv6 Remote Access Server check box is selected on this tab.

Making this change requires you to stop and restart the RRAS service, but that's OK because the snap-in will do it for you. Then you must configure VPN ports, as shown in the following sections.

Configuring a VPN

VPN configuration is extremely simple, at least for PPTP. Either a server can accept VPN calls or it can't. If it can, it will have a certain number of VPN ports, all of which are configured identically. You don't have to change or tweak much to get a VPN server set up, but you can adjust a few things as you like.

Configuring VPN Ports

The biggest opportunity to configure your VPN server is to adjust the number and kind of VPN ports available for clients to use. You can enable or disable either PPTP or L2TP, depending on what you want your remote users to be able to access. You accomplish this through the Ports Properties dialog box.

For conventional remote access servers, this dialog box shows you a list of hardware ports, but for servers that support VPN connections, there are two WAN Miniport device selections: one for PPTP and one for L2TP. (These aren't really devices; they're actually virtual ports maintained by RRAS for accepting VPN connections.) You configure these ports by selecting one and clicking the Configure button, which displays the Configure Device – WAN Miniport (PPTP) dialog box (see Figure 13.7).

FIGURE 13.7 The Configure Device – WAN Miniport (PPTP) dialog box

Three controls are pertinent to a VPN configuration:

- The Remote Access Connections (Inbound Only) check box must be activated in order to accept VPN connections with this port type. To disable a VPN type (for instance, if you want to turn off L2TP), uncheck this box.
- The Demand-Dial Routing Connections (Inbound And Outbound) check box controls whether this VPN type can be used for demand-dial connections. By default, this box is checked; you'll need to uncheck it if you don't want to use VPN connections to link your network with other networks.
- The Maximum Ports control lets you set the number of inbound connections that this port type will support. By default, you get 5 PPTP and 5 L2TP ports when you install RRAS; you can use from 0 to 250 ports of each type by adjusting the number here.

You can also use the Phone Number For This Device field to enter the IP address of the public interface to which VPN clients connect. You might want to do this if your remote access policies accept or reject connections based on the number called by the client. Because you can assign multiple IP addresses to a single adapter, you can control VPN traffic by throttling which clients can connect to which addresses through a policy.

Troubleshooting VPNs

The two primary problems you might encounter with VPN are as follows:

- Inability to establish a connection at all
- Inability to reach some needed resource once connected

There's a lot of common ground between the process of troubleshooting a VPN connection and the process of troubleshooting an ordinary remote access connection.

The following are some extremely simple—but sometimes overlooked—things to check when your VPN clients can't connect. First, make sure your clients can make the underlying connection to their ISP; then, check the following:

- Is RRAS installed and configured on the server?
  - Is the server configured to allow remote access? Check the General tab of the server's Properties dialog box.
  - Is the server configured to allow VPN traffic? Check the Ports Properties dialog box to make sure that the appropriate VPN protocol is enabled and that the number of ports for that protocol is greater than 0.
  - Are there any available VPN ports? If you have 10 L2TP ports allocated, the 11th caller will not be able to connect.
- Do the client and server match?
  - Is the VPN protocol used by the client enabled on the server? Windows 2000 and newer clients will try L2TP first and switch to PPTP as a second choice. However, clients on other OSs (including Windows NT) can normally expect L2TP, PPTP, or SSTP (2008 or higher).

- Are the client and server authenticated correctly?
  - Are the username and password correct?
  - Does the user account in question have remote access permissions, either directly on the account or through a policy?
  - Do the authentication settings in the server's policies (if any) match the supported set of authentication protocols?

If you check all of the simple stuff and find nothing wrong, it's time to move on to checking more complex issues. These tend to affect more than one user, as opposed to the simple (and generally user-specific) issues just outlined. The problems include the following:

Policy Problems If you're using a native-mode Windows Server 2012 R2 domain and you're using policies, those policies may cause some subtle problems that show up under some circumstances:

- Are there any policies whose Allow or Deny settings conflict with each other? Remember that all conditions of all policies must match to gain user access; if any condition of any policy fails or if there are any policies that deny access, the connection will be denied.
- Does the user match all of the necessary conditions that are in place, such as time and date?

Network Problems If you're using dynamic IP addressing, are there any addresses left in the pool? If the VPN server can't assign an address, it won't accept the connection.

Domain Problems Windows Server 2012 R2 RRAS servers can coexist with Windows NT RRAS servers, and both of them can interoperate with RADIUS servers from Microsoft and other vendors. Sometimes, though, this interoperation doesn't work exactly as you'd expect. Here are some questions to ask:

- Is the RRAS server's domain membership correct? Your RRAS servers don't have to be domain members unless you want to use native-mode features such as remote access policies.
- If you're in a domain, are the server's group memberships correct? The server account must be a member of the RAS group and Internet Authentication Servers security group.

Managing Your Remote Access Server

RRAS server management is generally pretty easy because, in most cases, there's not much to manage. You set up the server, and it answers calls. You'll probably find it necessary to monitor the server's ongoing activity, however, and you may find it necessary to log activity for accounting or security purposes.

You can monitor your server's activity in a number of ways, including having the server keep local copies of its logs or having it send logging data to a remote RADIUS server. In addition, you can monitor the current status of any of the ports on your system.

Microsoft's documentation distinguishes between event logging, which records significant things that happen such as the RRAS service starting up and shutting down, and authentication and accounting logging, which tracks things like when a user logged on and logged off. The settings for both types of logging are intermingled in the RRAS snap-in.

Managing Remote Users with a RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) allows for maintaining and managing your remote users. A RADIUS server allows Remote Access Service (RAS) clients and dial-up routers to be authenticated.

Network Policy Server (NPS) is Microsoft's implementation of a RADIUS server in Windows Server 2012. NPS is replacing Windows Server 2003 Internet Authentication Service (IAS). NPS, working as a RADIUS server, allows for authentication, authorization, and accounting for wireless and VPN networks.

NPS allows a server to perform the duties of a RADIUS proxy. A RADIUS proxy allows the routing of RADIUS messages between RADIUS clients (RAS) and RADIUS servers. NPS also gives you the ability to record information about forwarded messages in an accounting log.

Monitoring Overall Activity

The Server Status node in the RRAS snap-in shows you a summary of all the RRAS servers known to the system. When you select the Server Status item, the right pane of the MMC will list each known RRAS server. Each entry in the list tells you whether the server is up, what kind of server it is, how many ports it has, how many ports are currently in use, and how long the server has been up. You can right-click any Windows Server 2012 R2 RRAS server in this view to start, stop, restart, pause, or resume its RRAS service; disable RRAS on the server; or remove the server's advertisement from Active Directory (provided, of course, that you're using Active Directory).

Controlling Remote Access Logging

A standard RRAS installation will always log some data locally, but that's pretty useless unless you know what gets logged and where it goes. Each RRAS server on your network has its own set of logs, which you manage through the `Remote Access Logging` folder. Within that folder, you'll usually see a single item labeled *Local File*, which is the log file stored on that particular server.

If you don't have Windows accounting or Windows authentication turned on, you won't have a local log file. Depending on whether you're using RADIUS accounting and logging, you may see additional entries.

Setting Server Logging Properties

You can control server logging at the server level. You use the Logging tab to control what level of detail you want in the server's event log.

These controls regulate all logging by RRAS, not just remote access log entries.

You have four choices for the level of logged detail:

- The Log Errors Only radio button instructs the server to log errors and nothing else. This gives you an adequate indication of problems after they happen, but it doesn't point out potential problems noted by warning messages.
- The Log Errors And Warnings radio button is the default choice. This forces the server to log error and warning messages to the event log, giving you a nice balance between information content and log volume.
- The Log All Events radio button causes the RRAS service to log mass quantities of messages, literally covering everything the server does. Although this voluminous output is useful for troubleshooting (or even for getting a better understanding of how remote access works), it's overkill for everyday use.
- The Do Not Log Any Events radio button turns off all event logging for RRAS.

Don't use the Do Not Log Any Events option. The service's logs are important in case of a problem.

The Log Additional Routing And Remote Access Information check box allows you to turn on the logging of all PPP negotiations and connections. This can provide valuable information when you're trying to figure out what's wrong, but it adds a lot of unnecessary bulk to your log files. Don't turn it on unless you're trying to pin down a problem.

Setting Log File Properties

By selecting an individual log file in the snap-in, you can change what events will be logged in that file. The Local Log File Properties dialog box has two tabs:

- The Settings tab controls what gets logged in the file:
  - Accounting Requests governs whether events related to the service will be logged (as well as accounting data). You should always leave this checked.

  - Authentication Requests adjusts whether successful and failed logon requests are logged. You should always leave this checked.
  - Periodic Status controls whether interim accounting packets are permanently stored on disk. You should usually leave this checked.
  - Periodic Authentication Requests adjusts whether successful and failed logon requests are periodically logged. You should always leave this checked.
- The Log File tab (see Figure 13.8) controls the format of the file, specifically, how the log file is written to disk. You use this tab to designate three things:
  - The Directory field shows where the log file is stored. By default, each server logs its data in `systemroot\system32\LogFiles`. You can change this location to wherever you want.
  - The Format controls determine the format of the log file. By default, Windows Server 2000, 2003, 2008/2008 R2, and 2012/2012 R2 use the database-compatible file format. This format makes it easy for you to take log data and store it in a database, enabling more sophisticated postprocessing for things such as billing and chargebacks.
  - The Create A New Log File controls determine how often new log files are created. For example, some administrators prefer to start a new log file each week or each month, whereas others are content to let the log file grow without end. You can choose to have RRAS start new log files every day, week, month, never, or when the log file reaches a certain size.

FIGURE 13.8 The Log File tab

Having correct accounting and authorization data is critical to maintaining a good level of security. Exercise 13.2 walks you through configuring remote access logging.

EXERCISE 13.2

Changing Remote Access Logging Settings

1. Open the RRAS MMC snap-in by pressing the Windows key and selecting Administrative Tools ➢ Routing And Remote Access.
2. Navigate to the `Remote Access Logging and Policies` folder. Right-click the folder and select Launch NPS.
3. On the left pane, click Accounting. On the right side, click Change Log File Properties.

4. The Local File Logging dialog box appears. On the Settings tab, make sure that all check boxes are marked.
5. Switch to the Log File tab, and in the Create A New Log File controls, select the When Log File Reaches This Size option. Enter **50** to set the maximum size of the log file to 50MB.
6. Click the OK button. Close the Network Policy Server window.

Reviewing the Remote Access Event Log

You use the Log File tab to specify the format, size, and location of the log file. Once you have a log file, however, what do you do with the log information? Windows Server 2012 R2 online help has an exhaustive list of all of the fields logged for each connection attempt and accounting record. Because of the availability of online help, you don't need to have all of those fields memorized, and you don't have to remember exactly how to make sense of the log entries.

Why bother reviewing the logs? One nice feature is that each entry in the authentication log indicates which remote access policy was applied (either to accept or to reject the

connection). This is a good way to identify problems with policies because sometimes multiple policies can combine to have an effect that you didn't expect.

Furthermore, if it's desirable in your environment, you can use the logged data to generate accounting reports to tell you things such as the average utilization of your dial-in ports, the top 10 users of dial-in connect time, or how much online time accounts or certain Windows groups use.

Monitoring Ports and Port Activity

You can monitor port status and activity from the RRAS snap-in. The `Ports` folder under the server contains one entry for each defined port. When you select the `Ports` folder, you'll see a list of the ports and their current status. The list indicates whether each port is a dial-in or VPN port and whether it's active, so you can get a quick summary of your server's workload at any time.

Double-clicking an individual port displays the Port Status dialog box (see Figure 13.9). This dialog box shows information such as a port's line speed (Line BPS), the amount of transmitted and received data (Bytes In and Bytes Out), and the network address for each protocol being carried on the port. This is a useful tool for verifying whether a port is in active use, and it gives you a count of the number of transmission and reception errors on the port.

FIGURE 13.9 The Port Status dialog box

Network Address Translation

Network Address Translation (NAT) provides an advantage with routing and tunneling. NAT (also referred to as network masquerading) allows a router to translate one IP address to another across the tunnel. This allows you to use private IP addressing internally but use pubic addresses between the tunnels.

The huge advantage of NAT is the ability for you to share a single public IP address and single Internet connection between multiple locations using private IP addressing schemes. The nodes on the private network use nonroutable private addresses. NAT maps the private addresses to the public address.

Implementing NAT

Implementing NAT is an easy process. I am going to show you the steps needed to implement NAT, but I am not going to do it as an exercise. To set up NAT in an exercise without a tunnel or without multiple networks is not always an easy thing to do. So, I will just show you how to implement NAT in case you need to do it at work. To run these steps, you must be a member of at least the local Administrators group or higher. The following steps show you how to implement NAT:

1. Start the Routing and Remote Access MMC snap-in (under Administrative Tools). Right-click your server name and choose Configure And Enable Routing And Remote Access.
2. At the Welcome Screen, click Next.
3. Choose the Custom Configuration radio button. Click Next.
4. Click NAT and click Next.
5. Start Service.
6. Expand your server name.
7. Expand IPv4.

At this point, you can configure NAT. If you need to install NAT, you must have a system with multiple NIC devices or a demand-dial setup.

NAT is also commonly used for Internet connections, but this is done through your firewall or router. For example, let's say you have an Internet service provider that issues you only four valid Internet TCP/IP addresses for you to use on your network. You can set up NAT and program it to use those four valid addresses. Then, when a user from the network wants to access the Internet, NAT swaps the user's internal IP address for one of the valid IP addresses.

Configuring a VPN Client

Dial-up RAS clients and VPN clients are similar. Almost all of the options that are available when you set up a RAS client are also available when you set up a VPN client. The main differences are as follows:

- VPN clients specify the server's IP address, whereas RAS clients specify the server's phone number.
- VPN clients require an underlying connection to the Internet.

Client configuration is not a focus of the exam, so in this chapter you will learn how to configure a VPN client but not a RAS client. Just remember that the RAS client configuration is extremely similar and that RAS clients are slowly fading away. Thus, here I will focus on VPN settings only.

VPN connections are almost always created on client workstations, so this section describes the settings in Windows 7 and Windows 8.

When you establish a virtual private network connection, you're actually building an encrypted tunnel between you and some other machine. The tunneled data is carried over an insecure network, such as the Internet.

Once you've created a connection, you can change its properties at any time by opening its Properties dialog box. The Dial-Up Connection Properties dialog box has a total of five tabs that you can use to adjust all of the pertinent settings for each connection.

Don't confuse these settings with the ones in the Local Area Connection Properties dialog box; they serve entirely different purposes.

The General Tab

The General tab of the Connection Properties dialog box (the box is called Dial-Up Connections or VPN Connections, depending on whether you're configuring dial-up RAS or VPN) is where you specify either the IP address of the VPN server or the modem and phone number to use with this particular connection. Some fields have been filled in already from when you used the Network Connection Wizard. Figure 13.10 shows the VPN settings.

FIGURE 13.10 General tab of the VPN Connection Properties dialog box

The General tab has a field where you enter the VPN server address or hostname. The First Connect group lets you specify which dial-up connection, if any, you want brought up before the VPN connection is established.

With the General tab, you can also do the following:

- Set VPN options:
  - Enter the VPN server address or hostname.
  - Specify whether to dial another connection automatically first and then specify the connection to dial.
- Set RAS options:
  - Change the modem this connection uses, or the settings for the modem you already have, with the Configure button.

When configuring dial-up, you can also use the Phone And Modem Options control panel to adjust a broader range of modem settings.

The Options Tab

The Options tab holds settings that control how DUN dials and redials the connection. The controls in this dialog box are segregated into two groups. The Dialing Options group holds controls that govern DUN's interface behavior while dialing, and the Redialing Options group controls whether and how DUN will redial if it doesn't immediately connect (see Figure 13.11).

FIGURE 13.11 Options tab of the VPN Connection Properties dialog box

Dialing Options

Four dialing options are available in the Dialing Options group:

- The Display Progress While Connecting check box (selected by default) instructs DUN to keep you updated on its progress as it attempts to raise the connection.
- The Prompt For Name And Password, Certificate, Etc. check box is also selected by default. When it's on, Windows will prompt you for any credentials it needs to authenticate your connection to the remote server. This may be a username, a password, a public key certificate, or some combination of the three, depending on what the remote end requires.
- The Include Windows Logon Domain check box is unchecked by default. It forces DUN to include the domain name of the domain to which you're logged on as part of the authentication credential. Leave this unchecked unless you're dialing into a Windows NT/2000 network that has a trust relationship with your logon domain.
- For RAS connections, a Prompt For Phone Number check box tells DUN to display the phone number in the connection dialog box. This box is checked by default. This gives you a chance to edit the phone number before dialing; you may want to uncheck it if you (or your users) are prone to making accidental changes.

Redialing Options

The settings in the Redialing Options group control how DUN will attempt to redial the specified number if the remote end is busy or doesn't answer with a recognizable carrier tone. These settings are as follows:

- The Redial Attempts field controls how many attempts DUN will make to raise the other end before giving up. The default value is 3, but you can set any value from 0 (meaning that DUN won't attempt to redial) to 999,999,999.
- The Time Between Redial Attempts drop-down menu controls how long DUN will wait after each failed call before it tries again. Values in the drop-down menu range from 1 second all the way up to 10 minutes, with various increments in between.
- The Idle Time Before Hanging Up drop-down menu lets you specify an inactivity timer. If your connection is idle for longer than the specified period, your client will terminate the call. Note that the remote end may drop the call sooner than your client, depending on how it's configured. By default, this drop-down menu is set to Never, meaning that your client will never drop a call. If you want an inactivity timer, you can pick values ranging from 1 minute to 24 hours.
- The Redial If Line Is Dropped check box automatically redials the number if you are disconnected.

The Security Tab

How useful you find the Security tab will depend on whom you're calling. The default settings it provides will work fine with most Internet service providers and corporate

dial-up facilities, but Windows 7 and Windows 8 have a broad range of security settings that you can change if you require. The Security Options group contains controls that directly affect the security of your connection. The Advanced (Custom Settings) radio button controls settings such as encryption and authentication protocols.

Security Options

The controls in the Security Options group are pretty straightforward. The security settings in effect for this connection are governed by your choice between the Typical (Recommended Settings) and Advanced (Custom Settings) radio buttons (see Figure 13.12).

FIGURE 13.12 Security tab of the VPN Connection Properties dialog box

Typical (Recommended Settings)

Usually, it's best to stick with the Typical (Recommended Settings) option and use its subordinate controls to pick a canned setting that matches your needs. These subordinate controls are as follows:

- The Validate My Identity As Follows drop-down menu lets you choose among the following authentication methods:
  - Unsecured passwords (the default, and the only type of authentication that most networks support)

  - Secured passwords
  - Smart card authentication (useful only when calling another Windows 2000, 2003, 2008/2008 R2, or 2012/2012 R2 network)
- If you choose to require a secured password, the Automatically Use My Windows Logon Name And Password (And Domain If Any) check box instructs DUN to offer to the remote end the logon credentials you used to log on to the computer or domain. This is useful only if you're dialing into a network that has access to your domain authentication information.
- If you require a secured password or smart card authentication, the Require Encryption (Disconnect If None) check box allows you to have either an encrypted connection or none at all. If you check this box, your client and the remote server will attempt to negotiate a common encryption method. If they can't (perhaps because the remote end doesn't offer encryption), your client will hang up.

Advanced (Custom Settings)

If you select the Advanced (Custom Settings) radio button and then click the Settings button, you'll see the Advanced Security Settings dialog box. Its controls are more complex than the ones on the Security tab.

The first field is the Data Encryption drop-down menu. Windows 8 offers you the opportunity to encrypt both sides of network connections using IPsec. This capability extends to dial-up connections too. The drop-down menu gives you the following four choices:

- No Encryption Allowed means that the server will drop your call if it requires encryption because you can't provide it.
- Optional Encryption tells the client to request encryption but to continue the call if it's not available.
- Require Encryption tells the client to request encryption and to refuse to communicate with servers that don't support it.
- Maximum Strength Encryption tells the client to communicate only with servers that offer the same strength encryption it does. For example, with this setting in force, a North American Windows Server 2008 R2 machine running 3DES won't communicate with a French Windows XP machine because the French machine uses the weaker exportable encryption routines.

The Authentication section controls which authentication protocols this client can use. The default setting, Use Extensible Authentication Protocol (EAP), is for standard Windows authentication (using the MD5-Challenge method) or certificate-based authentication (using the Smart Card Or Other Certificate choice in the drop-down menu).

The Allow These Protocols radio button is followed by a long list of authentication protocols. Although the specifics of how they work are different, the basic idea behind all of these protocols is the same. Each provides a secure way for a client to prove its identity to a server. By selecting the appropriate check boxes, you can make your client use the same protocols as the remote end.

The Networking Tab

You use the Networking tab (see Figure 13.13) to control which protocols your client will attempt to use when communicating with other servers.

FIGURE 13.13 Networking tab of the VPN Connection Properties dialog box

The list box in the middle of the tab shows the network protocols installed on the client. Protocols marked with a check are available for use with this connection. Usually, when configuring RAS, you'll see TCP/IP and Client For Microsoft Networks marked, which indicates that those two protocols can be used over the connection.

The Install, Uninstall, and Properties buttons work just as they do in the Local Area Connection Properties dialog box. By using them, you can control which protocols are on your machine and their settings.

It's worth mentioning that selecting Internet Protocol (TCP/IP) in the protocols list and opening its Properties dialog box gives you access to a set of properties that are completely distinct from any TCP/IP settings that may apply to your LAN interfaces. Usually, the dial-up TCP/IP settings are configured to obtain an IP address and DNS information from the remote server, although if you need to, you can override these settings.

The Sharing Tab

Internet Connection Sharing allows other users to connect to the Internet through this machine. The machine on which you enable this feature works like a gateway to the Internet (see Figure 13.14).

FIGURE 13.14 Sharing tab of the VPN Connection Properties dialog box

Configuring a Web Application Proxy

One of the new advantages of using the Remote Access role service in Windows Server 2012 R2 is the Web Application Proxy. Normally, your users access applications on the Internet from your corporate network. The *Web Application Proxy* reverses this feature, and it allows your corporate users to access applications from any device outside the network.

Administrators can choose which applications to provide reverse proxy features, and this allows administrators the ability to give access selectively to corporate users for the desired application that you want to set up for the Web Application Proxy service.

The Web Application Proxy feature allows applications running on servers inside the corporate network to be accessed by any device outside the corporate network. The process of allowing an application to be available to users outside of the corporate network is known as *publishing*.

Publishing Applications

One disadvantage to corporate networks are that the machines that access the network are normally devices issued by the organization. That's where Web Application Proxy publishing can help.

Web Application Proxy allows an administrator to publish an organization's applications, thus allowing corporate end users the ability to access the applications from their own devices. This is becoming a big trend in the computer industry called *bring your own device* (BYOD).

In today's technology world, users are buying and using many of their own devices, even for business work. Because of this, the users are comfortable with their own devices. Web Application Proxy allows an organization to set up applications and enable their corporate users to use these applications with the devices the users already own including computers, tablets, and smartphones.

The client side is easy to use as long as the end user has a standard browser or Office client. End users can also use apps from the Microsoft Windows Store that allow the client system to connect to the Web Application Proxy.

Configuring Pass-Through Authentication

Now when setting up the Web Application Proxy so that your users can access applications, you must have some kind of security or everyone with a device would be able to access and use your applications.

Because of this, Active Directory Federation Services (AD FS) must always be deployed with Web Application Proxy. AD FS gives you features such as single sign-on (SSO). *Single sign-on* allows you to log in one time with a set of credentials and use that set of credentials to access the applications over and over.

Pass-through authentication is truly a great benefit for your end users. Think of having a network where a user has to log in every time that user wants to access an application. The more times you make your end users log into an application, the more chances there are that the end user will encounter possible issues. Pass-through authentication works in the following way:

1. The client enters a URL address on their device, and the client system attempts to access the published web application.
2. The Web Application Proxy sends the request to the proxy server.
3. If the backend server needs the user to authenticate, the end user needs to enter their credentials only once.
4. After the server authenticates the credentials, the client has access to the published web application.

When an administrators sets up applications to use pass-through pre-authentication, additional features of AD FS will not function. For example, you will not be able to use AD FS Workplace Join, multifactor authentication (MFA), and multifactor access control.

Understanding DirectAccess

DirectAccess was a new technology that was introduced in the Windows Server 2008 R2 and Windows 7 operating systems. DirectAccess has been improved upon, and it is also available for Windows 8 and Windows Server 2012 R2.

DirectAccess allows a remote user to work on their corporate network when they are away from the office without the need for a VPN. As long as the remote user is connected to the Internet, DirectAccess will automatically connect the remote user to the corporate network without the need for any user intervention.

When a user's DirectAccess-enabled laptop is connected to the Internet, a bidirectional connection is automatically established with the user's corporate network. Because the connection is bidirectional, the IT administrator can also remotely manage the Windows 7 or Windows 8 machine while the machine is away from the network.

DirectAccess vs. VPNs

There really is no debate between VPN or DirectAccess—DirectAccess is the better way to go. The downside to DirectAccess is that it requires a great deal of time, resources, and knowledge to set it up properly.

There are a few problems with using VPNs to connect to a network. One issue is that when a user gets disconnected from their VPN connection, they must reestablish the VPN connection.

Another issue with VPNs is that many organizations filter VPN connection traffic. It may not be possible for an organization to open a firewall to allow VPN traffic. Also, if your intranet and your Internet connections are the same as your VPN connections, this can cause your Internet to be slower.

DirectAccess does not face the same limitations of a VPN. DirectAccess allows a laptop or desktop that is configured properly to connect automatically using a bidirectional connection between the client and the server.

To establish this connection, DirectAccess uses Internet Protocol Security (IPsec) and IPv6. IPsec provides a high level of security between the client and the server, and IPv6 is the protocol that the machines use.

Understanding the DirectAccess Process

Before you can set up the features and benefits of DirectAccess, there are some prerequisites that I must first go over. DirectAccess is great way to get your users to access the network from the road, but it is not the easiest thing to set up, and it must be done correctly.

DirectAccess Prerequisites

As with any software package, role, or feature, when you install any one of these, there are always prerequisites that you must deal with. DirectAccess is no different. The following is a list of DirectAccess Server with Advanced Settings prerequisites:

- A public key infrastructure must be deployed.
- ISATAP in the corporate network is not supported. If you are using ISATAP, you should remove it and use native IPv6.
- Computers that are running the following operating systems are supported as DirectAccess clients:
  - Windows Server 2012 R2
  - Windows 8.1 Enterprise
  - Windows Server 2012
  - Windows 8 Enterprise
  - Windows Server 2008 R2
  - Windows 7 Ultimate
  - Windows 7 Enterprise
- Force tunnel configuration is not supported with KerbProxy authentication.
- Changing policies by using a feature other than the DirectAccess management console or Windows PowerShell cmdlets is not supported.
- Separating NAT64/DNS64 and IPHTTPS server roles on another server is not supported.

The following is the list of prerequisites if you want to manage DirectAccess clients remotely:

- Windows Firewall must be enabled on all profiles.
- ISATAP in the corporate network is not supported. If you are using ISATAP, you should remove it and use native IPv6.
- Computers that are running the following operating systems are supported as DirectAccess clients:
  - Windows Server 2012 R2
  - Windows 8.1 Enterprise
  - Windows Server 2012
  - Windows 8 Enterprise
  - Windows Server 2008 R2
  - Windows 7 Ultimate
  - Windows 7 Enterprise
- Changing policies by using a feature other than the DirectAccess management console or Windows PowerShell cmdlets is not supported.

Understanding DirectAccess

To understand DirectAccess better, it helps to understand the process involved with how DirectAccess operates. The following steps, taken from the Microsoft white papers, show how DirectAccess operates.

1. The Windows 8 DirectAccess client determines whether the machine is connected to a network or the Internet.
2. The Windows 8 DirectAccess computer tries to connect to the web server specified during the DirectAccess setup configuration.
3. The Windows 8 DirectAccess client computer connects to the Windows Server 2012 R2 DirectAccess server using IPv6 and IPsec. Because most users connect to the Internet using IPv4, the client establishes an IPv6-over-IPv4 tunnel using 6to4 or Teredo.
4. If an organization has a firewall that prevents the DirectAccess client computer using 6to4 or Teredo from connecting to the DirectAccess server, the Windows 8 client automatically attempts to connect using the IP-HTTPS protocol.
5. As part of establishing the IPsec session, the Windows 8 DirectAccess client and server authenticate each other using computer certificates for authentication.
6. The DirectAccess server uses Active Directory membership, and the DirectAccess server verifies that the computer and user are authorized to connect using DirectAccess.
7. The DirectAccess server begins forwarding traffic from the DirectAccess client to the intranet resources to which the user has been granted access.

Now that you understand how DirectAccess works, let's look at the requirements for setting up DirectAccess on your network.

Knowing the DirectAccess Infrastructure Requirements

To set up DirectAccess, you must make sure that your network infrastructure meets some minimum requirements. The following are the requirements for setting up DirectAccess:

- Windows Server 2012 R2 configured to use DirectAccess. The Windows Server 2012 R2 machine will be set up as a multihomed system. This means your server will need two network adapters so that one adapter is connected directly to the Internet and a second adapter is connected to the intranet. Each network adapter will be configured with its own TCP/IP address.
- Windows 7 or Windows 8 client machines configured to use DirectAccess.
- Minimum of one domain controller and one Domain Name System (DNS) server running Windows Server 2008 SP2, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.

- Certificate authority (CA) server that will issue computer certificates, smart card certificates, or health certificates.
- IPsec policies to specify protection for traffic.
- IPv6 on the DirectAccess server that uses ISATAP, Teredo, or 6to4.

Summary

In this chapter, you learned how to install and configure Routing and Remote Access Services to handle dial-in connections, how to configure appropriate encryption and security settings so that communication between the client and server is encrypted and authenticated, how to install RRAS to provide VPN service using the PPTP and L2TP protocols, how to configure VPN services on the server and client, and, finally, how to troubleshoot common problems with VPNs.

Exam Essentials

Know how to install and configure RAS at the server level. The RAS installation process is driven by the Routing and Remote Access Server Setup Wizard, which you use to set up a dial-up server. You can specify whether the server acts as a remote access server, specify what authentication providers and settings you want the server to use, control the settings applied to each protocol you have installed, specify which PPP protocols (including multilink) the clients on this server are allowed to use, and control what level of log detail is kept for incoming connections.

Know how to install and configure a VPN server. If you don't have RRAS installed, you'll need to install it, activate it, and configure it as a VPN server. If you're already using RRAS for IP routing or remote access, you can enable it as a VPN server without reinstalling. VPN configuration is extremely simple, at least for PPTP. Either a server can accept VPN calls or it can't. If it can, it will have a certain number of VPN ports, all of which are configured identically.

Know how to configure an RRAS client. Most client connections are made on Windows 8, Windows 7, Windows Vista, or Windows XP Professional workstations. Dial-in and VPN connections are configured similarly, but when creating a VPN connection, you must substitute an IP address for a phone number.

Review Questions

1. You have a local DHCP server for your dial-in clients, but you also want to use the DHCP relay agent to forward requests to a remote DHCP server if the local server doesn't answer a request. To do this, you must do which of the following?
   - **A.** Add a static route to the remote server.
   - **B.** Adjust the boot threshold on the DHCP relay agent interface for the remote network so that the local server has enough time to respond.
   - **C.** Adjust the DHCP Forwarding Time parameter in the registry.
   - **D.** Adjust the forwarding time in the DHCP Relay Agent Global Properties dialog box.

2. You are considering multilink PPP in order to increase bandwidth available for a dial-up client. Which of the following is not a benefit of multilink?
   - **A.** Multilink can make the client experience faster by combining multiple phone lines and creating one logical PPP connection.
   - **B.** Multilink enables the encryption of data between the client and the server.
   - **C.** Multilink can be relatively low in cost and can utilize existing infrastructure.
   - **D.** Multilink is easy to use and included in Windows Server 2012 R2 for both inbound and outbound calls.

3. Your company has offices in five locations around the country. Most of the users' activity is local to their own network. Occasionally, some of the users in one location need to send confidential information to one of the other four locations or to retrieve information from one of them. The communication between the remote locations is sporadic and relatively infrequent, so you have configured RRAS to use demand-dial lines to set up the connections. Management's only requirement is that any communication between the office locations be appropriately secured. Which of the following steps should you take to ensure compliance with this requirement? (Choose all that apply.)
   - **A.** Configure CHAP on all the RRAS servers.
   - **B.** Configure PAP on all the RRAS servers.
   - **C.** Configure MPPE on all the RRAS servers.
   - **D.** Configure L2TP on all the RRAS servers.
   - **E.** Configure MS-CHAPv2 on all the RRAS servers.

4. Your small financial consulting company has a stand-alone Windows 2012 R2 server that provides a central location for your home-based consultants to upload and download spreadsheet files using Windows 8. A few of the consultants still use Windows XP Professional workstations. You want to set up VPN connections between the consultants and the RRAS server. The RRAS server is connected to a small peer-to-peer network of five Windows XP Professional workstations that use the network for storing files, including the files that the consultants are uploading and downloading. What authentication protocol should you use for the VPN?
   - **A.** CHAP
   - **B.** MS-CHAPv2
   - **C.** EAP-TLS
   - **D.** PAP

5. You recently migrated your company's Windows 2003 network to Windows Server 2012 R2. This migration includes 300 Windows 7 and Windows 8 workstations and 8 Windows Server 2012 R2 servers. Your company has just acquired another company with offices down the street. It has a Windows NT network that needs to be migrated to Windows Server 2012 R2 as well, and you have already begun to move the servers to the new operating system and associated services. Because you have a tight cap on expenses for network additions, you currently can't afford leased lines between the buildings. Until you can get support for them, you are going to create a VPN that is both encrypted and authenticated between the two facilities over the Internet connections that already exist. What do you need to implement to achieve this goal? (Choose all that apply.)
   - **A.** L2TP
   - **B.** PPTP
   - **C.** IPsec
   - **D.** RADIUS
   - **E.** MS-CHAPv2

6. You have implemented VPNs to connect the various locations of your organization. These locations include offices in New York, Sacramento, Memphis, and Omaha, with a significant LAN in each one. The RRAS server is set up such that the users aren't aware of the intricacies of the connections. You are beginning to have problems with the connections between the offices and, as a result, the number of support calls is growing dramatically. What configurations could you use to troubleshoot the communication problems?
   - **A.** L2TP using MPPE
   - **B.** L2TP unencrypted
   - **C.** L2TP using IPsec in transport mode
   - **D.** L2TP using IPsec in tunnel mode

7. Your company's 450 sales reps are finally going to receive laptops so that they can communicate with the corporate office whenever they need information stored on the corporate network. The corporate network is fully upgraded to Windows Server 2012 R2, including the default configuration of the RRAS server for the remote connectivity over VPNs. You have installed Windows 8 with the default configuration on all of the laptops and have added the sales reps to a special group in Active Directory. After you test the laptops, everything appears to work fine. You ship them out and, as they reach the sales reps, you monitor their initial connections. During the next few days, you begin receiving support calls from people complaining they cannot connect to the network. What is the most likely cause of the problem?
   - **A.** The Windows 8 clients are not configured to support a VPN.
   - **B.** The default RRAS configuration does not support VPNs.
   - **C.** The default RRAS configuration does not support enough VPN connections.
   - **D.** The default RRAS configuration does not support L2TP.
   - **E.** The Windows 8 client default configuration does not support L2TP.

8. You are the network administrator for a company with two offices; one is located on the East Coast and the other is located on the West Coast. Sales information needs to be sent from the East Coast to the West Coast office on a regular basis, and some payroll information and accounting reports need to be sent back to the East Coast. The owner of your company has been reading stories in the press about security problems on the Internet and refuses to allow any company information to travel through the Internet, regardless of how much you talk about securing those transmissions. The communications between the sites occur approximately once a week. What steps would you take to ensure secure authentication and secure transmission while not spending too much money? (Choose all that apply.)
   - **A.** Configure PAP as the authentication method between the servers.
   - **B.** Install RRAS on a server at each location and keep the line open with an ISDN connection that will always be available for the communication.
   - **C.** Install RRAS on a server at each location and configure demand-dial to open the connection each time the transmission occurs.
   - **D.** Configure CHAP as the authentication method between the servers.
   - **E.** Configure MS-CHAPv2 as the authentication method between the servers.
   - **F.** Configure IPsec as the encryption method between the servers.
   - **G.** Configure MPPE as the encryption method between the servers.
   - **H.** Configure L2TP as the encryption method between the servers.

9. You are using an RRAS server to manage remote access to your small Windows Server 2012 R2 network that serves a single location. RRAS provides access to several remote users and to the people who have machines on the local network but occasionally want to access the network from home or from hotels when on the road. Regardless of the category of user, everyone is authenticated through Active Directory. You haven't spent much time reviewing the use of this remote connectivity since you configured the system, but now there is a concern about unauthorized users as well as intermittent problems that remote users are experiencing when connecting to the network. You've been asked to prepare a report for management describing the extent of these problems in the company. You recall that when you set up the system, you configured the logging to track all connection attempts using local Windows accounting. Where will you find the logging information that you need for preparing your report?

A. The Performance Monitor log

B. Active Directory

C. The `systemroot\System32\LogFiles` folder

D. The system event log

E. The RRAS authentication log

10. Your area of responsibility at the All-Terrain Vehicle Rentals Company is to build, deploy, and maintain the remote access system for the Windows Server 2012 R2 network. The system consists of four RRAS servers that serve 200 users across the country. The users often travel from location to location, and they access different servers depending on where they call in. You put together a management station to monitor all of the RRAS servers so that you can keep an eye on this critical aspect of your network. What tool do you use to accomplish this?

A. The Server Monitor of the RRAS snap-in

B. The Server Status node of the RRAS snap-in

C. The System Monitor snap-in

D. The MMC

Chapter

14

Configure a Network Policy Server Infrastructure

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure Network Policy Server (NPS)**

- Configure a NPS server including RADIUS proxy
- Configure RADIUS clients
- Configure NPS templates
- Configure RADIUS accounting
- Configure certificates

✓ **Configure NPS policies**

- Configure connection request policies
- Configure network policies for VPN clients (multilink and bandwidth allocation, IP filters, encryption, IP addressing)
- Import and export NPS policies

✓ **Configure Network Access Protection (NAP)**

- Configure System Health Validators (SHVs)
- Configure health policies
- Configure NAP enforcement using DHCP and VPN
- Configure isolation and remediation of non-compliant computers using DHCP and VPN
- Configure NAP client settings

In Chapter 13, "Configure Routing and Remote Access," you were introduced to VPNs and RADIUS. In this chapter, I will take that a step further. I will still talk about remote access, but I will get more into the security part of the access. I will talk about how to limit access to your users based on the rules and policies that you preset. When a user logs onto the domain from a remote location, if their system doesn't meet minimum requirements, you can limit how much, if any, access the user has on the network.

I will also cover Network Access Protection (NAP) to show you how to start to protect your network, and you will look into Network Policy Server (NPS). NPS allows you to set policies that your users must follow or get limited-to-no access to the domain.

Overview of Wireless Access

In today's computer world, it seems like everyone has a laptop. We all do a lot of traveling, and at any airport it seems like everyone is working on a laptop while waiting for a plane.

Because laptops have grown in popularity, IT professionals must account for them on their networks. Laptops offer IT administrators a unique set of challenges that must be dealt with on a day-to-day basis.

One major concern for IT administrators is security. Years ago, we never had to worry about users copying documents to a desktop computer and then walking out with the computer. However, today users can copy company documents to laptop computers and then walk out the door with the computer and the documents. So, I will discuss wireless networks, protocols, and security.

Windows 8, Windows 7, Windows Vista, Windows 2008/2008 R2, Windows Server 2012, and Windows Server 2012 R2 have enhanced the IEEE 802.11 wireless support to include some of the following changes:

- Single sign-on
- 802.11 wireless diagnostics
- WPA2 support
- Native Wi-Fi architecture
- User interface improvements for wireless connections
- Wireless Group Policy enhancements
- Changes in wireless auto-configuration
- Integration with Network Access Protection when using 802.1X authentication

- EAP host infrastructure
- Command-line support for configuring wireless settings
- Network location awareness and network profiles
- Next-generation TCP/IP stack enhancements for wireless environments

Configuring Wireless Access

Windows 8, Windows 7, Windows Vista, Windows XP, and Windows Server 2003, 2008/2008 R2, and 2012/2012 R2 provide built-in support for 802.11 wireless LAN networking. Inside the `Network Connections` folder, an installed 802.11 wireless LAN network adapter appears as a wireless network connection. The following are some of the items you can configure:

Operating Modes There are two types of operating modes:

Infrastructure Mode This mode uses at least one wireless access point (WAP) and/or a device that bridges the wireless computers to each other.

Ad Hoc Mode Using this mode, wireless network computers connect directly to each other without the use of an access point (AP) or bridge.

Wired Equivalent Privacy All of us (on a laptop) have tried to find a wireless network at one time or another. *Wired Equivalent Privacy (WEP)* is a wireless encryption that was originally defined in 802.11. WEP helps to prevent unauthorized wireless users from accessing your wireless network by the use of a shared secret key:

- If your wireless network is using the infrastructure mode, the WEP key must be configured on the wireless AP and all of the wireless clients.
- If your wireless network is using the ad hoc mode, the WEP key must be configured on all of the wireless clients.

The WEP key can be either 40-bit or 104-bit, depending on what your hardware can accommodate.

Wi-Fi Protected Access An organization of wireless equipment vendors called the Wi-Fi Alliance created an interim standard called *Wi-Fi Protected Access (WPA)* while the IEEE 802.11i wireless LAN security standard was still being completed. WPA uses a strong encryption method called the *Temporal Key Integrity Protocol (TKIP)* to replace the weaker WEP standard. You have the ability to use the *Advanced Encryption Standard (AES)* for encryption that is provided by WPA.

WPA can be used in two different mode types:

WPA-Personal This is used for a home office or small company. In the WPA-Personal model, you would use a preshared or passphrase code to gain authorization onto the network.

WPA-Enterprise This was designed for a midsize to large organization. WPA-Enterprise has all of the same features as WPA-Personal, but it also includes the ability to use a 802.1X RADIUS server.

Wi-Fi Protected Access 2 Wi-Fi Protected Access 2 (WPA2) was officially designed to replace the WEP standard. WPA2 certifies that equipment used in a wireless network is compatible with the IEEE 802.11i standard. This certification is used to help standardize the use of the additional security features of the IEEE 802.11i standard that are not already included in WPA.

WPA2 can be used in two different mode types:

WPA2-Personal This is used for a home office or small company. In the WPA-Personal model, you would use a preshared or passphrase code to gain authorization onto the network.

WPA2-Enterprise This was designed for a midsize to large organization. WPA-Enterprise has all of the same features as WPA-Personal, but it also includes the ability to use a 802.1X RADIUS server.

Service Set Identifier To specify a wireless network by name, you specify the *service set identifier (SSID)*, also known as the *wireless network name*:

Infrastructure Mode The SSID is configured on the wireless access point.

Ad Hoc Mode The SSID is configured on the initial wireless client.

To help wireless clients discover and join the wireless network, the wireless AP or the initial wireless client periodically advertises the SSID. (This can be disabled for security.)

Group Policies for Wireless You have the ability to use Group Policy settings for Vista, Windows 7, Windows 8, Windows 2008/2008 R2, and Windows Server 2012/2012 R2 for WPA2. Group Policy settings allow you to configure WPA2 options at the server for all wireless clients.

Remote Access Security

In the past, remote access was seldom part of most companies' networks. It was too hard to implement, too hard to manage, and too hard to secure. It's reasonably easy to secure your networks from unauthorized physical access, but it was perceived to be much harder to do so for remote access. Recently, a number of security policies, protocols, and technologies have been developed to ease this problem. First I'll discuss the user authentication protocols.

User Authentication

One of the first steps in establishing a secure remote access connection involves allowing the user to present some credentials to the server. You can use any or all of the following authentication protocols that Windows Server 2012 R2 supports:

Password Authentication Protocol The *Password Authentication Protocol (PAP)* is the simplest authentication protocol. It transmits all authentication information in

cleartext with no encryption, which makes it vulnerable to snooping if attackers can put themselves between the modem bank and the remote access server. However, this type of attack is unlikely in most networks. The security risk with PAP is largely overemphasized considering the difficulty of setting up a sniffer in between the modems and the remote access server. If an attacker has the ability to install a sniffer this deep in the network, you have larger problems to address. PAP is the most widely supported authentication protocol, and therefore you may find that you need to leave it enabled.

Microsoft CHAPv2 Microsoft created *Microsoft CHAPv2 (MS-CHAPv2)* as an extension of the CHAP protocol to allow the use of Windows authentication information. Version 2 is more secure than version 1, and version 1 is not supported by Windows Server 2008 and newer. Some other operating systems (besides Microsoft) support MS-CHAP version 1.

Extensible Authentication Protocol The *Extensible Authentication Protocol (EAP)* doesn't provide any authentication itself. Instead, it relies on external third-party authentication methods that you can retrofit to your existing servers. Instead of hardwiring any one authentication protocol, a client-server pair that understands EAP can negotiate an authentication method. The computer that asks for authentication (the *authenticator*) is free to ask for several pieces of information, making a separate query for each one. This allows the use of almost any authentication method, including smart cards, secure access tokens such as SecurID, one-time password systems such as S/Key, or ordinary username/password systems.

Each authentication scheme supported in EAP is called an *EAP type*. Each EAP type is implemented as a plug-in module. Windows Server 2012 R2 can support any number of EAP types at once; the Routing and Remote Access Services (RRAS) server can use any EAP type to authenticate if you've allowed that module to be used and the client has the module in question.

Windows Server 2012 R2 comes with *EAP-Transport Level Security* (EAP-TLS). This EAP type allows you to use public key certificates as an authenticator. TLS is similar to the familiar Secure Sockets Layer (SSL) protocol used for web browsers. When EAP-TLS is turned on, the client and server send TLS-encrypted messages back and forth. EAP-TLS is the strongest authentication method you can use; as a bonus, it supports smart cards. However, EAP-TLS requires your RRAS server to be part of a Windows 2000, Windows Server 2003, Windows Server 2008/2008 R2, or Windows Server 2012 R2 domain.

EAP-RADIUS is another authentication method included with Windows Server 2012 R2. EAP-RADIUS is a fake EAP type that passes any incoming message to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

PEAP-MS-CHAP v2 This protocol is founded on the authenticated wireless access design, and it's based on Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2). This authentication protocol utilizes the user account credentials (username and password) stored in Active Directory Domain Services to authenticate wireless access clients instead of using smart cards or user and computer certificates for client authentication.

PEAP-MS-CHAP v2 is an EAP-type protocol that is easier to deploy than Extensible Authentication Protocol with Transport Level Security (EAP-TLS). It is easier because user authentication is accomplished by using password-based credentials (username and password) instead of digital certificates or smart cards. Only servers running Network Policy Server or PEAP-MS-CHAP v2 are required to have a certificate. The server certificate used by NPS can be issued by your organization's private trusted root CA deployed on your network or by a public CA that is already trusted by the client computer.

Just in case you missed the very important line above, I will say it again: Servers that are running Network Policy Server or PEAP-MS-CHAP v2 are *required* to have a certificate.

TLS/SSL (Schannel) *TLS/SSL (Schannel)* implements both the Secure Sockets Layer and Transport Layer Security Internet standard authentication protocols. Administrators can use TLS/SSL to authenticate servers and client computers. Administrators also have the ability to use the protocol to encrypt messages between the authenticated parties (client and server).

The Transport Layer Security protocol, Secure Sockets Layer protocol, Datagram Transport Layer Security (DTLS), and Private Communications Transport (PCT) protocol are all based on the public key cryptography. The Security Channel authentication protocol suite provides these protocols, and this protocol is based on the client-server model.

NTLMv2 *NTLMv2* (Windows NT LAN Manager) helps the authentication process for Windows NT 4 systems or earlier, and it allows for transactions between any two computers running these older systems. Networks that use NTLMv2 are referred to as *mixed mode*.

Kerberos The *Kerberos authentication protocol* is used to perform Active Directory domain authentication. By default, all computers joined to a Windows Server 2012 R2 domain use the Kerberos authentication protocol. Kerberos allows for single sign-on to network resources on a domain or on a trusted domain. Administrators have the ability to control certain parameters through the Kerberos security settings of the account policies.

802.1X The IEEE has a standard for wireless authentication called 802.1X. 802.1X allows wireless networks to authenticate onto wired Ethernet networks or wireless 802.11 networks. The IEEE 802.1X standard uses EAP for exchanging messages during the authentication process.

Connection Security

You can use some additional features to provide connection-level security for your remote access clients:

- The *Callback Control Protocol (CBCP)* allows your RRAS servers or clients to negotiate a callback with the other end. When CBCP is enabled, either the client or the

server can ask the server at the other end to call the client back at a number supplied by the client or a prearranged number stored on the server.

- You can program the RRAS server to accept or reject calls based on the caller ID or automatic number identification (ANI) information transmitted by the phone company. For example, you can instruct your primary RRAS server to accept calls from only your home analog line. This means you can't call the server when you're on the road, and it also keeps the server from talking to strangers.
- You can specify various types and levels of encryption to protect your connection from interception or tampering.

Real World Scenario

The Limits of Caller ID

It's risky to rely on ANI information for any type of authentication or caller verification. First, caller ID information can be forged. Therefore, if an attacker knows the telephone numbers from which your network accepted calls, they could make their ANI report as one of those numbers and be authenticated onto the network.

Another problem with relying on ANI for authentication is that not all telephone companies pass ANI information with the call. Therefore, if your users are in remote locations (which is why they'd be dialing in anyway), they might not be able to authenticate. Even when ANI information is sent, some telephone companies pass different pieces of the information, which can also result in authentication failures.

Finally, not all incoming line types support ANI. If your site uses a network access server or modem bank that doesn't receive this information based on the type of T1 connection used for incoming calls, the ANI information might not be there at all.

Access Control

Apart from the connection-level measures that you can use to prohibit outside callers from talking to your servers, you can restrict which users can make remote connections in a number of ways:

- You can allow or disallow remote access from individual user accounts. This is the same limited control you have in Windows NT, but it's just the start for Windows Server 2012 R2.
- You can use network access policies to control whether users can get access.

  Like group policies, network access policies give you an easy way to apply a consistent set of policies to groups of users. However, the policy mechanism is a little different: You create rules that include or exclude the users whom you want in the policy.

Unlike group policies, network access policies are available only in Windows 2000 native, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 domain functional level (that is, in domains in which there are no Windows NT domain controllers present). This means you may not have the option to use network access policies until your Windows 2000, Windows Server 2003, Windows Server 2008/2008 R2, and Windows Server 2012 R2 deployment is further along.

In the next sections, you will learn how to configure user access control.

Configuring User Access

Now it's time to determine who can actually use the remote access services. You do this in two ways:

- By setting up remote access profiles on individual accounts
- By creating and managing network access policies that apply to groups of users

This distinction is subtle but important because you manage and apply profiles and policies in different places.

Setting Up User Profiles

Windows Server 2012 R2 stores a lot of information for each user account. Collectively, this information is known as the account's *profile*, and it's normally stored in Active Directory. Some settings in the user's profile are available through one of the two user-management snap-ins:

- If your RRAS server is part of an Active Directory domain, the user profile settings are in the Active Directory Users and Computers snap-in.
- If your RRAS server is *not* part of an Active Directory domain, the user profile settings are in the Local Users and Groups snap-in.

In either case, the interesting part of the profile is the Dial-In tab of the user's Properties dialog box (see Figure 14.1). This tab has a number of controls that regulate how the user account can be used for dial-in access.

These controls include the following:

Network Access Permission Control Group The first, and probably most familiar, controls on this tab are in the Network Access Permission control group. These options control whether the user has dial-in permission. Windows Server 2012 R2 has a feature that, in addition to explicitly allowing or denying access, lets you control access through Network Access Protection.

Verify Caller-ID Check Box RRAS can verify a user's caller ID information and use the results to allow or deny access. When you check the Verify Caller-ID check box and enter

FIGURE 14.1 The Dial-In tab of the user's Properties dialog box

a phone number in the field, you're telling RRAS to reject a call from anyone who provides that username and password but whose caller ID information doesn't match what you enter. This means the user can call in only from a single phone number.

Callback Options Control Group The Callback Options control group gives you three choices for regulating callback:

No Callback This is the default setting. It means that the server will never honor callback requests from this account.

Set By Caller This setting allows the calling system to specify a number at which it wants to be called back. The RRAS server will call the client back at that number.

Always Callback To This setting allows you to enter a number that the server will call back no matter from where the client is actually calling. This option is less flexible but more secure than the Set By Caller option.

Assign Static IP Addresses Check Box If you want this user always to get the same static IP address, you can arrange to do so by selecting the Assign Static IP Addresses check box and then entering the desired IP address. This allows you to set up nondynamic DNS records for individual users, guaranteeing that their machines will always have a valid DNS entry. On the other hand, this can be more prone to typographical errors on setup than the dynamic DNS-DHCP combination you could use instead.

Apply Static Routes Check Box In an ordinary LAN, you don't have to do anything special to clients to enable them to route packets—just configure them with a default gateway, and the gateway handles the rest. For dial-up connections, though, you may want

to define a list of static routes that will enable the remote client to reach hosts on your network, or elsewhere, without requiring that packets be sent to a gateway in between. Depending on the remote access server, though, the client may be able to use Address Resolution Protocol (ARP) for local devices too. If you want to define a set of static routes on the client, you'll have to do it manually. If you want to assign static routes on the server, select the Apply Static Routes check box and then use the Static Routes button to add and remove routes as necessary.

Remember that these settings apply to individual users, so you can assign different routes, caller ID, or callback settings to each user.

Using Network Access Policies

Windows Server 2012 R2 includes support for additional configuration systems:

- Network access policies (which used to be called *remote access policy*).
- Remote access profiles.
- Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2012. NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003.

Policies determine who can and cannot connect; you define rules with conditions that the system evaluates to see whether a particular user can connect.

You can have any number of policies in a native Windows Server 2012 R2 domain; each policy must have exactly one profile associated with it.

Settings in an individual user's profile override settings in a network access policy.

You manage network access policies through the `Remote Access Logging & Policies` folder in the RRAS snap-in. Policies contain conditions that you pick from a list. When a caller connects, the policy's conditions are evaluated, one by one, to see whether the caller gets in. All of the conditions in the policy must match for the user to gain access. If there are multiple policies, they're evaluated according to an order you specify.

In the following sections, you will see how to create and configure network access policies.

Network Policy Attributes

To create a policy, right-click the `Remote Access Logging & Policies` folder and select Launch NPS (see Figure 14.2). Then right-click Network Policies and choose New.

FIGURE 14.2 The Launch NPS option in RRAS

This command starts the New Network Policy Wizard, which uses a series of steps to help you define the policy.

The Select Condition dialog box (see Figure 14.3) is part of the New Network Policy Wizard. It lists the attributes you can evaluate in a policy. Table 14.1 describes the attributes that you can set. These attributes are drawn from the RADIUS standards, so you can (and in some cases, should) intermix your Windows Server 2012 R2 RRAS servers with RADIUS servers.

When setting up any policies, you must base your policy on company rules and standards. Remember, policies can allow or restrict users from remotely accessing your network. The needs of the organization determine the policy and when to use it.

Once you choose an attribute and click the Add button, its corresponding editor appears. You use the editor to set the value of the attribute. For example, if you select the Day And Time Restrictions attribute, you'll see the Time Of Day Constraints dialog box, which offers a calendar grid that lets you select which days and times are available for logging on.

FIGURE 14.3 Select Condition dialog box of New Network Policy Wizard

TABLE 14.1 Network access policy attributes

Attribute name	What it specifies
Authentication Type	Specifies the authentication methods required to match this policy.
Allowed EAP Types	Specifies the EAP types required for the client computer authentication method configuration to match this policy.
Called Station Id	Specifies the phone number of the remote access port called by the caller.
Calling Station Id	Specifies the caller's phone number.
Client Friendly Name	Specifies the name of the RADIUS server that's attempting to validate the connection.
Client IP Address (IPv4 and IPv6)	Specifies the IP address of the RADIUS server that's attempting to validate the connection.
Client Vendor	Specifies the vendor of the remote access server that originally accepted the connection. This is used to set different policies for different hardware.
Day And Time Restrictions	Specifies the weekdays and times when connection attempts are accepted or rejected.
Framed Protocol	Specifies the protocol to be used for framing incoming packets (for example, PPP, SLIP, and so on).

HCAP (Host Credential Authorization Protocol) User Groups	Used for communications between NPS and some third-party network access servers (NASs).
Location Groups	Specifies the HCAP location groups required to match this policy. This is used for communications between HCAP and some third-party network access servers (NASs).
MS RAS Vendor	Specifies the vendor identification number of the network access server (NAS) that is requesting authentication.
NAS Identifier	Specifies the friendly name of the remote access server that originally accepted the connection.
NAS IP Address (IPv4 and IPv6)	Specifies the IP address of the remote access server that originally accepted the connection.
NAS Port Type	Specifies the physical connection (for example, ISDN, POTS) used by the caller.
Service Type	Specifies Framed or Async (for PPP) or login (Telnet).
Tunnel Type	Specifies which tunneling protocol should be used (L2TP or PPTP).
Windows Groups	Specifies which Windows groups are allowed access.

After you select an attribute and give it a value, you can add more attributes or move to the next page by clicking the Next button on the Select Condition page.

Once you're finished setting attributes, you arrive at the Specify Access Permission page of the wizard. This page has only two radio buttons: Grant Remote Access Permissions and Deny Remote Access Permissions. These buttons specify whether the policy you create *allows* users to connect or *prevents* users from connecting. The page also includes an Access Is Determined By User Dial-In Properties check box. If this box is checked and there is a conflict between the network policy and user dial-in properties, the user dial-in properties take precedence.

Creating a Network Access Policy

In Exercise 14.1, you'll create an adjunct policy that adds time and day restrictions to the default policy. (An *adjunct policy* is one used in conjunction with another policy.) This exercise requires that you have completed the previous exercises in this chapter.

EXERCISE 14.1

Creating a Network Access Policy

1. Open the RRAS MMC snap-in by pressing the Windows key and selecting Administrative Tools ➢ Routing And Remote Access.
2. Expand the server you want to configure in the left pane of the MMC.
3. Right-click the Remote Access Logging And Policies folder.
4. Right-click and then select Launch NPS.
5. Once the Network Policy Server page appears, right-click Network Policies and then choose New.

6. The New Network Policy Wizard starts. In the Policy Name box, enter **Test Policy** and then click Next (leave the other settings as they are).

7. On the Specify Conditions page, click the Add button.
8. In the Select Condition dialog box, scroll down and click Day And Time Restrictions. Click Add.

9. The Time Of Day Constraints dialog box appears. Use the calendar controls to allow remote access Monday through Saturday from 7 a.m. to 7 p.m. and then click the OK button.

10. The Select Conditions dialog box reappears, this time with the new condition listed. Click the Next button.
11. The Specify Access Permission page appears. Select the Access Granted radio button and click Next to continue.
12. The Configure Authentication Methods page appears next. This page is where you choose which authentication methods will be used for this connection. Make sure that MS-CHAP and MS-CHAPv2 are both checked, along with the check boxes associated with them. Click Next.

EXERCISE 14.1 *(continued)*

13. The Configure Constraints page appears. Under Constraints, click Session Timeout. On the right side, click the Disconnect After The Following Maximum Session Time box, and type **60** in the field (the value represents minutes). Click Next.

14. The Configure Settings page appears. This page allows you to configure any additional settings for this network policy. Click Next.

15. On the Completing New Network Policy page, click Finish.

NPS as a RADIUS Proxy Server

When a user tries to log into a domain through the use of a RADIUS server, the RADIUS server processes the connection request and helps the user log into the network.

RADIUS proxy servers work in a different way. When a connection request comes into a RADIUS proxy server, the RADIUS proxy server forwards the request to another RADIUS server for authentication onto the network. Servers that are running Network Policy Server can act both as a RADIUS server and as a RADIUS proxy.

When an administrator sets up NPS as a RADIUS server, NPS provides some of the following actions to help the RADIUS server work properly:

- RADIUS clients send an access request to the central authentication and authorization service. NPS uses Active Directory to authenticate the user's credentials. NPS accesses the Active Directories user's dial-in properties and policies to authorize the connection.
- When using NPS, the RADIUS server also records all accounting information on how much the RADIUS server is used. This is helpful when you have to bill other

departments for the RADIUS use. Many organizations require that each department pay for its RADIUS use for its users, and using NPS allows an administrator to do this.

When you set up NPS as a RADIUS proxy, NPS provides all of the routing between all of the RADIUS servers and RADIUS clients. NPS is the main switching and routing service when you use RADIUS as a proxy server.

NPS Configuration

Now that you know that NPS can be set up as a RADIUS server, let's take a look at some of those details of how to do it. When an administrator sets up NPS as a RADIUS proxy, network access servers are then configured as the RADIUS clients. The RADIUS proxy server receives requests from the RADIUS clients, and then the RADIUS server forwards those requests to the appropriate servers. Using NPS to set up a RADIUS proxy should be done when the following conditions are needed:

- If you are the administrator of an organization that offers VPN or wireless network access to multiple clients, the RADIUS server can authenticate and authorize the user through their authentication server.
- If you are an administrator of a domain and you want users who are not members of your domain to authenticate into your domain, you can use an NPS server with a RADIUS proxy. To make this situation work, you must set up a two-way trust (two one-way trusts in opposite directions).
- Another great example of when to set up a RADIUS proxy server is when you are using a non-Microsoft-based database. RADIUS servers have the ability to communicate with different types of databases, allowing users still to be authenticated even when it's not a Microsoft authentication database; an example is a Novell Directory Services (NDS) database.

Another configuration that you may need to set when configuring NPS and RADIUS is the priority. The higher the RADIUS priority number, the less that the RADIUS server gets used. For example, if I have two RADIUS servers named Server1 and Server2 and I want Server2 used only when Server1 is unavailable, I would set the RADIUS priority from 1 to 10. This way it will get used only when Server1 is having issues or is unresponsive.

RADIUS Clients

Network access servers that are RADIUS RFC compliant (2865 and 2866) are considered RADIUS clients when used with NPS and a RADIUS server or proxy.

NPS allows an administrator to enable the use of wireless, switches, remote access, or VPN equipment as long as they are heterogeneous or homogenous sets. Network administrators can allow authentication and authorization through the use of NPS network connection requests as long as administrators deploy the following types of network access servers and technologies:

- Wired access with 802.1X-secured and RADIUS-compliant authenticating switches
- Wireless access with 802.1X-secured and RADIUS-compliant wireless access points

NPS Templates

Templates can be a valuable tool when used properly. Templates allow you to create something once and then use that template to create the same thing over and over again.

You can use templates when creating Active Directory users, when setting up GPOs, and now even when setting up NPS. NPS templates allow an administrator to save time and thus also save the cost required to manage and configure NPS on multiple servers. Multiple NPS templates are available in the Templates Management MMC for an administrator to configure:

- Shared Secrets
- RADIUS Clients
- Remote RADIUS Servers
- IP Filters
- Health Policies
- Remediation Server Groups

One advantage of creating a template is that once the template is created, there is no interference with the actual NPS server's performance. Creating templates does not affect an operational NPS server in any way. Once you load the template to the appropriate location, the template becomes active.

Creating Templates

To create a template in the Template Management MMC, right-click the template type you want to create (such as Health Policies) and click New. The New Template dialog box appears, and you just fill in all of your configuration information.

Importing and Exporting NPS Policies

Importing/exporting NPS is a pretty easy thing. It just happens to depend on which version of Windows you are exporting from. In the following examples, I will explain how to export from Windows Server 2008 R2 using the Windows MMC and how to import into Windows Server 2012 R2.

Exporting from Windows Server 2008 R2

To export NPS from Windows Server 2008 R2, follow these steps:

1. On the source server, open Server Manager.
2. In the Server Manager console tree, open Roles\Network Policy and Access Services\NPS.
3. Right-click NPS and then click Export Configuration.
4. In the dialog box that appears, select the check box I Am Aware That I Am Exporting All Shared Secrets and then click OK.

5. For File Name, type **file.xml**, navigate to the migration store file location, and then click Save.
6. In the console tree, right-click Templates Management and then click Export Templates To A File.
7. For File Name, type **iastemplates.xml**, navigate to the migration store file location, and then click Save.
8. If you have configured SQL logging, you must manually record detailed SQL configuration settings.

   To record these settings, follow these steps:

   a. In the NPS console tree, click Accounting and then click Change SQL Server Logging Properties.
   b. Record the configuration settings on the Settings tab and then click Configure.
   c. Manually record all configuration settings from the Connection and Advanced tabs by copying them into the `sql.txt` file. Alternatively, you can click the All tab and enter Name and Value settings displayed on each line into the `sql.txt` file.
9. Copy the `file.xml`, `iastemplates.xml`, and `sql.txt` files to the migration store file location. This information will be required to configure the destination server.

Importing to Windows Server 2012 R2

To import NPS from Windows Server 2012 R2, follow these steps

1. Copy the configuration files `file.xml`, `iastemplates.xml`, and `sql.txt` that were exported to the migration store file location to the destination NPS server. Alternatively, you can import configuration settings directly from the migration store file location by supplying the appropriate path to the file in the import command. If you have custom settings that were recorded using the NPS Server Migration: Appendix A—Data Collection Worksheet, they must be configured manually on the destination server.
2. On the destination server, open Server Manager.
3. In the Server Manager console tree, click All Servers; then, from the list of servers in the right pane, right-click the relevant server and select Network Policy Server.
4. To import template configuration settings, complete the remaining steps in this list. If you do not have template settings, skip to step 7.
5. In the console tree, right-click Templates Management and then click Import Templates from a file.
6. Select the template configuration file `iastemplates.xml` that you copied from the source server and then click Open.
7. In the console tree, right-click NPS and then click Import Configuration.

8. Select the configuration file `file.xml` or `ias.txt` that you copied from the source server and then click Open.
9. Verify that a message appears indicating the import was successful.
10. Configure SQL accounting if required using the `sql.txt` file and the data collection worksheet. To configure SQL accounting, complete the remaining steps in this list.
11. In the NPS console tree, click Accounting and then click Change SQL Server Logging Properties in the details pane.
12. Modify the properties on the Settings tab if required and then click Configure to enter detailed settings.
13. Using information recorded in the `sql.txt` file, enter the required settings on the Connection and Advanced tabs and then click OK.

Using Remote Access Profiles

Remote access profiles are an integral part of network access policies. Profiles determine what happens during call setup and completion. Each policy has a profile associated with it; the profile determines what settings will be applied to connections that meet the conditions stated in the policy.

For security reasons, it's usually a good idea to limit access to the administrative accounts on your network. In particular, as a consultant, I usually tell clients to restrict remote access for the administrator account; that way, the potential exposure from a dial-up compromise is reduced. In Exercise 14.2, you will learn how to configure the administrator account's user profile to restrict dial-up access.

EXERCISE 14.2

Restricting a User Profile for Dial-In Access

1. Log on to your computer using an account that has administrative privileges.
2. If you're using an RRAS server that's part of an Active Directory domain, open the Active Directory Users and Computers snap-in by pressing the Windows key and selecting Administrative Tools ➢ Active Directory Users And Computers. If not, open the Local Users and Groups snap-in by pressing the Windows key and selecting Administrative Tools ➢ Computer Management ➢ Local Users And Groups.
3. Expand the tree to the `Users` folder. Right-click the Administrator account in the right pane and choose Properties. The Administrator Properties dialog box appears.
4. Switch to the Dial-In tab. On machines that participate in Active Directory, make sure the Control Access Through NPS Network Policy option (in the Permissions group) is selected.

5. Click the Deny Access radio button to prevent the use of this account over a dial-in connection.
6. Click the OK button.

You can create one profile for each policy. The profile contains settings that fit into specific areas. Each area has its own link in the profile's Properties dialog box.

The Constraints Tab

The Constraints tab has most of the settings that you think of when you consider dial-in access controls. The controls here allow you to adjust how long the connection can be idle before it gets dropped, how long it can be up, the dates and times for establishing the connection, and what dial-in port and medium can be used to connect.

Authentication Link

In the Authentication Methods pane (see Figure 14.4), you can specify which authentication methods are allowed on this specific policy. Note that these settings, like the other policy settings, will be useful only if the server's settings match. For example, if you turn EAP authentication off in the server's Properties dialog box, turning it on in the Authentication Methods pane of the profile's Properties dialog box will have no effect.

FIGURE 14.4 Authentication Methods settings

You'll notice that each authentication method has a check box. Check the appropriate boxes to control the protocols that you want this profile to use. If you enable EAP, you can also choose which specific EAP type you want the profile to support. You can also choose to allow totally unauthenticated access (which is unchecked by default).

Settings Tab

The Settings tab of the policy's Properties dialog box has several useful sections, which are described in the following list:

IP Settings Pane The IP Settings pane (see Figure 14.5) gives you control over the IP-related settings associated with an incoming call. If you think back to the server-specific settings covered earlier, you'll remember that the server preferences include settings for protocols other than IP; this is not so in the network access profile. In this pane, you can specify where the client gets its IP address.

FIGURE 14.5 IP Settings pane of the Settings tab

Multilink And Bandwidth Allocation Protocol (BAP) Pane The profile mechanism gives you a degree of control over how the server handles multilink calls. You exert this control

through the Multilink And Bandwidth Allocation Protocol (BAP) pane of the profile Properties dialog box. Your first choice is to decide whether to allow multilink calls at all and, if so, how many ports you want to let a single client use at once. Normally, this setting is configured so that the server-specific settings take precedence, but you can override them.

Bandwidth Allocation Protocol Group The Bandwidth Allocation Protocol control group gives you a way to control what happens during a multilink call when the bandwidth usage drops below a certain threshold. For example, why tie up three analog lines to provide 168Kbps of bandwidth when the connection is using only 56Kbps? You can tweak the capacity and time thresholds. By default, a multilink call will drop one line every time the bandwidth usage falls to less than 50 percent of the available bandwidth and stays there for two minutes. The Require BAP For Dynamic Multilink Requests check box allows you to refuse calls from clients that don't support BAP. This is an easy way to make sure that no client can hog your multilink bandwidth.

Encryption Pane The Encryption pane of the Settings tab (see Figure 14.6) controls which type of encryption you want your remote users to be able to access.

FIGURE 14.6 Encryption pane of the Settings tab of the policy's Properties dialog box

The following radio buttons are on the Encryption pane:

- Basic Encryption (MPPE 40-Bit) means single Data Encryption Standard (DES) for IPsec or 40-bit Microsoft Point-to-Point Encryption (MPPE) for Point-to-Point Tunneling Protocol (PPTP).
- Strong Encryption (MPPE 56-Bit) means 56-bit encryption (single DES for IPsec; 56-bit MPPE for PPTP).
- Strongest Encryption (MPPE 128-Bit) means triple DES for IPsec or 128-bit MPPE for PPTP connections.
- No Encryption allows users to connect using no encryption at all. Unless this button is selected, a remote connection must be encrypted, or it'll be rejected.

In Exercise 14.3, you'll force all connections to your server to use encryption. Any client that can't use encryption will be dropped. You must complete Exercise 14.1 before you do this exercise.

WARNING

Don't do this exercise on your production RRAS server unless you're sure that all of your clients are encryption-capable.

EXERCISE 14.3

Configuring Encryption

1. Open the RRAS MMC snap-in by pressing the Windows key and selecting Administrative Tools ➢ Routing And Remote Access.
2. Expand the server you want to configure in the left pane of the MMC.
3. Right-click the `Remote Access Logging & Policies` folder.
4. Select Launch NPS.
5. Once the Network Policy Server page appears, click the hours policy you created in Exercise 14.3. (I named mine Test Policy.)
6. Select Action ➢ Properties. The policy's Properties dialog box appears.
7. Click the Settings tab. Select Encryption in the left pane.
8. In the right pane, uncheck the No Encryption check box. Make sure that the Basic, Strong, and Strongest check boxes are all selected.
9. Click the OK button. When the policy Properties dialog box reappears, click the OK button.

Setting Up a VPN Network Access Policy

Earlier in this chapter, you learned how to use the Network Access Policy mechanism on a Windows Server 2012 R2 domain. Now it's time to apply what you've learned to a virtual private network (VPN). Recall that you have two ways to control which specific users can access a remote access server:

- You can grant and deny dial-up permission to individual users in each user's Properties dialog box.
- You can create a network access policy that embodies whatever restrictions you want to impose.

It turns out that you can do the same thing for VPN connections, but there are a few additional things to consider.

Granting and Denying Per-User Access

To grant or deny VPN access to individual users, all you have to do is make the appropriate change on the Dial-In tab of each user's Properties dialog box. Although this is the easiest method to understand, it gets tedious quickly if you need to change VPN permissions for more than a few users. Furthermore, this method offers you no way to distinguish between dial-in and VPN permissions.

Creating a Network Access Policy for VPNs

You may find it helpful to create network access policies that enforce the permissions that you want end users to have. You can accomplish this result in a number of ways; which one you use will depend on your overall use of network access policies.

The simplest way is to create a policy that allows all of your users to use a VPN. Earlier in this chapter, you learned how to create network access policies and specify settings for them; one thing you may have noticed was that there's a NAS-Port-Type attribute that you can use in the policy's conditions. That attribute is the cornerstone of building a policy that allows or denies remote access via VPN because you use it to accept or reject connections arriving over a particular type of VPN connection. For best results, you'll use the Tunnel-Type attribute in conjunction with the NAS-Port-Type attribute, as described in Exercise 14.4.

EXERCISE 14.4

Creating a VPN Network Access Policy

1. Open the RRAS MMC snap-in by pressing the Windows key and selecting Administrative Tools ➢ Routing And Remote Access.
2. Expand the server you want to configure in the left pane of the MMC.
3. Right-click the `Remote Access Logging & Policies` folder.
4. Select Launch NPS.

EXERCISE 14.4 *(continued)*

5. Once the Network Policy Server page appears, right-click Network Policies and choose New.
6. The New Network Policy Wizard starts. In the Policy Name box, enter **VPN Network Policy** and click Next (leave the other settings as they are).
7. On the Specify Conditions page, click the Add button.
8. On the Select Condition page, scroll down, click NAS-Port-Type Attribute, and click Add. When the NAS Port Type page appears, click Virtual VPN in the Common Dial-Up And VPN Tunnel Types box. Click OK and then click the Next button.
9. The Specify Conditions page reappears, this time with the new condition listed. Click the Next button.
10. The Specify Access Permission page appears. Select the Access Granted radio button and click Next to continue.
11. Next the Configure Authentication Methods page will appear. This page is where you choose which authentication methods will be used for this connection. Make sure that MS-CHAP and MS-CHAPv2 are both checked along with their associated check boxes. Click Next.
12. The Configure Constraints page appears. Under Constraints, click Session Timeout. On the right side, click the Disconnect After The Following Maximum Session Time box and type **60** in the box (the value specifies minutes). Click Next.
13. The Configure Settings page appears. This page allows you to configure any additional settings for this network policy. Click Next.
14. At the Completing New Network Policy page, click Finish.

If you don't want to grant VPN access to everyone, you can make some changes to the process in Exercise 14.6 to fine-tune it. First you'll probably want to move the VPN policy to the top of the list. (When you first add the policy described in the exercise, it is placed at the end of the policy list. Unless you move it, the default policies will take effect before the VPN-specific policy does.)

Next you can create an Active Directory group and put your VPN users in it. You can then create a policy using the two conditions outlined in Exercise 14.6 plus a condition that uses the Windows-Groups attribute to specify the new group. You can also use this process to allow everyone dial-up access and reserve VPN capability for a smaller group.

Connection Manager

To help administrators create and manage remote access connections, Microsoft includes a suite of components called Connection Manager within Windows Server 2012 R2. Connection Manager is not installed by default. You can install the Connection Manager using Server Manager ➢ Add Roles ➢ Network Access Services.

Connection Manager allows an administrator to create remote access connections called *service profiles*. These profiles then appear on client machines as network connections. You can use these network connections to connect client machines to VPNs or remote networks.

Configuring Security

When configuring remote access security, you must consider several aspects, the most fundamental of which involves configuring the types of authentication and encryption that the server will use when accepting client requests. You will look at each of these in the following sections.

Controlling Server Security

The Security tab of the server's Properties dialog box (see Figure 14.7) allows you to specify which authentication and accounting methods RRAS uses. You can choose one of two authentication providers by using the Authentication Provider drop-down list.

FIGURE 14.7 The Security tab of the RRAS server's Properties dialog box

Your choices include the following:

Windows Authentication This is a built-in authentication suite included with Windows Server 2012 R2.

RADIUS Authentication This authentication allows you to send all authentication requests heard by your server to a RADIUS server for approval or denial.

You can also use the Accounting Provider drop-down list on the Security tab to choose between the following:

Microsoft-Developed Accounting With this type of accounting, connection requests are maintained in the event log.

RADIUS Accounting In this type of accounting, all accounting events, such as call start and call stop, are sent to a RADIUS server for action.

RADIUS Authentication Settings

When you select the RADIUS Authentication option from the Authentication Provider drop-down menu, you are enabling a RADIUS client that passes authentication duties to a RADIUS server. This communication is sent via UDP on port 1645 or 1812, depending on the version of RADIUS being used.

Click the Configure button to open the RADIUS Authentication dialog box. From here, you can set the following options:

- Click the Add button to add the name or address of a RADIUS server to which the RAS server will pass authentication duties.
- You must also enter the correct secret, which is initially set by the RADIUS server.
- The Time-Out option determines how long the RRAS server will attempt to authenticate the remote user before giving up.
- The Initial Score option is similar to the cost value used by routers. The RAS server will attempt to authenticate users on the RADIUS server with the highest score first. If that attempt fails, the RAS server will use the RADIUS server with the next highest score, and so on.
- Although the Port option can be changed, the default setting is part of RFC 2866, "RADIUS Accounting," and it should not be altered unless extraordinary circumstances call for it.

The Internet Assigned Numbers Authority (IANA) is the official source for port number assignment. You can view current port number assignments and other valuable information at `www.iana.org/assignments/port-numbers`.

Windows Authentication Settings

Select the Windows Authentication option from the Authentication Provider drop-down menu if you want the local machine to authenticate your remote access users. To configure the server by telling it which authentication methods you want it to use, click the Authentication Methods button, which displays the Authentication Methods dialog box. If you look at the list of authentication protocols earlier in the chapter, you'll find that each one has a corresponding check box here: EAP, MS-CHAPv2, CHAP, and PAP. You can also turn on unauthenticated access by checking the Allow Remote Systems To Connect Without Authentication box, but that is not recommended because it allows anyone to connect to, and use, your server (and thus by extension your network).

There's actually a special set of requirements for using CHAP because it requires access to each user's encrypted password. Windows Server 2012 R2 normally doesn't store user passwords in a format that CHAP can use, so you have to take some additional steps if you want to use CHAP:

1. Enable CHAP at the server and policy levels.
2. Edit the default domain GPO's Password Policy object to turn on the Store Password Using Reversible Encryption policy setting.
3. Change or reset each user's password, which forces Windows Server 2012 R2 to store the password using reversible encryption.

After these steps are completed for an account, that account can be used with CHAP.

These steps aren't required for MS-CHAPv2; for that protocol, you just enable MS-CHAPv2 at the server and policy levels.

Configuring Network Access Protection

Another way that you can have security is to allow users to access resources based on the identity of the client computer. This new security solution is called *Network Access Protection*. Determined by the client needs, network administrators now have the ability to define granular levels of network access using NAP. NAP also allows administrators to determine client access based on compliancy with corporate governance policies. The following are some of the NAP features:

Network Layer Protection *Network layer protection* is the ability to secure communications at the Network layer of the OSI model.

All communications travel through the seven layers of the OSI model. Starting at the top (layer 7), the seven layers are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical layers.

DHCP Enforcement If a computer wants to receive unlimited IPv4 network access, the computer must be compliant with corporate governance policies. *DHCP enforcement* verifies that a computer is compliant before granting unlimited access. If a computer is noncompliant, the computer receives an IPv4 address that has limited network access and a default user profile. One advantage of using DHCP is that you can set up user classes so that specific machines (for example, noncompliant DHCP systems) can get specific rules or limited access to the network.

When a client computer attempts to receive an IP address from DHCP, the DHCP enforcement checks the health policy requirements of the system to make sure they meet the compliancy.

VPN Enforcement *VPN enforcement* works a lot like DHCP enforcement, except that VPN enforcement verifies the compliancy of the system before the VPN connection is given full access to the network.

IPsec Enforcement *IPsec enforcement* will allow a computer to communicate with other computers as long as the computers are IPsec compliant. You have the ability to configure the requirements for secure communications between the two compliant computer systems. You can configure the IPsec communications based on IP address or TCP/UDP port numbers.

802.1X Enforcement For a computer system to have 802.1X unlimited access to network connections (Ethernet 802.11 or wireless access point), the computer system must be 802.1X compliant. *802.1X enforcement* verifies that the connecting system is 802.1X connection compliant. Noncompliant computers will obtain only limited access to network connections.

Flexible Host Isolation *Flexible host isolation* allows a server and domain to isolate computers to help make it possible to design a layer of security between computers or networks. Even if a hacker gains access to your network using an authorized username and password, the server and domain isolation can stop the attack because the computer is not an authorized domain computer.

Multiconfiguration System Health Validator This feature allows you to specify multiple configurations of a *system health validator (SHV)*. When an administrator configures a network policy for health evaluation, the administrator will select a specific health policy. Using this feature allows you to specify different network policies for different sets of health requirements based on a specific configuration of the SHV. For example, an administrator can create a network policy that specifies that all internal computers must have antivirus software enabled and a different network policy that specifies that VPN-connected computers must have their antivirus software enabled and signature files up-to-date.

NAP Monitoring

There may be many times when you will need to monitor how NAP is running and what NAP policies are being enforced. There are multiple ways that you can monitor NAP. You can use the Network Access Protection MMC snap-in to look at how things are running.

But there is another tool that you can use called Logman. Logman creates and manages Event Trace Session and Performance logs and allows an administrator to monitor many different applications through the use of the command line. Table 14.2 shows some of the different Logman switches you can use.

TABLE 14.2 Logman switches

Switch	Description
Logman create	Creates a counter, trace, configuration data collector, or API
Logman query	Queries data collector properties
Logman start | stop	Starts or stops data collection
Logman delete	Deletes an existing data collector
Logman update	Updates the properties of an existing data collector
Logman import | export	Imports a data collector set from an XML file or exports a data collector set to an XML file

Summary

In this chapter, I talked about the different ways that you can secure your remote access connections. You learned how to configure appropriate security settings so that communication between the client and server is secure because of NAP and NPS settings.

I talked about how to verify that client machines meet the minimum requirements in order to gain either full or limited access to your network.

I also discussed wireless networking and what types of security encryption you can use to help support your wireless network. You learned about the different components of wireless access and using group policies to configure wireless clients.

Exam Essentials

Understand what NAP can do for your network. Understand that NAP allows administrators to determine client access based on compliancy with corporate governance policies. Some of the settings are Network Layer Protection, DHCP Enforcement, VPN Enforcement, IPsec Enforcement, 802.1X Enforcement, Flexible Host Isolation, and Multi-configuration System Health Validator.

Understand what NPS can do for your network. Understand how to use NPS to manage network access centrally through a variety of network access servers, including RADIUS-compliant 802.1X-capable wireless access points, VPN servers, dial-up servers, and 802.1X-capable Ethernet switches.

Review Questions

1. You are the network administrator for a large Active Directory domain named Panek.com. The domain contains a server named Saturn that runs Windows Server 2012 R2. Saturn has the DHCP Server role installed. The network contains 400 client computers that run Windows 7 and Windows 8. All of the client computers are joined to the domain and are configured DHCP clients. You install a new server named Jupiter that runs Windows Server 2012 R2. On Jupiter, you install the Network Policy Server (NPS) role service, and you configure Network Access Protection (NAP) to use the DHCP enforcement method. You need to ensure that Saturn provides a valid default gateway only to computers that pass the system health validation. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)
   - **A.** From the DHCP console, configure the 016 Swap Server option.
   - **B.** From the DHCP console, enable NAP on all scopes.
   - **C.** From the NAP Client Configuration console, enable the DHCP Quarantine Enforcement client.
   - **D.** From the DHCP console, create a new policy.
   - **E.** From Server Manager, install the Network Policy Server role service.

2. Your network contains an Active Directory domain named Panek.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy Server (NPS) role service installed. You plan to configure Server1 as a Network Access Protection (NAP) health policy server for VPN enforcement by using the Configure NAP Wizard. You need to ensure that you can configure the VPN enforcement method on Server1 successfully. What should you install on Server1 before you run the Configure NAP Wizard?
   - **A.** The Host Credential Authorization Protocol (HCAP)
   - **B.** A system health validator (SHV)
   - **C.** The Remote Access server role
   - **D.** A computer certificate

3. You are a network administrator of an Active Directory domain named Stellacon.com. You have a server named Earth that runs Windows Server 2012 R2. Earth has the DHCP Server role and the Network Policy Server (NPS) role service installed. You enable Network Access Protection (NAP) on all of the DHCP scopes on Earth. You need to create a DHCP policy that will apply to all of the NAP noncompliant DHCP clients. Which criteria should you specify when you create the DHCP policy?
   - **A.** The relay agent information
   - **B.** The user class
   - **C.** The vendor class
   - **D.** The client identifier

4. Your network contains an Active Directory domain named contoso.com. Network Access Protection (NAP) is deployed to the domain. You need to create NAP event trace log files on a client computer. What should you run?
   - **A.** Register-ObjectEvent
   - **B.** Register-EngineEvent
   - **C.** tracert
   - **D.** logman

5. Your network contains four Network Policy Server (NPS) servers named ServerA, ServerB, ServerC, and ServerD. Server1 is configured as a RADIUS proxy that forwards connection requests to a remote RADIUS server group named Group1. You need to ensure that ServerB and ServerC receive connection requests. ServerD should receive connection requests only if both ServerB and ServerC are unavailable. How should you configure Group1?
   - **A.** Change the weight of ServerB and ServerC to 10.
   - **B.** Change the weight of ServerD to 10.
   - **C.** Change the priority of ServerB and ServerC to 10.
   - **D.** Change the priority of ServerD to 10.

6. Your network contains an Active Directory domain named Stellacon.com. The domain contains a RADIUS server named Server1 that runs Windows Server 2012 R2. You add a VPN server named Server2 to the network. On Server1, you create several network policies. You need to configure Server1 to accept authentication requests from Server2. Which tool should you use on Server1?
   - **A.** Set-RemoteAccessRadius
   - **B.** CMAK
   - **C.** NPS
   - **D.** Routing and Remote Access

7. Your network contains an Active Directory domain named Panek.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the following role services installed:
   - DirectAccess and VPN (RRAS)
   - Network Policy Server

   Remote users have client computers that run either Windows XP, Windows 7, or Windows 8. You need to ensure that only the client computers that run Windows 7 or Windows 8 can establish VPN connections to Server1. What should you configure on Server1?
   - **A.** A vendor-specific RADIUS attribute of a Network Policy Server (NPS) connection request policy
   - **B.** A condition of a Network Policy Server (NPS) network policy

C. A condition of a Network Policy Server (NPS) connection request policy

D. A constraint of a Network Policy Server (NPS) network policy

8. You are the network administrator for a large organization that contains an Active Directory domain named Stellacon.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed. You plan to deploy 802.1X authentication to secure the wireless network. You need to identify which Network Policy Server (NPS) authentication method supports certificate-based mutual authentication for the 802.lX deployment. Which authentication method should you identify?

A. PEAP-MS-CHAP v2

B. MS-CHAP v2

C. EAP-TLS

D. MS-CHAP

9. You are the administrator of a large organization that contains an Active Directory domain named Stellacon.com. The domain contains a server named ServerA that runs Windows Server 2012 R2. ServerA has the Network Policy and Access Services server role installed. Your company's security policy requires that certificate-based authentication be used by some network services. You need to identify which Network Policy Server (NPS) authentication methods comply with the security policy. Which two authentication methods should you identify? (Choose two.)

A. MS-CHAP

B. PEAP-MS-CHAP v2

C. CHAP

D. EAP-TLS

E. MS-CHAP v2

10. You are the network administrator, and you have been asked to set up an accounting system so each department is responsible for their cost of using network services. Your network contains a Network Policy Server (NPS) server named ServerA. The network contains a server named Database1 that has Microsoft SQL server installed. All servers run Windows Server 2012 R2. You configure NPS on ServerA to log accounting data to a database on Database1. You need to ensure that the accounting data is captured if Database1 fails. The solution must minimize cost. What should you do?

A. Implement Failover Clustering.

B. Implement database mirroring.

C. Run the Accounting Configuration Wizard.

D. Modify the SQL Server Logging properties.

Chapter

15

Configure and Manage Active Directory

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure service authentication**

- Create and configure Service Accounts
- Create and configure Group Managed Service Accounts
- Configure Kerberos delegation
- Manage Service Principal Names (SPNS)
- Configure virtual accounts

✓ **Configure Domain Controllers**

- Transfer and seize operations master roles
- Install and configure a read-only domain controller (RODC)
- Configure domain controller cloning

✓ **Maintain Active Directory**

- Back up Active Directory and SYSVOL
- Manage Active Directory offline
- Optimize an Active Directory database
- Clean up metadata
- Configure Active Directory snapshots
- Perform object- and container-level recovery
- Perform Active Directory restore
- Configure and restore objects by using the Active Directory Recycle Bin

✓ **Configure account policies**

- Configure domain and local user password policy settings
- Configure and apply Password Settings Objects (PSOs)
- Delegate password settings management
- Configure account lockout policy settings
- Configure Kerberos policy settings

In this chapter, we will dive deeper into the Active Directory realm.

I have covered many important aspects of Active Directory. The most important aspect of any network, including Active Directory, is security. If your network is not secure, then hackers (internal or external) can make your life as a member of an IT department a living nightmare.

In this chapter, you'll learn how to implement security within Active Directory. By using Active Directory tools, you can quickly and easily configure the settings that you require in order to protect information.

Proper planning for security permissions is an important prerequisite of setting up Active Directory. Security is always one of the greatest concerns for an IT administrator.

You should have a security policy that states what is expected of every computer user in your company. Fine-tuning Active Directory to comply with your security policy and allowing end users to function without any issues should be your goals.

You should know how to use Active Directory to apply permissions to resources on the network, and you should pay particular attention to the evaluation of permissions when applied to different groups and the flow of permissions through the organizational units (OUs) via group policies. With all of this in mind, let's start looking at how you can manage security within Active Directory.

NOTE

Some of the text in this chapter is repeated in Chapter 19 due to its relevancy and importance to both Exam 70-411 and Exam 70-412.

Active Directory Security Overview

One of the fundamental design goals for Active Directory is to define a single, centralized repository of users and information resources. Active Directory records information about all of the users, computers, and resources on your network. Each domain acts as a logical boundary, and members of the domain (including workstations, servers, and domain controllers) share information about the objects within them.

The information stored within Active Directory determines which resources are accessible to which users. Through the use of permissions that are assigned to Active Directory objects, you can control all aspects of network security.

Throughout this chapter, you'll learn the details of security as it pertains to Active Directory. Note, however, that Active Directory security is only one aspect of overall network security. You should also be sure that you have implemented appropriate access control settings for the file system, network devices, and other resources. Let's start by looking at the various components of network security, which include working with security principals and managing security and permissions, access control lists (ACLs), and access control entries (ACEs).

When you are setting up a network, you should always keep in mind that 90 percent of all hacks on a network are internal. This means internal permissions and security (as well as external security) need to be as strong as possible while still allowing users to do their jobs.

Understanding Active Directory Features

I talked about many of these features in Part I, but just in case you are starting with Part II and exam 70-411, let's take a look at some of the Active Directory features and what each feature can do for you as an administrator.

Active Directory is the heart and soul of a Microsoft domain, and I can never talk enough about the roles and features included with Active Directory. Many of these features have already been discussed, but what follows will be a good review for the 70-411 exam:

Active Directory Certificate Services Active Directory Certificate Services (AD CS) provides a customizable set of services that allows you to issue and manage public key infrastructure (PKI) certificates. These certificates can be used in software security systems that employ public key technologies.

Active Directory Domain Services Active Directory Domain Services (AD DS) includes new features that make deploying domain controllers simpler and lets you implement them faster. AD DS also makes the domain controllers more flexible, both to audit and to authorize access to files. Moreover, AD DS has been designed to make performing administrative tasks easier through consistent graphical and scripted management experiences.

Active Directory Rights Management Services Active Directory Rights Management Services (AD RMS) provides management and development tools that let you work with industry security technologies, including encryption, certificates, and authentication. Using these technologies allows organizations to create reliable information protection solutions.

Hyper-V Hyper-V is one of the most changed features in Windows Server 2012 R2. Microsoft's new slogan is "Windows Server 2012 R2, built from the cloud up," and this has a lot to do with Hyper-V. It allows an organization to consolidate servers by creating and managing a virtualized computing environment. It does this by using virtualization technology that is built into Windows Server 2012 R2.

IPAM IP Address Management (IPAM) was one of the new features introduced with Windows Server 2012. IPAM allows an administrator to customize and monitor the IP address infrastructure on a corporate network.

Kerberos Authentication Windows Server 2012 R2 uses the Kerberos authentication (version 5) protocol and extensions for password-based and public-key authentication. The Kerberos client is installed as a security support provider (SSP), and it can be accessed through the Security Support Provider Interface (SSPI).

Managed Service Accounts Stand-alone managed service accounts, originally created for Windows Server 2008 R2 and Windows 7, are configured domain accounts that allow automatic password management and service principal names (SPNs) management, including the ability to delegate management to other administrators.

Security Auditing Security auditing gives an organization the ability to help maintain the security of an enterprise. By using security audits, you can verify authorized or unauthorized access to machines, resources, applications, and services. One of the best advantages of security audits is to verify regulatory compliance.

TLS/SSL (Schannel SSP) Schannel is a security support provider (SSP) that uses the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols together. The Security Support Provider Interface (SSPI) is an API used by Windows systems to allow security-related functionality, including authentication.

Windows Deployment Services Windows Deployment Services allows an administrator to install Windows operating systems remotely. Administrators can use Windows Deployment Services to set up new computers by using a network-based installation.

Understanding Security Principals

Security principals are Active Directory objects that are assigned *security identifiers (SIDs)*. An SID is a unique identifier that is used to manage any object to which permissions can be assigned. Security principals are assigned permissions to perform certain actions and access certain network resources.

The following basic types of Active Directory objects serve as security principals:

User Accounts User accounts identify individual users on your network by including information such as the user's name and their password. User accounts are the fundamental unit of security administration.

Groups There are two main types of groups: security groups and distribution groups. Both types can contain user accounts. System administrators use security groups to ease the management of security permissions. They use distribution groups, on the other hand, solely to send email. Distribution groups are not security principals. You'll see the details of groups in the next section.

Computer Accounts Computer accounts identify which client computers are members of particular domains. Because these computers participate in the Active Directory database, system administrators can manage security settings that affect the computer.

They use computer accounts to determine whether a computer can join a domain and for authentication purposes. As you'll see later in this chapter, system administrators can also place restrictions on certain computer settings to increase security. These settings apply to the computer and, therefore, also apply to any user who is using it (regardless of the permissions granted to the user account).

Note that other objects—such as OUs—do not function as security principals. What this means is that you can apply certain settings (such as Group Policy) on all of the objects within an OU; however, you cannot specifically set permissions with respect to the OU itself. The purpose of OUs is to organize other Active Directory objects logically based on business needs, add a needed level of control for security, and create an easier way to delegate.

You can manage security by performing the following actions with security principals:

- You can assign them permissions to access various network resources.
- You can give them user rights.
- You can track their actions through auditing (covered later in this chapter).

The major types of security principals—user accounts, groups, and computer accounts—form the basis of the Active Directory security architecture. As a system administrator, you will likely spend a portion of your time managing permissions for these objects.

It is important to understand that, since a unique SID defines each security principal, deleting a security principal is an irreversible process. For example, if you delete a user account and then later re-create one with the same name, you'll need to reassign permissions and group membership settings for the new account. Once a user account is deleted, its SID is deleted.

Users and groups are two types of fundamental security principals employed for security administration. In the following sections, you'll learn how users and groups interact and about the different types of groups you can create.

Types of Groups

When dealing with groups, you should make the distinction between local security principals and domain security principals:

Local Users and Groups You use local users and groups to assign the permissions necessary to access the local machine. For example, you may assign the permissions you need to reboot a domain controller to a specific domain local group.

Domain Users and Groups Domain users and groups, on the other hand, are used throughout the domain. These objects are available on any of the computers within the Active Directory domain and between domains that have a trust relationship.

Here are the two main types of groups used in Active Directory:

Security Groups Security groups are considered security principals. They can contain user accounts, computers, or groups. To make administration simpler, system administrators usually grant permissions to groups. This allows you to change permissions easily at the Active Directory level (instead of at the level of the resource on which the permissions are assigned).

You can also place Active Directory contact objects within security groups, but security permissions will not apply to them.

Distribution Groups Distribution groups are not considered security principals because they do not have SIDs. As mentioned earlier, they are used only for the purpose of sending email messages. You can add users to distribution groups just as you would add them to security groups. You can also place distribution groups within OUs so that they are easier to manage. You will find them useful, for example, if you need to send email messages to an entire department or business unit within Active Directory.

Understanding the differences between security and distribution groups is important in an Active Directory environment. For the most part, system administrators use security groups for the daily administration of permissions. On the other hand, system administrators who are responsible for maintaining email distribution lists generally use distribution groups to group members of departments and business units logically. (A system administrator can also email all of the users within a security group, but to do so, they would have to specify the email addresses for the accounts.)

When you are working in Windows Server 2003, Server 2008, Server 2008 R2, or Server 2012 functional-level domains, you can convert security groups to or from distribution groups. When group types are running in a Windows 2000 mixed domain functional level, you cannot change them.

It is vital that you understand group types when you are getting ready to take the Microsoft exams. Microsoft likes to include trick questions about putting permissions on distribution groups. Remember, only security groups can have permissions assigned to them.

Group Scope

In addition to being classified by type, each group is given a specific scope. The scope of a group defines two characteristics. First, it determines the level of security that applies to a group. Second, it determines which users can be added to the group. Group scope is an important concept in network environments because it ultimately defines which resources users are able to access.

The three types of group scope are as follows:

Domain Local The scope of domain local groups extends as far as the local domain. When you're using the Active Directory Users and Computers tool, domain local accounts apply to the computer for which you are viewing information. Domain local groups are used to assign permissions to local resources, such as files and printers. They can contain domain locals, global groups, universal groups, and user accounts.

Global The scope of global groups is limited to a single domain. Global groups may contain any of the users that are part of the Active Directory domain in which the global groups reside or may contain other global groups. Global groups are often used for managing domain security permissions based on job functions. For example, if you need to specify permissions for the Engineering department, you could create one or more global groups (such as EngineeringManagers and EngineeringDevelopers). You could then assign security permissions to each group.

Universal Universal groups can contain accounts or other universal groups from any domains within an Active Directory forest. Therefore, system administrators use them to manage security across domains. When you are managing multiple domains, it often helps to group global groups within universal groups. For instance, if you have an Engineering global group in the `research.stellacon.com` domain and an Engineering global group in the `asia.stellacon.com` domain, you can create a universal AllEngineers group that contains both of the global groups. Now whenever you must assign security permissions to all engineers within the organization, you need only assign permissions to the AllEngineers universal group.

For domain controllers to process authentication between domains, information about the membership of universal groups is stored in the global catalog (GC). Keep this in mind if you ever plan to place users directly into universal groups and bypass global groups because all of the users will be enumerated in the GC, which will impact size and performance.

Fortunately, universal group credentials are cached on domain controllers that universal group members use to log on. This process is called *universal group membership caching*. The domain controller obtains the cached data whenever universal group members log on, and then it is retained on the domain controller for eight hours by default. This is especially useful for smaller locations, such as branch offices, which run less-expensive domain controllers. Most domain controllers at these locations cannot store a copy of the entire GC, and frequent calls to the nearest GC would require an inordinate amount of network traffic.

When you create a new group using the Active Directory Users and Computers tool, you must specify the scope of the group. Figure 15.1 shows the New Object – Group dialog box and the available options for the group scope.

However, changing group scope can be helpful when your security administration or business needs change. You can change group scope easily using the Active Directory Users and Computers tool. To do so, access the properties of the group. As shown in Figure 15.2, you can make a group scope change by clicking one of the options.

FIGURE 15.1 The New Object – Group dialog box

FIGURE 15.2 The Domain Admins Security Group's Properties dialog box

Built-in Service Account Groups

System administrators use built-in domain local groups to perform administrative functions on the local server. Because these have pre-assigned permissions and privileges, they allow system administrators to assign common management functions easily. Figure 15.3 shows the default built-in groups that are available on a Windows Server 2012 domain controller.

FIGURE 15.3 Default built-in local groups

The list of built-in local groups includes some of the following:

Account Operators These users can create and modify domain user and group accounts. Members of this group are generally responsible for the daily administration of Active Directory.

Administrators By default, members of the Administrators group are given full permissions to perform any functions within the Active Directory domain and on the local computer. This means they can access all files and resources that reside on any server within the domain. As you can see, this is a powerful account.

In general, you should restrict the number of users who are included in this group because most common administration functions do not require this level of access.

Backup Operators One of the problems associated with backing up data in a secure network environment is that you need to provide a way to bypass standard file system security so that you can copy files. Although you could place users in the Administrators group, doing so usually provides more permissions than necessary. Members of the Backup Operators group can bypass standard file system security for the purpose of backup and recovery only. They cannot, however, directly access or open files within the file system.

Generally, backup software applications and data use the permissions assigned to the Backup Operators group.

Certificate Service DCOM Access Members of the Certificate Service DCOM Access group can connect to certificate authority servers in the enterprise.

Cryptographic Operators Members of the Cryptographic Operators group are authorized to perform cryptographic operations. Cryptography allows the use of codes to convert data, which then allows a specific recipient to read it using a key.

Guests Typically, you use the Guests group to provide access to resources that generally do not require security. For example, if you have a network share that provides files that should be made available to all network users, you can assign permissions to allow members of the Guests group to access those files.

Print Operators By default, members of the Print Operators group are given permissions to administer all of the printers within a domain. This includes common functions such as changing the priority of print jobs and deleting items from the print queue.

Replicator The Replicator group allows files to be replicated among the computers in a domain. You can add accounts used for replication-related tasks to this group to provide those accounts with the permissions they need to keep files synchronized across multiple computers.

Server Operators A common administrative task is managing server configuration. Members of the Server Operators group are granted the permissions they need to manage services, shares, and other system settings.

Users The Users built-in domain local group is used to administer security for most network accounts. Usually, you don't give this group many permissions, and you use it to apply security settings for most employees within an organization.

Windows Server 2012 also includes many different default groups, which you can find in the `Users` folder. As shown in Figure 15.4, these groups are of varying scopes, including domain local, global, and universal groups. You'll see the details of these groups in the next section.

Three important user accounts are created during the promotion of a domain controller:

- The *Administrator account* is assigned the password a system administrator provides during the promotion process, and it has full permissions to perform all actions within the domain.
- The Guest account is disabled by default. The purpose of the *Guest account* is to provide anonymous access to users who do not have an individual logon and password to use within the domain. Although the Guest account might be useful in some situations, it is generally recommended that this account be disabled to increase security.
- Only the operating system uses the *krbtgt*, or *Key Distribution Center Service account*, for Kerberos authentication. This account is disabled by default. Unlike other user accounts, the krbtgt account cannot be used to log on to the domain, and therefore it does not need to be enabled. Since only the operating system uses this account, you do not need to worry about hackers gaining access by using this account.

FIGURE 15.4 Contents of the default `Users` folder

Managed Service Account and Virtual Accounts

One issue that many administrators run into is how to handle application accounts. What I mean by this is, what type of account and what permissions are needed when installing an application such as Microsoft Exchange?

If you were the administrator for the local system, you could just configure Exchange to run as a Local Service. The problem with using these types of accounts is that they are normally used multiple times among different applications.

Another option that you could have is just to create a domain account for each application. For example, an administrator can create a specific domain account that Exchange could use. The problem with this option is that you have to remember to change the password frequency, and once you change that password, you have to remember which services you configured to use that account and change the passwords for each service. This is not an ideal way to set up an application service.

The two types of accounts available in Windows Server 2012 R2 are the managed service account and the virtual account. These two accounts were originally created in Windows Server 2008 R2 and Windows 7. These accounts are specifically designed for use with applications, and an administrator does not need to change the credentials manually every few months. These two domain accounts provide automatic password management and simplified service principal names management.

Virtual accounts even take it a step further because no password management is needed, and they can access the network using a computer identity from the domain environment.

To use the managed service account and the virtual account, your server needs to be running at least Windows Server 2008 R2 or Windows 7/8. When you are using managed service accounts, a managed service account can be used only for services on a single

computer. You are not allowed to share managed service accounts between multiple computers. This also means you can't use managed service accounts in a server that is going to be part of a cluster.

To configure or manipulate your managed service account or virtual account on a server, you need to use Windows PowerShell cmdlets or any utility that allows you to work with these types of accounts (`Dsacls.exe`, Services snap-in mmc, `SetSPN.exe`, and so forth).

Predefined Global Groups

As mentioned earlier in this chapter, you use global groups to manage permissions at the domain level. Members of each of these groups can perform specific tasks related to managing Active Directory.

The following predefined global groups are installed in the `Users` folder:

Cert Publishers Certificates are used to increase security by allowing for strong authentication methods. User accounts are placed within the *Cert Publishers group* if they must publish security certificates. Generally, Active Directory security services use these accounts.

Domain Computers All of the computers that are members of the domain are generally members of the *Domain Computers group*. This includes any workstations or servers that have joined the domain, but it does not include the domain controllers.

Domain Admins Members of the *Domain Admins group* have full permissions to manage all of the Active Directory objects for this domain. This is a powerful account; therefore, you should restrict its membership only to those users who require full permissions.

Domain Controllers All of the domain controllers for a given domain are generally included within the *Domain Controllers group*.

Domain Guests Generally, by default, members of the *Domain Guests group* are given minimal permissions with respect to resources. System administrators may place user accounts in this group if they require only basic access or temporary permissions within the domain.

Domain Users The *Domain Users group* usually contains all of the user accounts for the given domain. This group is generally given basic permissions to resources that do not require higher levels of security. A common example is a public file share.

Enterprise Admins Members of the *Enterprise Admins group* are given full permissions to perform actions within the entire forest. This includes functions such as managing trust relationships and adding new domains to trees and forests.

Group Policy Creator Owners Members of the *Group Policy Creator Owners group* are able to create and modify Group Policy settings for objects within the domain. This allows them to enable security settings on OUs (and the objects that they contain).

Schema Admins Members of the *Schema Admins group* are given permissions to modify the Active Directory schema. As a member of Schema Admins, you can create additional fields of information for user accounts. This is a powerful function because any changes to the schema will be propagated to all of the domains and domain controllers within an

Active Directory forest. Furthermore, you cannot undo changes to the schema (although you can disable some).

In addition to these groups, you can create new ones for specific services and applications that are installed on the server. (You'll notice that the list in Figure 15.4 includes more than just the ones in the preceding list.) Specifically, services that run on domain controllers and servers will be created as security groups with domain local scope. For example, if a domain controller is running the DNS service, the DnsAdmins and DnsUpdateProxy groups become available. In addition, there are two read-only domain controller (RODC) local groups: the Allowed RODC Password Replication and the Denied RODC Password Replication groups. Similarly, if you install the DHCP service, it automatically creates the DHCP Users and DHCP Administrators groups. The purpose of these groups depends on the functionality of the applications being installed.

Foreign Security Principals

In environments that have more than one domain, you may need to grant permissions to users who reside in multiple domains. Generally, you manage this using Active Directory trees and forests. However, in some cases, you may want to provide resources to users who belong to domains that are not part of the forest.

Active Directory uses the concept of *foreign security principals* to allow permissions to be assigned to users who are not part of an Active Directory forest. This process is automatic and does not require the intervention of system administrators. You can then add the foreign security principals to domain local groups for which, in turn, you can grant permissions for resources within the domain. You can view a list of foreign security principals by using the Active Directory Users and Computers tool. Figure 15.5 shows the contents of the `ForeignSecurityPrincipals` folder.

FIGURE 15.5 The `ForeignSecurityPrincipals` folder

Managing Security and Permissions

Now that you understand the basic issues, terms, and Active Directory objects that pertain to security, it's time to look at how you can apply this information to secure your network resources. The general practice for managing security is to assign users to groups and then grant permissions and logon parameters to the groups so that they can access certain resources.

For management ease and to implement a hierarchical structure, you can place groups within OUs. You can also assign Group Policy settings to all of the objects contained within an OU. By using this method, you can combine the benefits of a hierarchical structure (through OUs) with the use of security principals. Figure 15.6 provides a diagram of this process.

FIGURE 15.6 An overview of security management

The primary tool you use to manage security permissions for users, groups, and computers is the Active Directory Users and Computers tool. Using this tool, you can create and manage Active Directory objects and organize them based on your business needs. Common tasks for many system administrators might include the following:

- Resetting a user's password (for example, in cases where they forget their password)
- Creating new user accounts (when, for instance, a new employee joins the company)
- Modifying group memberships based on changes in job requirements and functions
- Disabling user accounts (when, for example, users will be out of the office for long periods of time and will not require network resource access)

Once you've properly grouped your users, you need to set the actual permissions that affect the objects within Active Directory. The actual permissions available vary based on the type of object. Table 15.1 provides an example of some of the permissions that you can apply to various Active Directory objects and an explanation of what each permission does.

TABLE 15.1 Permissions of Active Directory objects

Permission	Explanation
Control Access	Changes security permissions on the object
Create Child	Creates objects within an OU (such as other OUs)
Delete Child	Deletes child objects within an OU
Delete Tree	Deletes an OU and the objects within it
List Contents	Views objects within an OU
List Object	Views a list of the objects within an OU
Read	Views properties of an object (such as a username)
Write	Modifies properties of an object

Using ACLs and ACEs

Each object in Active Directory has an *access control list*. The ACL is a list of user accounts and groups that are allowed to access the resource. For each ACL, there is an access control entry that defines what a user or a group can actually do with the resource. Deny permissions are always listed first. This means that if users have Deny permissions through user or group membership, they will not be allowed to access the object, even if they have explicit Allow permissions through other user or group permissions. Figure 15.7 shows an ACL for the Sales OU.

FIGURE 15.7 The ACL for an OU named Sales

The Security tab is enabled only if you selected the Advanced Features option from the View menu in the Active Directory Users and Computers tool.

Real World Scenario

Using Groups Effectively

You are a new system administrator for a medium-sized organization, and your network spans a single campus environment. The previous administrator had migrated the network from Windows 2003 to Windows Server 2012 R2, and everyone seems fine with the network and new workstations. As you familiarize yourself with the network, you realize that the previous administrator applied a very ad hoc approach. Many of the permissions to resources had been given to individual accounts on request. It seems that there was no particular strategy with regard to administration.

Management tells you that the company has acquired another company, ideally the first of several acquisitions. They tell you about these plans because they do not want any hiccups in the information system as necessary changes ensue.

You immediately realize that management practices of the past must be replaced with the best practices that have been developed for networks over the years. One of the fundamental practices that you need to establish for this environment is the use of groups to apply permissions and give privileges to users throughout the network.

It is quite simple to give permissions individually, and in some cases, it seems like overkill to create a group, give permissions to the group, and then add a user to the group. Using group-based permissions really pays off in the long run, however, regardless of how small your network is today.

One constant in the networking world is that networks grow. When they grow, it is much easier to add users to a well-thought-out system of groups and consistently applied policies and permissions than it is to patch these elements together for each individual user.

Don't get caught up in the "easy" way of dealing with each request as it comes down the pike. Take the time to figure out how the system will benefit from a more structured approach. Visualize your network as already large with numerous accounts, even if it is still small; this way, when it grows, you will be well positioned to manage the network as smoothly as possible.

Implementing Active Directory Security

So far, you have looked at many different concepts that are related to security within Active Directory. You began by exploring security principals and how they form the basis for administering Active Directory security. Then you considered the purpose and function of groups, how group scopes can affect how these groups work, and how to create a list of the predefined users and groups for new domains and domain controllers. Based on all of this information, it's time to see how you can implement Active Directory security.

In this section, you'll take a look at how you can create and manage users and groups. The most commonly used tool for working with these objects is the Active Directory Users and Computers tool. Using this tool, you can create new user and group objects within the relevant OUs of your domain, and you can modify group membership and group scope.

In addition to these basic operations, you can use some additional techniques to simplify the administration of users and groups. One method involves using user templates. Additionally, you'll want be able to specify who can make changes to user and group objects. That's the purpose of delegation. Both of these topics are covered later in this section.

Let's start with the basics. In Exercise 15.1, you learn how to create and manage users and groups. If you went through Part I for exam 70-410, then you may have already completed this exercise, and you can use these same users for the rest of the exercises.

WARNING

This exercise involves creating new OUs and user accounts within an Active Directory domain. Be sure that you are working in a test environment to avoid any problems that might occur because of the changes you make.

EXERCISE 15.1

Creating and Managing Users and Groups

1. Open the Active Directory Users and Computers MMC snap-in by pressing the Windows key (on the keyboard) and choosing Administrative Tools ➢ Active Directory Users And Computers.
2. Create the following top-level OUs:

   Sales

   Marketing

   Engineering

   HR

3. Create the following User objects within the Sales container (use the defaults for all fields not listed):

   a. First Name: **John**

   Last Name: **Sales**

   User Logon Name: **JSales**

   b. First Name: **Linda**

   Last Name: **Manager**

   User Logon Name: **LManager**

4. Create the following User objects within the Marketing container (use the defaults for all fields not listed):

   a. First Name: **Jane**

   Last Name: **Marketing**

   User Logon Name: **JMarketing**

   b. First Name: **Monica**

   Last Name: **Manager**

   User Logon Name: **MManager**

EXERCISE 15.1 *(continued)*

5. Create the following User object within the Engineering container (use the defaults for all fields not listed):

   First Name: **Bob**

   Last Name: **Engineer**

   User Logon Name: **BEngineer**

6. Right-click the HR container, and select New ➢ Group. Use the name **Managers** for the group and specify Global for the group scope and Security for the group type. Click OK to create the group.

7. To assign users to the Managers group, right-click the Group object and select Properties. Change to the Members tab and click Add. Enter **Linda Manager** and **Monica Manager** and then click OK. You will see the group membership list. Click OK to finish adding the users to the group.

8. When you have finished creating users and groups, close the Active Directory Users and Computers tool.

Notice that you can add users to groups regardless of the OU in which they're contained. In Exercise 15.1, for example, you added two user accounts from different OUs into a group that was created in a third OU. This type of flexibility allows you to manage user and group accounts easily based on your business organization.

The Active Directory Users and Computers tool also allows you to perform common functions simply by right-clicking an object and selecting actions from the context menu. For example, you could right-click a user account and select Add Members To Group to change group membership quickly. You even have the ability in Active Directory Users and Computers to drag users from one OU and drop them into another.

You may have noticed that creating multiple users can be a fairly laborious and a potentially error-prone process. As a result, you are probably ready to take a look at a better way to create multiple users—by using user templates, which is discussed in the next section.

Using User Templates

Sometimes you will need to add several users with the same security settings. Rather than creating each user from scratch and making configuration changes to each one manually, you can create one user template, configure it, and copy it as many times as necessary. Each copy retains the configuration, group membership, and permissions of the original, but you must specify a new username, password, and full name to make the new user unique.

In Exercise 15.2, you create a user template, make configuration changes, and create a new user based on the template. This exercise shows you that the new user you create will

belong to the same group as the user template you copied it from. You must have completed Exercise 15.1 first before you begin this one.

EXERCISE 15.2

Creating and Using User Templates

1. Open the Active Directory Users and Computers tool.
2. Create the following User object within the Sales container (use the defaults for all fields not listed):

   First Name: **Sales User**

   Last Name: **Template**

   User Logon Name: **SalesUserTemplate**
3. Create a new global security group called Sales Users and add SalesUserTemplate to the group membership.
4. Right-click the SalesUserTemplate User object and select Copy from the context menu.
5. Enter the username, first name, and last name for the new user.
6. Click the Next button to move on to the password screen and enter the new user's password information. Close the Copy Object—User dialog box when you've finished.
7. Right-click the user that you created in step 5, select Properties, and click the Member Of tab.
8. Verify that the new user is a member of the Sales Users group.

Delegating Control of Users and Groups

A common administrative function related to the use of Active Directory involves managing users and groups. You can use OUs to group objects logically so that you can easily manage them. Once you have placed the appropriate Active Directory objects within OUs, you are ready to delegate control of these objects.

Delegation is the process by which a higher-level security administrator assigns permissions to other users. For example, if Admin A is a member of the Domain Admins group, Admin A is able to delegate control of any OU within the domain to Admin B. You can access the Delegation Of Control Wizard through the Active Directory Users and Computers tool. You can use it to perform common delegation tasks quickly and easily. The wizard walks you through the steps of selecting the objects for which you want to perform delegation, what permission you want to allow, and which users will have those permissions.

Exercise 15.3 walks through the steps required to delegate control of OUs. To complete the steps in this exercise, you must first have completed Exercise 15.1.

EXERCISE 15.3

Delegating Control of Active Directory Objects

1. Open the Active Directory Users and Computers tool.
2. Create a new user within the Engineering OU using the following information (use the default settings for any fields not specified):

   First Name: **Robert**

   Last Name: **Admin**

   User Logon Name: **radmin**

   Password: **P@ssw0rd**
3. Right-click the Sales OU and select Delegate Control. This starts the Delegation Of Control Wizard. Click Next.
4. To add users and groups to whom you want to delegate control, click the Add button. In the Add dialog box, enter **Robert Admin** for the name of the user to add. Note that you can specify multiple users or groups using this option.
5. Click OK to add the account to the delegation list, which is shown in the Users Or Groups page. Click Next to continue.
6. On the Tasks To Delegate page, you must specify which actions you want to allow the selected user to perform within this OU. Select the Delegate The Following Common Tasks option and place a check mark next to the following options:

   Create, Delete, And Manage User Accounts

   Reset User Passwords And Force Password Change At Next Logon

   Read All User Information

   Create, Delete And Manage Groups

   Modify The Membership Of A Group

7. Click Next to continue. The wizard summarizes the selections that you have made on the Completing The Delegation Of Control Wizard page. To complete the process, click Finish to have the wizard commit the changes.

   Now when the user Robert Admin logs on (using *radmin* as his logon name), he will be able to perform common administrative functions for all of the objects contained within the Sales OU.

8. When you have finished, close the Active Directory Users and Computers tool.

Understanding Dynamic Access Control

One of the advantages of Windows Server 2012 R2 is the ability to apply data governance to your file server. This will help control who has access to information and auditing. You get these advantages through the use of *Dynamic Access Control (DAC)*. Dynamic Access Control allows you to identify data by using data classifications (both automatic and manual) and then control access to these files based on these classifications.

DAC also gives administrators the ability to control file access by using a central access policy. This central access policy will also allow an administrator to set up audit access to files for reporting and forensic investigation.

DAC allows an administrator to set up Active Directory Rights Management Service encryption for Microsoft Office documents. For example, you can set up encryption for any documents that contain financial information.

Dynamic Access Control gives an administrator the flexibility to configure file access and auditing to domain-based file servers. To do this, DAC controls claims in the authentication token, resource properties, and conditional expressions within permission and auditing entries.

Administrators have the ability to give users access to files and folders based on Active Directory attributes. For example, a user named Dana is given access to the file server share because in the user's Active Directory (department attribute) properties, the value contains the value Sales.

NOTE

For DAC to function properly, an administrator must enable Windows 8 computers and Windows Server 2012 R2 file servers to support claims and compound authentication.

Using Group Policy for Security

As discussed in Chapter 6, "Manage GPOs," a useful and powerful feature of Active Directory is a technology known as a *Group Policy*. Through the use of Group Policy settings, system administrators can assign thousands of different settings and options for

users, groups, and OUs. Specifically, in relation to security, you can use many different options to control how important features such as password policies, user rights, and account lockout settings can be configured.

The general process for making these settings is to create a *Group Policy object (GPO)* with the settings you want and then link it to an OU or other Active Directory object.

Table 15.2 lists many Group Policy settings, which are relevant to creating a secure Active Directory environment. Note that this list is not comprehensive—many other options are available through Windows Server 2012's administrative tools.

TABLE 15.2 Group Policy settings used for security purposes

Setting section	Setting name	Purpose
Account Policies ➢ Password Policy	Enforce Password History	Specifies how many passwords will be remembered. This option prevents users from reusing the same passwords whenever they're changed.
Account Policies ➢ Password Policy	Minimum Password Length	Prevents users from using short, weak passwords by specifying the minimum number of characters that the password must include.
Account Policies ➢ Account Lockout Policy	Account Lockout Threshold	Specifies how many bad password attempts can be entered before the account gets locked out.
Account Policies ➢ Account Lockout Policy	Account Lockout Duration	Specifies how long an account will remain locked out after too many bad password attempts have been entered. By setting this option to a reasonable value (such as 30 minutes), you can reduce administrative overhead while still maintaining fairly strong security.
Account Policies ➢ Account Lockout Policy	Reset Account Lockout Counter After	Specifies how long the Account Lockout Threshold counter will hold failed logon attempts before resetting to 0.
Local Policies ➢ Security Options	Accounts: Rename Administrator Account	Often, when trying to gain unauthorized access to a computer, individuals attempt to guess the administrator password. One method for increasing security is to rename this account so that no password allows entry using this logon.

Setting section	Setting name	Purpose
Local Policies ➢ Security Options	Domain Controller: Allow Server Operators To Schedule Tasks	This option specifies whether members of the built-in Server Operators group are allowed to schedule tasks on the server.
Local Policies ➢ Security Options	Interactive Logon: Do Not Display Last User Name	Increases security by not displaying the name of the last user who logged onto the system.
Local Policies ➢ Security Options	Shutdown: Allow System To Be Shut Down Without Having To Log On	Allows system administrators to perform remote shutdown operations without logging on to the server.

You can use several different methods to configure Group Policy settings using the tools included with Windows Server 2012. Exercise 15.4 walks through the steps required to create a basic group policy for the purpose of enforcing security settings. To complete the steps of this exercise, you must have completed Exercise 15.1.

EXERCISE 15.4

Applying Security Policies by Using Group Policy

1. Open the Group Policy Management Console tool.
2. Expand Domains and then click the domain name.
3. In the right pane, right-click the Default Domain Policy and choose Edit.
4. In the Group Policy Management Editor window, expand Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Account Policies ➢ Password Policy.
5. In the right pane, double-click the Minimum Password Length setting.
6. In the Security Policy Setting dialog box, make sure the box labeled Define This Policy Setting Option is checked. Increase the Password Must Be At Least value to eight characters.
7. Click OK to return to the Group Policy Management Editor window.

EXERCISE 15.4 *(continued)*

8. Expand User Configuration ➢ Policies ➢ Administrative Templates ➢ Control Panel. Double-click Prohibit Access To The Control Panel And PC settings, select Enabled, and then click OK.
9. Close the Group Policy window.

Fine-Grained Password Policies

The Windows 2012 R2 operating systems allow an organization to have different password and account lockout policies for different sets of users in a domain. In versions of Active Directory before 2008, an administrator could set up only one password policy and account lockout policy per domain.

The Default Domain policy for the domain is where these policy settings were configured. Because domains could have only one password and account lockout policy, organizations that wanted multiple password and account lockout settings had to either create a password filter or deploy multiple domains.

Fine-grained password policies allow you to specify multiple password policies within a single domain. Let's say you want administrators not to have to change their password as frequently as salespeople. Fine-grained password policies allow you to do just that.

Password Settings objects (PSOs) are created so that you can create fine-grained password policies. You create PSOs using the ADSI editor and then you can use those PSOs to create your fine-grained password policies.

Exercise 15.5 walks through the creation of a custom password policy using the ADSI Edit tool, and then you will link that policy to a group using Active Directory Users and Computers. Before completing this exercise, create a new global group named Passgroup in Active Directory Users and Computers.

EXERCISE 15.5

Fine-Grained Password Policy

1. Open ADSI Edit by pressing the Windows key and choosing ADSI Edit.
2. Right-click ADSI Edit and then choose Connect To.
3. When the Connection Settings dialog box appears, click OK.
4. In the window on the left, expand Default Naming Context ➢ DC=yourdomainname,DC=com ➢ CN=System ➢ CN=Password Settings Container.
5. Right-click CN=Password Settings Container and choose New ➢ Object.
6. In the Select A Class box, choose msDS-PasswordSettings and click Next.
7. At the Common Name screen, type **CustomPolicy** and click Next.
8. At the Password Settings Precedence screen, enter **10** as the value. This works as a cost value. The lowest priority takes precedence.
9. At the Password Reversible Encryption Status For Users Accounts screen, set the value to False (recommended by Microsoft).

EXERCISE 15.5 *(continued)*

10. The Password History Length screen shows how many passwords are remembered before a password can be used again. You can set this for up to 1,024 remembered passwords. Set the value to **12**. Click Next.

11. At the Password Complexity screen, set the value to True.

12. The next screen will be the Minimum Password Length screen. Set the value to **8** and click Next.

13. At the Minimum Password Age screen, you must enter a value for the amount of time you want the password to be used at a minimum. Time is done in the I8 format, like so:

    –600000000 = 1 minute

    –36000000000 = 1 hour

    –864000000000 = 1 day

    So if you want the minimum to be 10 days, you must calculate –864000000000 × 10 (equaling –8640000000000).

    Enter –**8640000000000** (10 zeros) as your value for 10 days and click Next. You must put the – (minus) sign in the front of the value.

14. At the Maximum Password Age screen, set the value as **–51840000000000** (10 zeros). This value equals 60 days. Click Next.
15. At the Lockout Threshold screen, enter **3** and click Next.
16. At the Observation Window screen, enter **–3000000000** (5 minutes) and click Next.
17. At the Lockout Duration screen, enter **–18000000000** (30 minutes) and click Next.
18. Click Finished. If you received any errors, check all of your times to be sure the – (minus) sign appears in front of the number.
19. Close ADSI Edit.
20. Open the Active Directory Users and Computers snap-in.
21. On the View menu along the top, make sure Advanced Features is checked.
22. In the window on the left, expand Active Directory Users and Computers ➢ *yourdomain* ➢ System ➢ Password Settings Container.
23. In the details pane on the right side, right-click CustomPolicy and choose Properties.
24. Click the Attribute Editor tab.
25. Scroll down and select the `msDS-PsoAppliesTo` attribute. Click Edit.
26. In the Multi-valued Distinguished Name dialog box, click Add Windows Account.
27. Type in **Passgroup** (this is the group you created before the exercise) and click the Check Name button. Click OK.
28. Click OK twice more, and then you are finished. Close the Active Directory Users and Computers snap-in.

Managing Multiple Domains

You can easily manage most of the operations that must occur *between* domains by using the Active Directory Domains and Trusts administrative tool. On the other hand, if you want to configure settings *within* a domain, you should use the Active Directory MMC tools. In the following sections, you'll look at managing *single-master operations* (FSMO) roles.

Managing Single-Master Operations

For the most part, Active Directory functions in what is known as *multimaster replication*. That is, every domain controller within the environment contains a copy of the Active

Directory database that is both readable and writable. This works well for most types of information. For example, if you want to modify the password of a user, you can easily do this on *any* of the domain controllers within a domain. The change is then automatically propagated to the other domain controllers.

However, some functions are not managed in a multimaster fashion. These operations are known as *operations masters*. You must perform single-master operations on specially designated domain controllers within the Active Directory forest. There are five main single-master functions: two that apply to an entire Active Directory forest and three that apply to each domain.

Forest Operations Masters

You use the Active Directory Domains and Trusts tool to configure forest-wide roles. The following single-master operations apply to the entire forest:

Schema Master Earlier you learned that all of the domain controllers within a single Active Directory environment share the same schema. This ensures information consistency. However, developers and system administrators can modify the Active Directory schema by adding custom information. A trivial example might involve adding a field to employee information that specifies a user's favorite color.

When you need to make these types of changes, you must perform them on the domain controller that serves as the *Schema Master* for the environment. The Schema Master is then responsible for propagating all of the changes to all the other domain controllers within the forest.

Domain Naming Master The purpose of the *Domain Naming Master* is to keep track of all the domains within an Active Directory forest. You access this domain controller whenever you need to add/remove new domains to a tree or forest.

Domain Operations Masters

You use the Active Directory Users and Computers snap-in to administer roles within a domain. Within each domain, at least one domain controller must fulfill each of the following roles:

Relative ID (RID) Master Every security object within Active Directory must be assigned a unique identifier so that it is distinguishable from other objects. For example, if you have two OUs named IT that reside in different domains, you must have some way to distinguish easily between them. Furthermore, if you delete one of the IT OUs and then later re-create it, the system must be able to determine that it is not the same object as the other IT OU. The unique identifier for each object is made up of a domain identifier and a relative identifier (RID). RIDs are always unique within an Active Directory domain and are used for managing security information and authenticating users. The *RID Master* is responsible

for creating these values within a domain whenever new Active Directory objects are created.

PDC Emulator Master Within a domain, the *PDC Emulator Master* is responsible for maintaining backward compatibility with Windows 95, 98, and NT clients. The PDC emulator is also responsible for processing password changes between a domain user account and all of the domain controllers throughout the domain.

The PDC emulator is also the default time server for all of the domain controllers in the domain. This is why it's a good practice to make sure that your PDC emulator has the proper time. It's the system that all others will rely on for time accuracy.

The PDC Emulator Master serves as the default domain controller to process authentication requests if another domain controller is unable to do so. The PDC Emulator Master also receives preferential treatment whenever domain security changes are made. PDC emulators are also the preferred point of contact for many services and applications that run on the domain.

Infrastructure Master Whenever a user is added to or removed from a group, all of the other domain controllers should be made aware of this change. The role of the domain controller that acts as an *Infrastructure Master* is to ensure that group membership information stays synchronized within an Active Directory domain.

Unless there is only one domain controller, you should not place the Infrastructure Master on a global catalog server. If the Infrastructure Master and global catalog are on the same domain controller, the Infrastructure Master will not function.

Another service that a server can control for the network is the Windows Time service. The Windows Time service uses a suite of algorithms in the Network Time Protocol (NTP). This helps ensure that the time on all computers throughout a network is as accurate as possible. All client computers within a Windows Server 2012 R2 domain are synchronized with the time of an authoritative computer.

Assigning Single-Master Roles

Now that you are familiar with the different types of single-master operations, take a look at Exercise 15.6. This exercise shows you how to assign these roles to servers within the Active Directory environment. In this exercise, you will assign single-master operations roles to various domain controllers within the environment. To complete the steps in this exercise, you need one Active Directory domain controller.

EXERCISE 15.6

Assigning Single-Master Operations

1. Open the Active Directory Domains and Trusts administrative tool.
2. Right-click Active Directory Domains And Trusts and choose Operations Masters.
3. In the Operations Masters dialog box, note that you can change the operations master by clicking the Change button. If you want to move this assignment to another computer, first you need to connect to that computer and then make the change. Click Close to continue without making any changes.
4. Close the Active Directory Domains and Trusts administrative tool.
5. Open the Active Directory Users and Computers administrative tool.
6. Right-click the name of a domain and select Operations Masters. This brings up the RID tab of the Operations Masters dialog box.

   Notice that you can change the computer that is assigned to the role. To change the role, first you need to connect to the appropriate domain controller. Notice that the PDC and Infrastructure roles have similar tabs. Click Close to continue without making any changes.
7. When you have finished, close the Active Directory Users and Computers tool.

TIP

Remember that you manage single-master operations with three different tools. You use the Active Directory Domains and Trusts tool to configure the Domain Name Master role, while you use the Active Directory Users and Computers snap-in to administer roles within a domain. Although this might not seem intuitive at first, it can help you remember which roles apply to domains and which apply to the whole forest. The third tool, the Schema Master role, is a bit different than these other two. To change the Schema Master role, you must install the Active Directory Schema MMS snap-in and change it there.

Seizing Roles

Changing roles from one domain controller to another is really simple. An administrator goes into Active Directory or PowerShell and changes an FSMO role from one machine to another. The problem happens when a machine with one of the roles crashes and goes down. You can't just switch the role from a machine that is not working.

So, what is an administrator to do? Well, at that point, what you need to do is seize control of the role. You do this through the use of PowerShell. Let's look at how to seize a role using PowerShell.

You may be familiar with seizing FSMO roles from previous versions of Windows Server. In previous versions, you would use the `NTDSUtil.exe` command-line utility, but in Windows Server 2012 R2 it needs to be done in PowerShell.

Normally, I would show you how to seize control of an FSMO role using an exercise, but since you probably don't have dozens of Microsoft Windows Server 2012 R2 domain controllers just lying around, I will show you how to seize control through a step-by-step process.

To show you how to set up a step-by-step process, you first have to know what FSMO roles are assigned to what FSMO numbers. The following roles each have a corresponding number:

FSMO role	Number
PDCEmulator	0
RIDMaster	1
InfrastructureMaster	2
SchemaMaster	3
DomainNamingMaster	4

Now that you know the role and the number associated to it, you just need to know the PowerShell commands to seize control of the role. The following is an example of how to use PowerShell commands to seize control of one of the FSMO roles.

I am using the `-Identity` switch to specify the target domain controller (I am calling my target domain controller DC1) and the `-OperationMasterRole` to specify which role to transfer. I've also used the `-Force` command because my current FSMO holder is offline. I will be moving all of the roles to the target domain controller, DC1.

1. On a domain controller, log in as an administrator and start PowerShell with elevated privileges.
2. In PowerShell, type the following command:

   ```
   Move-ADDirectoryServerOperationMasterRole -Identity DC1
   -OperationMasterRole 0,1,2,3,4 -Force
   ```

3. Either type **Y** on each role move prompt or type **A** to accept all prompts.
4. After a few minutes, all of the FSMO roles should be successfully moved.

Finally, I want to show you a couple of useful PowerShell commands so that you can view which domain controller owns which FSMO role.

```
Get-ADForest DomainName | FT SchemaMaster,DomainNamingMaster
Get-ADDomain DomainName | FT PDCEmulator,RIDMaster,InfrastructureMaster
```

Maintain Active Directory

If you have deployed Active Directory in your network environment, your users now depend on it to function properly in order to do their jobs. From network authentications to file access to print and web services, Active Directory has become a mission-critical component of your business. Therefore, the importance of backing up the Active Directory data store should be evident.

As I discussed in earlier chapters, it is important to have multiple domain controllers available to provide backup in case of a problem. The same goes for Active Directory itself—it too should be backed up by being saved. This way, if a massive disaster occurs in which you need to restore your directory services, you will have that option available to you.

Backups are just good common sense, but here are several specific reasons to back up data:

Protect Against Hardware Failures Computer hardware devices have finite lifetimes, and all hardware eventually fails. We discussed this when we mentioned *Mean Time Between Failures (MTBF)* earlier. MBTF is the average time a device will function before it actually fails. There is also a rating derived from benchmark testing of hard disk devices that tells you when you may be at risk for an unavoidable disaster. Some types of failures, such as corrupted hard disk drives, can result in significant data loss.

Protect Against Accidental Deletion or Modification of Data Although the threat of hardware failures is very real, in most environments, mistakes in modifying or deleting data are much more common. For example, suppose a systems administrator accidentally deletes all of the objects within a specific OU. Clearly, it's very important to be able to retrieve this information from a backup.

Keep Historical Information Users and systems administrators sometimes modify files and then later find out that they require access to an older version of the file. Or a file is accidentally deleted, and a user does not discover that fact until much later. By keeping multiple backups over time, you can recover information from prior backups when necessary.

Protect Against Malicious Deletion or Modification of Data Even in the most secure environments, it is conceivable that unauthorized users (or authorized ones with malicious intent!) could delete or modify information. In such cases, the loss of data might require valid backups from which to restore critical information.

Windows Server 2012 R2 includes a Backup utility that is designed to back up operating system files and the Active Directory data store. It allows for basic backup functionality, such as scheduling backup jobs and selecting which files to back up. Figure 15.8 shows the main screen of the Windows Server 2012 R2 Backup utility.

In the following sections, we'll look at the details of using the Windows Server 2012 R2 Backup utility and how you can restore Active Directory when problems do occur.

FIGURE 15.8 The main screen of the Windows Server 2012 Backup utility

Overview of the Windows Server 2012 R2 Backup Utility

Although the general purpose behind performing backup operations—protecting information—is straightforward, system administrators must consider many options when determining the optimal backup-and-recovery scenario for their environment. Factors include what to back up, how often to back up, and when the backups should be performed.

In this section, you'll see how the Windows Server 2012 R2 Backup utility makes it easy to implement a backup plan for many network environments.

TIP

Although the Windows Server 2012 R2 Backup utility provides the basic functionality required to back up your files, you may want to investigate third-party products that provide additional functionality. These applications can provide options for specific types of backups (such as those for Exchange Server and SQL Server) as well as disaster recovery options, networking functionality, centralized management, and support for more advanced hardware.

Backup Types

One of the most important issues you will have to deal with when you are performing backups is keeping track of which files you have backed up and which files you need to back up. Whenever a backup of a file is made, the archive bit for the file is set. You can view the attributes of system files by right-clicking them and selecting Properties. By clicking the Advanced button in the Properties dialog box, you will access the Advanced Attributes dialog box. Here you will see the option Folder Is Ready For Archiving. Figure 15.9 shows an example of the attributes for a folder.

FIGURE 15.9 Viewing the Archive attributes for a folder

Although it is possible to back up all of the files in the file system during each backup operation, it's sometimes more convenient to back up only selected files (such as those that have changed since the last backup operation). When performing backups, you can back up to removable media (DVD) or to a network location.

It is recommended by Microsoft to do a backup to a network location. The reason for this is that if your company suffers from a disaster (fire, hurricane, and so forth), your data can all still be lost—including the backup. If you back up to a removable media source, a copy of the backup can be taken off-site. This protects against a major disaster. Several types of backups can be performed:

NOTE

Although Windows Server 2012 R2 does not support all of these backup types, it's very important that you understand the most common backup types. Most Administrators use third-party software for their backups. That's why it's important to know all of the different types.

Normal Normal backups (also referred to as *system* or *full backups*) back up all of the selected files and then mark them as backed up. This option is usually used when a full system backup is made. Windows Server 2012 R2 supports this backup.

Copy *Copy backups* back up all of the selected files but do not mark them as backed up. This is useful when you want to make additional backups of files for moving files offsite or you want to make multiple copies of the same data for archival purposes.

Incremental *Incremental backups* copy any selected files that are marked as ready for backup (typically because they have not been backed up or they have been changed since the last backup) and then mark the files as backed up. When the next incremental backup is run, only the files that are not marked as having been backed up are stored. Incremental backups are used in conjunction with normal (full) backups.

The most common backup process is to make a full backup and then make subsequent incremental backups. The benefit to this method is that only files that have changed since the last full or incremental backup will be stored. This can reduce backup times and disk or tape storage space requirements.

When recovering information from this type of backup method, a system administrator must first restore the full backup and then restore each of the incremental backups.

Differential *Differential backups* are similar in purpose to incremental backups with one important exception: Differential backups copy all of the files that are marked for backup but do not mark the files as backed up. When restoring files in a situation that uses normal and differential backups, you need only restore the normal backup and the latest differential backup.

Daily *Daily backups* back up all of the files that have changed during a single day. This operation uses the file time/date stamps to determine which files should be backed up and does not mark the files as having been backed up.

Backing Up System State Data

When you are planning to back up and restore Active Directory, be aware that the most important component is known as the *System State data*. System State data includes the components upon which the Windows Server 2012 R2 operating system relies for normal operations. The Windows Server 2012 R2 Backup utility offers you the ability to back up the System State data to another type of media (such as a hard disk or network share). Specifically, it will back up the following components for a Windows Server 2012 R2 domain controller:

Active Directory The *Active Directory data store* is at the heart of Active Directory. It contains all of the information necessary to create and manage network resources, such as users and computers. In most environments that use Active Directory, users and system administrators rely on the proper functioning of these services in order to do their jobs.

Boot Files *Boot files* are the files required for booting the Windows Server 2012 R2 operating system and can be used in the case of boot file corruption.

COM+ Class Registration Database The *COM+ Class Registration database* is a listing of all of the COM+ Class registrations stored on the computer. Applications that run on a Windows Server 2012 R2 computer might require the registration of various share code components. As part of the System State backup process, Windows Server 2012 R2 stores all of the information related to Component Object Model+ (COM+) components so that it can be quickly and easily restored.

Registry The Windows Server 2012 R2 *Registry* is a central repository of information related to the operating system configuration (such as desktop and network settings), user settings, and application settings. Therefore, the Registry is absolutely vital to the proper functioning of Windows Server 2012 R2.

***Sysvol* Directory** The *Sysvol directory* includes data and files that are shared between the domain controllers within an Active Directory domain. Many operating system services rely on this information in order to function properly.

Bare Metal Backups and Restores

One of the options you have in Windows Server 2012 R2 is to do a *Bare Metal Restore (BMR)*. This is a restore of a machine after the machine has been completely wiped out and formatted. This type of restore is done usually after a catastrophic machine failure or crash.

Windows Server 2012 R2 gives you the ability to backup all of the files needed for a Bare Metal Restore by choosing the Bare Metal Recovery checkbox (see Figure 15.10).

FIGURE 15.10 Bare Metal Option

When you choose the Bare Metal Restore option in Windows Server 2012 R2, all of the sub-options (System State, System Reserved, and Local disk) automatically get checked.

When preparing your network for a Bare Metal Backup, you want to make sure that you have everything you need on hand to complete this type of restore. You may want to keep

a copy of the server software, server drivers, and so forth on hand and ready to go, just in case you have to do a full restore.

Scheduling Backups

In addition to specifying which files to back up, you can schedule backup jobs to occur at specific times. Planning *when* to perform backups is just as important as deciding *what* to back up. Performing backup operations can reduce overall system performance; therefore, you should plan to back up information during times of minimal activity on your servers.

To add a backup operation to the schedule, you can simply click the Add button on the Specify Backup Time window.

Restoring System State Data

In some cases, the Active Directory data store or other System State data may become corrupt or unavailable. This could be due to many different reasons. A hard disk failure might, for example, result in the loss of data. Or the accidental deletion of an OU and all of its objects might require a restore operation to be performed.

The actual steps involved in restoring System State data are based on the details of what has caused the data loss and what effect this data loss has had on the system. In the best-case scenario, the System State data is corrupt or inaccurate but the operating system can still boot. If this is the case, all you must do is boot into a special *Directory Services Restore Mode (DSRM)* and then restore the System State data from a backup. This process will replace the current System State data with that from the backup. Therefore, any changes that have been made since the last backup will be completely lost and must be redone.

In a worst-case scenario, all of the information on a server has been lost or a hardware failure is preventing the machine from properly booting. If this is the case, here are several steps that you must take in order to recover System State data:

1. Fix any hardware problem that might prevent the computer from booting (for example, replace any failed hard disks).
2. Reinstall the Windows Server 2012 R2 operating system. This should be performed like a regular installation on a new system.
3. Reinstall any device drivers that may be required by your backup device. If you backed up information to the file system, this will not apply.
4. Restore the System State data using the Windows Server 2012 Backup utility.

I'll cover the technical details of performing restores later in this section. For now, however, you should understand the importance of backing up information and, whenever possible, testing the validity of backups.

Backing Up and Restoring Group Policy Objects

Group Policy Objects (GPOs) are a major part of Active Directory. When you back up Active Directory, GPOs can also get backed up. You also have the ability to back up GPOs

through the Group Policy Management Console (GPMC). This gives you the ability to back up and restore individual GPOs.

To back up all GPOs, open the GPMC and right-click the Group Policy Objects container. You will see the option Back Up All. After you choose this option, a wizard will start asking you for the backup location. Choose a location and click Backup.

To back up an individual GPO, right-click the GPO (in the Group Policy Objects container) and choose Backup. Again, after you choose this option, a wizard will start asking you for the backup location. Choose a location and click Backup.

To restore a GPO, it's the same process as above except, instead of choosing Backup, you will either choose Manage Backups (to restore all GPOs) or Restore (for an individual GPO).

Setting Up an Active Directory Backup

The Windows Server 2012 R2 Backup utility makes it easy to back up the System data (including Active Directory) as part of a normal backup operation. We've already covered the ideas behind the different backup types and why and when they are used.

Exercise 15.7 walks you through the process of backing up the domain controller. In order to complete this exercise, the local machine must be a domain controller, and you must have a DVD burner or network location to back up the System State.

The Windows Server 2012 R2 Backup utility is not installed by default. If you have already installed the Windows Server 2012 R2 Backup utility, skip to step 9.

EXERCISE 15.7

Backing Up Active Directory

1. To install the Windows Server 2012 R2 Backup utility, click the Start Key ➢ Administrative Tools ➢ Server Manager.
2. In the center console, click the link for Add Roles And Features.
3. At the Select Installation Type screen, choose role-based or feature-based installation and click Next.
4. The Select Destination Server screen appears. Choose Select A Server From The Server Pool, and choose your server under Server Pool. Click Next.
5. Click Next at the Select Server Roles screen.
6. At the Select Features screen, scroll down and check the box next to Windows Server Backup. Click Next.

7. At the Confirmation screen, click the checkbox to Restart the destination server automatically. This will bring up a dialog box. Click Yes, and then click the Install button.

8. Click the Close button when finished. Close Server Manager.

9. Open Windows Backup by clicking the Windows Key ➢ Administrative Tools ➢ Windows Server Backup.

EXERCISE 15.7 *(continued)*

10. On the left-hand side, click Local Backup. Then, under Actions, click Backup Once.
11. When the Backup Once Wizard appears, click Different Options and click Next.

12. At the Select Backup Configuration screen, choose Custom and click Next.
13. Click the Add Items button. Choose System State and click OK. Click Next.

14. At the Specify Destination Type, choose Remote Shared Folder. Click Next.
15. Put in the shared path you want to use and click Next.
16. At the Confirmation screen, click the Backup button.

17. Once the backup is complete, close the Windows Server Backup utility.

Restoring Active Directory

Active Directory has been designed with fault tolerance in mind. For example, it is highly recommended by Microsoft that each domain have at least two domain controllers. Each of these domain controllers contains a copy of the Active Directory data store. Should one of the domain controllers fail, the available one can take over the failed server's functionality. When the failed server is repaired, it can then be promoted to a domain controller in the existing environment. This process effectively restores the failed domain controller without incurring any downtime for end users because all of the Active Directory data is replicated to the repaired server in the next scheduled replication.

In some cases, you might need to restore Active Directory from a backup. For example, suppose a system administrator accidentally deletes several hundred users from the domain and does not realize it until the change has been propagated to all of the other domain controllers. Manually re-creating the accounts is not an option because the objects' security identifiers will be different (and all permissions must be reset). Clearly, a method

for restoring from backup is the best solution. You can elect to make the Active Directory restore authoritative or nonauthoritative, as described in the following sections.

Overview of Authoritative Restore

Restoring Active Directory and other System State data is an important process should system files or the Active Directory data store become corrupt or otherwise unavailable. Fortunately, the Windows Server 2012 R2 Backup utility allows you to restore data easily from a backup, should the need arise.

I mentioned earlier that in the case of the accidental deletion of information from Active Directory, you might need to restore the Active Directory from a recent backup. But what happens if there is more than one domain controller in the environment? Even if you did perform a restore, the information on this domain controller would be seen as outdated and it would be overwritten by the data from another domain controller. This data from the older domain controller is exactly the information you want to replace. The domain controller that was reloaded using a backup would have an older time stamp, and the other domain controllers would re-delete the information from the backup.

Fortunately, Windows Server 2012 R2 and Active Directory allow you to perform what is called an *authoritative restore*. The authoritative restore process specifies a domain controller as having the authoritative (or master) copy of the Active Directory data store. When other domain controllers communicate with this domain controller, their information will be overwritten with Active Directory data stored on the local machine.

Now that you have an idea of how an authoritative restore is supposed to work, let's move on to looking at the details of performing the process.

Performing an Authoritative Restore

When you are restoring Active Directory information on a Windows Server 2012 R2 domain controller, make sure that Active Directory services are not running. This is because the restore of System State data requires full access to system files and the Active Directory data store. If you attempt to restore System State data while the domain controller is active, you will see an error message.

In general, restoring data and operating system files is a straightforward process. It is important to note that restoring a System State backup will replace the existing Registry, Sysvol, and Active Directory files, so that any changes you made since the last backup will be lost.

In addition to restoring the entire Active Directory database, you can also restore only specific subtrees within Active Directory using the `restoresubtree` command in the `ntdsutil` utility. This allows you to restore specific information, and it is useful in case of accidental deletion of isolated material.

Following the authoritative restore process, Active Directory should be updated to the time of the last backup. Furthermore, all of the other domain controllers for this domain will have their Active Directory information overwritten by the results of the restore operation. The result is an Active Directory environment that has been recovered from media.

Overview of Nonauthoritative Restore

Now that you understand why you would use an authoritative restore and how it is performed, it's an easy conceptual jump to understand a *nonauthoritative restore*. Remember that by making a restore authoritative, you are simply telling other domain controllers in the domain to recognize the restored machine as the newest copy of Active Directory for replication purposes. If you only have one domain controller, the authoritative restore process becomes moot; you can simply skip the steps required to make the restore authoritative and begin using the domain controller immediately after the normal restore is complete.

If you have more than one domain controller in the domain and you need to perform a nonauthoritative restore, simply allow the domain controller to receive Active Directory database information from other domain controllers in the domain using normal replication methods.

Active Directory Recycle Bin

The Active Directory Recycle Bin is a great feature that allows an administrator to restore an active directory object that has been deleted.

Let's say that you have a junior administrator who has been making changes to Active Directory for hours. The junior admin then deletes an OU from Active Directory. You would then have to reload the OU from a tape backup, or even worse, you may have to reload the entire Active Directory (depending on your backup software), thus losing the hours of work the junior admin has completed.

The problem here is that when you delete a security object from Active Directory, the object's Security ID (SID) gets removed. All users' rights and permissions are associated with the users' SID number and not their account name. This is where the AD Recycle Bin can help.

The *Active Directory Recycle Bin* allows you to preserve and restore accidentally deleted Active Directory objects without the need of using a backup.

The Active Directory Recycle Bin works for both the Active Directory Domain Services (AD DS) and the Active Directory Lightweight Directory Services (AD LDS) environments.

By enabling (disabled by default) the Active Directory Recycle Bin, any deleted Active Directory objects are preserved and Active Directory objects can be restored, in their entirety, to the same condition that they were in immediately before deletion. This means that all group memberships and access rights that the object had before deletion will remain intact.

To enable the Active Directory Recycle Bin, you must do the following (you must be a member of the Schema Admins group):

- Run the `adprep /forestprep` command to prepare the forest on the server that holds the schema master to update the schema.
- Run the `adprep /domainprep /gpprep` command to prepare the domain on the server that holds the infrastructure operations master role.

- If a read-only domain controller (RODC) is present in your environment, you must also run the `adprep /rodcprep` command.
- Make sure that all domain controllers in your Active Directory forest are running Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.
- Make sure that the forest functional level is set to Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

Restartable Active Directory

Administrators have the ability to stop and restart Active Directory in the Windows Server 2012 operating system without the need to reboot the entire system. Administrators can perform these actions either by using the Microsoft Management Console (MMC) snap-ins or the command line.

With *Restartable Active Directory Services*, an administrator has the ability to stop Active Directory Services so that updates and other tasks can be applied to a domain controller. One task that an administrator can perform while Active Directory is stopped is an offline defragmentation of the database.

One of the advantages of a Restartable Active Directory is that other services running on the same server do not depend on Active Directory to continue to function properly while Active Directory is stopped. An administrator has the ability to stop and restart the Active Directory Domain Services in the Local Services MMC snap-in.

Offline Maintenance

As you learned in the preceding section, there are times when you have to be offline to do maintenance. For example, you need to perform authoritative and nonauthoritative restores while the domain controller is offline. The main utility we use for offline maintenance is `ntdsutil`.

Ntdsutil.exe

The primary method by which system administrators can do offline maintenance is through the `ntdsutil` command-line tool. You can launch this tool by simply entering **`ntdsutil`** at a command prompt. For the commands to work properly, you must start the command prompt with elevated privileges. The `ntdsutil` command is both interactive and context sensitive. That is, once you launch the utility, you'll see an `ntdsutil` command prompt. At this prompt, you can enter various commands that set your context within the application. For example, if you enter **`domain management`**, you'll be able to enter domain-related commands. Several operations also require you to connect to a domain, a domain controller, or an Active Directory object before you perform a command.

Table 15.3 provides a list of some of the domain-management commands supported by the `ntdsutil` tool. You can access this functionality by typing the command at an elevated

command prompt. Once you are in the `ntdsutil` prompt, you can use the question mark to see all of the commands available.

TABLE 15.3 `Ntdsutil` offline maintenance commands

`Ntdsutil` **Domain Management Command**	**Purpose**
`Help` or `?`	Displays information about the commands that are available within the Domain Management menu of the `ntdsutil` utility.
`Activate instance %s`	Sets NTDS or a specific AD LDS instance as the active instance.
`Authoritative restore`	Sets the domain controller for the Authoritative restore of the Active Directory database.
`Change service account`	This allows an administrator to change the AD LDS service account to user name and password. You can use a "NULL" for a blank password, and you can use `*` to prompt the user to enter a password.
`configurable settings`	Allows an administrator to manage configurable settings.
`DS behavior`	Allows an administrator to view and modify AD DS or AD LDS behavior.
`files`	This command allows an administrator to manage the AD DS or AD LDS database files.
`Group Membership Evaluation`	Allows an administrator to evaluate the security IDs (SIDs) in a token for a given user or group.
`LDAP policies`	Administrators can manage the Lightweight Directory Access Protocol (LDAP) protocol policies.
`metadata cleanup`	Removes metadata from decommissioned domain controllers.
`security account management`	This command allows an administrator to manage SIDs.
`Set DSRM Password`	Resets the Directory Service Restore mode administrator account password.

Active Directory Database Mounting Tool

One issue that an administrator may run into when trying to restore Active Directory is the need to restore several backups to compare the Active Directory data that each backup contains. Windows Server 2012 R2 has a utility called the Active Directory database mounting tool (`Dsamain.exe`), which can resolve this issue.

The `Dsamain.exe` tool can help the recovery processes by giving you a way to compare data as it exists in snapshots (taken at different times) so that you have the ability to decide which Active Directory database to restore.

Creating snapshots on a regular basis will allow you to have enough data so that you can keep accurate records of how the Active Directory database changes over time. The `ntdsutil` utility allows you to take snapshots by using the `ntdsutil snapshot` operation.

You are not required to run the `ntdsutil snapshot` operation to use `Dsamain.exe`. You have the ability to use a backup of the Active Directory database.

You must be a member of the Domain Admins group or the Enterprise Admins group to view any snapshots taken due to the fact that these snapshots contain sensitive Active Directory data.

Compact the Directory Database File (Offline Defragmentation)

One task that all of us having been doing for years is the process of defragging the operating systems that we run. We have used the defragmentation utility since Windows NT. Defragging a system helps return free space from data to the hard drive.

You can also use the defragmentation process to compact the Active Directory database while it's offline. Offline defragmentation helps return free disk space and check Active Directory database integrity.

To perform an offline defragmentation, you would use the `ntdsutil` command. When you perform a defragmentation of the Active Directory database, a new compacted version of the database is created. This new database file can be created on the same machine (if space permits) or on a network location. After the new file is created, copy the compacted `Ntds.dit` file back to the original location.

It is a good practice, if space allows, to maintain a copy of the older, original database file. You can either rename the older database file and keep it in its current location or copy the older database file to an alternate location.

Monitoring Replication

At times you may need to keep an eye on how your replication traffic is working on your domain controllers. We are going to examine the replication utility that you can use to help determine if there are problems on your domain.

Repadmin Utility

The `Repadmin` utility is included when you install Windows Server 2012 R2. This command-line tool helps administrators diagnose replication problems between Windows domain controllers.

`Repadmin` allows administrators to view the replication topology of each domain controller as seen from the domain controller's perspective. Administrators can also use `Repadmin` to create the replication topology manually. By manually creating the replication topology, administrators can force replication events between domain controllers and view the replication metadata vectors.

To access the `Repadmin` utility, open a command prompt using an elevated privilege (Run ➢ CMD). At the command prompt, type **`Repadmin.exe`**, and all of the available options will appear.

Using the ADSI Editor

Another utility (explained earlier in the chapter) that allows you to manage objects and attributes in Active Directory is the Active Directory Service Interfaces Editor (ADSI Edit). Earlier we used ADSI Edit (`Adsiedit.msc`) to create multiple password policies to allow for fine-grained password policies. ADSI Edit allows you to view every object and attribute in an Active Directory forest.

One advantage to using the `Adsiedit.msc` MMC snap-in is that this tool allows you to query, view, create, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap-ins.

ADSI Edit allows you to administer an AD LDS instance. To do this, you must first connect and bind to the instance. After you connect and bind to the instance, you can administer the containers and objects within the instance by browsing to the containers or objects and then right-clicking them. To complete this task, you must be a member of the Administrators group for the AD LDS instance.

Wbadmin Command Line Utility

The `wbadmin` command allows you to back up and restore your operating system, volumes, files, folders, and applications from a command prompt.

You must be a member of the Administrators group to configure a backup schedule. You must be a member of the Backup Operators or the Administrators group (or you must have been delegated the appropriate permissions) to perform all other tasks using the `wbadmin` command.

To use the `wbadmin` command, you must run `wbadmin` from an elevated command prompt (to open an elevated command prompt, click Start, right-click Command Prompt, and then click Run As Administrator). Table 15.4 shows some of the `wbadmin` commands.

TABLE 15.4 `Wbadmin` commands

Command	Description
`Wbadmin enable backup`	Configures and enables a daily backup schedule.
`Wbadmin disable backup`	Disables your daily backups.
`Wbadmin start backup`	Runs a one-time backup.
`Wbadmin stop job`	Stops the currently running backup or recovery operation.
`Wbadmin get items`	Lists the items included in a specific backup.
`Wbadmin start recovery`	Runs a recovery of the volumes, applications, files, or folders specified.
`Wbadmin get status`	Shows the status of the currently running backup or recovery operation.
`Wbadmin start systemstaterecovery`	Runs a system state recovery.
`Wbadmin start systemstatebackup`	Runs a system state backup.
`Wbadmin start sysrecovery`	Runs a recovery of the full system state.

Summary

In this chapter, I talked about important items that pertain to security, such as which default groups are available after a base install of the operating system and how to secure the most vulnerable accounts.

I then covered how passwords and tokens work within Windows Server 2012 R2 and also how to create a separate password policy using the ADSI Edit utility. I discussed the different Operation Master roles (FSMO) and how to change or seize the role to another domain controller.

Finally, in this chapter, you also learned about how important it is to back up and restore a Windows Server 2012 R2 domain controller machine in the event of a hardware or software failure. I also explained how some of the features such as the Active Directory Recycle Bin and `ntdsutil` are part of Windows Server 2012 R2 domain controller and how these utilities make an administrator's life easier.

Exam Essentials

Understand the various backup types available with the Windows Server 2012 Backup utility. The Windows Server 2012 R2 Backup utility can perform full and incremental backup operations. Some third-party backup utilities also support differential and daily backups. You can use each of these operations as part of an efficient backup strategy.

Know how to back up Active Directory. The data within the Active Directory database on a domain controller is part of the system state data. You can back up the system state data to a file using the Windows Server 2012 R2 Backup utility.

Know how to restore Active Directory. Restoring the Active Directory database is considerably different from other restore operations. To restore some or the entire Active Directory database, you must first boot the machine into Directory Services Restore mode.

Understand the importance of an authoritative restore process. You use an authoritative restore when you want to restore earlier information from an Active Directory backup, and you want the older information to be propagated to other domain controllers in the environment.

Understand offline maintenance using `ntdsutil`. The `ntdsutil` command-line tool is a primary method by which system administrators perform offline maintenance. Understand how to launch this tool by entering **`ntdsutil`** at a command prompt.

Review Questions

1. You are the administrator of a large company, and you need to ensure that you can recover your Windows Server 2012 R2 Active Directory configuration and data if the computer's hard disk fails. What should you do?
   - **A.** Create a complete PC Backup and Restore image.
   - **B.** Create a backup of all file categories.
   - **C.** Perform an automated system recovery (ASR) backup.
   - **D.** Create a system restore point.

2. You need to back up the existing data on a computer before you install a new application. You also need to ensure that you are able to recover individual user files that are replaced or deleted during the installation. What should you do?
   - **A.** Create a system restore point.
   - **B.** Perform an automated system recovery (ASR) backup and restore.
   - **C.** In the Windows Server Backup utility, click the Backup Once link.
   - **D.** In the Backup And Restore Center window, click the Back Up Computer button.

3. You are the administrator of a large organization. While setting up your Windows Server 2012 R2 domain controller, you are creating a data recovery strategy that must meet the following requirements:
   - Back up all data files and folders in `C:\Data`.
   - Restore individual files and folders in `C:\Data`.
   - Ensure that data is backed up to and restored from external media.

   What should you do?
   - **A.** Use the Previous Versions feature to restore the files and folders.
   - **B.** Use the System Restore feature to perform backup and restore operations.
   - **C.** Use the NTBackup utility to back up and restore individual files and folders.
   - **D.** Use the Windows Server Backup to back up and restore files.

4. You are a network administrator, and you want to create multiple password policies for the users in your domain. What utility do you use to complete this task?
   - **A.** MMC
   - **B.** Schema Editor
   - **C.** ADSI Edit
   - **D.** `Secedit.exe`

5. You are the system administrator for a large organization with multiple Active Directory domain controllers. Currently, the environment supports many different domain controllers, some of which are running Windows 2008 and Windows Server 2012 R2. When you are running domain controllers in this type of environment, which of the following types of groups can you *not* use? (Choose all that apply.)
   - **A.** Universal security groups
   - **B.** Global groups
   - **C.** Domain local groups
   - **D.** None—you can use all group types

6. You are the network administrator for your organization. A new company policy has been released wherein if a user enters their password incorrectly three times within 5 minutes, they are locked out for 30 minutes. What three actions do you need to set to comply with this policy? (Choose all that apply.)
   - **A.** Set Account Lockout Duration to 5 minutes.
   - **B.** Set Account Lockout Duration to 30 minutes.
   - **C.** Set the Account Lockout Threshold setting to 3 invalid logon attempts.
   - **D.** Set the Account Lockout Threshold setting to 30 minutes.
   - **E.** Set the Reset Account Lockout Counter setting to 5 minutes.
   - **F.** Set the Reset Account Lockout Counter setting to 3 times.

7. You are teaching a Microsoft Active Directory class, and one of your students asks you which of the following folders in the Active Directory Users and Computers tool is used when users from outside the forest are granted access to resources within a domain? What answer would you give your student?
   - **A.** `Users`
   - **B.** `Computers`
   - **C.** `Domain Controllers`
   - **D.** `Foreign Security Principals`

8. Your manager has decided that your organization needs to use an Active Directory application data partition. Which command can you use to create and manage application data partitions?
   - **A.** `DCPromo.exe`
   - **B.** `NTDSUtil.exe`
   - **C.** `ADUtil.exe`
   - **D.** `ADSI.exe`

9. Robert is a system administrator who is responsible for performing backups on several servers. Recently, he has been asked to take over the operations of several new servers, including backup operations. He has the following requirements:

- The backup must finish as quickly as possible.
- The backup must use the absolute minimum amount of storage space.
- He must perform backup operations at least daily with a full backup at least weekly.

Robert decides to use the Windows Server 2012 R2 Windows Server Backup utility to perform the backups. He wants to choose a set of backup types that will meet all of these requirements. He decides to back up all files on each of these servers every week. Then he decides to store only the files that have changed since the last backup operation (regardless of type) during the weekdays. Which of the following types of backup operations should he use to implement this solution? (Choose two.)

A. Normal

B. Daily

C. Copy

D. Differential

E. Incremental

10. You are removing a domain controller from your network. This domain controller holds the forestwide operations master roles. Which roles would you need to transfer to another machine before you remove the domain controller? (Choose all that apply.)

A. PDC Emulator Master

B. Schema Master

C. RID Master

D. Domain Naming Master

E. Infrastructure Master

Chapter 16

Configure and Manage Group Policy

THE FOLLOWING 70-411 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure Group Policy processing**

- Configure processing order and precedence
- Configure blocking of inheritance
- Configure enforced policies
- Configure security filtering and wmi filtering
- Configure loopback processing
- Configure and manage slow-link processing and group policy caching
- Configure client-side extension (CSE) behavior
- Force group policy update

✓ **Configure Group Policy settings**

- Configure settings including software installation, folder redirection, scripts, and administrative template settings
- Import security templates
- Import custom administrative template file
- Convert administrative templates using admx migrator
- Configure property filters for administrative templates

✓ **Manage Group Policy objects (GPOs)**

- Back up, import, copy, and restore GPOs
- Create and configure Migration Table
- Reset default GPOs
- Delegate Group Policy management

✓ **Configure Group Policy Preferences (GPP)**

- Configure GPP settings including printers, network drive mappings, power options, custom registry settings, Control Panel settings, Internet Explorer settings, file and folder deployment, and shortcut deployment
- Configure item-level targeting

One of the most important system administration features in Windows Server 2012 R2 and Active Directory is administering *Group Policy objects (GPOs)*. By using GPOs, administrators can quickly and easily define restrictions on common actions and then apply them at the site, domain, or organizational unit (OU) level. In this chapter, you will see how group policies work, and then you will look at how to implement them within an Active Directory environment.

This chapter will show Windows Server 2012 R2 administrators how to build, link, and deploy GPOs. GPOs are a great way to set policies throughout your entire forest. GPOs are one of the tools that many administrators never use, but once you start using them, you won't be able to stop. Not only can GPOs help you set policies for your users and computers, you can also install software and updates using GPOs.

If you have read this book from Chapter 1, you are familiar with the content of this chapter from Chapter 6, "Manage GPOs." But if you are just starting Part II to get ready for exam 70-411, then you will need to study all of this material. And if you have already taken and passed exam 70-410, then this chapter will be a good refresher with some added material and tips; this material will be on the 70-411 exam, so it will be best to take the extra time and go through the content again.

Introducing Group Policy Objects

Just like everything else, there are always pros and cons to whatever you are working on. Microsoft Windows-based operating systems have an advantage because of their flexibility and manageability. Administrators have the ability to lock down the Microsoft operating systems by placing some rules or policies onto the domain.

Administrators can configure many different options to suit the network environment and help follow corporate policies. However, having the flexibility to configure the network and the Windows operating system comes at a price—generally, end users on a network have the ability to configure many options that they should not be changing. For example, TCP/IP configuration and security policies should remain consistent for all client computers. In fact, end users really don't need to be able to change these types of settings in the first place because many end users do not understand the purpose of these settings.

Windows Server 2012 R2 *group policies* are designed to provide system administrators with the ability to customize end-user settings and to place restrictions on the types of actions those users can perform. Group policies can be easily created by system administrators and then later applied to one or more users or computers within the

environment. Although they ultimately do affect registry settings, it is much easier to configure and apply settings through the use of Group Policy than it is to make changes to the registry manually. To make management easy, Microsoft has given administrators the ability to change all Group Policy settings from within one Microsoft Management Console (MMC) snap-in called the Group Policy Management Console (GPMC).

Group policies have several potential uses. I'll cover the use of group policies for software deployment, and I'll also focus on the technical background of group policies and how they apply to general configuration management.

Let's begin by looking at how group policies function.

Understanding Group Policy Settings

Group Policy settings are based on *Group Policy administrative templates*. These templates provide a list of user-friendly configuration options and specify the system settings to which they apply. For example, an option for a user or computer that reads Require A Specific Desktop Wallpaper Setting would map to a key in the registry that maintains this value. When the option is set, the appropriate change is made in the registry of the affected users and computers.

By default, Windows Server 2012 R2 comes with several administrative template files that you can use to manage common settings. Additionally, system administrators and applications developers can create their own administrative template files to set options for specific functionality.

Most Group Policy items have three different settings options:

Enabled Specifies that a setting for this GPO has been configured. Some settings require values or options to be set.

Disabled Specifies that this option is disabled for client computers. Note that disabling an option *is* a setting. That is, it specifies that the system administrator wants to disallow certain functionality.

Not Configured Specifies that these settings have been neither enabled nor disabled. Not Configured is the default option for most settings. It simply states that this group policy will not specify an option and that other policy settings may take precedence.

The specific options available (and their effects) will depend on the setting. Often, you will need additional information. For example, when setting the Account Lockout policy, you must specify how many bad login attempts may be made before the account is locked out. With this in mind, let's look at the types of user and computer settings that can be managed.

Group Policy settings can apply to two types of Active Directory objects: User objects and Computer objects. Because both users and computers can be placed into groups and organized within OUs, this type of configuration simplifies the management of hundreds, or even thousands, of computers.

The main options you can configure within user and computer group policies are as follows:

Software Settings *Software Settings* options apply to specific applications and software that might be installed on the computer. System administrators can use these settings to

make new applications available to end users and to control the default configuration for these applications.

Windows Settings *Windows Settings* options allow system administrators to customize the behavior of the Windows operating system. The specific options that are available here are divided into two types: user and computer. User-specific settings let you configure Internet Explorer (including the default home page and other settings). Computer settings include security options, such as Account Policy and Event Log options.

Administrative Templates *Administrative Templates* options are used to configure user and computer settings further. In addition to the default options available, system administrators can create their own administrative templates with custom options.

Group Policy Preferences The Windows Server 2012 R2 operating system includes *Group Policy Preferences (GPPs)* options, which give you more than 20 new Group Policy extensions. These extensions, in turn, give you a vast range of configurable settings within a Group Policy object. Included in the new Group Policy preference extensions are settings for folder options, mapped drives, printers, the registry, local users and groups, scheduled tasks, services, and the Start menu.

Besides providing easier management, Group Policy preferences give an administrator the ability to deploy settings for client computers without restricting the users from changing the settings. This gives an administrator the flexibility needed to decide which settings to enforce and which not to enforce.

Figure 16.1 shows some of the options that you can configure with Group Policy.

FIGURE 16.1 Group Policy configuration options

ADMX Central Store Another consideration in GPO settings is whether to set up an *ADMX Central Store*. GPO administrative template files are saved as ADMX (`.admx`) files and AMXL (`.amxl`) for the supported languages. To get the most benefit out of using administrative templates, you should create an ADMX Central Store.

You create the Central Store in the `SYSVOL` folder on a domain controller. The Central Store is a repository for all of your administrative templates, and the Group Policy tools checks it. The Group Policy tools then use any ADMX files that they find in the Central Store. These files then replicate to all domain controllers in the domain.

If you want your clients to be able to edit domain-based GPOs by using the ADMX files that are stored in the ADMX Central Store, you must be using Windows Vista, Windows 7, Windows 8, Server 2008, Server 2008 R2, Server 2012, or Server 2012 R2.

Security Template *Security templates* are used to configure security settings through a GPO. Some of the security settings that can be configured are settings for account policies, local policies, event logs, restricted groups, system services, and the registry.

Starter GPOs *Starter Group Policy objects* give administrators the ability to store a collection of Administrative Template policy settings in a single object. Administrators then have the ability to import and export Starter GPOs to distribute the GPOs easily to other environments. When a GPO is created from a Starter GPO, as with any template, the new GPO receives the settings and values that were defined from the Administrative Template policy in the Starter GPO.

The Security Settings Section of the GPO

One of the most important sections of a GPO is the Security Settings section. The Security Settings section, under the Windows Settings section, allows an administrator to secure many aspects of the computer and user policies. The following are some of the configurable options for the Security Settings section:

Computer Section Only of the GPO

- Account Policies
- Local Policies
- Event Policies
- Restricted Groups
- System Services
- Registry
- File System
- Wired Network
- Windows Firewall with Advanced Security
- Network List Manager Policies

- Wireless Networks
- Network Access Protection
- Application Control Policies
- IP Security Policies
- Advanced Audit Policy Configuration

Computer and User Sections of the GPO

- Public Key Policies
- Software Restriction Policy

Restricted Groups *Restricted Groups* allows you to control group membership by using a GPO. The group membership to which I am referring is the normal Active Directory groups (domain local, global, and universal). Restricted Groups offers two configurable properties: Members and Members Of.

The users on the Members list do not belong to the restricted group. The users on the Members Of list do belong to the restricted group. When you configure a Restricted Group policy, members of the restricted group that are not on the Members list are removed. Users who are on the Members list who are not currently a member of the restricted group are added.

Software Restriction Policy *Software restriction policies* allow administrators to identify software and to control its ability to run on the user's local computer, organizational unit, domain, or site. This prevents users from installing unauthorized software. Software Restriction Policy is discussed in greater detail in this chapter in the "Implementing Software Deployment" section.

Group Policy Objects

So far, I have discussed what group policies are designed to do. Now it's time to drill down to determine exactly how you can set up and configure them.

To make them easier to manage, group policies may be placed in items called *Group Policy Objects (GPOs)*. GPOs act as containers for the settings made within Group Policy files, which simplifies the management of settings. For example, as a system administrator, you might have different policies for users and computers in different departments. Based on these requirements, you could create a GPO for members of the Sales department and another for members of the Engineering department. Then you could apply the GPOs to the OU for each department. Another important concept you need to understand is that Group Policy settings are hierarchical; that is, system administrators can apply Group Policy settings at four different levels. These levels determine the GPO processing priority:

Local Every Windows operating system computer has one Group Policy object that is stored locally. This GPO functions for both the computer and user Group Policy processing.

Sites At the highest level, system administrators can configure GPOs to apply to entire sites within an Active Directory environment. These settings apply to all of the domains and servers that are part of a site. Group Policy settings managed at the site level may apply to more than one domain within the same forest. Therefore, they are useful when you want to make settings that apply to all of the domains within an Active Directory tree or forest.

Domains Domains are the third level to which system administrators can assign GPOs. GPO settings placed at the domain level will apply to all of the User and Computer objects within the domain. Usually, system administrators make master settings at the domain level.

Organizational Units The most granular level of settings for GPOs is the OU level. By configuring Group Policy options for OUs, system administrators can take advantage of the hierarchical structure of Active Directory. If the OU structure is planned well, you will find it easy to make logical GPO assignments for various business units at the OU level.

Based on the business needs and the organization of the Active Directory environment, system administrators might decide to set up Group Policy settings at any of these four levels. Because the settings are cumulative by default, a User object might receive policy settings from the site level, from the domain level, and from the OUs in which it is contained.

You can also apply Group Policy settings to the local computer (in which case Active Directory is not used at all), but this limits the manageability of the Group Policy settings.

Group Policy Inheritance

In most cases, Group Policy settings are cumulative. For example, a GPO at the domain level might specify that all users within the domain must change their password every 60 days, and a GPO at the OU level might specify the default desktop background for all users and computers within that OU. In this case, both settings apply, and users within the OU are forced to change their password every 60 days and have the default desktop setting.

So, what happens if there's a conflict in the settings? For example, suppose you create a scenario where a GPO at the site level specifies that users are to use red wallpaper and another GPO at the OU level specifies that they must use green wallpaper. The users at the OU layer would have green wallpaper by default. Although hypothetical, this raises an important point about *inheritance*. By default, the settings at the most specific level (in this case, the OU that contains the User object) override those at more general levels. As a friend of mine from Microsoft always says, "Last one to apply wins."

Although the default behavior is for settings to be cumulative and inherited, system administrators can modify this behavior. They can set two main options at the various levels to which GPOs might apply:

Block Policy Inheritance The *Block Policy Inheritance* option specifies that Group Policy settings for an object are not inherited from its parents. You might use this, for example,

when a child OU requires completely different settings from a parent OU. Note, however, that you should manage blocking policy inheritance carefully because this option allows other system administrators to override the settings made at higher levels.

Force Policy Inheritance The *Enforced option* (sometimes referred as the *No Override*) can be placed on a parent object and ensures that all lower-level objects inherit these settings. In some cases, system administrators want to ensure that Group Policy inheritance is not blocked at other levels. For example, suppose it is corporate policy that all network accounts are locked out after five incorrect password attempts. In this case, you would not want lower-level system administrators to override the option with other settings.

System administrators generally use this option when they want to enforce a specific setting globally. For example, if a password expiration policy should apply to all users and computers within a domain, a GPO with the *Force Policy Inheritance* option enabled could be created at the domain level.

You must consider one final case: If a conflict exists between the computer and user settings, the user settings take effect. If, for instance, a system administrator applies a default Desktop setting for the Computer policy and a different default Desktop setting for the User policy, the one they specify in the User policy takes effect. This is because the user settings are more specific, and they allow system administrators to make changes for individual users regardless of the computer that they're using.

Planning a Group Policy Strategy

Through the use of Group Policy settings, system administrators can control many different aspects of their network environment. As you'll see throughout this chapter, system administrators can use GPOs to configure user settings and computer configurations. Windows Server 2012 R2 includes many different administrative tools for performing these tasks. However, it's important to keep in mind that, as with many aspects of using Active Directory, a successful Group Policy strategy involves planning.

Because there are hundreds of possible Group Policy settings and many different ways to implement them, you should start by determining the business and technical needs of your organization. For example, you should first group your users based on their work functions. You might find, for example, that users in remote branch offices require particular network configuration options. In that case, you might implement Group Policy settings best at the site level. In another instance, you might find that certain departments have varying requirements for disk quota settings. In this case, it would probably make the most sense to apply GPOs to the appropriate department OUs within the domain.

The overall goal should be to reduce complexity (for example, by reducing the overall number of GPOs and GPO links) while still meeting the needs of your users. By taking into account the various needs of your users and the parts of your organization, you can often determine a logical and efficient method of creating and applying GPOs. Although it's rare

that you'll come across a right or wrong method of implementing Group Policy settings, you will usually encounter some that are either better or worse than others.

By implementing a logical and consistent set of policies, you'll also be well prepared to troubleshoot any problems that might come up or to adapt to your organization's changing requirements. Later in this chapter, you'll learn about some specific methods for determining effective Group Policy settings before you apply them.

Implementing Group Policy

Now that I've covered the basic layout and structure of group policies and how they work, let's look at how you can implement them in an Active Directory environment. In the following sections, you'll start by creating GPOs. Then you'll apply these GPOs to specific Active Directory objects, and you'll take a look at how to use administrative templates.

Creating GPOs

In Windows Server 2000 and 2003, you could create GPOs from many different locations. For example, in Windows Server 2003, you could use Active Directory Users and Computers to create GPOs on your OUs along with other GPO tools. In Windows Server 2012 R2, things are simpler. You can create GPOs for OUs in only one location: the Group Policy Management Console (GPMC). You have your choice of three applications for setting up policies on your Windows Server 2012 R2 computers:

Local Computer Policy Tool This administrative tool allows you to access quickly the Group Policy settings that are available for the local computer. These options apply to the local machine and to users who access it. You must be a member of the local administrators group to access and make changes to these settings.

Group Policy Management Console You must use the GPMC to manage Group Policy deployment. The GPMC provides a single solution for managing all Group Policy–related tasks, and it is also best suited to handle enterprise-level tasks, such as forest-related work.

The GPMC allows administrators to manage Group Policy and GPOs all from one easy-to-use console whether their enterprise solution spans multiple domains and sites within one or more forests or it is local to one site. The GPMC adds flexibility, manageability, and functionality. Using this console, you can also perform other functions, such as backup and restore, importing, and copying.

`Auditpol.exe` `Auditpol.exe` is a command-line utility that works with Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. An administrator has the ability to display information about policies and also to perform some functions to manipulate audit policies. Table 16.1 shows some of the switches available for `auditpol.exe`.

TABLE 16.1 `Auditpol.exe` switches

Switch	Explanation
`/?`	This is the `auditpol.exe` help command.
`/get`	Allows you to display the current audit policy.
`/set`	Allows you to set a policy.
`/list`	Displays selectable policy elements.
`/backup`	Allows you to save the audit policy to a file.
`/restore`	Restores a policy from previous backup.
`/clear`	Clears the audit policy.
`/remove`	Removes all per-user audit policy settings and disables all system audit policy settings.
`/ResourceSACL`	Configures the Global Resource SACL.

Exercise 16.1 walks you through the process of installing the Group Policy Management MMC snap-in for editing Group Policy settings and creating a GPO. If you started reading this book from Chapter 1, then this lab has been completed. I changed some of the parameters if you would like to create this GPO a bit differently.

WARNING You should be careful when making Group Policy settings because certain options might prevent the proper use of systems on your network. Always test Group Policy settings on a small group of users before you deploy them throughout your organization. You'll probably find that some settings need to be changed to be effective.

EXERCISE 16.1

Creating a Group Policy Object Using the GPMC

1. Press the Windows button and choose Administrative Tools ➢ Group Policy Management. The Group Policy Management tool opens.
2. Expand the Forest, Domains, *your domain name,* and North America containers. Right-click the Corporate OU and then choose Create A GPO In This Domain, And Link It Here.

EXERCISE 16.1 *(continued)*

3. When the New GPO dialog box appears, type **Logon Message** in the Name field. Click OK.
4. The New GPO will be listed on the right side of the Group Policy Management window. Right-click the GPO and choose Edit.

5. In the Group Policy Management Editor, expand the following: Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options. On the right side, scroll down and double-click Interactive Logon: Message Text For Users Attempting To Log On.
6. Click the box labeled Define This Policy Setting In The Template. In the text box, type **Welcome to the domain. Domain members only are welcome** and then click OK. Close the GPO and return to the GPMC main screen.

7. Under the domain name (in the GPMC), right-click Group Policy Objects and choose New.
8. When the New GPO dialog box appears, type **Unlinked Test GPO** in the Name field. Click OK.
9. On the right side, the new GPO will appear. Right-click Unlinked Test GPO and choose Edit.
10. In the User Configuration section, click Policies ➢ Administrative Templates ➢ Desktop. On the right side, double-click Hide And Disable All Items On The Desktop and then click Enabled. Click OK and then close the GPMC.

NOTE

Note that Group Policy changes may not take effect until the next user logs in (some settings may even require that the machine be rebooted). That is, users who are currently working on the system will not see the effects of the changes until they log off and log in again. GPOs are reapplied every 90 minutes with a 30-minute offset. In other words, users who are logged in will have their policies reapplied every 60 to 120 minutes. Not all settings are reapplied (for example, software settings and password policies).

Linking Existing GPOs to Active Directory

Creating a GPO is the first step in assigning group policies. The second step is to link the GPO to a specific Active Directory object. As mentioned earlier in this chapter, GPOs can be linked to sites, domains, and OUs.

Exercise 16.2 walks you through the steps you must take to assign an existing GPO to an OU within the local domain. In this exercise, you will link the Test Domain Policy GPO to an OU. To complete the steps in this exercise, you must have completed Exercise 16.1.

EXERCISE 16.2

Linking Existing GPOs to Active Directory

1. Open the Group Policy Management Console.
2. Expand the Forest and Domain containers and right-click the Africa OU.
3. Choose Link An Existing GPO.
4. The Select GPO dialog box appears. Click Unlinked Test GPO and click OK.
5. Close the Group Policy Management Console.

Note that the GPMC tool offers a lot of flexibility in assigning GPOs. You can create new GPOs, add multiple GPOs, edit them directly, change priority settings, remove links, and delete GPOs all from within this interface. In general, creating new GPOs using the GPMC tool is the quickest and easiest way to create the settings you need.

To test the Group Policy settings, you can simply create a user account within the Africa OU that you used in Exercise 16.2. Then, using another computer that is a member of the same domain, you can log on as the newly created user.

Forcing a GPO to Update

There will be times when you need a GPO to get processed immediately. If you are testing a GPO, you will not want to wait for the GPO to process in its own time or you may not want to have to log off the domain and log back onto the domain just to get the GPO processed.

Windows Server 2012 R2 has changed how GPOs get processed. In a Windows Server 2012 R2 domain, when a user logs onto the domain, the latest version of the Group Policy gets downloaded from the domain controller, and it writes that policy to the local store.

If you have your GPOs set up and running in synchronous mode, then the next time the computer restarts, it will use the most recently downloaded GPO from the local store and

not download the GPO from the domain. This is a new feature in Windows Server 2012 R2, and it helps to reduce the time it takes to log onto the domain because the GPO policy doesn't need to be downloaded each time.

So, now that you understand how GPOs get processed in Windows Server 2012 R2, let's look at a few different ways that you can force a GPO to get processed immediately.

Forcing the GPO from the Server

Windows Server 2012 R2 has an MMC called Group Policy Management Console (GPMC), and by using this MMC, you can remotely refresh an organizational unit (OU) and force the GPO on all users and computers within that OU. The GPMC remote refresh automatically updates all settings, including security settings, which are configured in the GPO that is linked to the OU. In the OU's context menu, you can choose to refresh remotely the OU and the GPOs associated with that OU. When you remotely refresh an OU, the following steps occur:

1. Windows Server 2012 R2 does an Active Directory query, and that query returns a list of all users and computers that belong to the OU.
2. Windows Management Instrumentation (WMI) queries all users and computers that are currently logged into the domain and creates a list that will be used.
3. Using the list that was created in step 2, a remote scheduled task is created, and a `GPUpdate.exe /force` is executed on all of the users and computers that are logged into the domain. The remote scheduled task is then scheduled to execute with a 10-minute random delay to help decrease the load on network traffic.

When you are using the GPMC to force a GPO update, you do not have the ability to change the 10-minute random delay, but if you force the GPO through the use of PowerShell, you have the ability to set the delay.

Another way that you can force a GPO to update immediately is to use Windows PowerShell. By using the PowerShell command `Invoke-GPUpdate` cmdlet, you cannot only force the GPO but also set the parameters to be more granular.

Forcing the GPO from the Client

As an administrator, you have the ability also to force a GPO onto a client machine on which you may be working. The `GPUpdate.exe` command allows you to run a GPO on a client machine. The `GPUpdate` command will run on all Windows client machines from Windows Vista to Windows Server 2012 R2. Table 16.2 shows some of the `GPUpdate` switches you can use.

TABLE 16.2 `GPUpdate.exe` switches

Switch	Description
`/target:{Computer | User}`	Updates only the User or Computer policy settings for the computer or user specified.
`/force`	Forces the GPO to reapply all policy settings. By default, only policy settings that have changed are applied.
`/wait:<VALUE>`	Determines the number of seconds that the system will wait after a policy is processed before returning to the command prompt.
`/logoff`	The domain user account will automatically log off the computer after the Group Policy settings are updated.
`/boot`	The computer will automatically restart after the Group Policy settings are applied.
`/sync`	This switch forces the next available foreground policy application to be done synchronously. Foreground policies are applied when the computer boots up and the user logs in.
`/?`	Displays help at the command prompt.

Managing Group Policy

Now that you have implemented GPOs and applied them to sites, domains, and OUs within Active Directory, it's time to look at some ways to manage them. In the following sections, you'll look at how multiple GPOs can interact with one another and ways that you can provide security for GPO management. Using these features is an important part of working with Active Directory, and if you properly plan Group Policy, you can greatly reduce the time the help desk spends troubleshooting common problems.

Managing GPOs

One of the benefits of GPOs is that they're modular and can apply to many different objects and levels within Active Directory. This can also be one of the drawbacks of GPOs if they're not managed properly. A common administrative function related to using GPOs is finding all of the Active Directory links for each of these objects. You can do this when you are viewing the Linked Group Policy Objects tab of the site, domain, or OU in the GPMC (shown in Figure 16.2).

FIGURE 16.2 Viewing GPO links to an Active Directory OU

In addition to the common action of delegating permissions on OUs, you can set permissions regarding the modification of GPOs. The best way to accomplish this is to add users to the Group Policy Creator/Owners built-in security group. The members of this group are able to modify security policy.

Windows Management Instrumentation

Windows Management Instrumentation (WMI) scripts are used to gather information or to help GPOs deploy better. The best way to explain this is to give an example. Let's say you wanted to deploy Microsoft Office 2013 to everyone in the company. You would first set up a GPO to deploy the Office package (explained later in the section "Deploying Software Through a GPO").

You can then place a WMI script on the GPO stating that only computers with 10GB of hard disk space actually deploy Office. Now if a computer has 10GB of free space, the Office GPO would get installed. If the computer does not have the 10GB of hard disk space, the GPO will not deploy. You can use WMI scripts to check for computer information such as MAC addresses. WMI is a powerful tool because if you know how to write scripts, the possibilities are endless. The following script is a sample of a WMI that is checking for at least 10GB of free space on the `C:` partition/volume:

```
Select * from Win32_LogicalDisk where FreeSpace > 10737418240 AND
Caption = "C:"
```

Security Filtering of a Group Policy

Another method of securing access to GPOs is to set permissions on the GPOs themselves. You can do this by opening the GPMC, selecting the GPO, and clicking the Advanced button in the Delegation tab. The Unlinked Test GPO Security Settings dialog box appears (see Figure 16.3).

FIGURE 16.3 A GPO's Security Settings dialog box

The following permissions options are available:

- Full Control
- Read
- Write
- Create All Child Objects
- Delete All Child Objects
- Apply Group Policy

You might have to scroll the Permissions window to see the Apply Group Policy item. Of these, the Apply Group Policy setting is particularly important because you use it to filter the scope of the GPO. *Filtering* is the process by which selected security groups are included or excluded from the effects of the GPOs. To specify that the settings should apply to a GPO, you should select the Allow check box for both the Apply Group Policy setting and the Read setting. These settings will be applied only if the security group is also contained within a site, domain, or OU to which the GPO is linked. To disable GPO access

for a group, choose Deny for both of these settings. Finally, if you do not want to specify either Allow or Deny, leave both boxes blank. This is effectively the same as having no setting.

In Exercise 16.3, you will filter Group Policy using security groups. To complete the steps in this exercise, you must have completed Exercises 16.1 and 16.2.

EXERCISE 16.3

Filtering Group Policy Using Security Groups

1. Open the Active Directory Users and Computers administrative tool.
2. Create a new OU called **Group Policy Test**.
3. Create two new global security groups within the Group Policy Test OU, and name them **PolicyEnabled** and **PolicyDisabled**.
4. Exit Active Directory Users and Computers and open the GPMC.
5. Right-click the Group Policy Test OU and select Link An Existing GPO.
6. Choose Unlinked Test GPO and click OK.
7. Expand the Group Policy Test OU so that you can see the GPO (Unlinked Test GPO) underneath the OU.
8. Click the Delegation tab and then click the Advanced button in the lower-right corner of the window.
9. Click the Add button and type **PolicyEnabled** in the Enter The Object Names To Select field. Click the Check Names button. Then click OK.
10. Add a group named **PolicyDisabled** in the same way.
11. Highlight the PolicyEnabled group and select Allow for the Read and Apply Group Policy permissions. This ensures that users in the PolicyEnabled group will be affected by this policy.
12. Highlight the PolicyDisabled group and select Deny for the Read and Apply Group Policy permissions. This ensures that users in the PolicyDisabled group will not be affected by this policy.
13. Click OK. You will see a message stating that you are choosing to use the Deny permission and that the Deny permission takes precedence over the Allow entries. Click the Yes button to continue.
14. When you have finished, close the GPMC tool.

Delegating Administrative Control of GPOs

So far, you have learned about how to use Group Policy to manage user and computer settings. What you haven't done yet is to determine who can modify GPOs. It's important to establish the appropriate security on GPOs themselves for two reasons:

- If the security settings aren't set properly, users and system administrators can easily override them. This defeats the purpose of having the GPOs in the first place.
- Having many different system administrators creating and modifying GPOs can become extremely difficult to manage. When problems arise, the hierarchical nature of GPO inheritance can make it difficult to pinpoint the problem.

Fortunately, through the use of delegation, determining security permissions for GPOs is a simple task. Exercise 16.4 walks you through the steps you must take to grant the appropriate permissions to a user account. Specifically, the process involves delegating the ability to manage Group Policy links on an Active Directory object (such as an OU). To complete this exercise, you must have completed Exercises 16.1 and 16.2.

EXERCISE 16.4

Delegating Administrative Control of Group Policy

1. Open the Active Directory Users and Computers tool.
2. Expand the local domain, and create a user named **Policy Admin** within the Group Policy Test OU.
3. Exit Active Directory Users and Computers and open the GPMC.
4. Click the Group Policy Test OU and select the Delegation tab.
5. Click the Add button. In the field labeled Enter The Object Name To Select, type **Policy Admin** and click the Check Names button.
6. The Add Group Or User dialog box appears. In the Permissions drop-down list, make sure that the item labeled Edit Settings, Delete, Modify Security is chosen. Click OK.

7. At this point, you should be looking at the Group Policy Test Delegation window. Click the Advanced button in the lower-right corner.

8. Highlight the Policy Admin account and check the Allow Full Control box. This user now has full control of these OUs and all child OUs and GPOs for these OUs. Click OK.

   If you just want to give individual rights to this user, then in the Properties window (step 8), click the Advanced button and then the Effective Permissions tab. This is where you can also choose a user and give them only the rights that you want them to have.

9. When you have finished, close the GPMC tool.

Understanding Delegation

Although I have talked about delegation throughout the book, it's important to discuss it again in the context of OUs, Group Policy, and Active Directory.

Once configured, Active Directory administrative delegation allows an administrator to delegate tasks (usually administration related) to specific user accounts or groups. What this means is that if you don't manage it all, the user accounts (or groups) you choose will be able to manage their portions of the tree.

It's important to be aware of the benefits of Active Directory Delegation (AD Delegation). *AD Delegation* will help you manage the assigning of administrative control over objects in Active Directory, such as users, groups, computers, printers, domains, and sites. AD Delegation is used to create more administrators, which essentially saves time.

For example, let's say you have a company whose IT department is small and situated in a central location. The central location connects three other smaller remote sites. These sites do not each warrant a full-time IT person, but the manager on staff (for example) at each remote site can become an administrator for their portion of the tree. If the user accounts for the staff at the remote site are managed by that manager, this reduces the burden on the system administrator of trivial administrative work, such as unlocking user accounts or changing passwords, and thus it reduces costs.

Controlling Inheritance and Filtering Group Policy

Controlling inheritance is an important function when you are managing GPOs. Earlier in this chapter, you learned that, by default, GPO settings flow from higher-level Active Directory objects to lower-level ones. For example, the effective set of Group Policy settings for a user might be based on GPOs assigned at the site level, at the domain level, and in the OU hierarchy. In general, this is probably the behavior you would want.

In some cases, however, you might want to block Group Policy inheritance. You can accomplish this easily by selecting the object to which a GPO has been linked. Right-click the object and choose Block Inheritance (see Figure 16.4). By enabling this option, you are

FIGURE 16.4 Blocking GPO inheritance

effectively specifying that this object starts with a clean slate; that is, no other Group Policy settings will apply to the contents of this Active Directory site, domain, or OU.

System administrators can also force inheritance. By setting the Enforced option, they can prevent other system administrators from making changes to default policies. You can set the Enforced option by right-clicking the GPO and choosing the Enforced item (see Figure 16.5).

FIGURE 16.5 Setting the Enforced GPO option

Assigning Script Policies

System administrators might want to make several changes and implement certain settings that would apply while the computer is starting up or the user is logging on. Perhaps the most common operation that logon scripts perform is mapping network drives. Although users can manually map network drives, providing this functionality within login scripts ensures that mappings stay consistent and that users only need to remember the drive letters for their resources.

Script policies are specific options that are part of Group Policy settings for users and computers. These settings direct the operating system to the specific files that should be processed during the startup/shutdown or logon/logoff processes. You can create the scripts by using the *Windows Script Host (WSH)* or with standard batch file commands. WSH allows developers and system administrators to create scripts quickly and easily using Visual Basic Scripting Edition (VBScript) or JScript (Microsoft's implementation of JavaScript). Additionally, WSH can be expanded to accommodate other common scripting languages.

To set script policy options, you simply edit the Group Policy settings. As shown in Figure 16.6, there are two main areas for setting script policy settings.

FIGURE 16.6 Viewing Startup/Shutdown script policy settings

Startup/Shutdown Scripts These settings are located within the Computer Configuration ➢ Windows Settings ➢ Scripts (Startup/Shutdown) object.

Logon/Logoff Scripts These settings are located within the User Configuration ➢ Windows Settings ➢ Scripts (Logon/Logoff) object.

To assign scripts, simply double-click the setting and its Properties dialog box appears. For instance, if you double-click the Startup setting, the Startup Properties dialog box appears (see Figure 16.7). To add a script filename, click the Add button. When you do, you will be asked to provide the name of the script file (such as `MapNetworkDrives.vbs` or `ResetEnvironment.bat`).

FIGURE 16.7 Setting scripting options

Note that you can change the order in which the scripts are run by using the Up and Down buttons. The Show Files button opens the directory folder in which you should store the Logon script files. To ensure that the files are replicated to all domain controllers, you should be sure that you place the files within the SYSVOL share.

Understanding the Loopback Policy

There may be times when the user settings of a Group Policy object should be applied to a computer based on its location instead of the user object. Usually, the user Group Policy processing dictates that the GPOs be applied in order during computer startup based on the computers located in their organizational unit. User GPOs, on the other hand, are applied in order during logon, regardless of the computer to which they log on.

In some situations, this processing order may not be appropriate. A good example is a kiosk machine. You would not want applications that have been assigned or published to a user to be installed when the user is logged on to the kiosk machine. *Loopback Policy* allows two ways to retrieve the list of GPOs for any user when they are using a specific computer in an OU:

Merge Mode The GPOs for the computer are added to the end of the GPOs for the user. Because of this, the computer's GPOs have higher precedence than the user's GPOs.

Replace Mode In Replace mode, the user's GPOs are not used. Only the GPOs of the Computer object are used.

Managing Network Configuration

Group policies are also useful in network configuration. Although administrators can handle network settings at the protocol level using many different methods, such as Dynamic Host Configuration Protocol (DHCP), Group Policy allows them to set which functions and operations are available to users and computers.

Figure 16.8 shows some of the features that are available for managing Group Policy settings. The paths to these settings are as follows:

Computer Network Options These settings are located within Computer Configuration ➢ Administrative Templates ➢ Network ➢ Network Connections folder.

User Network Options These settings are located within User Configuration ➢ Administrative Templates ➢ Network.

FIGURE 16.8 Viewing Group Policy User network configuration options

Here are some examples of the types of settings available:

- The ability to allow or disallow the modification of network settings.

  In many environments, the improper changing of network configurations and protocol settings is a common cause of help desk calls.

- The ability to allow or disallow the creation of Remote Access Service (RAS) connections.

  This option is very useful, especially in larger networked environments, because the use of modems and other WAN devices can pose a security threat to the network.

- The ability to set offline files and folders options.

  This is especially useful for keeping files synchronized for traveling users, and it is commonly configured for laptops.

Each setting includes detailed instructions in the description area of the GPO Editor window. By using these configuration options, system administrators can maintain consistency for users and computers and avoid many of the most common troubleshooting calls.

Automatically Enrolling User and Computer Certificates in Group Policy

You can also use Group Policy to enroll user and computer certificates automatically, making the entire certificate process transparent to your end users. Before proceeding further, you should understand what certificates are and why they are an important part of network security.

Think of a digital certificate as a carrying case for a public key. A certificate contains the public key and a set of attributes, including the key holder's name and email address. These attributes specify something about the holder: their identity, what they're allowed to do with the certificate, and so on. The attributes and the public key are bound together because the certificate is digitally signed by the entity that issued it. Anyone who wants to verify the certificate's contents can verify the issuer's signature.

Certificates are one part of what security experts call a *public-key infrastructure (PKI)*. A PKI has several components that you can mix and match to achieve the desired results. Microsoft's PKI implementation offers the following functions:

Certificate Authorities CAs issue certificates, revoke certificates they've issued, and publish certificates for their clients. Big CAs like Thawte and VeriSign do this for millions of users. If you want, you can also set up your own CA for each department or workgroup in your organization. Each CA is responsible for choosing which attributes it will include in a certificate and what mechanism it will use to verify those attributes before it issues the certificate.

Certificate Publishers They make certificates publicly available, inside or outside an organization. This allows widespread availability of the critical material needed to support the entire PKI.

PKI-Savvy Applications These allow you and your users to do useful things with certificates, such as encrypt email or network connections. Ideally, the user shouldn't have to know (or even be aware of) what the application is doing—everything should work seamlessly and automatically. The best-known examples of PKI-savvy applications are web

browsers such as Internet Explorer and Firefox and email applications such as Outlook and Outlook Express.

Certificate Templates These act like rubber stamps. By specifying a particular template as the model you want to use for a newly issued certificate, you're actually telling the CA which optional attributes to add to the certificate as well as implicitly telling it how to fill some of the mandatory attributes. Templates greatly simplify the process of issuing certificates because they keep you from having to memorize the names of all the attributes that you may potentially want to put in a certificate.

Learn More About PKI

When discussing certificates, it's also important to mention PKI and its definition. The exam doesn't go deeply into PKI, but I recommend you do some extra research on your own because it is an important technology and shouldn't be overlooked. PKI is actually a simple concept with a lot of moving parts. When broken down to its bare essentials, PKI is nothing more than a server and workstations utilizing a software service to add security to your infrastructure. When you use PKI, you are adding a layer of protection. The auto-enrollment Settings policy determines whether users and/or computers are automatically enrolled for the appropriate certificates when necessary. By default, this policy is enabled if a certificate server is installed, but you can make changes to the settings, as shown in Exercise 16.5.

In Exercise 16.5, you will learn how to configure automatic certificate enrollment in Group Policy. You must have first completed the other exercises in this chapter in order to proceed with Exercise 16.5.

EXERCISE 16.5

Configuring Automatic Certificate Enrollment in Group Policy

1. Open the Group Policy Management Console tool.
2. Right-click the North America OU that you created in the previous exercises in this book.
3. Choose Create A GPO In This Domain And Link It Here and name it **Test CA**. Click OK.
4. Right-click the Test CA GPO and choose Edit.
5. Open Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Public Key Policies.
6. Double-click Certificate Services Client – Auto-Enrollment in the right pane.

EXERCISE 16.5 *(continued)*

7. The Certificate Services Client – Auto-Enrollment Properties dialog box will appear.
8. For now, don't change anything. Just become familiar with the settings in this dialog box. Click OK to close it.

Redirecting Folders

Another set of Group Policy settings that you will learn about are the *folder redirection settings*. Group Policy provides a means for redirecting the `Documents`, `Desktop`, and `Start Menu` folders, as well as cached application data, to network locations. Folder redirection is particularly useful for the following reasons:

- When they are using roaming user profiles, a user's `Documents` folder is copied to the local machine each time they log on. This requires high-bandwidth consumption and time if the `Documents` folder is large. If you redirect the `Documents` folder, it stays in the redirected location, and the user opens and saves files directly to that location.
- Documents are always available no matter where the user logs on.
- Data in the shared location can be backed up during the normal backup cycle without user intervention.
- Data can be redirected to a more robust server-side administered disk that is less prone to physical and user errors.

When you decide to redirect folders, you have two options, basic and advanced:

- Basic redirection redirects everyone's folders to the same location (but each user gets their own folder within that location).
- Advanced redirection redirects folders to different locations based on group membership. For instance, you could configure the Engineers group to redirect their folders to `//Engineering1/Documents/` and the Marketing group to `//Marketing1/Documents/`. Again, individual users still get their own folder within the redirected location.

To configure folder redirection, follow the steps in Exercise 16.6. You must have completed the other exercises in this chapter to proceed with this exercise.

EXERCISE 16.6

Configuring Folder Redirection in Group Policy

1. Open the GPMC tool.
2. Open the North America OU and then edit the Test CA GPO.
3. Open User Configuration ➢ Policies ➢ Windows Settings ➢ Folder Redirection ➢ Documents.

4. Right-click `Documents` and select Properties.
5. On the Target tab of the Documents Properties dialog box, choose the Basic – Redirect Everyone's Folder To The Same Location selection from the Settings drop-down list.

EXERCISE 16.6 *(continued)*

6. Leave the default option for the Target Folder Location drop-down list and specify a network path in the Root Path field.
7. Click the Settings tab. All of the default settings are self-explanatory and should typically be left at the defaults. Click OK when you have finished.

Folder Redirection Facts

Try not to mix up the concepts of *folder redirection* and *offline folders*, especially in a world with ever-increasing numbers of mobile users. Folder redirection and offline folders are different features.

Windows Server 2012 R2 folder redirection works as follows: The system uses a pointer that moves the folders you want to a location that you specify. Users do not see any of this—it is transparent to them. One problem with folder redirection is that it does not work for mobile users (users who will be offline and who will not have access to files that they may need).

Offline folders, however, are copies of folders that were local to you. Files are now available locally to you on the system you have with you. They are also located back on the server where they are stored. The next time you log in, the folders are synchronized so that both folders contain the latest data. This is a perfect feature for mobile users, whereas folder redirection provides no benefit for the mobile user.

Managing GPOs with Windows PowerShell Group Policy Cmdlets

As stated earlier in this book, *Windows PowerShell* is a Windows command-line shell and scripting language. Windows PowerShell can also help an administrator automate many of the same tasks that you perform using the Group Policy Management Console.

Windows Server 2012 R2 helps you perform many of the Group Policy tasks by providing more than 25 cmdlets. Each of these cmdlets is a simple, single-function command-line tool.

The Windows PowerShell Group Policy cmdlets can help you perform some of the following tasks for domain-based Group Policy objects:

- Maintain, create, remove, back up, and import GPOs.
- Create, update, and remove GPO links to Active Directory containers.
- Set Active Directory OUs and domain permissions and inheritance flags.

- Configure Group Policy registry settings.
- Create and edit Starter GPOs.

The requirement for Windows PowerShell Group Policy cmdlets is Windows Server 2012 R2 on either a domain controller or a member server that has the GPMC installed. Windows 7 and Windows 8 also have the ability to use Windows PowerShell Group Policy cmdlets if it has Remote Server Administration Tools (RSAT) installed. RSAT includes the GPMC and its cmdlets. PowerShell is also a requirement.

Item-Level Targeting

Administrators have the ability to apply individual preference items only to selected users or computers using a GPO feature called item-level targeting. *Item-level targeting* allows an administrator to select specific items that the GPO will look at and then apply that GPO only to the specific users or computers. Administrators have the ability to include multiple preference items, and each item can be customized for specific users or computers to use.

The target item has a value that belongs to it, and the value can be either true or false. Administrators can get even more granular by using the operation command of AND or OR while building this GPO, and this will allow an administrator to combine the targeted items with the preceding one. Once all of the conditions are executed, if the final value is false, then the GPO is not applied. If the final value is true, the GPO is applied to the users or computers that were previously determined. Administrators have the ability to item-target the following items:

- Battery Present Targeting
- Computer Name Targeting
- CPU Speed Targeting
- Date Match Targeting
- Disk Space Targeting
- Domain Targeting
- Environment Variable Targeting
- File Match Targeting
- IP Address Range Targeting
- Language Targeting
- LDAP Query Targeting
- MAC Address Range Targeting
- MSI Query Targeting
- Network Connection Targeting
- Operating System Targeting
- Organizational Unit Targeting

- PCMCIA Present Targeting
- Portable Computer Targeting
- Processing Mode Targeting
- RAM Targeting
- Registry Match Targeting
- Security Group Targeting
- Site Targeting
- Terminal Session Targeting
- Time Range Targeting
- User Targeting
- WMI Query Targeting

Administrators can easily set up item-level targeting by following these steps:

1. Open the Group Policy Management Console. Select the GPO that will contain the new preferences by right-clicking the GPO and then choose Edit.
2. In the console tree under Computer Configuration or User Configuration, expand the Preferences folder and then browse to the preference extension.
3. Double-click the node for the preference extension and then right-click the preference item and click Properties.
4. In the Properties dialog box, click the Common tab.
5. Select Item-Level Targeting and then click Targeting.
6. Click New Item. If you are configuring multiple targeted items, on the Item Option menu, click the logical operation (AND or OR). Then click OK when finished.
7. Click the OK button on the Properties dialog box, and you are all set.

Backup, Restore, Import, Copy, and Migration Tables

One of the biggest advantages of using the Group Policy Management Console is that it is a one-stop shopping utility. You can do everything you need to do for GPOs in one location. The GPMC not only allows you to create and link a GPO but also lets you backup, restore, import, copy, and use migration tables.

Backing Up a GPO

Since this book is about Windows Server 2012 R2 and everything you should do to set up the server properly, then you most likely already understand what backups can do for you.

The reason we back up data as an administrator is in the event of a crash or major error that requires us to reload data to the server. Backups should be done daily on all data that

is important to your organization. Backups can be done either by using Windows Server 2012 R2's backup utility, or you can purchase third party software/hardware to back up your data.

I am an IT Director, and data recoverability is one of the most critical items that I deal with on a daily basis. I use a third-party hardware device from a company called Unitrends. This is just one of many companies that helps protect an organization's data.

This hardware device does hourly backups for all of my servers. One of the nice features of the Unitrends box is that it backs up onto the hardware device and then sends my data up to the cloud automatically for an offsite backup. This way, if I need to recover just one piece of data, I can grab it off the hardware device. But if I have a major issue, such as a fire that destroys the entire server room, I have an offsite backup from which I can retrieve my data.

It's the same for GPOs. You need to make sure you back up your GPOs in the event of an issue that requires you to do a reload. To back up your GPOs manually, you can go into the GPMC MMC and, under Group Policy Objects, you can right click and choose Backup All or right click on the specific GPO and choose Backup.

Restoring a GPO

There may be times when you have to restore a GPO that was previously backed up. There are normally two reasons why you have to restore a GPO—you accidently deleted the GPO, or you need to restore the GPO to a previous state. (This normally happens if you make changes and it causes an issue.) Restoring a GPO is simple.

1. Open the Group Policy Management Console.
2. In the console tree, right-click Group Policy Objects and choose Manage Backups.
3. Choose the backup you want to restore and click the Restore button.

Importing or Copying GPOs

As an administrator, there may be times when you need to import or copy a GPO from one domain to another domain. Administrators do this so that the second domain has the same settings as the first domain.

An administrator can use the import or copy-to-transfer settings from one GPO to another GPO within the same domain, to a GPO in another domain in the same forest, or to a GPO in a domain in a different forest.

Importing or copying a GPO is an easy process. To do this, an administrator completes the following steps:

1. Open the Group Policy Management Console.
2. In the console tree, right-click Group Policy Objects and choose either Import Settings or Copy.

Migration Tables

One issue that we run into when copying or moving a GPO from one system to another is that when some GPOs are built, they are domain specific. This can be a problem when they are moved to a system in another domain. This is where migration tables can help you out.

Migration tables will tell you how domain specific settings should be treated when the GPO is moved from the domain in which it was created to another domain.

Migration tables are files that are used to map previous domain information (such as users and groups) to the new domain's object-specific data. Migration tables have mapping entries that map the old data to the new data.

Migration tables store their mapping data in an XML format, and the migration tables have their own extension name, `.migtable`. If you want to create your own migration table, you can use the *Migration Table Editor (MTE)*. The MTE is an easy-to-use utility for configuring or just viewing migration tables.

It does not matter if you decide to copy or import a GPO, migration tables apply to any of the settings within the GPO. However, if you copy a GPO instead of move it, you have the option of bringing the Discretionary Access Control List (DACL) option over with the copy.

If you are looking at using migration tables, there are three settings that can be used:

Do Not Use A Migration Table If an administrator chooses this option, the GPO is copied over exactly as is. All security objects and UNC paths are copied over without any modification.

Use A Migration Table If an administrator chooses this option, the GPO has all of the options that can be in the migration table mapped.

Use A Migration Table Exclusively If an administrator chooses this option, all security principals and UNC path information in the GPO are chosen. If any of this information is not included in the migration table, the operation will fail.

To open the Migration Table Editor, perform the following steps:

1. Open the Group Policy Management Console.
2. In the console tree, right-click Group Policy Objects and choose Open Migration Table Editor.

Resetting the Default GPO

There may be a time when you need to reset the default GPO to its original settings. This is easy to do as long as you understand how to use the DCGPOFix command-line utility. This command-line utility is just what it spells—it fixes the domain controller's GPO. To use this command, you would use the following syntax:

```
DCGPOFix [/ignoreschema] [/target: {Domain | DC | Both}] [/?]
```

So, let's take a look at the switches in the previous command. The `/ignoreschema` switch ignores the current version of the Active Directory Schema. The reason you use this switch

is because this command works only on the same schema version as the Windows version in which the command was shipped. By using this switch, you don't need to worry about what schema you have on the system.

The next switch is `[/target: {Domain | DC | Both}]`. This switch specifies the GPO you are going to restore. An administrator has the ability to restore the Default Domain Policy GPO, the Default Domain Controllers GPO, or both. The final switch, `/?`, displays the help for this command.

Deploying Software Through a GPO

It's difficult enough to manage applications on a stand-alone computer. It seems that the process of installing, configuring, and uninstalling applications is never finished. Add in the hassle of computer reboots and reinstalling corrupted applications, and the reduction in productivity can be substantial.

Software administrators who manage software in network environments have even more concerns:

- First and foremost, they must determine which applications specific users require.
- Then IT departments must purchase the appropriate licenses for the software and acquire any necessary media.
- Next, the system administrators need to install the applications on users' machines. This process generally involves help desk staff visiting computers, or it requires end users to install the software themselves. Both processes entail several potential problems, including installation inconsistency and lost productivity from downtime experienced when the applications were installed.
- Finally, software administrators still need to manage software updates and remove unused software.

One of the key design goals for Active Directory was to reduce some of the headaches involved in managing software and configurations in a networked environment. To that end, Windows Server 2012 R2 offers several features that can make the task of deploying software easier and less error prone. Before you dive into the technical details, however, you need to examine the issues related to software deployment.

The Software Management Life Cycle

Although it may seem that the use of a new application requires only the installation of the necessary software, the overall process of managing applications involves many more steps. When managing software applications, there are three main phases to their life cycle:

Phase 1: Deploying Software The first step in using applications is to install them on the appropriate client computers. Generally, some applications are deployed during the initial configuration of a PC, and others are deployed when they are requested. In the latter

case, this often meant that system administrators and help desk staffs had to visit client computers and manually walk through the installation process. With Windows Server 2012 R2 and GPOs, the entire process can be automated.

Before You Install, Stop

It is important to understand that just because you can easily deploy software, it does not necessarily mean that you have the right to do so. Before you install software on client computers, you must make sure you have the appropriate licenses for the software. Furthermore, it's important to take the time to track application installations. As many system administrators have discovered, it's much more difficult to inventory software installations after they've been performed. Another issue you may encounter is that you lack available resources (for instance, your system does not meet the minimum hardware requirements) and face problems such as limited hard disk space or memory that may not be able to handle the applications that you want to load and use. You may also find that your user account does not have the permission to install software. It's important to consider not only how you will install software but also whether you can or not.

Phase 2: Maintaining Software Once an application is installed and in use on client computers, you need to ensure that the software is maintained. You must keep programs up-to-date by applying changes due to bug fixes, enhancements, and other types of updates. This is normally done with service packs, hot fixes, and updates. As with the initial software deployment, software maintenance can be tedious. Some programs require older versions to be uninstalled before updates are added. Others allow for automatically upgrading over existing installations. Managing and deploying software updates can consume a significant amount of the IT staff's time.

Using Windows Update

Make sure you learn about Windows Update, a service that allows you to connect to Microsoft's website and download what your system may need to bring it up to compliance. This tool is helpful if you are running a stand-alone system, but if you want to deploy software across the enterprise, the best way to accomplish this is first to test the updates you are downloading and make sure you can use them and that they are not bug ridden. Then you can use a tool such as the Windows Server Update Service (WSUS), which was formerly called the Software Update Services (SUS).

You can check for updates at Microsoft's website (`http://update.microsoft.com`). Microsoft likes to ask many types of questions about WSUS on its certification exams. WSUS is described in detail in other Sybex certification series books.

Phase 3: Removing Software The end of the life cycle for many software products involves the actual removal of unused programs. Removing software is necessary when applications become outdated or when users no longer require their functionality. One of the traditional problems with uninstalling applications is that many of the installed files may not be removed. Furthermore, removing shared components can sometimes cause other programs to stop functioning properly. Also, users often forget to uninstall applications that they no longer need, and these programs continue to occupy disk space and consume valuable system resources.

The Microsoft Windows Installer (MSI) manages each of these three phases of the software maintenance life cycle. Now that you have an overview of the process, let's move forward to look at the steps involved in deploying software using Group Policy.

The *Microsoft Windows Installer* (sometimes referred to as Microsoft Installer or Windows Installer) is an application installation and configuration service. An instruction file (the Microsoft Installer package) contains information about what needs to be done to install a product. It's common to confuse the two.

The Windows Installer

If you've installed newer application programs (such as Microsoft Office 2013), you've probably noticed the updated setup and installation routines. Applications that comply with the updated standard use the *Windows Installer specification* and MSI software packages for deployment. Each package contains information about various setup options and the files required for installation. Although the benefits may not seem dramatic on the surface, there's a lot of new functionality under the hood.

The Windows Installer was created to solve many of the problems associated with traditional application development. It has several components, including the Installer service (which runs on Windows 2000, XP, Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 R2 computers), the Installer program (`msiexec.exe`) that is responsible for executing the instructions in a *Windows Installer package*, and the specifications third-party developers use to create their own packages. Within each installation package file is a relational structure (similar to the structure of tables in databases) that records information about the programs contained within the package.

To appreciate the true value of the Windows Installer, you'll need to look at some of the problems with traditional software deployment mechanisms and then at how the Windows Installer addresses many of them.

Application Installation Issues

Before the Windows Installer, applications were installed using a setup program that managed the various operations required for a program to operate. These operations

included copying files, changing registry settings, and managing any other operating system changes that might be required (such as starting or stopping services). However, this method had several problems:

- The setup process was not robust, and aborting the operation often left many unnecessary files in the file system.
- The process included uninstalling an application (this also often left many unnecessary files in the file system) and remnants in the Windows registry and operating system folders. Over time, these remnants would result in reduced overall system performance and wasted disk space.
- There was no standard method for applying upgrades to applications, and installing a new version often required users to uninstall the old application, reboot, and then install the new program.
- Conflicts between different versions of *dynamic link libraries (DLLs)*—shared program code used across different applications—could cause the installation or removal of one application to break the functionality of another.

Benefits of the Windows Installer

Because of the many problems associated with traditional software installation, Microsoft created the *Windows Installer*. This system provides for better manageability of the software installation process and gives system administrators more control over the deployment process. Specifically, the Windows Installer provides the following benefits:

Improved Software Removal The process of removing software is an important one because remnants left behind during the uninstall process can eventually clutter up the registry and file system. During the installation process, the Windows Installer keeps track of all of the changes made by a setup package. When it comes time to remove an application, all of these changes can then be rolled back.

More Robust Installation Routines If a typical setup program is aborted during the software installation process, the results are unpredictable. If the actual installation hasn't yet begun, then the installer generally removes any temporary files that may have been created. However, if the file copy routine starts before the system encounters an error, it is likely that the files will not be removed automatically from the operating system. In contrast, the Windows Installer allows you to roll back any changes when the application setup process is aborted.

Ability to Use Elevated Privileges Installing applications usually requires the user to have Administrator permissions on the local computer because file system and registry changes are required. When installing software for network users, system administrators have two options. First they can log off of the computer before installing the software and then log back on as a user who has Administrator permissions on the local computer. This method is tedious and time-consuming. The second option is to give users Administrator

permissions temporarily on their own machines. This method could cause security problems and requires the attention of a system administrator.

Through the use of the Installer service, the Windows Installer is able to use temporarily elevated privileges to install applications. This allows users, regardless of their security settings, to execute the installation of authorized applications. This saves time and preserves security.

Support for Repairing Corrupted Applications Regardless of how well a network environment is managed, critical files are sometimes lost or corrupted. Such problems can prevent applications from running properly and can cause crashes. Windows Installer packages provide you with the ability to verify the installation of an application and, if necessary, replace any missing or corrupted files. This support saves time and lessens end-user headaches associated with removing and reinstalling an entire application to replace just a few files.

Prevention of File Conflicts Generally, different versions of the same files should be compatible with each other. In the real world, however, this isn't always the case. A classic problem in the Windows world is the case of one program replacing DLLs that are used by several other programs. Windows Installer accurately tracks which files are used by certain programs and ensures that any shared files are not improperly deleted or overwritten.

Automated Installations A typical application setup process requires end users or system administrators to respond to several prompts. For example, a user may be able to choose the program group in which icons will be created and the file system location to which the program will be installed. Additionally, they may be required to choose which options are installed. Although this type of flexibility is useful, it can be tedious when you are rolling out multiple applications. By using features of the Windows Installer, however, users are able to specify setup options before the process begins. This allows system administrators to ensure consistency in installations, and it saves users' time.

Advertising and On-Demand Installations One of the most powerful features of the Windows Installer is its ability to perform on-demand software installations. Prior to the Windows Installer, application installation options were quite basic—either a program was installed or it was not. When setting up a computer, system administrators would be required to guess which applications the user might need and install all of them.

The Windows Installer supports a function known as advertising. *Advertising* makes applications appear to be available via the Start menu. However, the programs themselves may not actually be installed on the system. When a user attempts to access an advertised application, the Windows Installer automatically downloads the necessary files from a server and installs the program. The result is that applications are installed only when they are needed, and the process requires no intervention from the end user. We'll cover the details of this process later in this chapter.

To anyone who has managed many software applications in a network environment, all of these features of the Windows Installer are likely welcome ones. They also make life easier for end users and applications developers; they can focus on the "real work" that their jobs demand.

Windows Installer File Types

When performing software deployment with the Windows Installer in Windows Server 2012 R2, you may encounter several different file types:

Microsoft Windows Installer Packages To take full advantage of Windows Installer functionality, applications must include Microsoft Windows Installer (MSI) packages. Third-party application vendors and software developers normally create these packages, and they include the information required to install and configure the application and any supporting files.

Microsoft Transformation Files *Microsoft Transformation (MST) files* are useful when you are customizing the details of how applications are installed. When a system administrator chooses to assign or publish an application, they may want to specify additional options for the package. For example, if a system administrator wants to allow users to install only the Microsoft Word and Microsoft PowerPoint components of Office 2013, they could specify these options within a transformation file. Then, when users install the application, they will be provided only with the options related to these components.

Microsoft Patches To maintain software, patches are often required. Patches may make registry and/or file system changes. *Patch files (MSP)* are used for minor system changes and are subject to certain limitations. Specifically, a patch file cannot remove any installed program components and cannot delete or modify any shortcuts created by the user.

Initialization Files To provide support for publishing non–Windows Installer applications, *initialization files* can be used. These files provide links to a standard executable file that is used to install an application. An example might be `\\server1\software\program1\setup.exe`. These files can then be published and advertised, and users can access the *Programs and Features* icon to install them over the network.

Application Assignment Scripts *Application assignment scripts (AAS)* store information regarding assigning programs and any settings that the system administrator makes. These files are created when Group Policy is used to create software package assignments for users and computers.

Each of these types of files provides functionality that allows the system administrator to customize software deployment. Windows Installer packages have special properties that you can view by right-clicking the file in Windows Explorer and choosing Properties (see Figure 16.9).

FIGURE 16.9 Viewing the properties of an MSI package file

Deploying Applications

The functionality provided by Windows Installer offers many advantages to end users who install their own software. However, that is just the beginning in a networked environment. As you'll see later in this chapter, the various features of Windows Installer and compatible packages allow system administrators to determine centrally which applications users will be able to install.

There are two main methods of making programs available to end users using Active Directory: assigning and publishing. Both assigning and publishing applications greatly ease the process of deploying and managing applications in a network environment.

In the following sections, you'll look at how the processes of assigning and publishing applications can make life easier for IT staff and users alike. The various settings for assigned and published applications are managed through the use of GPOs.

Assigning Applications

Software applications can be assigned to users and computers. *Assigning* a software package makes the program available for automatic installation. The applications advertise their availability to the affected users or computers by placing icons within the `Programs` folder of the Start menu.

When applications are assigned to a user, programs will be advertised to the user regardless of which computer they are using. That is, icons for the advertised program will appear within the Start menu regardless of whether the program is installed on that computer. If the user clicks an icon for a program that has not yet been installed on the

local computer, the application will automatically be accessed from a server and it will be installed.

When an application is assigned to a computer, the program is made available to any users of the computer. For example, all users who log on to a computer that has been assigned Microsoft Office 2013 will have access to the components of the application. If the user did not previously install Microsoft Office 2013, they will be prompted for any required setup information when the program first runs.

Generally, applications that are required by the vast majority of users should be assigned to computers. This reduces the amount of network bandwidth required to install applications on demand and improves the end-user experience by preventing the delay involved when installing an application the first time it is accessed. Any applications that may be used by only a few users (or those with specific job tasks) should be assigned to users.

Publishing Applications

When applications are *published*, they are advertised, but no icons are automatically created. Instead, the applications are made available for installation using the Add Or Remove Programs icon in Control Panel.

Windows Vista, Windows 7, and Windows 8 do not have the Add Or Remove Programs feature. They use the Programs and Features icon in Control Panel to install the software.

Implementing Software Deployment

So far, you have become familiar with the issues related to software deployment and management from a theoretical level. Now it's time to drill down into the actual steps required to deploy software using the features of Active Directory and the GPMC. In the following sections, you will walk through the steps required to create an application distribution share point, to publish and assign applications, to update previously installed applications, to verify the installation of applications, and to update Windows operating systems.

Preparing for Software Deployment

Before you can install applications on client computers, you must make sure that the necessary files are available to end users. In many network environments, system administrators create shares on file servers that include the installation files for many applications. Based on security permissions, either end users or system administrators can then connect to these shares from a client computer and install the needed software. The efficient organization of these shares can save the help desk from having to carry around a library of CD-ROMs, and it allows you to install applications easily on many computers at once.

One of the problems in network environments is that users frequently install applications whether or not they really need them. They may stumble upon applications that are stored on common file servers and install them out of curiosity. These actions can often decrease productivity and may violate software licensing agreements. You can help to avoid this by placing all of your application installation files in hidden shares (for example, `software$`).

Exercise 16.7 walks you through the process of creating a software distribution share point. In this exercise, you will prepare for software deployment by creating a directory share and placing certain types of files in this directory. To complete the steps in this exercise, you must have access to the Microsoft Office 2010 or Microsoft Office 2013 installation files (via CD-ROM or through a network share) and have 2000MB of free disk space. For this exercise, I used Microsoft Office 2010.

EXERCISE 16.7

Creating a Software Deployment Share

1. Using Windows Explorer, create a folder called `Software` that you can use with application sharing. Be sure that the volume on which you create this folder has at least 2000MB of available disk space.
2. Create a folder called `Office 2010` within the `Software` folder.
3. Copy all the installation files for Microsoft Office 2010 from the CD-ROM or network share containing the files to the `Office 2010` folder you created in step 2. If you prefer, you can use switches to install all the Office 2010 installation files. You can find these switches at `http://technet.microsoft.com/en-us/library/ff521767.aspx`.
4. Right-click the `Software` folder (created in step 1) and select Share. In the Choose People On Your Network To Share With dialog box, type **Everyone** and click the Add button. Next click the Share button. When you see a message that the sharing process is complete, click Done.

Once you have created an application distribution share, it's time to publish and assign the applications. This topic is covered next.

Software Restriction Policies

One of the biggest problems that we face as IT managers is that of users downloading and installing software. Many software packages don't cause any issues and are completely safe. Unfortunately, many software packages do have viruses and can cause problems. This is where software restriction policies can help. Software restriction policies help to identify software and to control its ability to run on a local computer, organizational unit, domain, or site.

Software restriction policies give administrators the ability to regulate unknown or untrusted software. Software restriction policies allow you to protect your computers from unwanted software by identifying and also specifying what software packages are allowed to be installed.

When configuring software restriction policies, an administrator is able to define a default security level of Unrestricted (software is allowed) or Disallowed (software is not allowed to run) for a GPO. Administrators can make exceptions to this default security level. They can create software restriction policy rules for specific software.

To create a software policy using the Group Policy Management Console, create a new GPO. In the GPO, expand the Windows Settings for either the user or computer configuration section, expand Security, right-click Software Restriction Policy, and choose New Software Restriction Policy. Set the policy for the level of security that you need.

Using AppLocker

AppLocker is a feature in Windows 7, Windows 8, and Windows Server 2012 R2. It is the replacement for Software Restriction Policies. *AppLocker* allows you to configure a Denied list and an Accepted list for applications. Applications that are configured on the Denied list will not run on the system, whereas applications on the Accepted list will operate properly.

The new capabilities and extensions of the AppLocker feature help reduce administrative overhead and help administrators control how users can access and use files, such as EXE files, scripts, Windows Installer files (MSI and MSP files), and DLLs.

Group Policy Slow Link Detection

When setting up GPOs, most of us assume that the connection speeds between servers and clients are going to be fast. In today's world, it is unlikely to see slow connections between locations, but they are still out there. Sometimes connection speeds can cause issues with the deployment of GPOs, specifically ones that are deploying software.

A setting in the Computer and User section of the GPO called *Group Policy Slow Link Detection* defines a slow connection for the purposes of applying and updating GPOs. If the data transfer rate from the domain controller providing the GPO to the computer is slower than what you have specified in this setting, the connection is considered to be a slow connection. If a connection is considered slow, the system response will vary depending on the policy. For example, if a GPO is going to deploy software and the connection is considered slow, the software may not be installed on the client computer. If you configure this option as 0, all connections are considered fast connections.

Publishing and Assigning Applications

As mentioned earlier in this section, system administrators can make software packages available to users by using publishing and assigning operations. Both of these operations allow system administrators to leverage the power of Active Directory and, specifically,

GPOs to determine which applications are available to users. Additionally, OUs can provide the organization that can help group users based on their job functions and software requirements.

The general process involves creating a GPO that includes software deployment settings for users and computers and then linking this GPO to Active Directory objects.

Exercise 16.8 walks you through the steps required to publish and assign applications. In this exercise, you will create applications and assign them to specific Active Directory objects using GPOs. To complete the steps in this exercise, you must have completed Exercise 16.7.

EXERCISE 16.8

Publishing and Assigning Applications Using Group Policy

1. Open the Active Directory Users and Computers tool from the Administrative Tools program group (using the Windows key).
2. Expand the domain and create a new top-level OU called **Software**.
3. Within the Software OU, create a user named **Jane User** with a login name of **juser** (choose the defaults for all other options).
4. Exit Active Directory Users and Computers and open the Group Policy Management Console.
5. Right-click the Software OU and choose Create A GPO In This Domain And Link It Here.
6. For the name of the new GPO, type **Software Deployment**.
7. To edit the Software Deployment GPO, right-click it and choose Edit. Expand the Computer Configuration ➢ Policies ➢ Software Settings object.
8. Right-click the Software Installation item and select New ➢ Package.
9. Navigate to the Software share you created in Exercise 16.7.
10. Within the Software share, double-click the `Office 2010` folder and select the appropriate MSI file depending on the version of Office 2010 that you have. Office 2010 Professional is being used in this example, so you'll see that the `OFFICEMUI.MSI` file is chosen. Click Open.
11. In the Deploy Software dialog box, choose Advanced. (Note that the Published option is unavailable because applications cannot be published to computers.) Click OK to return to the Deploy Software dialog box.
12. To examine the deployment options of this package, click the Deployment tab. Accept the default settings by clicking OK.
13. Within the Group Policy Object Editor, expand the User Configuration ➢ Software Settings object.

EXERCISE 16.8 *(continued)*

14. Right-click the Software Installation item and select New ➢ Package.
15. Navigate to the Software share you created in Exercise 16.7.
16. Within the Software share, double-click the `Office 2010` folder and select the appropriate MSI file. Click Open.
17. For the Software Deployment option, select Published in the Deploy Software dialog box and click OK.
18. Close the GPMC.

The overall process involved in deploying software using Active Directory is quite simple. However, you shouldn't let the intuitive graphical interface fool you—there's a lot of power under the hood of these software deployment features! Once you've properly assigned and published applications, it's time to see the effects of your work.

Applying Software Updates

The steps described in the previous section work only when you are installing a new application. However, software companies often release updates that you need to install on top of existing applications. These updates usually consist of bug fixes or other changes that are required to keep the software up-to-date. You can apply software updates in Active Directory by using the Upgrades tab of the software package Properties dialog box found in the Group Policy Object Editor.

In Exercise 16.9, you will apply a software update to an existing application. You should add the upgrade package to the GPO in the same way that you added the original application in steps 8 through 12 of Exercise 16.8. You should also have completed Exercise 16.8 before attempting this exercise.

EXERCISE 16.9

Applying Software Updates

1. Open the Group Policy Management Console from the Administrative Tools program group.
2. Click the Software OU, right-click the Software Deployment GPO, and choose Edit.
3. Expand the Computer Configuration ➢ Policies ➢ Software Settings ➢ Software Installation object.
4. Right-click the software package and select Properties from the context menu to bring up the Properties dialog box.

5. Select the Upgrades tab and click the Add button.
6. Click the Current Group Policy Object (GPO) radio button in the Choose A Package From section of the dialog box or click the Browse button to select the GPO to which you want to apply the upgrade. Consult your application's documentation to see whether you should choose the Uninstall The Existing Package, the Install The Upgrade Package radio button, or the Package Can Upgrade Over The Existing Package radio button.
7. Click Cancel to close the Add Upgrade Package dialog box.
8. Click Cancel and exit the GPMC.

You should understand that not all upgrades make sense in all situations. For instance, if the Stellacon 2010 files are incompatible with the Stellacon 2013 application, then your Stellacon 2012 users might not want you to perform the upgrade without taking additional steps to ensure that they can continue to use their files. In addition, users might have some choice about which version they use when it doesn't affect the support of the network.

Regardless of the underlying reason for allowing this flexibility, you should be aware that there are two basic types of upgrades that are available for administrators to provide to users:

Mandatory Upgrade Forces everyone who currently has an existing version of the program to upgrade according to the GPO. Users who have never installed the program for whatever reason will be able to install only the new upgraded version.

Nonmandatory Upgrade Allows users to choose whether they would like to upgrade. This upgrade type also allows users who do not have their application installed to choose which version they would like to use.

Verifying Software Installation

To ensure that the software installation settings you make in a GPO have taken place, you can log into the domain from a Windows 8, Windows 7, or Windows Vista computer that is within the OU to which the software settings apply. When you log in, you will notice two changes. First the application is installed on the computer (if it was not installed already). To access the application, a user needs to click one of the icons within the Program group of the Start menu. Note also that applications are available to any of the users who log on to this machine. Second, the settings apply to any computers that are contained within the OU and to any users who log on to these computers.

If you publish an application to users, the change may not be as evident, but it is equally useful. When you log on to a Windows 8, Windows 7, or Windows Vista computer that is a member of the domain, and when you use a user account from the OU where you published the application, you will be able to install any of the published applications automatically. On a Windows 8 or Windows 7 computer, you can do this by accessing the Programs icon in Control Panel. By clicking Add New Programs, you access a display of the applications available for installation. By clicking the Add button in the Programs and Features section

of the Programs dialog box, you will automatically begin the installation of the published application.

Configuring Automatic Updates in Group Policy

So far you've seen the advantages of deploying application software in a group policy. Group policies also provide a way to install operating system updates across the network for Windows 2000, XP, Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 R2 machines using Windows Update in conjunction with Windows Server Update Service. WSUS is the newer version of SUS, and it is used on a Windows Server 2012 R2 system to update systems. As you may remember, WSUS and SUS are patch-management tools that help you deploy updates to your systems in a controlled manner.

Windows Update is available through the Microsoft website, and it is used to provide the most current files for Windows operating systems. Examples of updates include security fixes, critical updates, updated help files, and updated drivers. You can access Windows Update by clicking the Windows Update icon in the system tray.

We will discuss WSUS in greater detail in Chapter 10, "Manage and Maintain Servers."

WSUS is used to leverage the features of Windows Update within a corporate environment by downloading Windows updates to a corporate server, which in turn provides the updates to the internal corporate clients. This allows administrators to test and have full control over what updates are deployed within the corporate environment.

Within an enterprise network that is using Active Directory, you would typically see automatic updates configured through Group Policy. Group policies are used to manage configuration and security settings via Active Directory. Group Policy is also used to specify what server a client will use for automatic updates.

If the WSUS client is part of an enterprise network that is using Active Directory, you would configure the client via a group policy.

Configuring Software Deployment Settings

In addition to the basic operations of assigning and publishing applications, you can use several other options to specify the details of how software is deployed. In the following sections, you will examine the various options that are available and their effects on the software installation process.

The Software Installation Properties Dialog Box

The most important software deployment settings are contained in the Software Installation Properties dialog box, which you can access by right-clicking the Software Installation item and selecting Properties from the context menu. The following sections describe the features contained on the various tabs of the dialog box.

Managing Package Defaults

On the Deployment tab of the Software Installation Properties dialog box, you'll be able to specify some defaults for any packages that you create within this GPO. Figure 16.10 shows the Deployment options for managing software installation settings.

FIGURE 16.10 Deployment tab of the Software Installation Properties dialog box

The following options are used for managing software installation settings:

Default Package Location This setting specifies the default file system or network location for software installation packages. This is useful if you are already using a specific share on a file server for hosting the necessary installation files.

New Packages These settings specify the default type of package assignment that will be used when you add a new package to either the user or computer settings. If you'll be assigning or publishing multiple packages, you may find it useful to set a default here. Selecting the Advanced option enables Group Policy to display the package's Properties dialog box each time a new package is added (see Figure 16.11).

FIGURE 16.11 Advanced Deployment dialog box

Installation User Interface Options When installing an application, system administrators may or may not want end users to see all of the advanced installation options. If Basic is chosen, the user will only be able to configure the minimal settings (such as the installation location). If Maximum is chosen, all of the available installation options will be displayed. The specific installation options available will depend on the package itself.

Uninstall Applications When They Fall Out of the Scope of Management So far, you have seen how applications can be assigned and published to users or computers. But what happens when effective GPOs change? For example, suppose User A is currently located within the Sales OU. A GPO that assigns the Microsoft Office 2013 suite of applications is linked to the Sales OU. You decide to move User A to the Engineering OU, which has no software deployment settings. Should the application be uninstalled, or should it remain?

If the Uninstall This Application When It Falls Out Of The Scope Of Management option is checked, applications will be removed if they are not specifically assigned or published within GPOs. In this example, this means that Office 2013 would be uninstalled for User A. If this box is left unchecked, however, the application will remain installed.

Managing File Extension Mappings

One of the potential problems associated with using many different file types is that it's difficult to keep track of which applications work with which files. For example, if you received a file with the filename extension `.abc`, you would have no idea which application you would need to view it.

Fortunately, through software deployment settings, system administrators can specify mappings for specific *filename extensions*. For example, you could specify that whenever users attempt to access a file with the extension `.vsd`, the operating system should attempt to open the file using Visio diagramming software. If Visio is not installed on the user's machine, the computer can automatically download and install it (assuming that the application has been properly advertised).

This method allows users to have applications automatically installed when they are needed. The following is an example of a sequence of events that might occur:

1. A user receives an email message that contains a PDF (`.pdf`) file attachment.
2. The computer realizes that the PDF file does not have the appropriate viewing application for this type of file installed. However, it also realizes that a filename extension mapping is available within the Active Directory software deployment settings.
3. The client computer automatically requests the PDF software package from the server, and it uses the Microsoft Windows Installer to install the application automatically.
4. The computer opens the attachment for the user.

Notice that all of these steps were carried out without any further interaction with the user.

You can manage filename extension mappings by right-clicking the Software Installation item, selecting Properties, and then clicking the File Extensions tab.

Creating Application Categories

In many network environments, the list of supported applications can include hundreds of items. For users who are looking for only one specific program, searching through a list of all of these programs can be difficult and time-consuming.

Fortunately, methods for categorizing the applications are available on your network. You can easily manage the application categories for users and computers by right-clicking the Software Installation item, selecting Properties, and then clicking the Categories tab.

Figure 16.12 shows you the categories tab of the Software Installation package. When creating categories, it is a good idea to use category names that are meaningful to users because it will make it easier for them to find the programs they're seeking.

FIGURE 16.12 The Categories tab of the Software Installation Properties dialog box

Once the software installation categories have been created, you can view them by clicking the Programs or Programs And Features icon in Control Panel. When you click Add New Programs, you'll see that several options appear in the Category drop-down list. Now when you select the properties for a package, you will be able to assign the application to one or more of the categories.

Removing Programs

As discussed in the beginning of the chapter, an important phase in the software management life cycle is the removal of applications. Fortunately, if you use the GPMC and the Windows Installer packages, the process is simple. To remove an application, you can right-click the package within the Group Policy settings and select All Tasks ➢ Remove (see Figure 16.13).

FIGURE 16.13 Removing a software package

When choosing to remove a software package from a GPO, you have two options:

Immediately Uninstall The Software From Users And Computers System administrators can choose this option to ensure that an application is no longer available to users who are affected by the GPO. When this option is selected, the program will be uninstalled automatically from users and/or computers that have the package. This option might be useful, for example, if the license for a certain application has expired or if a program is no longer on the approved applications list.

Allow Users To Continue To Use The Software, But Prevent New Installations This option prevents users from making new installations of a package, but it does not remove the software if it has already been installed for users. This is a good option if the company has run out of additional licenses for the software, but the existing licenses are still valid.

Figure 16.14 shows these two removal options.

FIGURE 16.14 Software removal options

If you no longer require the ability to install or repair an application, you can delete it from your software distribution share point by deleting the appropriate Windows Installer package files. This will free up additional disk space for newer applications.

Microsoft Windows Installer Settings

Several options influence the behavior of the Windows Installer; you can set them within a GPO. You can access these options by navigating to User Configuration ➢ Administrative Templates ➢ Windows Components ➢ Windows Installer (see Figure 16.15). The options are as follows:

FIGURE 16.15 GPO settings for Windows Installer

Always Install With Elevated Privileges This policy allows users to install applications that require elevated privileges. For example, if a user does not have the permissions necessary to modify the registry but the installation program must make registry changes, this policy will allow the process to succeed.

Prevent Removable Media Source For Any Install This option disallows the installation of software using removable media (such as CD-ROM or DVD-ROM). It is useful for ensuring that users install only approved applications.

Prohibit Rollback When this option is enabled, the Windows Installer does not store the system state information that is required to roll back the installation of an application. System administrators may choose this option to reduce the amount of temporary disk space required during installation and to increase the performance of the installation operation. However, the drawback is that the system cannot roll back to its original state if the installation fails and the application needs to be removed.

Specify the Order In Which Windows Installer Searches This setting specifies the order in which the Windows Installer will search for installation files. The options include *n* (for network shares), *m* (for searching removal media), and *u* (for searching the Internet for installation files).

With these options, system administrators can control how the Windows Installer operates for specific users who are affected by the GPO.

Troubleshooting Group Policies

Because of the wide variety of configurations that are possible when you are establishing GPOs, you should be aware of some common troubleshooting methods. These methods will help isolate problems in policy settings or GPO links.

One possible problem with GPO configuration is that logons and system startups may take a long time. This occurs especially in large environments when the Group Policy settings must be transmitted over the network and, in many cases, slow WAN links. In general, the number of GPOs should be limited because of the processing overhead and network requirements during logon. By default, GPOs are processed in a synchronous manner. This means that the processing of one GPO must be completed before another one is applied (as opposed to asynchronous processing, where they can all execute at the same time).

When a group policy gets processed on a Windows-based operating system, client-side extensions are the mechanisms that interpret the stored policy and then make the appropriate changes to the operating system environment. When an administrator is troubleshooting a given extension's application of policy, the administrator can view the

configuration parameters for that extension in the operating system's registry. To view the extension in the registry, you would view the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows CA
NT\CurrentVersion\Winlogon\GPExtensions
```

The most common issue associated with Group Policy is the unexpected setting of Group Policy options. In Windows Server 2000, administrators spent countless hours analyzing inheritance hierarchy and individual settings to determine why a particular user or computer was having policy problems. For instance, say a user named wpanek complains that the Run option is missing from his Start menu. The wpanek user account is stored in the New Hampshire OU, and you've applied group policies at the OU, domain, and site levels. To determine the source of the problem, you would have to sift through each GPO manually to find the Start menu policy as well as to figure out the applicable inheritance settings.

Windows Server 2012 R2 has a handy feature called *Resultant Set of Policy (RSoP)* that displays the exact settings that actually apply to individual users, computers, OUs, domains, and sites after inheritance and filtering have taken effect. In the example just described, you could run RSoP on the wpanek account and view a single set of Group Policy settings that represent the settings that apply to the wpanek account. In addition, each setting's Properties dialog box displays the GPO from which the setting is derived as well as the order of priority, the filter status, and other useful information, as you will see a bit later.

RSoP actually runs in two modes:

Logging Mode *Logging mode* displays the actual settings that apply to users and computers, as shown in the example in the preceding paragraph.

Planning Mode *Planning mode* can be applied to users, computers, OUs, domains, and sites, and you use it before you apply any settings. As its name implies, planning mode is used to plan GPOs.

Additionally, you can run the command-line utility `gpresult.exe` to get a quick snapshot of the Group Policy settings that apply to a user and/or computer. Let's take a closer look at the two modes and the `gpresult.exe` command.

RSoP in Logging Mode

RSoP in logging mode can query policy settings only for users and computers. The easiest way to access RSoP in logging mode is through the Active Directory Users and Computers tool, although you can run it as a stand-alone MMC snap-in if you want.

To analyze the policy settings for wpanek from the earlier example, you would right-click the user icon in Active Directory Users and Computers and select All Tasks ➢ Resultant Set of Policy (Logging). The Group Policy Results Wizard appears. The wizard walks you through the steps necessary to view the RSoP for wpanek.

The Computer Selection page, shown in Figure 16.16, requires you to select a computer for which to display settings. Remember that a GPO contains both user and computer settings, so you must choose a computer to which the user is logged on in order to continue with the wizard. If the user has never logged on to a computer, then you must run RSoP in planning mode because there is no logged policy information yet for that user.

FIGURE 16.16 The Computer Selection page of the Group Policy Results Wizard

The User Selection page, shown in Figure 16.17, requires you to select a user account to analyze. Because I selected a user from the Active Directory Users and Computers tool, the username is filled in automatically. This page is most useful if you are running RSoP in MMC mode and don't have the luxury of selecting a user contextually.

FIGURE 16.17 The User Selection page of the Group Policy Results Wizard

The Summary Of Selections page, shown in Figure 16.18, displays a summary of your choices and provides an option for gathering extended error information. If you need to make any changes before you begin to analyze the policy settings, you should click the Back button on the Summary screen. Otherwise, click Next.

FIGURE 16.18 The Summary Of Selections page of the Group Policy Results Wizard

After the wizard is complete, you will see the window shown in Figure 16.19. This window displays only the policy settings that apply to the user and computer that you selected in the wizard. You can see these users and computers at the topmost level of the tree.

FIGURE 16.19 The User Selection page for the administrator on computer SERVER1

Any warnings or errors appear as a yellow triangle or red *X* over the applicable icon at the level where the warning or error occurred. To view more information about the warning or error, right-click the icon, select Properties, and select the Error Information tab. Figure 16.20 shows an error message.

FIGURE 16.20 Details of event pertaining to the administrator account on computer SERVER1

You cannot make changes to any of the individual settings because RSoP is a diagnostic tool and not an editor, but you can get more information about settings by clicking a setting and selecting Properties from the context menu.

The Details tab of the user's Properties window, shown in Figure 16.21, displays the actual setting that applies to the user in question based on GPO inheritance.

FIGURE 16.21 The Details tab of the object's Properties window

RSoP in Planning Mode

Running RSoP in planning mode isn't much different from running RSoP in logging mode, but the RSoP Wizard asks for a bit more information than you saw earlier.

In the former example, wpanek couldn't see the Run option in the Start menu because the New Hampshire GPO in the San Jose OU affects his user account. As an administrator, you could plan to move his user account to the North America OU. Before doing so, you could verify his new policy settings by running RSoP in planning mode. Run the RSoP on the user wpanek under the scenario that you've already moved him from the San Jose OU to the North America OU. At this point, you haven't actually moved the user, but you can see what his settings would be if you did.

Using the *gpresult.exe* Command

The command-line utility `gpresult.exe` is included as part of the RSoP tool. Running the command by itself without any switches returns the following Group Policy information about the local user and computer:

- The name of the domain controller from which the local machine retrieved the policy information

- The date and time in which the policies were applied
- Which policies were applied
- Which policies were filtered out
- Group membership

You can use the switches shown in Table 16.3 to get information for remote users and computers and to enable other options.

Table 16.3 is not a complete list. To see a complete list of the `gpresult.exe` switches, visit Microsoft at `www.microsoft.com`.

TABLE 16.3 gpresult switches

Switch	Description
`/S` *`systemname`*	Generates RSoP information for a remote computer name.
`/USER` *`username`*	Generates RSoP information for a remote username.
`/x /h` *`filename`*	Generates a report in either XML (`/x`) or HTML (`/h`) format. The filename and location is specified by the *`filename`* parameter.
`/V`	Specifies verbose mode, which displays more verbose information such as user rights information.
`/Z`	Specifies an even greater level of verbose information.
`/SCOPE MACHINE`	Displays maximum information about the computer policies applied to this system.
`/SCOPE USER`	Displays maximum information about the user policies applied to this system.
`>`*`textfile.txt`*	Writes the output to a text file.

For example, to obtain information about user wpanek in a system called STELLACON, you would use the command `gpresult/S STELLACON/USERwpanek`.

Through the use of these techniques, you should be able to track down even the most elusive Group Policy problems. Remember, however, that good troubleshooting skills do not replace planning adequately and maintaining GPO settings!

Summary

In this chapter, you examined Active Directory's solution to a common headache for many systems administrators: policy settings. Specifically, I discussed topics that covered Group Policy.

I covered the fundamentals of Group Policy, including its fundamental purpose. You can use Group Policy to enforce granular permissions for users in an Active Directory environment. Group policies can restrict and modify the actions allowed for users and computers within the Active Directory environment.

Certain Group Policy settings may apply to users, computers, or both. Computer settings affect all users who access the machines to which the policy applies. User settings affect users regardless of the machines to which they log on.

You learned that you can link Group Policy objects to Active Directory sites, domains, or OUs. This link determines to which objects the policies apply. GPO links can interact through inheritance and filtering to result in an effective set of policies.

The chapter covered inheritance and how GPOs filter down. I showed you how to use the Enforced option on a GPO issued from a parent and how to block a GPO from a child.

You can also use administrative templates to simplify the creation of GPOs. There are some basic default templates that come with Windows Server 2012 R2.

In addition, administrators can delegate control over GPOs in order to distribute administrative responsibilities. Delegation is an important concept because it allows for distributed administration.

You can also deploy software using GPOs. This feature can save time and increase productivity throughout the entire software management life cycle by automating software installation and removal on client computers. The Windows Installer offers a more robust method for managing installation and removal, and applications that support it can take advantage of new Active Directory features. Make sure you are comfortable using the Windows Installer.

You learned about publishing applications via Active Directory and the difference between publishing and assigning applications. You can assign some applications to users and computers so that they are always available. You can also publish them to users so that the user can install them with minimal effort when required.

You also learned how to prepare for software deployment. Before your users can take advantage of automated software installation, you must set up an installation share and provide the appropriate permissions.

The final portion of the chapter covered the Resultant Set of Policy (RSoP) tool, which you can use in logging mode or planning mode to determine exactly which set of policies apply to users, computers, OUs, domains, and sites.

Exam Essentials

Understand the purpose of Group Policy. System administrators use Group Policy to enforce granular permissions for users in an Active Directory environment.

Understand user and computer settings. Certain Group Policy settings may apply to users, computers, or both. Computer settings affect all users who access the machines to which the policy applies. User settings affect users, regardless of the machines to which they log on.

Know the interactions between Group Policy objects and Active Directory. GPOs can be linked to Active Directory objects. This link determines to which objects the policies apply.

Understand filtering and inheritance interactions between GPOs. For ease of administration, GPOs can interact via inheritance and filtering. It is important to understand these interactions when you are implementing and troubleshooting Group Policy.

Know how Group Policy settings can affect script policies and network settings. You can use special sets of GPOs to manage network configuration settings.

Understand how delegation of administration can be used in an Active Directory environment. Delegation is an important concept because it allows for distributed administration.

Know how to use the Resultant Set of Policy (RSoP) tool to troubleshoot and plan Group Policy. Windows Server 2012 R2 includes the RSoP feature, which you can run in logging mode or planning mode to determine exactly which set of policies applies to users, computers, OUs, domains, and sites.

Identify common problems with the software life cycle. IT professionals face many challenges with client applications, including development, deployment, maintenance, and troubleshooting.

Understand the benefits of the Windows Installer. Using the Windows Installer is an updated way to install applications on Windows-based machines. It offers a more robust method for making the system changes required by applications, and it allows for a cleaner uninstall. Windows Installer–based applications can also take advantage of new Active Directory features.

Understand the difference between publishing and assigning applications. Some applications can be assigned to users and computers so that they are always available. Applications can be published to users so that the user may install the application with a minimal amount of effort when it is required.

Know how to prepare for software deployment. Before your users can take advantage of automated software installation, you must set up an installation share and provide the appropriate permissions.

Know how to configure application settings using Active Directory and Group Policy. Using standard Windows Server 2012 R2 administrative tools, you can create an application policy that meets your requirements. You can use automatic, on-demand installation of applications as well as many other features.

Create application categories to simplify the list of published applications. It's important to group applications by functionality or the users to whom they apply, especially in organizations that support a large number of programs.

Review Questions

1. The process of assigning permissions to set Group Policy for objects within an OU is known as:
   - **A.** Promotion
   - **B.** Inheritance
   - **C.** Delegation
   - **D.** Filtering

2. Which of the following statements is true regarding the actions that occur when a software package is removed from a GPO that is linked to an OU?
   - **A.** The application will be automatically uninstalled for all users within the OU.
   - **B.** Current application installations will be unaffected by the change.
   - **C.** The system administrator may determine the effect.
   - **D.** The current user may determine the effect.

3. You are the network administrator for your organization. You are working on creating a new GPO for the sales OU. You want the GPO to take effect immediately. Which command would you use?
   - **A.** GPForce
   - **B.** GPUpdate
   - **C.** GPResult
   - **D.** GPExecute

4. You are the network administrator for your organization. You are working on creating a new GPO for the Marketing OU. You want the GPO to take effect immediately, and you need to use Windows PowerShell. Which PowerShell cmdlet command would you use?
   - **A.** `Invoke-GPUpdate`
   - **B.** `Invoke-GPForce`
   - **C.** `Invoke-GPResult`
   - **D.** `Invoke-GPExecute`

5. You are the network administrator, and you have decided to set up a GPO with item-level targeting. Which of the following is *not* an option for item-level targeting?
   - **A.** Battery Present Targeting
   - **B.** Computer Name Targeting
   - **C.** CPU Speed Targeting
   - **D.** DVD Present Targeting

6. You are the network administrator for a large organization that uses Windows Server 2012 R2 domain controllers and DNS servers. All of your client machines currently have the Windows XP operating system. You want to be able to have client computers edit the domain-based GPOs by using the ADMX files that are located in the ADMX Central Store. How do you accomplish this task? (Choose all that apply.)
   - **A.** Upgrade your clients to Windows 8.
   - **B.** Upgrade your clients to Windows 7.
   - **C.** Add the client machines to the ADMX edit utility.
   - **D.** In the ADMX store, choose the box Allow All Client Privileges.

7. You work for an organization with a single Windows Server 2012 R2 Active Directory domain. The domain has OUs for Sales, Marketing, Admin, R&D, and Finance. You need the users in the Finance OU only to get Microsoft Office 2010 installed automatically onto their computers. You create a GPO named OfficeApp. What is the next step in getting all of the Finance users Office 2010?
   - **A.** Edit the GPO, and assign the Office application to the user's account. Link the GPO to the Finance OU.
   - **B.** Edit the GPO, and assign the Office application to the user's account. Link the GPO to the domain.
   - **C.** Edit the GPO, and assign the Office application to the computer account. Link the GPO to the domain.
   - **D.** Edit the GPO, and assign the Office application to the computer account. Link the GPO to the Finance OU.

8. You are hired as a consultant to the ABC Company. The owner of the company complains that she continues to have desktop wallpaper that she did not choose. When you speak with the IT team, you find out that a former employee created 20 GPOs and they have not been able to figure out which GPO is changing the owner's desktop wallpaper. How can you resolve this issue?
   - **A.** Run the RSoP utility against all forest computer accounts.
   - **B.** Run the RSoP utility against the owner's computer account.
   - **C.** Run the RSoP utility against the owner's user account.
   - **D.** Run the RSoP utility against all domain computer accounts.

9. You are the network administrator for a large organization that has multiple sites and multiple OUs. You have a site named SalesSite that is for the sales building across the street. In the domain, there is an OU for all salespeople called Sales. You set up a GPO for the SalesSite, and you need to be sure that it applies to the Sales OU. The Sales OU GPOs cannot override the SalesSite GPO. What do you do?
   - **A.** On the GPO, disable the Block Child Inheritance setting.
   - **B.** On the GPO, set the Enforce setting.
   - **C.** On the GPO, set the priorities to 1.
   - **D.** On the Sales OU, set the Inherit Parent Policy settings.

10. You are the administrator for an organization that has multiple locations. You are running Windows Server 2012 R2, and you have only one domain with multiple OUs set up for each location. One of your locations, Boston, is connected to the main location by a 256Kbps ISDN line. You configure a GPO to assign a sales application to all computers in the entire domain. You have to be sure that Boston users receive the GPO properly. What should you do?

A. Disable the Slow Link Detection setting in the GPO.

B. Link the GPO to the Boston OU.

C. Change the properties of the GPO to publish the application to the Boston OU.

D. Have the users in Boston run the `GPResult/force` command.

Exam 70-412: Configuring Advanced Windows Server 2012 R2 Services

CHAPTER 17 ■ Configure and Manage High Availability

CHAPTER 18 ■ Configure File and Storage Solutions

CHAPTER 19 ■ Implement Business Continuity and Disaster Recovery

CHAPTER 20 ■ Configure Advanced Network Services

CHAPTER 21 ■ Configure the Active Directory Infrastructure

CHAPTER 22 ■ Configure Access and Information Protection Solutions

Chapter

17

Configure and Manage High Availability

THE FOLLOWING 70-412 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure Network Load Balancing (NLB)**

- This objective may include, but is not limited to:
  - Install NLB nodes
  - Configure NLB prerequisites
  - Configure affinity
  - Configure port rules
  - Configure cluster operation mode
  - Upgrade an NLB cluster

✓ **Configure failover clustering**

- This objective may include, but is not limited to:
  - Configure Quorum
  - Configure cluster networking
  - Restore single node or cluster configuration
  - Configure cluster storage
  - Implement cluster aware updating
  - Upgrade a cluster

✓ **Manage failover-clustering roles**

- This objective may include, but is not limited to:
  - Configure role-specific settings including continuously available shares

- Configure VM monitoring
- Configure failover and preference settings

✓ **Manage Virtual Machine (VM) Movement**

- This objective may include, but is not limited to:
  - Configure Virtual Machine network health protection
  - Configure drain on shutdown
  - Perform quick, live and storage migrations
  - Import/export/copy of VMS

The R2 update to Windows Server 2012 has improved upon the rich high availability capabilities already present in Windows Server 2012. The management, reporting, and ease of use of the feature set are all worth mentioning, but the expansion of features is the greatest benefit of the R2 update with regard to high availability.

The exam will cover the new features at a high level, and it will cover the basic configuration and operational functions for both a failover cluster and a network load balancer. This chapter will introduce how to achieve high availability with hardware and operational changes as well as how to use the high availability features of Windows Server 2012 R2.

Any discussion of high availability, network load balancers, and clustering would not be complete without a discussion of high availability in general. The chapter will first cover what it means, both from a purely technical perspective and from a business perspective.

Components of High Availability

High availability is a buzzword that many application and hardware vendors like to throw around to get you to purchase their products. Many different options are available to achieve high availability, and there also seems to be a number of definitions and variations that help vendors sell their products as high-availability solutions.

When it comes right down to it, however, high availability simply means providing services with maximum uptime by avoiding unplanned downtime. Often, *disaster recovery (DR)* is also closely lumped into discussions of high availability, but DR encompasses the business and technical processes that are used to recover once a disaster has happened.

Defining a high availability plan usually starts with a *service level agreement (SLA)*. At its most basic, an SLA defines the services and metrics that must be met for the availability and performance of an application or service. Often, an SLA is created for an IT department or service provider to deliver a specific level of service. An example of this might be an SLA for a Microsoft Exchange server. The SLA for an Exchange server might have uptime metrics on how much time during the month the mailboxes need to be available to end users, or it might define performance metrics for the amount of time it takes for email messages to be delivered.

When determining what goes into an SLA, two other factors need to be considered. However, you will often see them discussed only in the context of disaster recovery, even though they are important for designing a highly available solution. These factors are the *recovery point objective (RPO)* and the *recovery time objective (RTO)*.

An RTO is the length of time an application can be unavailable before service must be restored to meet the SLA. For example, a single component failure would have an RTO of less than five minutes, and a full-site failure might have an RTO of three hours. An RPO is essentially the amount of data that must be restored in the event of a failure. For example, in a single server or component failure, the RPO would be 0, but in a site failure, the RPO might allow for up to 20 minutes of lost data.

SLAs, on the other hand, are usually expressed in percentages of the time the application is available. These percentages are also often referred to by the number of nines the percentage includes, as shown in Table 17.1.

TABLE 17.1 Availability percentages

Availability rating	Allowed unplanned downtime/year
99 percent	3.7 days
99.9 percent	8.8 hours
99.99 percent	53 minutes
99.999 percent	5.3 minutes

Two important factors that affect an SLA are the *mean time between failure (MTBF)* and the *mean time to recovery (MTTR)*. To be able to reduce the amount of unplanned downtime, the time between failures must be increased, and the time it takes to recover must be reduced. Modifying these two factors will be addressed in the next several sections of this chapter.

Achieving High Availability

Windows Server 2012 R2 is the most secure and reliable Windows version to date. It also is the most stable, mature, and capable of any version of Windows. Although similar claims have been made for previous versions of Windows Server, you can rest assured that Windows Server 2012 R2 is much better than previous versions for a variety of reasons.

An honest look at the feature set and real-world use should prove that this latest version of Windows provides the most suitable foundation for creating a highly available solution. However, more than just good software is needed to be able to offer high availability for applications.

High Availability Foundation

Just as a house needs a good foundation, a highly available Windows server needs a stable and reliable hardware platform on which to run. Although Windows Server 2012 R2 will

technically run on desktop-class hardware, high availability is more easily achieved with server-class hardware. What differentiates desktop-class from server-class hardware? *Server-class hardware* has more management and monitoring features built into it so that the health of the hardware is capable of being monitored and maintained.

Another large difference is that server-class hardware has redundancy options. Server-class hardware often has options to protect from drive failures, such as RAID controllers, and to protect against power supply failures, such as multiple power supplies. Enterprise-class servers have even more protection.

More needs to be done than just installing Windows Server 2012 R2 to ensure that the applications remain running with the best availability possible. Just as a house needs maintenance and upkeep to keep the structure in proper repair, so too does a server. In the case of a highly available server, this means *patch management*.

Installing Patches

Microsoft releases monthly updates to fix security problems with its software, both for operating system fixes and for applications. To ensure that your highly available applications are immune to known vulnerabilities, these patches need to be applied in a timely manner during a scheduled maintenance window. Also, to address stability and performance issues, updates and service packs are released regularly for many applications, such as Microsoft SQL Server, Exchange Server, and SharePoint Portal Server. Many companies have a set schedule—daily, weekly, or monthly—to apply these patches and updates after they are tested and approved.

Desired Configuration Manager (DCM), an option in Microsoft System Center Configuration Manager 2012 and newer, is a great tool for helping to validate that your cluster nodes are patched. It can leverage the SCCM client to collect installed patches and help reporting within the enterprise on compliancy with desired system states based on the software installed.

To continue with the house analogy, if you were planning to have the master bath remodeled, would you rather hire a college student on spring break looking to make some extra money to do the job or a seasoned artisan? Of course, you would want someone with experience and a proven record of accomplishment to remodel your master bath.

Likewise, with any work that needs to be done on your highly available applications, it's best to hire only decidedly qualified individuals. This is why obtaining a Microsoft certification is definitely an excellent start to becoming qualified to configure a highly available server properly. There is no substitute for real-life and hands-on experience. Working with highly available configurations in a lab and in production will help you know not only what configurations are available but also how the changes should be made.

For example, it may be possible to use Failover Clustering for a WINS server, but in practice WINS replication may be easier to support and require less expensive hardware in order to provide high availability. This is something you would know only if you had enough experience to make this decision.

As with your house, once you have a firm and stable foundation built by skilled artisans and a maintenance plan has been put into place, you need to ascertain what more is

needed. If you can't achieve enough uptime with proper server configuration and mature operational processes, a cluster may be needed.

Windows Server 2012 R2 provides two types of clustering: *Failover Clustering* and *Network Load Balancing (NLB)*. Failover clustering is used for applications and services such as SQL Server and Exchange Server. Network Load Balancing is used for network-based services such as web and FTP servers. The remaining sections of this chapter will cover both of these clustering options in depth.

To Cluster or Not to Cluster

Clustering is often thrown into the mix when someone wants to achieve higher availability. This is a good step toward improved availability, but the return on the investment of a cluster doesn't always add up. Although Windows Server 2012 R2 greatly simplifies both the creation and management of a failover cluster, there is added complexity and cost in terms of hardware, software, and personnel.

How do you determine whether to cluster applications? Sometimes, even though it is possible to cluster applications, they perform worse when clustered. At other times, only a small improvement is made when a cluster is created. You have to balance the slight improvement over the increased hardware cost, complexity, and level of training required for administrators.

Configure Network Load Balancing

Network Load Balancing is a form of clustering where the nodes are highly available for a network-based service. This is typically a port listener configuration where a farm of, say, Microsoft Internet Information Services servers all listen on ports 80 and 443 for incoming web traffic from client endpoints. These nodes, while not fully clustered in a technical sense, are load balanced, where each node handles some of the distributed network traffic.

NOTE

Network Load Balancing at the software level (as I will discuss here) is generally reserved for light loads or loads in lower-budget environments, such as a test or QA environment, for example. Generally speaking, Network Load Balancing in large production environments relies on hardware-based solutions to front-end network load balancing and distributes it on a session-based load to multiple hosts. This type of configuration, however, is out of scope for this book.

Install NLB Nodes

You can install NLB nodes like any other server build. You want the host patched, provisioned with appropriate resources (typically with multiple network interface cards for capacity and responsiveness), and monitored for health and reliability. In Exercise 17.1, you'll install NLB nodes.

EXERCISE 17.1

Installing NLB Nodes

1. Once you have multiple hosts ready for the installation of NLB, simply run the Add Roles And Features Wizard and select Network Load Balancing in the Features area of the wizard.

2. This wizard places a new application in your Start menu, the Network Load Balancing Manager (shown here), the execution of which loads the console.

EXERCISE 17.1 *(continued)*

3. Right-click Network Load Balancing Clusters and select New Cluster. You are then presented with the connection wizard where you can specify the name of one of your hosts.

4. The next screen reveals a prompt to add any additional IPs and assign a priority level. You can do all this later, so hit Next.

5. The next wizard screen is where you specify the cluster IP address. This is the address that the endpoints or clients or users of the NLB cluster will contact. Typically the network team will assign a cluster IP address for this use.

EXERCISE 17.1 *(continued)*

6. On the next screen, you configure the operation mode and specify a name.

With regard to the cluster operation modes, the differences between them are as follows:

Unicast

The cluster adapters for all nodes are assigned the same MAC address.

The outgoing MAC address for each packet is modified based on priority to prevent upstream switches from discovering that all nodes have the same MAC address.

Communication between cluster nodes (other than heartbeat and other administrative NLB traffic) is not possible unless there are additional adapters (because all nodes have the same MAC address).

Depending on load, this configuration can cause switch flooding since all inbound packets are sent to all ports on the switch.

Multicast

The cluster adapters for all nodes are assigned their own MAC unicast address.

The cluster adapters for all nodes are assigned a multicast MAC address (derived from the IP of the cluster).

Non-NLB network traffic between cluster nodes works fine since they all have their own MAC address.

IGMP Multicast

This is much like multicast, but the MAC traffic goes only to the switch ports of the NLB cluster, preventing switch flooding.

7. After selecting the appropriate settings, the next page is where port rules are configured. By default, it is set up to be wide open. Most implementations will limit NLB ports to just the ports needed for the application. For example, a web server would need port 80 enabled. It is also in this area where you can configure filtering mode.

The affinity sets a client's preference to a particular NLB host. It is not recommended to set affinity to None when UDP is an expected traffic type.

8. After clicking OK and finishing the wizard, you can add nodes to the NLB cluster by right-clicking and selecting Add Host To Cluster. Doing so presents a fairly straightforward wizard to add the host, specify a priority value, and then join the cluster. Shortly, your console will look similar to the one shown here.

Upgrading an NLB Cluster

Upgrading an NLB cluster is a fairly straightforward process. You execute a drainstop on the NLB cluster node or remove existing connections to the application on the local host, and then you can perform an in-place upgrade in a rolling manner.

Achieving High Availability with Failover Clustering

Taking high availability to the next level for enterprise services often means creating a failover cluster. In a failover cluster, all of the clustered application or service resources are assigned to one node or server in the cluster. Commonly clustered applications are SQL Server and Exchange Server; commonly clustered services are File and Print. Since the differences between a clustered application and a clustered service are primarily related to the number of functions or features, for simplicity's sake I will refer to both as *clustered applications*. Another, more frequently, clustered resource is a Hyper-V virtual machine.

If there is a failure of the primary node or if the primary node is taken offline for maintenance, the clustered application is started on another cluster node. The client requests are then automatically redirected to the new cluster node to minimize the impact of the failure.

How does Failover Clustering improve availability? By increasing the number of server nodes available on which the application or virtual machine can run, you can move the application or virtual machine to a healthy server if there is a problem, if maintenance needs to be completed on the hardware or the operating system, or if patches need to be applied. The clustered application being moved will have to restart on the new server regardless of whether the move was intentional. This is why the term *highly available* is used instead of *fault tolerant*. Virtual machines, however, can be moved from one node to another node using a process known as *live migration*. Live migration is where one or more virtual machines are intentionally moved from one node to another with their current memory state intact through the cluster network with no indicators to the virtual machine consumer that the virtual machine has moved from one server to another. However, in the event of a cluster node or virtual machine failure, the virtual machine will still fail and will then be brought online again on another healthy cluster node.

Figure 17.1 shows an example of SQL Server running on the first node of a Windows Server 2012 R2 failover cluster.

The clustered SQL Server in Figure 17.2 can be failed over to another node in the cluster and still service database requests. However, the database will be restarted.

Failover clustering is notorious for being complicated and expensive. Windows Server 2012 R2 makes strides in removing both of these concerns. Troubleshooting and other advanced concepts are outside of the scope of the Microsoft MCSA exams and thus this book, so I will cover only the basic requirements and concepts needed to configure a failover cluster.

FIGURE 17.1 Using Failover Clustering to cluster SQL Server

FIGURE 17.2 Failing the SQL Server service to another node

Failover Clustering Requirements

The Failover Clustering feature is available in the Datacenter, Standard, and Hyper-V editions of Windows Server 2012 R2.

To be able to configure a failover cluster, you must have the required components. A single failover cluster can have up to 64 nodes when using Windows Server 2012 R2, however, and the clustered service or application must support that number of nodes.

To create a failover cluster, an administrator must make sure that all the hardware involved meets the cluster requirements. To be supported by Microsoft, all hardware must be certified for Windows Server 2012 R2, and the complete failover cluster solution must

pass all tests in the Validate A Configuration Wizard. Although the exact hardware will depend on the clustered application, a few requirements are standard:

- Server components must be marked with the "Certified for Windows Server 2012 R2" logo.
- Although not explicitly required, server hardware should match and contain the same or similar components.
- All of the Validate A Configuration Wizard tests must pass.

The requirements for Failover Clustering storage have changed from previous versions of Windows. For example, Parallel SCSI is no longer a supported storage technology for any of the clustered disks. There are, however, additional requirements that need to be met for the storage components:

- Disks available for the cluster must be Fibre Channel, iSCSI, or Serial Attached SCSI.
- Each cluster node must have a dedicated network interface card for iSCSI connectivity. The network interface card you use for iSCSI should not be used for network communication.
- Multipath software must be based on Microsoft's Multipath I/O (MPIO).
- Storage drivers must be based on `storport.sys`.
- Drivers and firmware for the storage controllers on each server node in the cluster should be identical.
- Storage components must be marked with the "Certified for Windows Server 2012 R2" logo.

In addition, there are network requirements that must be met for Failover Clustering:

- Cluster nodes should be connected to multiple networks for communication redundancy.
- Network adapters should be the same make, use the same driver, and have the firmware version in each cluster node.
- Network components must be marked with the "Certified for Windows Server 2012 R2" logo.

There are two types of network connections in a failover cluster. These should have adequate redundancy because total failure of either could cause loss of functionality of the cluster. The two types are as follows:

Public Network This is the network through which clients are able to connect to the clustered service application.

Private Network This is the network used by the nodes to communicate with each other.

To provide redundancy for these two network types, additional network adapters would need to be added to the node and configured to connect to the networks.

In previous versions of Windows Server, support was given only when the entire cluster configuration was tested and listed on the Hardware Compatibility List. The tested configuration listed the server and storage configuration down to the firmware and driver versions. This proved to be difficult and expensive from both a vendor and a consumer perspective to deploy supported Windows clusters.

When problems did arise and Microsoft support was needed, it caused undue troubleshooting complexity as well. With Windows Server 2012 R2 Failover Clustering

and simplified requirements, including the "Certified for Windows Server 2012 R2" logo program and the Validate A Configuration Wizard, it all but eliminates the guesswork of getting the cluster components configured in a way that follows best practices and allows Microsoft support to assist you easily when needed.

Cluster Quorum

When a group of people sets out to accomplish a single task or goal, a method for settling disagreements and for making decisions is required. In the case of a cluster, the goal is to provide a highly available service in spite of failures. When a problem occurs and a cluster node loses communication with the other nodes because of a network error, the functioning nodes are supposed to try to bring the redundant service back online.

How, though, is it determined which node should bring the clustered service back online? If all the nodes are functional despite the network communications issue, each one might try. Just like a group of people with their own ideas, a method must be put in place to determine which idea, or node, to grant control of the cluster. Windows Server 2012 R2 Failover Clustering, like other clustering technologies, requires that a quorum exist between the cluster nodes before a cluster becomes available.

A *quorum* is a consensus of the status of each of the nodes in the cluster. Quorum must be achieved in order for a clustered application to come online by obtaining a majority of the votes available (see Figure 17.3). Windows Server 2012 R2 has four quorum models, or methods, for determining quorum and for adjusting the number and types of votes available:

- Node majority (no witness)
- Node majority with witness (disk or file share)
- Node and file share majority
- No majority (disk witness only)

FIGURE 17.3 Majority needed

Witness Configuration

Most administrators follow some basic rules. For example, when you configure a quorum, the voting components in the cluster should be an odd number. For example, if I set up a quorum for five elements and I lose one element, I continue to work. If I lose two elements, I continue to work. If I lose three elements, the cluster stops—as soon as it hits half plus 1, the cluster stops. This works well with an odd number.

If the cluster contains an even number of voting elements, an administrator should then configure a disk witness or a file share witness. The advantage of using a witness (disk or file share) is that the cluster will continue to run even if half of the cluster nodes simultaneously go down or are disconnected. The ability to configure a disk witness is possible only if the storage vendor supports read-write access from all sites to the replicated storage.

One of the advantages of Windows Server 2012 R2 is the advanced quorum configuration option. This option allows you to assign or remove quorum votes on a per-node basis. Administrators now have the ability to remove votes from nodes in certain configurations. For example, if your organization uses a multisite cluster, you may choose to remove votes from the nodes in the backup site. This way, those backup nodes would not affect your quorum calculations.

Dynamic Quorum Management

Another advantage in Windows Server 2012 R2 is dynamic quorum management. *Dynamic quorum management* automatically manages the vote assignment to nodes. With this feature enabled, votes are automatically added or removed from nodes when that node either joins or leaves a cluster. In Windows Server 2012 R2, dynamic quorum management is enabled by default.

Validating a Cluster Configuration

Configuring a failover cluster in Windows Server 2012 R2 is much simpler than in previous versions of Windows Server. Before a cluster can be configured, the Validate A Configuration Wizard should be run to verify that the hardware is configured in a fashion that is supportable. Before you can run the Validate A Configuration Wizard, however, the Failover Clustering feature needs to be installed using Server Manager. The account that is used to create a cluster must have administrative rights on each of the cluster nodes and have permissions to create a cluster name object in Active Directory. Follow these steps:

1. Prepare the hardware and software perquisites.
2. Install the Failover Clustering feature on each server.
3. Log in with the appropriate user ID and run the Validate A Configuration Wizard.
4. Create a cluster.
5. Install and cluster applications and services.

To install the Failover Clustering feature on a cluster node, follow the steps outlined in Exercise 17.2.

EXERCISE 17.2

Installing the Failover Cluster Feature

1. Press the Windows key and select Administrative Tools ➢ Server Manager.
2. Select number 2, Add Roles And Features.
3. At the Select Installation Type screen, choose a role-based or feature-based installation.
4. At the Select Destination Server screen, choose Select A Server From The Server Pool and click Next.
5. At the Select Server Roles screen, click Next.
6. At the Select Features screen, click the Failover Clustering check box. If the Add Features dialog box appears, click the Add Features button. Click Next.
7. At the Confirmation screen, click the Install button.
8. Once the installation is complete, click the Close button.
9. Close Server Manager.

Using the Validate A Configuration Wizard before creating a cluster is highly recommended. This wizard validates that the hardware configuration and the software configuration for the potential cluster nodes are in a supported configuration. Even if the configuration passes the tests, take care to review all warnings and informational messages so that they can be addressed or documented before the cluster is created.

Running the Validate A Configuration Wizard does the following:

- Conducts four types of tests (software and hardware inventory, network, storage, and system configuration)
- Confirms that the hardware and software settings are supportable by Microsoft support staff

You should run the Validate A Configuration Wizard before creating a cluster or after making any major hardware or software changes to the cluster. Doing this will help you identify any misconfigurations that could cause problems with the failover cluster.

Running the Validate a Configuration Wizard

The Validate A Configuration Wizard, shown in Figure 17.4, is simple and straightforward to use, as its "wizard" name would suggest. It should be run after the Failover Clustering feature has been installed on each of the cluster nodes, and it can be run as many times as required.

FIGURE 17.4 The Validate A Configuration Wizard

When you are troubleshooting cluster problems or have changed the configuration of the cluster hardware, it is a good idea to run the Validate A Configuration Wizard again to help pinpoint potential cluster configuration problems.

If you already have a cluster configured and want to run the Validate A Configuration Wizard, you can do so; however, you will not be able to run all of the storage tests without taking the clustered resources offline. You will be prompted either to skip the disruptive tests or to take the clustered resources offline so that the tests can complete.

Exercise 17.3 shows the exact steps to follow to run the Validate A Configuration Wizard successfully on clusters named NODEA and NODEB, which are not yet clustered.

I am using NODEA and NODEB in the exercises. You need to replace these two nodes with your own two servers to complete these exercises.

EXERCISE 17.3

Running the Validate A Configuration Wizard

1. Press the Windows key and select Administrative Tools ➢ Failover Cluster Management.
2. In the Actions pane (right side of screen), click Validate Configuration.

3. At the Before You Begin screen, click Next.
4. Type **NODEA** in the Enter Name field and click Add.
5. Type **NODEB** in the Enter Name field and click Add.

EXERCISE 17.3 *(continued)*

6. Click Next.
7. Leave Run All Tests (Recommended) selected and click Next.
8. Click Next at the Confirmation screen.
9. Let the test complete, review the report in the Summary window, and then click Finish.

Addressing Problems Reported by the Validate A Configuration Wizard

After the Validate A Configuration Wizard has been run, it will show the results, as shown in Figure 17.5. This report can also be viewed in detail later using a web browser. The report is named with the date and time the wizard was run, and it is stored in `%windir%\cluster\Reports`.

FIGURE 17.5 Validate A Configuration Wizard results

How should errors listed in the report be addressed? Often, the errors reported by the Validate A Configuration Wizard are self-explanatory; however, sometimes additional help is required. The following three guidelines should help troubleshoot the errors:

- Read all of the errors because multiple errors may be related.
- Use the checklists available in the Windows Server help files to ensure that all the steps have been completed.
- Contact the hardware vendor for updated drivers, firmware, and guidance for using the hardware in a cluster.

Multisite, Stretched, or Geographically Dispersed Clusters (Geoclustering)

One issue you may face is if you have multiple sites or if the cluster is geographically dispersed. If the failover cluster does not have a shared common disk, data replication between nodes might not pass the cluster validation "storage" tests.

Setting up a cluster in a multisite, stretched, or geocluster (these terms can be used interchangeably) configuration is a common practice. As long as the cluster solution does not require external storage to fail over, it will not need to pass the storage test to function properly.

Creating a Cluster

After you have successfully validated a configuration and the cluster hardware is in a supportable state, you can create a cluster. The process for creating a cluster is straightforward and similar to the process of running the Validate A Configuration Wizard. To create a cluster with two servers, follow the instructions in Exercise 17.4.

EXERCISE 17.4

Creating a Cluster

1. Open the Failover Cluster Management MMC.
2. In the Management section of the center pane, select Create A Cluster.
3. Read the Before You Begin information and click Next.
4. In the Enter Server Name box, type **NODEA** and then click Add.
5. Again, in the Enter Server Name box, type **NODEB** and then click Add. Click Next.
6. At the Validation screen, choose No for this exercise and then click Next.
7. In the Access Point For Administering The Cluster section, enter **Cluster1** for the cluster name.
8. Type an IP address and then click Next. This IP address will be the IP address of the cluster.

EXERCISE 17.4 *(continued)*

9. In the Confirmation dialog box, verify the information and then click Next.
10. On the Summary page, click Finish.

Working with Cluster Nodes

Once a cluster is created, a couple of actions are available. First you can add another node to the cluster by using the Add Node Wizard from the Failover Cluster Management Actions pane.

At this point, you also have the option to pause a node, which prevents resources from being failed over or moved to the node. You typically would pause a node when the node is involved in maintenance or troubleshooting. After a node is paused, it must be resumed to allow resources to be run on it again.

Another action available to perform on a node at this time is *evict*. Eviction is an irreversible process. Once you evict the node, it must be re-added to the cluster. You would evict a node when it is damaged beyond repair or is no longer needed in the cluster. If you evict a damaged node, you can repair or rebuild it and then add it back to the cluster using the Add Node Wizard.

Clustering Roles, Services, and Applications

Once the cluster is created, applications, services, and roles can be clustered. Windows Server 2012 R2 includes a number of built-in roles and features that can be clustered.

The following roles and features can be clustered in Windows Server 2012 R2 (see Figure 17.6):

FIGURE 17.6 High availability roles

- DFS Namespace Server
- DHCP Server
- Distributed Transaction Coordinator (DTC)
- File Server
- Generic Application
- Generic Script
- Generic Service
- Hyper-V Replica Broker
- iSCSI Target Server
- iSNS Server
- Message Queuing
- Other Server
- Virtual Machine
- WINS Server

In addition, other common services and applications can be clustered on Windows Server 2012 R2 clusters:

- Enterprise database services, such as Microsoft SQL Server
- Enterprise messaging services, such as Microsoft Exchange Server

To cluster a role or feature such as Print Services, the first step is to install the role or feature on each node of the cluster. The next step is to use the Configure A Service Or Application Wizard in the Failover Cluster Management tool. Exercise 17.5 shows you how to cluster the Print Services role once an appropriate disk has been presented to the cluster.

EXERCISE 17.5

Clustering the Print Services Role

1. Open the Failover Cluster Management MMC.
2. In the console tree, click the arrow next to the cluster name to expand the items underneath it.
3. Right-click Roles and choose Configure Role.

4. Click Next on the Before You Begin page.
5. Click Other Server on the Select Role screen and then click Next.
6. Type the name of the print server, such as **Print1**, and type in the IP address that will be used to access the print service, such as **80.0.0.34**. Then click Next.

7. At the Select Storage page, just click Next.
8. Click Next at the Confirmation page.
9. After the wizard runs and the Summary page appears, you can view a report of the tasks the wizard performed by clicking View Report.

10. Close the report and click Finish.

The built-in roles and features all are configured in a similar fashion. Other applications, such as Microsoft Exchange Server 2013, have specialized cluster configuration routines that are outside the scope of this exam. Applications that are not developed to be clustered can also be clustered using the Generic Application, Generic Script, or Generic Service option in the Configure A Service Or Application Wizard, as shown in Figure 17.7.

FIGURE 17.7 Configuring a generic application

Clustered Application Settings

Windows Server 2012 R2 has options that allow an administrator to fine-tune the failover process to meet the needs of their business. These options will be covered in the next few sections.

Failover occurs when a clustered application or service moves from one node to another. The process can be triggered automatically because of a failure or server maintenance or can be done manually by an administrator. The failover process works as follows:

1. The cluster service takes all of the resources in the application offline in the order set in the dependency hierarchy.
2. The cluster service transfers the application to the node that is listed next on the application's list of preferred host nodes.
3. The cluster service attempts to bring all of the application's resources online, starting at the bottom of the dependency hierarchy.

NOTE

These steps can change depending on the use of Live Migration.

In a cluster that is hosting multiple applications, it may be important to set specific nodes to be primarily responsible for each clustered application. This can be helpful from a troubleshooting perspective since a specific node is targeted for hosting service. To set a preferred node and an order of preference for failover, use the General tab in the Properties dialog box of the clustered application.

Also, the order of failover is set in this same dialog box by moving the order in which the nodes are listed. If NODEA should be the primary node and NODEC should be the server that the application fails to first, NODEA should be listed first and selected as the preferred owner. NODEC should be listed second, and the remaining cluster nodes should be listed after NODEC.

As shown in Figure 17.8, a number of failover settings can be configured for the clustered service. The failover settings control the number of times a clustered application can fail in a period of time before the cluster stops trying to restart it. Typically, if a clustered application fails a number of times, some sort of manual intervention will be required to return the application to a stable state.

FIGURE 17.8 Clustered application failover settings

Specifying the maximum number of failures will keep the application from trying to restart until it is manually brought back online after the problem has been resolved. This is beneficial because if the application continues to be brought online and then fails, it may show as being functional to the monitoring system, even though it continues to fail. After the application is put in a failed state, the monitoring system will not be able to contact the application and should report it as being offline.

Figure 17.8 also shows the failback settings for Print1. Failback settings control whether and when a clustered application would fail back to the preferred cluster node once it becomes available. The default setting is Prevent Failback. If failback is allowed, two additional options are available, either to fail back immediately after the preferred node is available or to fail back within a specified time.

The time is specified in the 24-hour format. If you want to allow failback between 10 p.m. and 11 p.m., you would set the failback time to be between 22 and 23. Setting a failback time to off-hours is an excellent way to ensure that your clustered applications are running on the designated nodes and automatically scheduling the failover process for a time when it will impact the fewest users.

One tool that is valuable in determining how resources affect other resources is the dependency viewer. The *dependency viewer* visualizes the dependency hierarchy created for an application or service. Using this tool can help when troubleshooting why specific resources are causing failures and allow an administrator to visualize the current configuration better and adjust it to meet business needs. Exercise 17.6 will show you how to run the dependency viewer.

EXERCISE 17.6

Using the Dependency Viewer

1. Open the Failover Cluster Management MMC.
2. In the console tree, click the arrow to expand the cluster.
3. Click Roles.
4. Under the Roles section in the center of the screen, click one of the roles (such as Print1).
5. Right-click the role and under More Actions click Show Dependency Report.

6. Review the dependency report.

7. Close the Dependency Report and close the Failover Cluster Manager.

Exercise 17.6 generated a dependency report that shows how the print service is dependent on a network name and a clustered disk resource. The network name is then dependent on an IP address.

Resource Properties

Resources are physical or logical objects, such as a file share or IP address, which the failover cluster manages. They may be a service or application available to clients, or they may be part of the cluster. Resources include physical hardware devices such as disks and logical items such as network names. They are the smallest configurable unit in a cluster and can run on only a single node in a cluster at a time.

Like clustered applications, resources have a number of properties available for meeting business requirements for high availability. This section covers resource dependencies and policies.

Dependencies can be set on individual resources and control how resources are brought online and offline. Simply put, a dependent resource is brought online after the resources that it depends on, and it is taken offline before those resources. As shown in Figure 17.9, dependencies can be set on a specific resource, such as the print spooler.

FIGURE 17.9 Resource dependencies

Resource policies are settings that control how resources respond when a failure occurs and how resources are monitored for failures. Figure 17.10 shows the Policies tab of a resource's Properties dialog box.

FIGURE 17.10 Resource policies

The Policies tab sets configuration options for how a resource should respond in the event of a failure. The options available are as follows:

If Resource Fails, Do Not Restart This option, as it would lead you to believe, leaves the failed resource offline.

If Resource Fails, Attempt Restart On Current Node With this option set, the resource tries to restart if it fails on the node on which it is currently running. There are two additional options if this is selected so that the number of restarts can be limited. They set the number of times the resource should restart on the current node in a specified length of time. For example, if you specify 5 for Maximum Restarts In The Specified Period and 10:00 (mm:ss) for Period For Restarts, the cluster service will try to restart the resource five times during that 10-minute period. After the fifth restart, the cluster service will no longer attempt to restart the service on the active node.

If Restart Is Unsuccessful, Fail Over All Resources In This Service Or Application If this option is selected, when the cluster service is no longer trying to restart the resource on the active node, it will fail the entire service or application to another cluster node. If you wanted to leave the application or service with a failed resource on the current node, you would clear this check box.

If All The Restart Attempts Fail, Begin Restarting Again After The Specified Period (hh:mm) If this option is selected, the cluster service will restart the resource at a specified interval if all previous attempts have failed.

Pending Timeout This option is used to set the amount of time in minutes and seconds that the cluster service should wait for this resource to respond to a change in states. If a resource takes longer than the cluster expects to change states, the cluster will mark it as having failed. If a resource consistently takes longer than this and the problem cannot be resolved, you may need to increase this value. Figure 17.11 shows the Advanced Policies tab.

FIGURE 17.11 Resource Advanced Policies

The options available on the Advanced Policies tab are as follows:

Possible Owners This option allows an administrator to remove specific cluster nodes from running this resource. Using this option is valuable when there are issues with a resource on a particular node and the administrator wants to keep the applications from failing over to that node until the problem can be repaired.

Basic Resource Health Check Interval This option allows an administrator to customize the health check interval for this resource.

Thorough Resource Health Check Interval This option allows an administrator to customize the thorough health check interval for this resource.

Run This Resource In A Separate Resource Monitor If the resource needs to be debugged by a support engineer or if the resource conflicts with other resources, this option may need to be used.

Windows Server 2012 R2 Clustering Features

Many new features are included in the Windows Server 2012 R2 release for clustering. It is a rich feature set of high availability with greatly improved flexibility based on the needs of IT organizations. The new features relate to quorum behavior, virtual machine hosting, Active Directory–detached clusters, and a new dashboard.

Windows PowerShell Cmdlets for Failover Clusters As I have explained throughout this book, Windows PowerShell is a command-line shell and scripting tool. Windows Server 2012 R2 clustering has new cmdlets that provide powerful ways to script cluster configuration and management tasks. Windows PowerShell cmdlets have now replaced the `Cluster.exe` command-line interface.

Cluster Shared Volumes *Cluster Shared Volumes (CSV)* allows for the configuration of clustered virtual machines. CSV allows you to do the following:

- Reduce the number of LUNs (disks) required for your virtual machines.
- Make better use of disk space. Any VHD file on that LUN can use the free space on a CSV volume.
- More easily track the paths to VHD files and other files used by virtual machines.
- Use a few CSV volumes to create a configuration that supports many clustered virtual machines.

CSV volumes also are utilized for the Scale-Out-File-Server cluster role.

Management of Large-Scale Clusters One new advantage of Windows Server 2012 R2 clusters is the ability for Server Manager to discover and manage the nodes in a cluster. By

starting the Failover Cluster Manager from Server Manager, you can do remote multiserver management and role and feature installation. Administrators now have the ability to manage a cluster from one convenient location.

Management and Mobility of Clustered Virtual Machines As I have stated in previous chapters, Microsoft has built Windows Server 2012 R2 "from the cloud up." Microsoft, as well as the industry as a whole, is moving toward the cloud and virtualization. With that in mind, administrators can now configure settings such as prioritizing the starting or placement of virtual machines in the clustered workloads. This allows administrators to allocate resources efficiently to your cluster.

Cluster-Aware Updating One issue that every administrator has dealt with is updating a system or application while it is running. For example, if you are running Microsoft Exchange and you want to do an Exchange update, when do you take the server offline to do the update? It always seems that someone is on the system 24 hours a day. Well, Windows Server 2012 R2 clustering has a solution. *Cluster-Aware Updating (CAU)* is a new automated feature that allows system updates to be applied automatically while the cluster remains available during the entire update process.

Scale-Out File Server for Application Data By utilizing *Microsoft Storage Spaces*, you can create a highly available clustered file share that utilizes SMB 3.0 and CSV to provide scalable access to data.

Scale-out file servers are useful for storing the following application data:

- Hyper-V virtual machine storage
- SQL Server database files

Be aware that scale-out file servers are not useful at all for typical file share data because they benefit only from applications that require a persistent connection to their storage.

Shared Virtual Hard Disks In the previous versions of Windows, Failover Cluster nodes running as virtual machines had to use iSCSI or virtual HBAs to connect directly to SAN-based storage. With Windows Server 2012 R2, you can set your Hyper-V virtualized cluster to use a shared VHDX virtual disk. Shared virtual hard disks can reside on the following:

- A scale-out file server failover cluster
- Cluster CSV volumes

Shared virtual hard disks are extremely useful in providing highly available shared storage for the following virtualized workloads:

- SQL Server
- Virtual Machine Manager
- Exchange Server

Virtual Machine Drain on Shutdown When needing to perform maintenance on a Hyper-V failover cluster, you may have a lot of virtual machines on one node of a cluster. Inevitably, you will need to restart a cluster node for updates or shut it down for maintenance.

In previous versions of Windows, virtual machines running on the cluster would save their state, and then the cluster node would shut down. Windows Server 2012 R2 helps alleviate this issue by automatically draining the virtual machines running on a node before it shuts down or restarts. Windows does this by attempting to live migrate all virtual machines on the cluster node to other nodes in the cluster when at all possible.

This feature is turned on by default, but it can be disabled through PowerShell.

Active Directory–Detached Clusters Previous versions of Windows Failover Clustering have depended on Active Directory to provide computer objects for the cluster name object as well as virtual computer objects. With Active Directory–detached failover clusters, communication to the cluster-form clients will use NTLM authentication rather than the normal Kerberos authentication. This is useful in maintaining high availability should a person accidently delete a virtual computer object in Active Directory that a clustered resource depends on for Kerberos authentication.

Dynamic Witness Earlier in this chapter, I mentioned the Dynamic Quorum model and how votes were dynamically adjusted based on the number of nodes in a cluster. In Windows Server 2012 R2, there is a new feature called *dynamic witness* that is enabled by default when the cluster is configured to use a dynamic quorum. Since it is preferred to have an odd number of votes at any one time in a cluster, the dynamic witness will turn on or off the witness vote in order to ensure that there are an odd number of votes in the cluster.

Tie Breaker For 50% Node Split Like the *dynamic witness* feature just described, the Tie Breaker For 50% Node Split option in Windows Server 2012 R2 dynamically adjusts cluster node votes in order to maintain an odd number of votes in a cluster where no witness is being used.

This is useful for a cluster in a multisite, stretched, or geocluster configuration.

Global Update Manager Mode Since the first release of Microsoft Cluster Services appearing in Windows NT 4.0 Enterprise, all nodes in a cluster maintain a local database that keeps a copy of the cluster configuration. The *Global Update Manager (GUM)* is a component of the cluster that ensures that before a change is marked as being committed for the entire cluster, all nodes have received and committed that change to their local cluster database. If one or more nodes do not report back or commit a change, the cluster node is kicked out of being a member of the cluster. Another issue that can occur is that for various clustered applications, such as SQL and Exchange, their performance can be negatively impacted by the time it takes the GUM to coordinate with all the nodes of a cluster for any changes. The GUM is only as fast as the slowest node in the cluster.

With Windows Server 2012 R2, a new feature was added to Failover Clustering called *Global Update Manager mode*. This feature allows you to configure the GUM read-write modes manually in order to greatly speed up the processing of changes by the GUM and to improve the performance of certain clustered resources.

Turn Off IPsec Encryption For Inter-node Cluster Communications In network environments where IPsec is used, slow Group Policy updates and other issues can cause

Active Directory Domain Services to be temporarily unavailable to cluster nodes. If the cluster intracluster communications protocol uses IPsec encryption, then these delays could cause cluster nodes to drop out of the cluster for failure to communicate in a timely manner with the rest of the nodes in the cluster. Windows Server 2012 R2 now provides a way to turn off IPsec encryption on the cluster communication network.

Cluster Dashboard Starting with Windows Server 2012, Failover Clustering supports up to 64 nodes in a cluster. Keeping track of the status and resources on all of these nodes can be an administrative headache! Managing more than one failover cluster and determining what a certain cluster hosts can be painful as well. Fortunately, in Windows Server 2012 R2, the *Failover Cluster Manager*'s main dashboard has been updated to make it easier to see the status and health of multiple clusters.

Hyper-V Replica Broker Starting with Windows Server 2012, Hyper-V supported continuous replication of virtual machines to another server or cluster for disaster recovery purposes. The Hyper-V Recovery Broker allows for virtual machines in a cluster to be replicated. The Hyper-V Recovery Broker keeps track of which cluster nodes virtual machines are residing on and ensures that replication is maintained.

Hyper-V Manager Integration into Failover Cluster Manager In Windows Server 2012 R2, the Hyper-V Management Console is integrated with Failover Cluster Manager for managing virtual machines that are clustered. Normal Hyper-V operations such as configuring, exporting, importing, configuring replication, stopping, starting, and live migrating virtual machines are supported directly through Failover Cluster Manager.

Virtual Machine Monitoring Starting with Windows Server 2012, Failover Clustering now supports Virtual Machine Monitoring for Windows Server 2012/2012 R2 virtual machines. Virtual Machine Monitoring monitors administrator-selected Windows services running within a virtual machine and will automatically restart a service if it should fail. If the service does not start for the configured number of restart attempts, the virtual machine will fail over to another node and then restart. For example, you can configure Failover Clustering to monitor the Print Spooler service on a Windows Server 2012 R2 virtual machine. If the Print Spooler service goes offline, then the cluster will attempt to restart the Print Spooler service within the virtual machine. If the service still fails, Failover Clustering will move the virtual machine to another node.

Summary

High availability is more than just clustering. It is achieved through improved hardware, software, and processes. This chapter focused on how to configure Failover Clustering and Network Load Balancing in order to achieve high availability and scalability.

High availability should be approached through proper hardware configuration, training, and operational discipline. Failover clustering provides a highly available base for many applications, such as databases and mail servers.

Network load-balanced clusters are used to provide high availability and scalability for network-based applications, such as VPNs and web servers. Network load balanced clusters can be configured with any edition of Windows Server 2012 R2 except for the Windows Server 2012 R2 Hyper-V Edition.

Exam Essentials

Know how to modify failover and failback settings. These settings are set on the clustered service or application, but they can be modified by settings on the resources.

Know the hardware requirements for Failover Clustering and Network Load Balancing. Failover clustering and Network Load Balancing have distinct hardware requirements. Know the differences.

Review Questions

1. Which of the following editions of Windows Server 2012 R2 can be configured in a failover cluster? (Choose all that apply.)
   - **A.** Windows Server 2012 R2 Hyper-V edition
   - **B.** Windows Server 2012 R2 Standard edition
   - **C.** Windows Server 2012 R2 Foundation edition
   - **D.** Windows Server 2012 R2 Datacenter edition

2. Which of the following editions of Windows Server 2012 can be configured in a Network Load Balancing cluster? (Choose all that apply.)
   - **A.** Windows Server 2012 R2 Essentials edition
   - **B.** Windows Server 2012 R2 Standard edition
   - **C.** Windows Server 2012 R2 Hyper-V edition
   - **D.** Windows Server 2012 R2 Datacenter edition

3. What is the maximum number of nodes that can participate in a Windows Server 2012 failover cluster?
   - **A.** 2
   - **B.** 4
   - **C.** 16
   - **D.** 64

4. Which of the following actions should be performed against an NLB cluster node if maintenance needs to be performed while not terminating current connections?
   - **A.** Evict
   - **B.** Drainstop
   - **C.** Pause
   - **D.** Stop

5. What is the maximum number of nodes that can participate in a Windows Server 2012 R2 NLB cluster?
   - **A.** 4
   - **B.** 8
   - **C.** 16
   - **D.** 32

6. Which of the following applications would be better suited on a failover cluster instead of a network load-balanced cluster? (Choose all that apply.)
   - **A.** SQL Server
   - **B.** Website
   - **C.** Exchange Mailbox Server
   - **D.** VPN services

7. Which of the following applications would be better suited on a Network Load Balancing cluster instead of a failover cluster? (Choose all that apply.)
   - **A.** SQL Server
   - **B.** Website
   - **C.** Database servers
   - **D.** Terminal Services

8. To configure an NLB cluster with unicast, what is the minimum number of network adapters required in each node?
   - **A.** One
   - **B.** Two
   - **C.** Three
   - **D.** Six

9. In a four-node cluster set to a Node And File Share Majority quorum model, how many votes can be lost before quorum is lost?
   - **A.** One
   - **B.** Two
   - **C.** Three
   - **D.** Four

10. In a three-node cluster set to a Node Majority quorum model, how many cluster nodes can be offline before quorum is lost?
    - **A.** Zero
    - **B.** One
    - **C.** Two
    - **D.** Three

Chapter 18

Configure File and Storage Solutions

THE FOLLOWING 70-412 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure advanced file services**

- Configure NFS data store
- Configure BranchCache
- Configure File Classification Infrastructure (FCI) using File Server Resource Manager (FSRM)
- Configure file access auditing

✓ **Implement Dynamic Access Control (DAC)**

- Configure user and device claim types
- Create and configure resource properties and lists
- Create and configure Central Access Rules and Policies
- Configure file classification
- Implement policy changes and staging
- Perform access-denied remediation

✓ **Configure and optimize storage**

- Configure iSCSI Target and Initiator
- Configure Internet Storage Name Server (iSNS)
- Implement thin provisioning and trim
- Manage server free space using Features on Demand
- Configure tiered storage

Taking the time to understand and configure file and storage solutions fully is essential to managing an IT infrastructure efficiently. Companies will rely heavily on your ability as an administrator to properly manage their users and data. In this chapter, you will learn about some of the tools that will help to make you successful in controlling how data is accessed and stored, as well as how users will interact with that data throughout their environment.

Configure Advanced File Services

Windows Server has come a long way in terms of its file and storage capabilities. I have talked quite a bit about the new features and functionality provided in Windows Server 2012 R2. In this section, you will take a closer look at some of the advanced configuration options available in the Network File System (NFS), BranchCache, and the File Server Resource Manager (FSRM).

Configure the NFS Data Store

The NFS role service and feature set gives IT administrators the ability to integrate a Windows Server–based environment with Unix-based operating systems. Most corporate environments today consist of a mixed operating system infrastructure to some extent. Using a Windows NFS file server, you can configure file shares for use by multiple operating systems throughout the environment.

Windows Server 2012 R2 takes those capabilities even further by enabling you to integrate with platforms such as ESXi. ESXi is VMware's exclusive operating system–independent hypervisor. ESXi is referred to as a *bare-metal* operating system because once it is installed on server virtualization hardware, guest virtual machines can be installed without requiring the use of any other underlying operating system. With Windows Server 2012 R2, you can use an NFS share efficiently as an ESXi data store to house all of your guest virtual machines. Let's take a look at configuring an NFS data store in Exercise 18.1.

For this exercise, you will need the following:

- A Windows Server 2012 R2 server
- A VMware ESXi 5 server

EXERCISE 18.1

Configure the NFS Data Store

1. Open Server Manager on your Windows Server 2012 R2 machine.
2. Launch the Add Roles And Features Wizard from the dashboard.
3. Install the Server for NFS role on the server. A reboot is not required.
4. Create a new folder on your server named `NFS_Datastore`, right-click and select Properties, and then navigate to the NFS Sharing tab, as shown here.

5. Click the Manage NFS Sharing button to open the NFS Advanced Sharing page and then check the Share This Folder box, as shown here. Notice how enabling the share also enables the share's default settings. The share settings let you configure share authentication and user access further if the need arises. The default settings will work just fine for this exercise.

EXERCISE 18.1 *(continued)*

6. Click the Permissions tab to open the NFS Share Permissions page. This is where you will configure the type of access that will be allowed by machines accessing this NFS data store. By default, the NFS share permissions are set to Read-Only and do not include root access. For this exercise, you will need to change the type of access to Read-Write and check the box to allow root access, as shown here.

7. Click OK to close the NFS Share Permissions page and then click Apply and OK on the NFS Advanced Sharing page. Your new NFS share is now built, ready to be presented as an NFS data store to a VMware ESXi host. Be sure to record the network path displayed

on the NFS Sharing tab of the share's Properties page. You will need that information to perform a proper mount on the ESXi host.

8. Switch to your ESXi host and launch the Add Storage Wizard from the Configuration tab.

9. On the Select Storage Type page of the wizard, select the Network File System storage type; click Next to continue to the Locate Network File System page.

10. On this page of the wizard, you will fill in the server and folder information for the NFS share that you will be using as a vSphere data store. Using the information recorded from step 7, properly fill out the server and folder fields and then name your new data store as shown here.

11. Click Next to continue to the Ready To Complete page of the wizard. Review the information and click Finish. Once the Create NAS data store task completes on the ESXi host, you are ready to use your Windows Server 2012 R2 shared folder as a vSphere ESXi data store. The graphic shown here confirms that the NFS share is mounted and available from the ESXi host.

The previous exercise shows how versatile Windows Server 2012 R2 shares can be. The same principals can be applied to making Windows Server shares available to other Unix-based operating systems such as ESXi. Now that you have configured a NFS data store, let's take a look at what BranchCache has to offer.

Configure BranchCache

BranchCache is a technology that was introduced with Windows Server 2008 R2 and Windows 7. BranchCache allows an organization with slower links between offices to cache data so that downloads between offices do not have to occur each time a file is accessed.

For example, John comes into work and logs into the network. John accesses the corporate website and downloads a media file that takes four minutes to download. With BranchCache enabled, when Judy comes into work, connects to the corporate website, and tries to download the same media file, the file will be cached from the previous download and Judy will have immediate access to the file.

You can set up two types of BranchCache configurations:

Distributed Cache Mode In the distributed cache mode configuration, all Windows 7 and Windows 8 client machines cache the files locally on the client machines. Thus, in the previous example, after John downloaded the media file, Judy would receive the cached media file from John's Windows 7 or Windows 8 machine.

Hosted Mode In the hosted mode configuration, the cache files are cached on a local (within the site) Windows Server 2012 R2 machine. So, in the previous example, after John downloads the media file, the cached file would be placed on a Windows Server 2012 R2 machine by default, and all other users (Judy) would download the media file from the Windows Server 2012 R2 machine.

Distributed Cache Mode Requirements

If you decide to install BranchCache in the distributed cache mode configuration, a hosted cache server running Windows Server 2012 R2 is not required at the branch office. To set up distributed cache mode, the client machines must be running Windows 7 Enterprise, Windows 7 Ultimate, Windows 8 Pro, or Windows 8 Enterprise.

The Windows 7 or Windows 8 machines would download the data files from the content servers at the main branch office, and then these machines become the local cache servers. To set up distributed cache mode, you must install a Windows Server 2012 R2 content server at the main office first. After the content server is installed, physical connections (WAN or VPN connections) between the sites and branch offices must be established.

Client computers running Windows 7 and Windows 8 have BranchCache installed by default. However, you must enable and configure BranchCache and configure firewall exceptions. Complete Exercise 18.2 to configure BranchCache firewall rule exceptions.

EXERCISE 18.2

Configuring BranchCache Firewall Exceptions

1. On a domain controller, open the Group Policy Management Console.
2. In the Group Policy Management Console, expand the following path: Forest ➢ Domains ➢ Group Policy Objects. Make sure the domain you choose contains the BranchCache Windows 7/Windows 8 client computer accounts that you want to configure.
3. In the Group Policy Management Console, right-click Group Policy Objects and select New. Name the policy **BranchCache Client** and click OK. Right-click BranchCache Client and click Edit. The Group Policy Management Editor console opens.
4. In the Group Policy Management Editor console, expand the following path: Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Windows Firewall With Advanced Security ➢ Windows Firewall With Advanced Security – LDAP ➢ Inbound Rules.
5. Right-click Inbound Rules and then click New Rule. The New Inbound Rule Wizard opens.
6. On the Rule Type screen, click Predefined, expand the list of choices, and then click BranchCache – Content Retrieval (Uses HTTP). Click Next.

EXERCISE 18.2 *(continued)*

7. On the Predefined Rules screen, click Next.
8. On the Action screen, ensure that Allow The Connection is selected and then click Finish. You must select Allow The Connection for the BranchCache client to be able to receive traffic on this port.

9. To create the WS-Discovery firewall exception, right-click Inbound Rules and click New Rule. The New Inbound Rule Wizard opens.
10. On the Rule Type screen, click Predefined, expand the list of choices, and then click BranchCache – Peer Discovery (Uses WSD). Click Next.
11. On the Predefined Rules screen, click Next.
12. On the Action screen, ensure that Allow The Connection is selected and then click Finish.
13. In the Group Policy Management Editor console, right-click Outbound Rules and then click New Rule. The New Outbound Rule Wizard opens.
14. On the Rule Type screen, click Predefined, expand the list of choices, and then click BranchCache – Content Retrieval (Uses HTTP). Click Next.
15. On the Predefined Rules screen, click Next.

16. On the Action screen, make sure that Allow The Connection is selected and then click Finish.
17. Create the WS-Discovery firewall exception by right-clicking Outbound Rules and then click New Rule. The New Outbound Rule Wizard opens.
18. On the Rule Type screen, click Predefined, expand the list of choices, and then click BranchCache – Peer Discovery (Uses WSD). Click Next.
19. On the Predefined Rules screen, click Next.
20. On the Action screen, make sure that Allow The Connection is selected and then click Finish.

Now that you have looked at the distributed cache mode configuration, let's take a look at the hosted mode configuration.

Hosted Mode Requirements

To set up a hosted mode BranchCache configuration, you must first set up a Windows Server 2012 R2 hosted cache server at the main and branch offices. You also need Windows 7 Enterprise, Windows 7 Ultimate, Windows 8 Pro, or Windows 8 Enterprise computers at the branch offices.

The Windows 7 or Windows 8 machines download the data from the main cache server, and then the hosted cache servers at the branch offices obtain a copy of the downloaded data for other users to access.

Your network infrastructure must also allow for physical connections between the main office and the branch offices. These connections can be VPNs or some type of WAN links. After these requirements are met, your cache server must obtain a server certificate so that the client computers in the branch offices can positively identify the cache servers.

Exercise 18.3 walks you through the process of installing the BranchCache feature on a Windows Server 2012 R2 machine. To begin this exercise, you must be logged into the Windows Server 2012 R2 machine as an administrator.

EXERCISE 18.3

Installing BranchCache on Windows Server 2012 R2

1. Open Server Manager by selecting the Server Manager icon or by running `servermanager.exe`.
2. Select Add Roles And Features.
3. Select Next at the Before You Begin pane (if shown).
4. Select Role-Based Or Feature-Based Installation and select Next to continue.
5. Select the Select A Server From The Server Pool option and click Next.
6. At the Select Server Roles screen, click Next.

EXERCISE 18.3 *(continued)*

7. At the Select Features screen, click the check box for BranchCache. Then click Next.

8. Check the Restart The Destination Server If Required box and then click the Install button. If a dialog box appears about restarting, click the Yes button. The system should restart.

9. After the system restarts, log in as the administrator.

Make sure to repeat this exercise on all branch office cache servers. One of the requirements for BranchCache is a physical connection between the main office and the branch offices.

BranchCache and PowerShell

As stated throughout this book, PowerShell is a command-line shell and scripting tool. BranchCache has many different PowerShell cmdlets that allow you to configure and maintain the BranchCache feature. Table 18.1 shows just some of the different PowerShell cmdlets for BranchCache.

TABLE 18.1 PowerShell cmdlets for BranchCache

Cmdlet	Description
`Add-BCDataCache Extension`	Increases the amount of cache storage space that is available on a hosted cache server by adding a new cache file
`Clear-BCCache`	Deletes all data in all data and hash files
`Disable-BC`	Disables the BranchCache service
`Disable-BCDowngrading`	Disables downgrading so that client computers that are running Windows 8 Consumer Preview do not request Windows 7–specific versions of content information from content servers
`Enable-BCDistributed`	Enables BranchCache and configures a computer to operate in distributed cache mode
`Enable-BCHostedClient`	Configures BranchCache to operate in hosted cache client mode
`Enable-BCHostedServer`	Configures BranchCache to operate in hosted cache server mode
`Enable-BCLocal`	Enables the BranchCache service in local caching mode
`Export-BCCachePackage`	Exports a cache package
`Export-BCSecretKey`	Exports a secret key to a file
`Get-BCClient Configuration`	Gets the current BranchCache client computer settings
`Get-BCContent ServerConfiguration`	Gets the current BranchCache content server settings
`Get-BCDataCache`	Gets the BranchCache data cache
`Get-BCStatus`	Gets a set of objects that provide BranchCache status and configuration information
`Import-BCCachePackage`	Imports a cache package into BranchCache
`Import-BCSecretKey`	Imports the cryptographic key that BranchCache uses for generating segment secrets
`Set-BCAuthentication`	Specifies the BranchCache computer authentication mode
`Set-BCCache`	Modifies the cache file configuration
`Set-BCSecretKey`	Sets the cryptographic key used in the generation of segment secrets

Enhanced Features in Windows Server 2012 R2 BranchCache

Microsoft continues to improve on many of the features of Windows Server, and BranchCache is no different. Microsoft has improved BranchCache in Windows Server 2012 R2 and Windows 8. The following list includes some of the enhanced features:

Office sizes and the number of branch offices are not limited. Windows Server 2012 R2 BranchCache allows any number of offices along with any number of users once an administrator deploys hosted cache mode with multiple hosted cache servers.

There are no requirements for a Group Policy object (GPO) for each office location, streamlining deployment. All that is required to deploy BranchCache is a single GPO that contains a small number of settings.

Client computer configuration is automatic. Administrators have the ability to configure their clients through the use of a Group Policy object. If this is done, client configuration will automatically be configured through the GPO, and if a client can't find a hosted cache server, the client will automatically self-configure as a hosted cache mode client.

BranchCache is deeply integrated with the Windows file server. BranchCache is automatically integrated with Windows file server technology. Because of this, the process of finding duplicate pieces in independent files is greatly improved.

Duplicate content is stored and downloaded only once. BranchCache stores only one instance of the content on a hosted cache server or content server, and because of this, you get greater disk storage savings. Since client computers at the remote offices download only one instance of any content, your network saves on additional WAN bandwidth.

Small changes to large files produce bandwidth savings. One advantage of BranchCache is the file server chunking system that helps divide files and web pages into smaller parts. Now when a file is changed, only the part of that file that has been changed gets replicated. This allows BranchCache to use lower bandwidth requirements.

Offline content creation improves performace. When BranchCache is deployed as content or file servers, the data is calculated offline before a client even has the chance to request it. Because of this, the systems get faster performance and bandwidth.

Cache encryption is enabled automatically. BranchCache stores its cached data as encrypted data. This guarantees data security without the need to encrypt the entire drive.

You can deploy multiple hosted cache servers. In Windows 7 and Windows Server 2008 R2, BranchCache was able to deploy only one hosted cache server per office location. Windows Server 2012 R2 allows you to deploy as many hosted cache servers as are needed at a location.

Configure File Classification Infrastructure Using File Server Resource Manager

The *File Server Resource Manager (FSRM)* is a suite of tools that allows an administrator to place quotas on folders or volumes, filter file types, and create detailed storage reports. These tools allow an administrator to plan and implement policies on data properly and as needed.

One of the advantages of using FSRM is all of the included features that allow administrators to manage the data that is stored on their file servers. Some of the features included with FSRM are as follows:

File Management Tasks FSRM allows an administrator to apply a policy or action to data files. Some of the actions that can be performed are encrypting files and running custom commands.

Quota Management Quotas give an administrator the ability to limit how much disk space a user can use on a file server. Administrators have the ability to limit space to an entire volume or to specific folders.

File Classification Infrastructure This feature uses rules to assign specific properties to files automatically and then performs tasks on those files based on the classification. A few examples of file classification properties are Country, Department, Birthday, and Social Security Number. The tasks performed using these classifications include restricting file access, implementing file encryption, and setting file expiration policies.

File Screening Management Administrators can set up file screening on the server and limit what types of files can be stored on that server. For example, an administrator can set a file screen on the server so that any file ending in `·bmp` gets rejected.

Storage Reports Administrators can create reports that show them how data is classified and accessed. You also have the ability to see what users are trying to save unauthorized file extensions.

Installing FSRM is easy when using either Server Manager or PowerShell. To install using Server Manager, you go into Add Features and choose File And Storage Services ➢ File Services ➢ File Server Resource Manager. To install FSRM using PowerShell, use the following command:

```
Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools
```

Configuring FSRM using the Windows GUI version is straightforward, but setting up FSRM using PowerShell is a bit more challenging. Table 18.2 describes some of the PowerShell commands for FSRM.

TABLE 18.2 PowerShell commands for FSRM

PowerShell cmdlet	Description
`Get-FsrmAutoQuota`	Gets auto-apply quotas on a server
`Get-FsrmClassification`	Gets the status of the running file classification
`Get-FsrmClassificationRule`	Gets classification rules
`Get-FsrmFileGroup`	Gets file groups

TABLE 18.2 PowerShell commands for FSRM *(continued)*

PowerShell cmdlet	Description
`Get-FsrmFileScreen`	Gets file screens
`Get-FsrmFileScreenException`	Gets file screen exceptions
`Get-FsrmQuota`	Gets quotas on the server
`Get-FsrmSetting`	Gets the current FSRM settings
`Get-FsrmStorageReport`	Gets storage reports
`New-FsrmAutoQuota`	Creates an auto-apply quota
`New-FsrmFileGroup`	Creates a file group
`New-FsrmFileScreen`	Creates a file screen
`New-FsrmQuota`	Creates an FSRM quota
`New-FsrmQuotaTemplate`	Creates a quota template
`Remove-FsrmClassificationRule`	Removes classification rules
`Remove-FsrmFileScreen`	Removes a file screen
`Remove-FsrmQuota`	Removes an FSRM quota from the server
`Set-FsrmFileScreen`	Changes configuration settings of a file screen
`Set-FsrmQuota`	Changes configuration settings for an FSRM quota

Configure File Access Auditing

One of the most important aspects of controlling security in networked environments is ensuring that only authorized users are able to access specific resources. Although system administrators often spend much time managing security permissions, it is almost always possible for a security problem to occur.

Sometimes the best way to find possible security breaches is actually to record the actions that specific users take. Then, in the case of a security breach (the unauthorized shutdown of a server, for example), system administrators can examine the log to find the cause of the problem.

The Windows Server 2012 R2 operating system and Active Directory offer you the ability to audit a wide range of actions. In the following sections, you'll see how to implement auditing for Active Directory.

Overview of Auditing

The act of *auditing* relates to recording specific actions. From a security standpoint, auditing is used to detect any possible misuse of network resources. Although auditing does not necessarily prevent resources from being misused, it does help determine when security violations have occurred (or were attempted). Furthermore, just the fact that others know that you have implemented auditing may prevent them from attempting to circumvent security.

You need to complete several steps in order to implement auditing using Windows Server 2012 R2:

1. Configure the size and storage settings for the audit logs.
2. Enable categories of events to audit.
3. Specify which objects and actions should be recorded in the audit log.

Note that there are trade-offs to implementing auditing. First, recording auditing information can consume system resources. This can decrease overall system performance and use up valuable disk space. Second, auditing many events can make the audit log impractical to view. If too much detail is provided, system administrators are unlikely to scrutinize all of the recorded events. For these reasons, you should always be sure to find a balance between the level of auditing details provided and the performance-management implications of these settings.

Implementing Auditing

Auditing is not an all-or-none type of process. As is the case with security in general, system administrators must choose specifically which objects and actions they want to audit.

The main categories for auditing include the following:

Audit account logon events

Audit account management

Audit directory service access

Audit logon events

Audit object access

Audit policy change

Audit privilege use

Audit process tracking

Audit system events

In this list of categories, four of the categories are related to Active Directory. Let's discuss these auditing categories in a bit more detail.

Audit Account Logon Events You enable this auditing event if you want to audit when a user authenticates with a domain controller and logs onto the domain. This event is logged in the security log on the domain controller.

Audit Account Management This auditing event is used when you want to watch what changes are being made to Active Directory accounts. For example, when another administrator creates or deletes a user account, it would be an audited event.

Audit Directory Service Access This auditing event occurs whenever a user or administrator accesses Active Directory objects. Let's say that an administrator opens Active Directory and clicks a user account; even if nothing is changed on that account, an event is logged.

Audit Logon Events Account logon events are created for domain account activity. For example, you have a user who logs onto a server so that they can access files; the act of logging onto the server creates this audit event.

Audit Object Access Audit object access allows you to audit objects within your network, such as folders, files, and printers. If you suspect that someone is trying to hack into an object (for example, the `finance` folder), this is the type of auditing you should use. You still would need to enable auditing on the actual object (the `finance` folder in this case).

Audit Policy Change Audit policy change allows you to audit changes to user rights assignment policies, audit policies, or trust policies. This auditing allows you to see whether anyone changes any of the other audit policies.

Audit Privilege Use Setting the audit privilege use allows an administrator to audit each instance of a user exercising a user right. For example, if a user changes the system time on a machine, this is a user right. Logging on locally is another common user right.

To audit access to objects stored within Active Directory, you must enable the Audit Directory Service Access option. Then you must specify which objects and actions should be tracked.

Exercise 18.4 walks you through the steps you must take to implement the auditing of Active Directory objects on domain controllers.

EXERCISE 18.4

Enabling Auditing of Active Directory Objects

1. Open the Local Security Policy tool (located in the Administrative Tools program group).
2. Expand Local Policies ➢ Audit Policy.
3. Double-click the Audit Directory Service Access setting.
4. In the Audit Directory Service Access Properties dialog box, place check marks next to Success and Failure. Click OK to save the settings.
5. Close the Local Security Policy tool.

Viewing Auditing Information

One of the most important aspects of auditing is regularly monitoring the audit logs. If this step is ignored, as it often is in poorly managed environments, the act of auditing is useless. Fortunately, Windows Server 2012 R2 includes the *Event Viewer* tool, which allows system administrators to view audited events quickly and easily. Using the filtering capabilities of Event Viewer, you can find specific events of interest.

Exercise 18.5 walks you through the steps that you must take in order to generate some auditing events and to examine the data collected for these actions. In this exercise, you will perform some actions that will be audited, and then you will view the information recorded within the audit logs.

EXERCISE 18.5

Generating and Viewing Audit Logs

1. Open the Active Directory Users and Computers tool.
2. Within an OU that has auditing enabled, right-click a user account and select Properties.
3. In the user's account Properties dialog box, add the middle initial **A** for this user account and enter **Software Developer** in the Description box. Click OK to save the changes.
4. Close the Active Directory Users and Computers tool.
5. Open the Event Viewer tool from the Administrative Tools program group. Select the Security item under Windows Logs. You will see a list of audited events categorized under Directory Service Access. Note that you can obtain more details about a specific item by double-clicking it.
6. When you have finished viewing the security log, close the Event Viewer tool.

Using the *Auditpol.exe* Command

There may be a time when you need to look at the auditing policies set on a user or system. This is where an administrator can use the `Auditpol.exe` command. Auditpol not only gives administrators the ability to view an audit policy but also lets them set, configure, modify, restore, and even remove an audit policy. Auditpol is a command-line utility, and there are multiple switches that can be used with Auditpol. The following is the syntax used with Auditpol, and table 18.3 describes some of the switches.

```
Auditpol command [<sub-command><options>]
```

Here's an example:

```
Auditpol /get /user:mrice /category:"Detailed Tracking" /r
```

TABLE 18.3 Auditpol commands

Command	Description
`/backup`	Allows an administrator to save the audit policy to a file
`/clear`	Allows an administrator to clear an audit policy
`/get`	Gives administrators the ability to view the current audit policy
`/list`	Allows you to view selectable policy elements
`/remove`	Removes all per-user audit policy settings and disables all system audit policy settings
`/restore`	Allows an administrator to restore an audit policy from a file that was previously created by using `auditpol /backup`
`/set`	Gives an administrator the ability to set an audit policy
`/?`	Displays help

Enhanced Features in Windows Server 2012 R2 Auditing

Auditing in Windows Server 2012 R2 and Windows 8 has been enhanced in many ways. Microsoft has increased the level of detail in the security auditing logs. Microsoft has also simplified the deployment and management of auditing policies. The following list includes some of the major enhancements:

Global Object Access Auditing Administrators using Windows Server 2012 R2 and Windows 8 have the ability to define computer-wide system access control lists (SACLs). Administrators can define SACLs either for the file system or for the registry. After the specified SACL is defined, the SACL is then applied automatically to every object of that type. This can be helpful to administrators for verifying that all critical files, folders, and registry settings on a computer are protected. This is also helpful for identifying when an issue occurs with a system resource.

"Reason For Access" Reporting When an administrator is performing auditing in Windows Server 2012 R2 and Windows 8, they can now see the reason why an operation was successful or unsuccessful. Previously, they lacked the ability to see the reason why an operation succeeded or failed.

Advanced Audit Policy Settings In Windows Server 2012 R2, there are 53 advanced audit policy settings that can be used in place of the 9 basic auditing settings. These advanced audit settings also help eliminate the unnecessary auditing activities that can make audit logs difficult to manage and decipher.

Expression-Based Audit Policies Administrators have the ability, because of Dynamic Access Control, to create targeted audit policies by using expressions based on user,

computer, and resource claims. For example, an administrator has the ability to create an audit policy that tracks all Read and Write operations for files that are considered high-business impact. Expression-based audit policies can be directly created on a file or folder or created through the use of a Group Policy.

Removable Storage Device Auditing Administrators have the ability to monitor attempts to use a removable storage device on your network. If an administrator decides to implement this policy, an audit event is created every time one of your users attempts to copy, move, or save a network resource onto a removable storage device.

Implement Dynamic Access Control

One of the advantages of Windows Server 2012 R2 is the ability to apply data governance to your file server. This will help control who has access to information and auditing. You get these advantages through the use of *Dynamic Access Control (DAC)*. Dynamic Access Control allows you to identify data by using data classifications (both automatic and manual) and then control access to these files based on these classifications.

DAC also gives administrators the ability to control file access by using a central access policy. This central access policy will also allow an administrator to set up audit access to files for reporting and forensic investigation.

DAC allows an administrator to set up Active Directory Rights Management Service (AD RMS) encryption for Microsoft Office documents. For example, you can set up encryption for any documents that contain financial information.

Dynamic Access Control gives an administrator the flexibility to configure file access and auditing to domain-based file servers. To do this, DAC controls claims in the authentication token, resource properties, and conditional expressions within permission and auditing entries.

Administrators have the ability to give users access to files and folders based on Active Directory attributes. For example, a user named Dana is given access to the file server share because in the user's Active Directory (department attribute) properties, the value contains the value Sales. Over the next few sections, you will take a deep dive into implementing Dynamic Access Control.

For DAC to function properly, an administrator must enable Windows 8 computers and Windows Server 2012 R2 file servers to support claims and compound authentication.

Configure User and Device Claim Types

Dynamic Access Control is a must-have for any corporate environment. DAC takes folder and file permissions to a whole new level by enabling more granular methods of access and

authentication within Active Directory. In this section, you will focus on configuring user and device claim types. Let's start off by enabling DAC (see Exercise 18.6).

EXERCISE 18.6

Enable Dynamic Access Control

1. On a domain controller, launch Server Manager and then navigate to the Group Policy Management Console under Tools.
2. Launch Group Policy Management and navigate to Default Domain Controllers Policy.
3. Right-click Default Domain Controllers Policy and select Edit to launch the Group Policy Management Editor.
4. Within the Group Policy Management Editor, navigate to Computer Configuration ➢ Policies ➢ Administrative Templates ➢ System ➢ KDC, as shown here.

5. Double-click the KDC Support For Claims, Compound Authentication, And Kerberos Armoring policy, and select the Enabled radio button, as shown here.

6. Click Apply and OK to save the new policy setting.

That's all there is to it. Now you are ready to take a look at user and device claims. For the next exercise, you will need to have a functional Active Directory environment populated with multiple users across multiple departments. A simple lab environment consisting of a domain controller and a domain-joined file server will be sufficient.

Now that you have successfully enabled DAC within the environment, everything is managed from the Active Directory Administrative Center on a domain controller. You can now set what's referred to as *conditions* on your environment's folder and file server hierarchy. Conditions are user or device claims that you can set. For example, you could set a condition on a folder or file that limits user access to a specific department, or you could set a condition that allows a user to view folders and files from only a specific workstation. Setting these types of conditions will make managing your environment easier, and it will do so with enhanced security. Allowing file and folder access from only domain-joined machines bars users from connecting with an unsecured personal device. Also, setting conditions based upon the Active Directory department attribute makes user access available to those files and folders based on them being in that specific department. Let's put this into practice (see Exercise 18.7).

EXERCISE 18.7

Configure User and Device Claim Types

1. On a domain controller, launch Server Manager and then navigate to the Active Directory Administrative Center under Tools.
2. Launch the Active Directory Administrative Center and navigate to Dynamic Access Control, as shown here.

3. Select New ➢ Claim Type to open the Create Claim Type dialog box.
4. This is where you will choose what claims will be used to define permissions. You can filter claim types with the search field. Search for and select the Department claim type, as shown here. Notice how the Display Name, Description, User Claim Type, and Protect From Accidental Deletion fields are enabled by default.

5. Click OK to finish creating the new claim type. You can now use the Active Directory department attribute as a condition for allowing access on file shares.
6. Navigate to a shared folder within the environment and open the Advanced Security Settings properties on that share.
7. Click the Add button to create a new permission entry.
8. Select a principal. A principal can be any Active Directory user or group. You must select a principal before the option Add A Condition becomes available.
9. Click Add A Condition to bring up the condition's parameters, as shown here. For this exercise, I have selected a user who belongs to the IT department. As long as that user remains in the IT department, the user will have full control over this file share.

10. Click OK to save this new conditional permission entry.

That was just one example of how Dynamic Access Control can be used to control folder and file access. Spend some time configuring different user and device claims types. It is really handy to be able to change a user's department, country, or office location in Active Directory and have that change automatically affect what folders and files that user can access throughout the environment.

Create and Configure Resource Properties and Lists

Now that you have a practical understanding of configuring user and device claims, the next logical Dynamic Access Control configuration is to configure resource properties

and lists. *Resource properties* are used to define additional properties that will appear on files and folders. These additional properties can be used for file access based on file classifications such as country or department. There are quite a few default resource properties already configured in DAC, and you can also create your custom resource properties as needed.

Once you have selected or created resource properties, they are added to the Global Resource Property List within DAC. The default resource properties have already been added for you. Note that any custom resource properties you create will also be added automatically to the Global Resource Property List. The list is then automatically pushed out via Group Policy and downloaded to all of the file servers within the environment. In Exercise 18.8, you will create and configure Resource Properties and Lists.

EXERCISE 18.8

Create and Configure Resource Properties and Lists

1. On a domain controller, launch Server Manager and then navigate to the Active Directory Administrative Center under Tools.
2. Launch the Active Directory Administrative Center and navigate to Dynamic Access Control.
3. Click and open Resource Properties. You will see that all of the default resource properties are listed, but they are all disabled by default.
4. Right-click and enable the Department resource property, as shown here.

5. You'll also create a custom resource property. On the same page that you enabled the Department resource property, click New ➢ Resource Property.
6. Name the resource property **Country** and then click Add to list all of the countries that will be values of this resource property, as shown here.

7. Click OK to create this new resource property.
8. Navigate to and open the global resource property list within the DAC management GUI to verify that both the Country and Department resource properties are enabled and ready to be downloaded to your file servers.

Now that you have defined resource properties, you can use those properties to create and configure central access rules and policies.

Create and Configure Central Access Rules and Policies

Central access rules are used to govern file and folder access based on the resource properties that have been previously defined, such as those you configured in the previous exercise. Let's say you wanted to limit access to a corporate software share to only corporate IT personnel. DAC uses central access rules and policies to accomplish this task. Once the rule has been created, Group Policy will be used to keep all of the environment's file servers up-to-date with all of your dynamic access control central access rules. Exercise 18.9 will demonstrate the configuration of Central Access Rules and Policies.

EXERCISE 18.9

Create and Configure Central Access Rules and Policies

1. On a domain controller, launch Server Manager and then navigate to the Active Directory Administrative Center under Tools.
2. Launch the Active Directory Administrative Center and navigate to Dynamic Access Control.
3. Click and open Central Access Rules. The list should be empty.
4. Click New ➢ Central Access Rule.
5. Provide a name and set proper permissions for the resource, as shown here. For this exercise, I have created a central access rule named Corporate IT Software & Installation Media Access, which will be used to limit user access to IT resources to only members of the IT department.

6. Click OK to create the new central access rule.
7. Navigate to and open Central Access Policies within the DAC management GUI.
8. Click New ➢ Central Access Policy. Note that a central access policy can contain multiple central access rules.
9. Name the central access policy and add the central access rule created in step 6 of this exercise. Your screen should look similar to what's shown here.

10. Now you can configure Group Policy in Active Directory to push out the new central access policy. Launch the Group Policy Manager on your domain controller and edit the default Domain Controllers Policy.

11. Drill down to Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ File System ➢ Central Access Policy and then right-click and select Manage Central Access Policies.

12. Add the central access policy, as shown here.

13. Click OK to save the new central access policy configuration.

By now, I'm sure you can see the power you have with Dynamic Access Control. By taking the time to configure central access rules and policies for your company's users and devices fully, you will enhance environmental security and ease of management significantly. Now that the new central access policy is applied to your environment, all you have to do to finish completely enabling DAC on your file shares is to configure file classification.

Configure File Classification

Administrators can set file classifications and then manage the data more effectively by using these classifications. By classifying files and then setting policies to those classifications, an administrator can set policies on those classifications that assist with managing environmental resources. These policies include restricting file access, file encryption, and file expirations. In Exercise 18.10, you will configure file classification through Dynamic Access Control and then test your work by using the Effective Access tab in the Advanced Security Settings of a file share.

EXERCISE 18.10

Configure File Classification

1. On a DAC-enabled file share, right-click and open Properties.
2. Select the Classification tab and enable values for both the Country and Department file classification properties, as shown here.

3. Click Apply to save the file classification.
4. Select the Security tab and click Advanced.
5. Select the Central Policy tab, making sure the central policy is set to the appropriate central access policy, as shown here. If you change the central access policy, make sure to click Apply before changing tabs.

6. Select the Effective Access tab and test the effective access of a user to test your work.

Implement Policy Changes and Staging

One of the nice features of DAC is its ability to stage and test the effects of a new central access policy before actually implementing it. In Exercise 18.11, you will stage a central access policy and then test the effects of that policy on a file share.

EXERCISE 18.11

Implement Policy Stages and Staging

1. On a domain controller, launch Server Manager and then navigate to the Active Directory Administrative Center under Tools.
2. Launch the Active Directory Administrative Center and navigate to Dynamic Access Control.
3. Click Central Access Rules.

EXERCISE 18.11 *(continued)*

4. Right-click and open the properties of a central access policy.
5. Click the Proposed Permissions section, as shown here, to edit and stage the newly proposed permissions. For demonstration purposes, I have staged a policy change that would allow authenticated users to view the contents of the software library under the conditions that the user is a domain user who is logged into a domain computer.

6. Click OK to set the new policy staging.
7. Switch to your file server and log in as an authenticated user.
8. Run a `gpupdate /force` from the command line to update the Group Policy settings on the file server.
9. As just an authenticated user, browse the share on which you staged your policy change. Notice how you have access as that authenticated user.
10. Now check the Event Viewer on the file server. Expand Windows Logs and then select Security. Under the Central Access Policy Staging task category, open the entries with Event ID 4818. You will notice how the authenticated user was allowed access to this share because of the staging policy.

11. Applying the staged policy is relatively straightforward. Switch to your domain controller and open the properties of the central access rule that was used in step 4 of this exercise. In the Proposed Permissions section, click Apply Proposed to save and enable the staged policy change, as shown here.

12. Verify that the current permissions reflect the applied proposed permissions and then click OK to close the Central Access Rules Properties dialog box.

Perform Access-Denied Remediation

One of the best features of Windows Server 2012 R2 is the ability to configure Access-Denied Assistance. With Access-Denied Assistance, you can set a preconfigured Windows error message to be displayed to users when they try to access resources to which they don't have proper permissions to access. The best part is that users can "request assistance" via the displayed error message. When a user requests assistance, an email notification can notify the administrator who is either on duty or on call that one of their users needs help accessing a resource. When the user requests assistance, they are provided with a dialog box that will be attached to the email sent to the administrator. Within the dialog box, the user can explain why they need access to the desired resource. In Exercise 18.12, you will configure and test Access-Denied Assistance using Group Policy.

EXERCISE 18.12

Configure Access-Denied Assistance

1. On a domain controller, launch Server Manager and then navigate to Group Policy Management under Tools.
2. Launch the Group Policy Management Tool and create a new GPO that targets both your file servers and domain-joined client machines.
3. Within the Group Policy Object Editor, navigate to Computer Configuration ➢ Policies ➢ Administrative Templates ➢ System ➢ Access-Denied Assistance and double-click Customize Message For Access Denied Errors.
4. Enable the policy, configure an access-denied message that will be displayed to users who are denied access, and check the box to enable users to request assistance, as shown here.

One of the great things about this policy is that it comes with preconfigured macros you can use to automate the access-denied message that will be displayed to users. Here are the four macros available within the access-denied message:

`[Original File Path]`: The original file path that was accessed by the user

`[Original File Path Folder]`: The parent folder of the original file path that was accessed by the user

`[Admin Email]`: The administrator email recipient list

`[Data Owner Email]`: The data owner email recipient list

For this exercise, I have configured the following access-denied message: "You do not currently have access to [*Original File Path*]. Please click the Request Assistance button to send [*Admin Email*] an email requesting assistance."

5. Click OK to save and close the policy.
6. Invoke the Enable Access-Denied Assistance On Client For All File Types policy here as well.
7. Launch the File Server Resource Manager on one of your file servers to configure the email notification settings for the access-denied assistance email service.
8. Within the File Server Resource Manager, click Configure Options to configure the SMTP server and email addresses that will be used for access-denied assistance email notifications, as shown here.

9. Click the Send Test Email button to verify your settings.
10. Click OK to save the configuration.
11. Test your work by trying to access a resource as a user who does not have permission for that resource and then use the Request Assistance feature to ask for help.

Configure and Optimize Storage

Disk storage is a requirement for just about every computer and application used in any corporate environment. Administrators have some familiarity with storage, whether it is internal storage, a locally attached set of disks, or network attached storage (NAS). In this section, you will examine the various aspects of Windows Server 2012 R2 file and storage solutions. Though I'll discuss the various types of file and storage technologies, this section will primarily focus on iSCSI because of the native features in Windows Server 2012 R2. You will also look at some of the advanced configuration options of implementing thin provisioning and trim, managing server free space, and configuring tiered storage.

Configure iSCSI Target and Initiator

Internet Small Computer System Interface (iSCSI) is an Internet protocol used to establish and manage a connection between a computer (initiator) and a storage device (target). It does this by using a connection through TCP port 3260, which allows it to be used over a LAN, a WAN, or the Internet. Each initiator is identified by its iSCSI Qualified Name (iqn), and it is used to establish its connection to an iSCSI target.

iSCSI was developed to allow block-level access to a storage device over a network. This is different from using a NAS device that connects through the use of Common Internet File System (CIFS) or NFS.

Block-level access is important to many applications that require direct access to storage. Microsoft Exchange and Microsoft SQL are examples of applications that require direct access to storage.

By being able to leverage the existing network infrastructure, iSCSI was also developed as an alternative to Fibre Channel storage by alleviating the additional hardware costs associated with a Fibre Channel storage solution.

iSCSI also has another advantage over Fibre Channel in that it can provide security for the storage devices. iSCSI can use Microsoft Challenge Handshake Authentication Protocol (CHAP or MS-CHAP) for authentication and Internet Protocol Security (IPsec) for encryption. Windows Server 2012 R2 is able to connect an iSCSI storage device out of the box with no additional software needing to be installed. This is because the Microsoft iSCSI initiator is built into the operating system.

Windows Server 2012 R2 supports two different ways to initiate an iSCSI session:

- Through the native Microsoft iSCSI software initiator that resides on Windows Server 2012 R2
- Using a hardware iSCSI host bus adapter (HBA) that is installed in the computer

Both the Microsoft iSCSI software initiator and iSCSI HBA present an iSCSI qualified name that identifies the host initiator. When the Microsoft iSCSI software initiator is used, the CPU utilization may be as much as 30 percent higher than on a computer with a hardware iSCSI HBA. This is because all of the iSCSI process requests are handled within the operating system. Using a hardware iSCSI HBA, process requests can be offloaded to

the adapter, thus freeing the CPU overhead associated with the Microsoft iSCSI software initiator. However, iSCSI HBAs can be expensive, whereas the Microsoft iSCSI software initiator is free.

It is worthwhile installing the Microsoft iSCSI software initiator and performing load testing to see how much overhead the computer will have prior to purchasing an iSCSI HBA or HBAs, depending on the redundancy level. Exercise 18.13 explains how to install and configure an iSCSI connection.

EXERCISE 18.13

Configuring iSCSI Storage Connection

1. Press the Windows key or the Start button in the lower-left corner and select Administrative Tools ➢ iSCSI Initiator.
2. If a dialog box appears, click Yes to start the service.
3. Click the Discovery tab.

4. In the Target Portals portion of the page, click Discover Portal.

EXERCISE 18.13 *(continued)*

5. Enter the IP address of the target portal and click OK.
6. The IP address of the target portal appears in the Target Portals box.

7. Click OK.

   To use the storage that has now been presented to the server, you must create a volume on it and format the space.

Configure Internet Storage Name Server

Internet Storage Name Service (iSNS) allows for the central registration of an iSCSI environment because it automatically discovers available targets on the network. The purpose of iSNS is to help find available targets on a large iSCSI network.

The Microsoft iSCSI initiator includes an iSNS client that is used to register with the iSNS. The iSNS feature maintains a database of clients that it has registered either through DCHP discovery or through manual registration. iSNS DHCP is available after the installation of the service, and it is used to allow iSNS clients to discover the location of the iSNS. However, if iSNS DHCP is not configured, iSNS clients must be registered manually with the `iscsicli` command.

To execute the command, launch a command prompt on a computer hosting the Microsoft iSCSI and type **`iscsicli addisnsserver server_name`**, where `server_name` is the name of the computer hosting iSNS. Exercise 18.14 walks you through the steps required to install the iSNS feature on Windows Server 2012 R2, and then it explains the different tabs in iSNS.

EXERCISE 18.14

Installing the iSNS Feature on Windows Server 2012 R2

1. Open Server Manager.
2. Launch the Add Roles And Features Wizard.
3. Choose role-based or featured-based installation and click Next.
4. Choose your server and click Next.
5. Click Next at the Roles screen.
6. At the Select Features screen, choose the iSNS Server Service check box. Click Next.

EXERCISE 18.14 *(continued)*

7. At the Confirmation screen, click the Install button.
8. Click the Close button. Close Server Manager and reboot.
9. Log in and open the iSNS server under Administrative Tools.
10. Click the General tab. This tab displays the list of registered initiators and targets. In addition to their iSCSI qualified names, it lists storage node type (Target or Initiator), alias string, and entity identifier (the fully qualified domain name [FQDN] of the machine hosting the iSNS client).
11. Click the Discovery Domains tab. The purpose of discovery domains is to provide a way to separate and group nodes. This is similar to zoning in Fibre Channel.

    The following options are available on the Discovery Domains tab:

    Create creates a new discovery domain.

    Refresh repopulates the Discovery Domain drop-down list.

    Delete deletes the currently selected discovery domain.

    Add adds nodes that are already registered in iSNS to the currently selected discovery domain.

    Add New adds nodes by entering the iSCSI qualified name of the node. These nodes do not have to be currently registered.

    Remove Used removes selected nodes from the discovery domain.

12. Click the Discovery Domain Sets tab. The purpose of discovery domain sets is to separate further discovery domains. Discovery domains can be enabled or disabled, giving administrators the ability to restrict further the visibility of all initiators and targets.

    The options on the Discovery Domain Sets tab are as follows:

    The *Enable* check box indicates the status of the discovery domain sets and turns them off and on.

    Create creates new discovery domain sets.

    Refresh repopulates the Discovery Domain Sets drop-down list.

    Delete deletes the currently selected discovery domain set.

    Add adds discovery domains to the currently selected discovery domain set.

    Remove removes selected nodes from the discovery domain sets.

13. Close the iSNS server.

Implement Thin Provisioning and Trim

Thin provisioning and trim can be useful features that allow organizations to get the most out of their storage arrays. These solutions apply directly to a virtualized environment using virtual disks that are thin provisioned.

Thin provisioning is a way of providing what is known as just-in-time allocations. Blocks of data are written to disk only as they are used instead of zeroing out all of the blocks of data that have been allocated to the virtual disk configuration. Thin provisioning is tricky to manage properly because you could easily find yourself in a position where you have an over-provisioned environment because of over-allocation.

For example, you have 100 VMs that are all provisioned with 40GB thin-provisioned virtual disks. Each VM is currently utilizing only 20GB of the total 40GB that has been allocated. The problem is that you have only 2TB worth of storage. Without realizing it, you've over-provisioned your environment by 200 percent because of thin provisioning.

This is where trim comes in to help us manage thin provisioning. *Trim* automatically reclaims free space that is not being used. In addition to trim, Windows Server 2012 R2 provides standardized notifications that will alert administrators when certain storage thresholds are crossed.

Manage Server Free Space Using Features on Demand

Features on Demand was first introduced in Windows Server 2012. This feature lets you conserve disk space within the environment by installing only basic operating system components with every new installation of a Windows Server 2012 R2 or Windows 8 machine. Instead of loading unnecessary payload files, those files are stored in a central repository and used as needed to install roles and features. When I talk about *payload files*, I am talking about the binaries for all permissions, settings, and components of a feature. Features on Demand gives you the ability not only to disable Windows Server features but also to remove all of the payloads. This lets administrators keep a tighter security footprint at the operating system level, which is similar to a Server Core installation but without the limitation of not being able to control which source files are loaded during operating system installation.

Configure Tiered Storage

Tiered storage is an excellent new feature in Windows Server 2012 R2 that gives administrators the ability to use solid-state drives (SSDs) and conventional hard-disk drives (HDDs) within the same storage pool. You can configure virtual disks that span SSD and HDD tiers, which are presented as a single LUN. One of the really nice things about this feature is that with Windows Server 2012 R2, data is automatically saved to either an SSD or an HDD based on actual usage within the environment. Most frequently accessed data is stored on an SSD, and the less frequently accessed data is stored on an HDD.

Quite a few organizations these days use some sort of charge-back or show-back application to track and even charge for hosted solutions and services. Having the capability to tier storage gives users more options in selecting a plan that works for them. It also makes it possible for administrators to keep high I/O servers and applications on faster and better-performing drives without having to move data manually across multiple tiers of storage.

Summary

In this chapter, I discussed how configuring file and storage solutions can be highly effective within your organization. You now have a better understanding of how Windows Server 2012 R2 can provide you with extended functionality for effectively controlling corporate data. Quite a few of these solutions are essential to managing a Windows Server environment to the best of your ability. Take the time to complete each exercise thoroughly until you are comfortable with performing the majority of these tasks without documentation.

You learned how to configure and test some of the great features provided by Dynamic Access Control. Many of the exam questions will involve using both DAC and FSRM to manage and control shared resources. You will also want to focus heavily on auditing capabilities and the storage solutions talked about throughout the chapter. Configure and test the full extent of all of these applications and solutions to prepare appropriately for the exam.

Exam Essentials

Understand the purpose and function of auditing. Auditing helps determine the cause of security violations and helps troubleshoot permissions-related problems. Configure and test the effects of auditing within a file share hierarchy in a lab environment.

Know storage technologies. Understand how to use the Fibre Channel, iSCSI, and NAS storage technologies. Know how to configure an iSCSI initiator and how to establish a connection to a target. Practice configuring tiered storage and using thin provisioning and trim.

Understand the features and functionality of BranchCache. BranchCache helps eliminate the problems of slow access and bandwidth issues when sharing data across multiple, geographically disparate locations. By syncing and caching data between sites, users can use company-wide shared resources more efficiently when slower site links exist between site locations.

Know how to configure Dynamic Access Control. DAC has a wide array of features and functionality that will make an administrator's job of controlling file and folder access much easier. It will also provide tighter data security and data classification throughout the environment.

Understand file classification. File classification is used when an administrator needs to manage and control both the type and the amount of data that is stored on their servers. You can use both Dynamic Access Control and the File Sever Resource Manager to implement file classification.

Review Questions

1. LaDonna is a system administrator for an Active Directory environment that is running in Native mode. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:
   - The accessing of certain sensitive files must be logged.
   - Modifications to certain sensitive files must be logged.
   - System administrators must be able to provide information about which users accessed sensitive files and when they were accessed.
   - All logon attempts for specific shared machines must be recorded.

   Which of the following steps should LaDonna take to meet these requirements? (Choose all that apply.)

   A. Enable auditing with the Computer Management tool.
   B. Enable auditing using the Group Policy Management Console.
   C. Enable auditing with the Active Directory Domains and Trusts tool.
   D. Enable auditing with the Event Viewer tool.
   E. View the audit log using the Event Viewer tool.
   F. View auditing information using the Computer Management tool.
   G. Enable failure and success auditing settings for specific files stored on NTFS volumes.
   H. Enable failure and success auditing settings for logon events on specific computer accounts.

2. What is the default TCP port for iSCSI?

   A. 3260
   B. 1433
   C. 21
   D. 3389

3. You create a GPO and link it to the Engineering OU. You want to monitor users in the Engineering OU who connect to the file server. What type of auditing do you enable?

   A. Audit object access
   B. Audit system events
   C. Audit logon events
   D. Audit process tracking

4. You have been hired by a small company to implement new Windows Server 2012 R2 systems. The company wants you to set up a server for users' home folder locations. What type of server would you be setting up?
   - **A.** File server
   - **B.** Web server
   - **C.** Exchange server
   - **D.** PDC server

5. Your company has decided to implement a Windows 2012 R2 server. The company IT manager before you always used FAT32 as the system partition. Your company wants to know whether it should move to NTFS. Which of the following are some advantages of NTFS? (Choose all that apply.)
   - **A.** Security
   - **B.** Quotas
   - **C.** Compression
   - **D.** Encryption

6. What command would be used to register an iSCSI initiator manually to an iSNS server?
   - **A.** `iscsicli refreshisnsserver server_name`
   - **B.** `iscsicli listisnsservers server_name`
   - **C.** `iscsicli removeisnsserver server_name`
   - **D.** `iscsicli addisnsserver server_name`

7. You are a server administrator, and you are trying to save hard drive space on your Windows Server 2012 R2 machine. Which feature can help you save hard disk space?
   - **A.** Features On Demand
   - **B.** `HDSaver.exe`
   - **C.** WinRM
   - **D.** ADDS

8. You are an IT administrator who manages an environment that runs multiple Windows Server 2012 R2 servers from multiple site locations across the United States. Your Windows Server 2012 R2 machines use iSCSI storage. Other administrators report it is difficult to locate available iSCSI resources on the network. You need to make sure other administrators can easily access iSCSI resources using a centralized repository. What feature should you deploy?
   - **A.** The iSCSI Target Storage Provider feature
   - **B.** The Windows Standards-Based Storage Management feature
   - **C.** The iSCSI Target Server role feature
   - **D.** The iSNS Server service feature

9. Your company is headquartered in Colorado Springs and has a remote site location in Tampa. The Colorado Spring office has a file server named FS01. FS01 has the BranchCache for Network Files role service installed. Your Tampa Office has a file server named FS02. FS02 has been configured as a BranchCache hosted cache server. You need to preload the data from the file shares on FS01 to the cache on FS02. You have already generated hashes for the file shares on FS01. Which cmdlet should you run next?
   - **A.** `Export-BCCachePackage`
   - **B.** `Publish-BCFileContent`
   - **C.** `Set-BCCache`
   - **D.** `Add-BCDataCacheExtension`

10. You have a Windows Server 2012 R2 file server named FS01. FS01 has the File Server Resource Manager role service installed. You attempt to delete a classification property, and you receive the error message "The classification property is in use and cannot be deleted." You need to delete the Contains Personal Information classification property. What should you do?
    - **A.** Clear the Contains Personal Information classification property value for all files.
    - **B.** Delete the classification rule that is assigned the Contains Personal Information classification property.
    - **C.** Disable the classification rule that is assigned the Contains Personal Information classification property.
    - **D.** Set files that have a Contains Personal Information classification property value of Yes to No.

Chapter 19

Implement Business Continuity and Disaster Recovery

THE FOLLOWING 70-412 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure and manage backups**

- Configure Windows Server backups
- Configure Windows Azure backups
- Configure role-specific backups
- Manage VSS settings using VSSAdmin

✓ **Recover Servers**

- Restore from backups
- Perform a Bare Metal Restore (BMR)
- Recover servers using Windows Recovery Environment (Win RE) and safe mode
- Configure the Boot Configuration Data (BCD) store

✓ **Configure site-level fault tolerance**

- Configure Hyper-V Replica including Hyper-V Replica Broker and VMs
- Configure multi-site clustering including network settings, Quorum, and failover settings
- Configure Hyper-V Replica extended replication
- Configure Global Update Manager
- Recover a multi-site failover cluster

Throughout this book, I have stressed the importance of setting up your network properly. Once your network is set up and running properly, your users will get the most functionality out of the network. Your users will also become dependent on the network. Try taking a network offline for even 10 minutes, and your users will scream and complain.

Now that you have your users hooked, you must protect the network and the data. If your company loses their data, can they survive? Probably not. Most companies would go bankrupt if they lost all of their data and had no way to recover it. Data protection and recoverability is one of the most critical jobs you have as an administrator.

It is important to have multiple servers available to provide backup in case of a problem. The same goes for Active Directory itself—it too should be backed up. This way, if there is a massive disaster after which you need to restore your directory services, you will have that option available to you.

The process of reformatting a computer from scratch after a catastrophic system failure is a bare-metal restore and usually involves reinstalling the operating system and all of the system software.

In this chapter, you will learn about all the different ways to protect and recover your system.

NOTE

Some of the text in this chapter is repeated from Chapter 15 due to its relevancy and importance to both Exam 70-411 and Exam 70-412.

Protecting the System

One of the worst events you will experience is a computer that won't boot. But far worse is discovering that there is no recent backup for that computer.

The first step in preparing for disaster recovery is to expect that a disaster will happen at some point and to take proactive measures to plan for recovery before the failure occurs. Here are some of the preparations you can make:

- Keep your computer up-to-date with Windows Update.
- Perform regular system backups.
- Use current software to scan for malware (such as viruses, spyware, and adware) and make sure you have the most recent updates.
- Perform regular administrative functions, such as monitoring the logs in the Event Viewer utility.

If you can't start Windows Server 2012 R2, you can use several options and utilities to identify and resolve Windows errors. The following is a broad list of troubleshooting options:

- If you have recently made a change to your computer's configuration by installing a new device driver or application and Windows Server 2012 R2 will not load properly, you can use the Last Known Good Configuration, roll back the driver, or use System Restore to restore a previous system configuration.
- If you can boot your computer to Safe Mode and you suspect you have a system conflict, you can temporarily disable an application or processes, troubleshoot services, or uninstall software.
- If your computer will not boot to Safe Mode, you can use the Startup Repair tool to replace corrupted system files.
- If necessary, you can use the Windows Server Backup utility to restore files from backup media and to restore a complete image of your computer.

To safeguard your server, one of the most important functions is to protect Active Directory. Active Directory is the heart and soul of a Microsoft network, and losing your data would be a catastrophic event. So, let's start by discussing how to protect Active Directory.

Backup and Recovery of Active Directory

If you have deployed Active Directory in your network environment, your users now depend on it to function properly in order to do their jobs. From network authentications to file access to print and web services, Active Directory has become a mission-critical component of your business. Therefore, the importance of backing up the Active Directory data store should be evident.

As I discussed in earlier chapters, it is important to have multiple domain controllers available to provide backup in case of a problem. The same goes for Active Directory itself—it too should be backed up by being saved. This way, if a massive disaster occurs in which you need to restore your directory services, you will have that option available to you.

Backups are just good common sense, but here are several specific reasons to back up data:

Protect Against Hardware Failures Computer hardware devices have finite lifetimes, and all hardware eventually fails. I discussed this when I mentioned MTBF earlier in the book. *Mean Time Between Failures (MTBF)* is the average time a device will function before it actually fails. There is also a rating derived from benchmark testing of hard disk devices that tells you when you may be at risk for an unavoidable disaster. Some types of failures, such as corrupted hard disk drives, can result in significant data loss.

Protect Against Accidental Deletion or Modification of Data Although the threat of hardware failures is real, in most environments mistakes in modifying or deleting data are much more common. For example, suppose a system administrator accidentally deletes all of the objects within a specific OU. Clearly, it's important to be able to retrieve this information from a backup.

Keep Historical Information Users and system administrators sometimes modify files and then later find out that they require access to an older version of the file. Or a file is accidentally deleted, and a user does not discover that fact until much later. By keeping multiple backups over time, you can recover information from prior backups when necessary.

Protect Against Malicious Deletion or Modification of Data Even in the most secure environments, it is conceivable that unauthorized users (or authorized ones with malicious intent!) could delete or modify information. In such cases, the loss of data might require valid backups from which to restore critical information.

Windows Server 2012 R2 includes a Backup utility that is designed to back up operating system files and the Active Directory data store. It allows for basic backup functionality, such as scheduling backup jobs and selecting which files to back up. Figure 19.1 shows the main screen of the Windows Server 2012 R2 Backup utility.

FIGURE 19.1 The main screen of the Windows Server 2012 R2 Backup utility

In the following sections, you'll learn about the details of using the Windows Server 2012 R2 Backup utility and how you can restore Active Directory when problems do occur.

Overview of the Windows Server 2012 R2 Backup Utility

Although the general purpose behind performing backup operations—protecting information—is straightforward, system administrators must consider many options when

determining the optimal backup-and-recovery scenario for their environment. Factors include what to back up, how often to back up, and when the backups should be performed.

In this section, you'll see how the Windows Server 2012 R2 Backup utility makes it easy to implement a backup plan for many network environments.

Although the Windows Server 2012 R2 Backup utility provides the basic functionality required to back up your files, you may want to investigate third-party products that provide additional functionality. These applications can provide options for specific types of backups (such as those for Exchange Server and SQL Server) as well as disaster recovery options, networking functionality, centralized management, and support for more advanced hardware.

Backup Types

One of the most important issues you will have to deal with when you are performing backups is keeping track of which files you have backed up and which files you need to back up. Whenever a backup of a file is made, the archive bit for the file is set. You can view the attributes of system files by right-clicking them and selecting Properties. By clicking the Advanced button in the Properties dialog box, you will access the Advanced Attributes dialog box. Here you will see the option Folder Is Ready For Archiving. Figure 19.2 shows an example of the attributes for a folder.

FIGURE 19.2 Viewing the archive attributes for a folder

Although it is possible to back up all of the files in the file system during each backup operation, it's sometimes more convenient to back up only selected files (such as those that have changed since the last backup operation). When performing backups, you can back up to removable media (DVD) or to a network location.

It is recommended by Microsoft to do a backup to a network location. The reason for this is that if your company suffers from a disaster (fire, hurricane, and so forth), your data can all still be lost—including the backup. If you back up to a removable media source, a copy of the backup can be taken offsite. This protects against a major disaster.

Although Windows Server 2012 R2 does not support all of these backup types, it's important to understand the most common backup types. Most administrators use third-party software for their backups. That's why it's important to know all of the different types.

Several types of backups can be performed:

Normal Normal backups (also referred to as *system* or *full backups*) back up all of the selected files and then mark them as backed up. This option is usually used when a full system backup is made. Windows Server 2012 R2 supports this backup.

Copy *Copy backups* back up all of the selected files but do not mark them as backed up. This is useful when you want to make additional backups of files for moving files offsite or you want to make multiple copies of the same data for archival purposes.

Incremental *Incremental backups* copy any selected files that are marked as ready for backup (typically because they have not been backed up or they have been changed since the last backup) and then mark the files as backed up. When the next incremental backup is run, only the files that are not marked as having been backed up are stored. Incremental backups are used in conjunction with normal (full) backups.

The most common backup process is to make a full backup and then make subsequent incremental backups. The benefit to this method is that only files that have changed since the last full or incremental backup will be stored. This can reduce backup times and disk or tape storage space requirements.

When recovering information from this type of backup method, a system administrator must first restore the full backup and then restore each of the incremental backups.

Differential *Differential backups* are similar in purpose to incremental backups with one important exception: Differential backups copy all files that are marked for backup but do not mark the files as backed up. When restoring files in a situation that uses normal and differential backups, you need only restore the normal backup and the latest differential backup.

Daily *Daily backups* back up all of the files that have changed during a single day. This operation uses the file time/date stamps to determine which files should be backed up and does not mark the files as having been backed up.

Backing Up System State Data

When you are planning to back up and restore Active Directory, be aware that the most important component is known as the *system state data*. System state data includes the components upon which the Windows Server 2012 R2 operating system relies for normal operations. The Windows Server 2012 R2 Backup utility offers you the ability to back up the system state data to another type of media (such as a hard disk or network share).

Specifically, it will back up the following components for a Windows Server 2012 R2 domain controller:

Active Directory The *Active Directory data store* is at the heart of Active Directory. It contains all of the information necessary to create and manage network resources, such as users and computers. In most environments that use Active Directory, users and system administrators rely on the proper functioning of these services in order to do their jobs.

Boot Files *Boot files* are the files required for booting the Windows Server 2012 R2 operating system and can be used in the case of boot file corruption.

COM+ Class Registration Database The *COM+ class registration database* is a listing of all the COM+ class registrations stored on the computer. Applications that run on a Windows Server 2012 R2 computer might require the registration of various share code components. As part of the system state backup process, Windows Server 2012 R2 stores all of the information related to Component Object Model+ (COM+) components so that it can be quickly and easily restored.

Registry The Windows Server 2012 R2 *registry* is a central repository of information related to the operating system configuration (such as desktop and network settings), user settings, and application settings. Therefore, the registry is absolutely vital to the proper functioning of Windows Server 2012 R2.

Sysvol Directory The *Sysvol directory* includes data and files that are shared between the domain controllers within an Active Directory domain. Many operating system services rely on this information in order to function properly.

Bare-Metal Backups and Restores

One of the options you have in Windows Server 2012 R2 is to do a *bare-metal restore (BMR)*. This is a restore of a machine after the machine has been completely wiped out and formatted. This type of restore is done usually after a catastrophic machine failure or crash.

Windows Server 2012 R2 gives you the ability to back up all of the files needed for a bare-metal restore by choosing the Bare Metal Recovery check box (see Figure 19.3).

FIGURE 19.3 Bare Metal Recovery option

When you choose the Bare Metal Recovery option in Windows Server 2012 R2, all of the suboptions (System State, System Reserved, and Local Disk) automatically get checked.

When preparing your network for a bare-metal backup, you want to make sure you have everything you need on hand to complete this type of restore. You may want to keep a copy of the server software, server drivers, and so forth, on hand and ready to go, just in case you have to do a full restore.

Scheduling Backups

In addition to specifying which files to back up, you can schedule backup jobs to occur at specific times. Planning *when* to perform backups is just as important as deciding *what* to back up. Performing backup operations can reduce overall system performance; therefore, you should plan to back up information during times of minimal activity on your servers.

To add a backup operation to the schedule, you can simply click the Add button in the Specify Backup Time window.

Restoring System State Data

In some cases, the Active Directory data store or other system state data may become corrupt or unavailable. This could be because of many different reasons. A hard disk failure might, for example, result in the loss of data. Or the accidental deletion of an OU and all of its objects might require a restore operation to be performed.

The actual steps involved in restoring system state data are based on the details of what has caused the data loss and what effect this data loss has had on the system. In the best-case scenario, the system state data is corrupt or inaccurate, but the operating system can still boot. If this is the case, all you must do is boot into a special *Directory Services Restore Mode (DSRM)* and then restore the system state data from a backup. DSRM is available only on a domain controller. This process will replace the current system state data with that from the backup. Therefore, any changes that have been made since the last backup will be completely lost and must be redone.

In a worst-case scenario, all of the information on a server has been lost or a hardware failure is preventing the machine from properly booting. If this is the case, here are the steps you must take in order to recover system state data:

1. Fix any hardware problem that might prevent the computer from booting (for example, replace any failed hard disks).
2. Reinstall the Windows Server 2012 R2 operating system. This should be performed like a regular installation on a new system.
3. Reinstall any device drivers that may be required by your backup device. If you backed up information to the file system, this will not apply.

4. Restore the system state data using the Windows Server 2012 R2 Backup utility. When restoring the system state data on a domain controller, you must specify either an authoritative or nonauthoritative restore.

I'll cover the technical details of performing restores later in this chapter. For now, however, you should understand the importance of backing up information and, whenever possible, testing the validity of backups.

Backing Up and Restoring Group Policy Objects

Group Policy objects (GPOs) are a major part of Active Directory. When you back up Active Directory, GPOs can also get backed up. You also have the ability to back up GPOs through the Group Policy Management Console (GPMC). This gives you the ability to back up and restore individual GPOs.

To back up all GPOs, open the GPMC and right-click the Group Policy Objects container. You will see the option Back Up All. After you choose this option, a wizard will start asking you for the backup location. Choose a location and click Backup.

To back up an individual GPO, right-click the GPO (in the Group Policy Objects container) and choose Backup. Again, after you choose this option, a wizard will start asking you for the backup location. Choose a location and click Backup.

To restore a GPO, it's the same process, except instead of choosing Backup, you will choose either Manage Backups (to restore all GPOs) or Restore (for an individual GPO).

Configure the Boot Configuration Data Store

`BCDEdit` is another great command-line utility that is used primarily for managing boot configuration data (BCD) stores. A *BCD store* is a set of configuration files that describe an operating system's boot applications and settings. These files essentially replace the `Boot.ini` file in your local Windows directory. You will notice that the `BCDEdit` command-line utility is similar to the `Bootcfg.exe` utility used in earlier versions of Windows operating systems. You can effectively use `BCDEdit` to create new boot parameters for your Windows boot loader, modify the existing BCD stores, and create new BCD stores as needed. Please note that administrative permissions are required to use `BCDEdit` to modify a BCD store.

Setting Up an Active Directory Backup

The Windows Server 2012 R2 Backup utility makes it easy to back up the system data (including Active Directory) as part of a normal backup operation. I've already covered the ideas behind the different backup types and why and when they are used.

Exercise 19.1 walks you through the process of backing up the domain controller. To complete this exercise, the local machine must be a domain controller, and you must have a DVD burner or network location to back up the system state.

The Windows Server 2012 R2 Backup utility is not installed by default. If you have already installed the Windows Server 2012 R2 Backup utility, skip to step 9.

EXERCISE 19.1

Backing Up Active Directory

1. To install the Windows Server 2012 R2 Backup utility, press the Windows key and select Administrative Tools ➢ Server Manager.
2. In the center console, click the Add Roles And Features link.
3. At the Select Installation Type screen, choose a role-based or feature-based installation and click Next.
4. The Select Destination Server screen appears. Choose Select A Server From The Server Pool and choose your server under Server Pool. Click Next.
5. Click Next at the Select Server Roles screen.
6. At the Select Features screen, scroll down and check the box next to Windows Server Backup. Click Next.

7. At the Confirmation screen, click the check box to restart the destination server automatically. This will bring up a dialog box. Click Yes and then click the Install button.

8. Click the Close button when finished. Close Server Manager.
9. Open Windows Backup by pressing the Windows key and selecting Administrative Tools ➢ Windows Server Backup.
10. On the left side, click Local Backup. Then, under Actions, click Backup Once.
11. When the Backup Once Wizard appears, click Different Options and click Next.

EXERCISE 19.1 *(continued)*

12. At the Select Backup Configuration screen, choose Custom and click Next.
13. Click the Add Items button. Choose System State and click OK. Click Next.

14. At the Specify Destination Type, choose Remote Shared Folder. Click Next.
15. Put in the shared path you want to use and click Next.
16. At the Confirmation screen, click the Backup button.

17. Once the backup is complete, close the Windows Server Backup utility.

Restoring Active Directory

Active Directory has been designed with fault tolerance in mind. For example, it is highly recommended by Microsoft that each domain have at least two domain controllers. Each of these domain controllers contains a copy of the Active Directory data store. Should one of the domain controllers fail, the available one can take over the failed server's functionality. When the failed server is repaired, it can then be promoted to a domain controller in the existing environment. This process effectively restores the failed domain controller without incurring any downtime for end users because all of the Active Directory data is replicated to the repaired server in the next scheduled replication.

In some cases, you might need to restore Active Directory from a backup. For example, suppose a system administrator accidentally deletes several hundred users from the domain and does not realize it until the change has been propagated to all of the other domain controllers. Manually re-creating the accounts is not an option because the objects' security identifiers will be different (and all permissions must be reset). Clearly, a method for restoring from backup is the best solution. You can elect to make the Active Directory restore authoritative or nonauthoritative, as described in the following sections.

Overview of Authoritative Restore

Restoring Active Directory and other system state data is an important process should system files or the Active Directory data store become corrupt or otherwise unavailable. Fortunately, the Windows Server 2012 R2 Backup utility allows you to restore data easily from a backup, should the need arise.

I mentioned earlier that in the case of the accidental deletion of information from Active Directory, you might need to restore Active Directory from a recent backup. But what happens if there is more than one domain controller in the environment? Even if you did perform a restore, the information on this domain controller would be seen as outdated, and it would be overwritten by the data from another domain controller. This data from the older domain controller is exactly the information you want to replace. The domain controller that was reloaded using a backup would have an older timestamp, and the other domain controllers would re-delete the information from the backup.

Fortunately, Windows Server 2012 R2 and Active Directory allow you to perform what is called an *authoritative restore*. The authoritative restore process specifies a domain controller as having the authoritative (or master) copy of the Active Directory data store. When other domain controllers communicate with this domain controller, their information will be overwritten with Active Directory data stored on the local machine.

Now that you have an idea of how an authoritative restore is supposed to work, let's move on to looking at the details of performing the process.

Performing an Authoritative Restore

When you are restoring Active Directory information on a Windows Server 2012 R2 domain controller, make sure Active Directory services are not running. This is because the restore of system state data requires full access to system files and the Active Directory data

store. If you attempt to restore system state data while the domain controller is active, you will see an error message.

In general, restoring data and operating system files is a straightforward process. It is important to note that restoring a system state backup will replace the existing registry, Sysvol, and Active Directory files so that any changes you made since the last backup will be lost.

In addition to restoring the entire Active Directory database, you can also restore only specific subtrees within Active Directory using the `restoresubtree` command in the `ntdsutil` utility. This allows you to restore specific information, and it is useful in case of accidental deletion of isolated material.

Following the authoritative restore process, Active Directory should be updated to the time of the last backup. Furthermore, all other domain controllers for this domain will have their Active Directory information overwritten by the results of the restore operation. The result is an Active Directory environment that has been recovered from media.

Overview of Nonauthoritative Restore

Now that you understand why you would use an authoritative restore and how it is performed, it's an easy conceptual jump to understand a *nonauthoritative restore*. Remember that by making a restore authoritative, you are simply telling other domain controllers in the domain to recognize the restored machine as the newest copy of Active Directory for replication purposes. If you have only one domain controller, the authoritative restore process becomes moot; you can simply skip the steps required to make the restore authoritative and begin using the domain controller immediately after the normal restore is complete.

If you have more than one domain controller in the domain and you need to perform a nonauthoritative restore, simply allow the domain controller to receive Active Directory database information from other domain controllers in the domain using normal replication methods.

Active Directory Recycle Bin

The Active Directory recycle bin is a great feature that allows administrators to restore an Active Directory object that has been deleted.

Let's say you have a junior administrator who has been making changes to Active Directory for hours. The junior admin then deletes an OU from Active Directory. You would then have to reload the OU from a tape backup, or even worse, you may have to reload the entire Active Directory (depending on your backup software), thus losing the hours of work the junior admin has completed.

The problem here is that when you delete a security object from Active Directory, the object's security ID (SID) gets removed. All users' rights and permissions are associated with the users' SID number and not their account name. This is where the AD recycle bin can help.

The *Active Directory recycle bin* allows you to preserve and restore accidentally deleted Active Directory objects without the need of using a backup.

The Active Directory recycle bin works for both the Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS) environments.

By enabling (disabled by default) the Active Directory recycle bin, any deleted Active Directory objects are preserved, and Active Directory objects can be restored, in their entirety, to their same condition immediately before the deletion. This means all group memberships and access rights that the object had before deletion will remain intact.

To enable the Active Directory recycle bin, you must do the following (you must be a member of the Schema Admins group):

1. Run the `adprep /forestprep` command to prepare the forest on the server that holds the schema master to update the schema.
2. Run the `adprep /domainprep /gpprep` command to prepare the domain on the server that holds the infrastructure operations master role.
3. If a read-only domain controller (RODC) is present in your environment, you must also run the `adprep /rodcprep` command.
4. Make sure that all domain controllers in your Active Directory forest are running Windows Server 2012 R2 or at least Windows Server 2008 R2.
5. Make sure that the forest functional level is set to Windows Server 2012 R2 or at least Windows Server 2008 R2.

Restartable Active Directory

Administrators have the ability to stop and restart Active Directory in the Windows Server 2012 R2 operating system without the need to reboot the entire system. Administrators can perform these actions by using either the Microsoft Management Console (MMC) snap-ins or the command line.

With *Restartable Active Directory Services*, an administrator has the ability to stop Active Directory Services so that updates and other tasks can be applied to a domain controller. One task that an administrator can perform while Active Directory is stopped is an offline defragmentation of the database.

One of the advantages of a restartable Active Directory is that other services running on the same server do not depend on Active Directory to continue to function properly while Active Directory is stopped. An administrator has the ability to stop and restart the Active Directory Domain Services in the Local Services MMC snap-in.

Offline Maintenance

As mentioned, sometimes you have to be offline to do maintenance. For example, you need to perform authoritative and nonauthoritative restores while the domain controller is offline. The main utility administrators use for offline maintenance is `ntdsutil`.

Ntdsutil.exe

The primary method by which system administrators can do offline maintenance is through the `ntdsutil` command-line tool. You can launch this tool by simply entering **`ntdsutil`** at

a command prompt. The `ntdsutil` command is both interactive and context sensitive. That is, once you launch the utility, you'll see an `ntdsutil` command prompt. At this prompt, you can enter various commands that set your context within the application. For example, if you enter **`domain management`**, you'll be able to enter domain-related commands. Several operations also require you to connect to a domain, a domain controller, or an Active Directory object before you perform a command.

Table 19.1 describes the domain-management commands supported by the `ntdsutil` tool. You can access this functionality by typing the command at a command prompt.

TABLE 19.1 `Ntdsutil` offline maintenance commands

`Ntdsutil` domain management command	**Purpose**
`Help` or `?`	Displays information about the commands that are available within the Domain Management menu of the `ntdsutil` utility
`compact to` (at the file maintenance prompt)	Allows you to compact the Active Directory database (offline defragmentation)
`metadata cleanup`	Removes metadata from decommissioned domain controllers
`Set DSRM Password`	Resets the Directory Service Restore mode administrator account password

Active Directory Database Mounting Tool

One issue that an administrator may run into when trying to restore Active Directory is the need to restore several backups to compare the Active Directory data that each backup contains. Windows Server 2012 R2 has a utility called the Active Directory database mounting tool (`Dsamain.exe`) that can resolve this issue.

The `Dsamain.exe` tool can help the recovery processes by giving you a way to compare data as it exists in snapshots (taken at different times) so that you have the ability to decide which Active Directory database to restore.

Creating snapshots on a regular basis will allow you to have enough data so that you can keep accurate records of how the Active Directory database changes over time. The `ntdsutil` utility allows you to take snapshots by using the `ntdsutil snapshot` operation.

You are not required to run the `ntdsutil snapshot` operation to use `Dsamain.exe`. You have the ability to use a backup of the Active Directory database.

You must be a member of the Domain Admins group or the Enterprise Admins group to view any snapshots taken because these snapshots contain sensitive Active Directory data.

Compact the Directory Database File (Offline Defragmentation)

One task you have probably done for years is defrag the operating systems that you run. Defragging a system helps return free space from data to the hard drive, and the defragmentation utility has been available since Windows NT.

You can also use the defragmentation process to compact the Active Directory database while it's offline. Offline defragmentation helps return free disk space and check Active Directory database integrity.

To perform an offline defragmentation, you use the `ntdsutil` command. When you perform a defragmentation of the Active Directory database, a new compacted version of the database is created. This new database file can be created on the same machine (if space permits) or on a network location. After the new file is created, copy the compacted `Ntds.dit` file to the original location.

It is a good practice, if space allows, to maintain a copy of the older, original database file. You can either rename the older database file and keep it in its current location or copy the older database file to an alternate location.

Monitoring Replication

At times you may need to keep an eye on how your replication traffic is working on your domain controllers. I will cover the replication utility that you can use to help determine whether there are problems on your domain.

Repadmin Utility

The `Repadmin` utility is included when you install Windows Server 2012 R2. This command-line tool helps administrators diagnose replication problems between Windows domain controllers.

`Repadmin` allows administrators to view the replication topology of each domain controller as seen from the domain controller's perspective. Administrators can also use `Repadmin` to create the replication topology manually. By manually creating the replication topology, administrators can force replication events between domain controllers and view the replication metadata vectors.

To access the `Repadmin` utility, open a command prompt using an elevated privilege (Run ➢ CMD). At the command prompt, type **`Repadmin.exe`**, and all of the available options will appear.

Using the ADSI Editor

Another utility that allows you to manage objects and attributes in Active Directory is the Active Directory Service Interfaces Editor (ADSI Edit). ADSI Edit allows you to view every object and attribute in an Active Directory forest.

One advantage to using the `Adsiedit.msc` MMC snap-in is that this tool allows you to query, view, create, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap-ins.

ADSI Edit allows you to administer an AD LDS instance. To do this, you must first connect and bind to the instance. After you connect and bind to the instance, you can administer the containers and objects within the instance by browsing to the containers or objects and then right-clicking them. To complete this task, you must be a member of the Administrators group for the AD LDS instance.

Wbadmin Command-Line Utility

The `wbadmin` command allows you to back up and restore your operating system, volumes, files, folders, and applications from a command prompt.

You must be a member of the Administrators group to configure a backup schedule. You must be a member of the Backup Operators or the Administrators group (or you must have been delegated the appropriate permissions) to perform all other tasks using the `wbadmin` command.

To use the `wbadmin` command, you must run `wbadmin` from an elevated command prompt (to open an elevated command prompt, click Start, right-click Command Prompt, and then click Run As Administrator). Table 19.2 describes some of the `wbadmin` commands.

TABLE 19.2 `Wbadmin` commands

Command	Description
`wbadmin enable backup`	Configures and enables a daily backup schedule
`wbadmin disable backup`	Disables your daily backups
`wbadmin start backup`	Runs a one-time backup
`wbadmin stop job`	Stops the currently running backup or recovery operation
`wbadmin get items`	Lists the items included in a specific backup
`wbadmin start recovery`	Runs a recovery of the volumes, applications, files, or folders specified
`wbadmin get status`	Shows the status of the currently running backup or recovery operation
`wbadmin start systemstaterecovery`	Runs a system state recovery
`wbadmin start systemstatebackup`	Runs a system state backup
`wbadmin start sysrecovery`	Runs a recovery of the full system state

Configure Windows Azure Backups

Microsoft continues to offer robust cloud solutions to assist administrators with effective backup options. With Windows Server 2012 R2, you can integrate with Windows Azure Online Services to store short-term backup data to an off-premises location. This solution comes with additional costs for storing the data after the initial free trial. The cost model is relatively straightforward, and it is comparable to other cloud storage solutions that are currently available. To run backup jobs from your organization to the Microsoft Azure cloud solution, your environment must be running System Center 2012 with Data Protection Manager.

Data Protection Manager

System Center 2012 *Data Protection Manager (DPM)* is an application that runs on the server and allows disk-based and tape-based data protection and recovery. This recovery is for all the computers in the Active Directory domain. One of the nice features of DPM is that all replication, synchronization, and recovery point creation is done by DPM.

Because you are able to use DPM and set up recoverability for your computers, if a system needs to be recovered, DPM provides reliable protection and rapid recovery of the computer's data either by the system administrator and/or by end users.

DPM uses multiple features to help keep the computers in your network safe. These features include replication, the Volume Shadow Copy Service (VSS) infrastructure, and a policy-driven engine. DPM helps provide protection and fast data recovery for businesses of all sizes.

Windows Azure Backup Prerequisites

Before you can start using the Windows Azure backup services, you must first have a few prerequisites set up within your environment. The following are the deployment prerequisites that you will need to accomplish the task:

- A Windows Server 2012 R2 server running Data Protection Manager in System Center 2012 R2.
- An active Windows Azure account with the Windows Azure Backup feature enabled.
- The Windows Azure backup agent must be installed on the DPM servers that you want to back up, and the DPM servers must have at least 2.5GB of free space reserved for caching. At least 15GB to 20GB of free space is recommended.
- A management certificate that will be uploaded to the backup vault in Windows Azure Backup.

  Please note the following in regard to the certificate parameters:

  - To upload to the certificate to the vault, you must export it as a `.cer` format file that contains the public key.
  - The certificate should be an x.509 v3 certificate.
  - The key length should be at least 2,048 bits.
  - The certificate must have a valid ClientAuthentication EKU.

- The certificate should be valid currently, with a validity period that does not exceed 3 years.
- The certificate should reside in the Personal certificate store of your local computer.
- The private key should be included during installation of the certificate.
- You can create a self-signed certificate using the `makecert` tool or use any valid SSL certificate issued by a certification authority (CA) trusted by Microsoft whose root certificates are distributed via the Microsoft Root Certificate Program.

Make sure to take full advantage of the Microsoft Azure free trial when preparing for your exam. You can start your free trial by following this web link: `http://azure.microsoft.com/en-us/pricing/free-trial/`.

Configure Backup Vaults for Windows Azure Backup

The Windows Azure backup vault is where your data will be stored in the cloud. After you obtain a Windows Azure account, you will be able to create and manage your cloud backups from the Windows Azure Management Portal. Before you can start storing data using Windows Azure, you must first configure the backup vault by following four easy configuration steps:

1. Obtain a management certificate that will be used by Windows Azure:
   - You can either use an existing management certificate or obtain one by using `makecert.exe`. If you want to register a server that was not used to run `makecert.exe`, you must export the `.pfx` file (containing the private key) from that server, copy it to the server that you want to register, and import it to the Personal certificate store on that computer.
2. Create a backup vault in Windows Azure:
   a. Log in to the Windows Azure Management Portal.
   b. Click Recovery Services and then click Create New. Point to Backup Vault and then click Quick Create.
   c. Name the Vault, specify the geographic region, enter your Windows Azure subscription, and then click Create Backup Vault. It usually takes only a few minutes for the backup vault to finish building. Notifications are provided at the bottom of the management portal.
3. Upload a management certificate to Windows Azure:
   a. Log in to the Windows Azure Management Portal.
   b. Click Recovery Services, click the backup vault you want to certify, and then open the Quick Start page by clicking the Quick Start icon.
   c. On the Quick Start page, click Manager Certificate. A dialog box will appear allowing you to browse your computer for the appropriate certificate that has been staged for upload. Select and upload that certificate.

4. Download and Install the Windows Azure Backup Agent onto each of your DPM servers that you want to back up:
   a. Log in to the Windows Azure Management Portal.
   b. Select Download Agent from the Quick Start page.
   c. Select the appropriate agent for your deployment to start the Agent Installation Wizard.
   d. Complete the installation wizard, keeping all defaults.

Register DPM Servers with the Backup Vault

Now that your Windows Azure Backup Vault is fully configured and all of your DPM servers have agents installed, it's time to register your DPM servers with the backup vault.

1. Launch the Windows Azure Backup application from one of your DPM servers.
2. Click the Register Server task in the Action pane to start the Register Server Wizard.
3. Follow the wizard, making appropriate selections suitable for your particular environment.
4. If the process is successful, a registration confirmation message is displayed, and you can close the wizard.

That's all there is to it. If you have completed these steps properly, you are ready to configure backup jobs to run from your DPM servers to your backup vault in Microsoft Azure. Make sure to spend lots of time running through all of the available options found in the Microsoft Azure Management Portal. The exam is likely to cover multiple scenarios surrounding the configuration and troubleshooting of backups using Microsoft Azure.

Understanding Shadow Copies

An excellent way to protect your shared folders is by using *shadow copies* (Volume Snapshot Service [VSS]). Shadow copies allow an administrator to back up shared folders to a remote location. Shadow copies are designed to help recover files that were accidentally deleted, that were overwritten, or that have become corrupt. One major advantage to shadow copies is that open files can be backed up. This means that even if users are currently working on files in a shared folder that has shadow copies enabled, the shadow copies will continue to function.

Once administrators have configured and enabled shadow copies (using the Computer Management snap-in), network users can restore earlier versions of files. After the initial shadow copy of the shared folder is created, only changes are copied and not the entire file.

You can enable shadow copies of entire volumes.

The following are some of the settings that you can configure when setting up shadow copies:

Schedule You have the ability to set the schedule of the shadow copies. You can set this schedule to run daily, weekly, monthly, once, at system startup, at logon, or when the system is idle. You can also set the time at which the shadow copy will run.

Storage Locations An administrator needs to set the location of the shadow copy backup. If you are on a network, it is a good idea to place the shadow copy on a network drive.

Maximum Size You can set a maximum size on your shadow copies, or you can specify that they have no size limit. One of the predetermined settings is 64 shadow copies per volume.

In Exercise 19.2, you'll set up a volume to make shadow copies every Monday at 7 a.m. To set up the shadow copies, you will use the Computer Management MMC snap-in.

EXERCISE 19.2

Configuring a Shadow Copy on a Volume

1. Open Computer Management by pressing the Windows key and selecting Administrative Tools ➢ Computer Management.
2. Expand Storage and then right-click Disk Management. Choose All Tasks ➢ Configure Shadow Copies.
3. When the Shadow Copies dialog box appears, click the Settings button.

4. When the Settings windows appears, click the Schedule button.
5. In the Schedule window, set the schedule task to weekly and the start time for 7 a.m. Uncheck all of the days-of-the-week boxes except Mon. Click OK.

6. When the Settings window reappears, click OK.
7. If the Enable button is enabled, click it. Then click OK.
8. Exit the Computer Management MMC.

To recover a previous version of a file from a shadow copy, you use the `\\servername\sharename` path. The operating system determines how you will gain access to the shared folders and shadow copies. Shadow copies are built into Windows XP (SP1), Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008/2008 R2, Windows Server 2012, and Windows Server 2012 R2. If you are using a different Microsoft operating system, you need to download the Shadow Copy Client Pack from the Microsoft download center.

VssAdmin Command

Another way to create, configure, and manage shadow copies is by using the `vssadmin.exe` command-line utility (see Figure 19.4). The `vssadmin.exe` command allows you to create, delete, list, and resize shadow copies and shadow storage.

FIGURE 19.4 `vssadmin.exe` command-line utility

Table 19.3 describes the `vssadmin.exe` command and the different commands associated with the `vssadmin` utility.

TABLE 19.3 `Vssadmin.exe` commands

Command	Description
`Add ShadowStorage`	Adds a new volume shadow copy storage association
`Create Shadow`	Creates a new volume shadow copy
`Delete Shadows`	Deletes volume shadow copies
`Delete ShadowStorage`	Deletes the volume shadow copy storage associations
`List Providers`	Lists registered volume shadow copy providers
`List Shadows`	Lists existing volume shadow copies
`List ShadowStorage`	Lists volume shadow copy storage associations
`List Volumes`	Lists volumes eligible for shadow copies
`List Writers`	Lists subscribed volume shadow copy writers
`Resize ShadowStorage`	Resizes a volume shadow copy storage association
`Revert Shadow`	Reverts a volume to a shadow copy
`Query Reverts`	Queries the progress of in-progress revert operations

Using Advanced Boot Options

The Windows Server 2012 R2 advanced startup options can be used to troubleshoot errors that keep Windows Server 2012 R2 from successfully booting.

To access the Windows Server 2012 R2 advanced startup options, start or reboot the computer and press the F8 key after the firmware POST process but before Windows Server 2012 R2 is loaded. This will bring up the Advanced Boot Options menu, which offers numerous options for booting Windows Server 2012 R2.

These advanced startup options are covered in the following three sections (see Figure 19.5).

FIGURE 19.5 Advanced Boot Options screen

Starting in Safe Mode

When your computer will not start, one of the fundamental troubleshooting techniques is to simplify the configuration as much as possible. This is especially important when you do not know the cause of your problem and you have a complex configuration. After you

have simplified the configuration, you can determine whether the problem is in the basic configuration or is a result of your complex configuration.

If the problem is in the basic configuration, you have a starting point for troubleshooting. If the problem is not in the basic configuration, you should proceed to restore each configuration option you removed, one at a time. This helps you to identify what is causing the error.

If Windows Server 2012 R2 will not load, you can attempt to load the operating system through *Safe Mode*. When you run Windows Server 2012 R2 in Safe Mode, you are simplifying your Windows configuration as much as possible. Safe Mode loads only the drivers needed to get the computer up and running.

The drivers that are loaded with Safe Mode include basic files and drivers for the mouse, monitor, keyboard, hard drive, standard video driver, and default system services. Safe Mode is considered a diagnostic mode, so you do not have access to all of the features and devices in Windows Server 2012 R2 that you have when you boot normally, including networking capabilities.

A computer booted to Safe Mode will show Safe Mode in the four corners of your desktop.

If you boot to Safe Mode, check all of your computer's hardware and software settings in Device Manager and try to determine why Windows Server 2012 R2 will not boot properly. After you take steps to fix the problem, try to boot to Windows Server 2012 R2 as you normally would.

In Exercise 19.3, you will boot your computer to Safe Mode.

EXERCISE 19.3

Booting Your Computer to Safe Mode

1. If your computer is currently running, restart the system.
2. During the boot process, press the F8 key to access the Advanced Boot Options menu.
3. Highlight Safe Mode and press Enter.
4. When Windows Server 2012 R2 starts, log in.
5. You will see a Help And Support dialog box letting you know what Safe Mode is. Exit Help And Support.
6. You should see that a network connection is not available in the lower-right corner.
7. Don't restart your computer yet; you will do this as a part of the next exercise.

Enabling Boot Logging

Boot logging creates a log file that tracks the loading of drivers and services. When you choose the Enable Boot Logging option from the Advanced Boot Options menu, Windows

Server 2012 R2 loads normally, not in Safe Mode. This allows you to log all of the processes that take place during a normal boot sequence.

This log file can be used to troubleshoot the boot process. When logging is enabled, the log file is written to `\WINDOWS\Ntbtlog.txt` (see Figure 19.6).

FIGURE 19.6 `Ntbtlog.txt` file

In Exercise 19.4, you will create and access a boot log file.

EXERCISE 19.4

Using Boot Logging

1. Restart your computer.
2. During the boot process, press the F8 key to access the Advanced Boot Options menu.
3. Highlight Enable Boot Logging and press Enter.
4. When Windows Server 2012 R2 starts, log in.
5. Click the Folders icon on the bottom left of the desktop and browse to `C:\WINDOWS\Ntbtlog.txt`. Double-click this file.
6. Examine the contents of your boot log file.
7. Shut down your computer and restart it without using Advanced Boot Options.

The boot log file is cumulative. Each time you boot to Safe Mode, you are writing to this file. This enables you to make changes, reboot, and see whether you have fixed any problems. If you want to start from scratch, you should manually delete this file and reboot to an Advanced Boot Options menu selection that supports logging.

Using Other Advanced Boot Options Menu Modes

In this section, you will learn about additional Advanced Boot Options menu modes. These include the following:

Safe Mode With Networking This is the same as the Safe Mode option, but it adds networking features. You might use this mode if you need networking capabilities to download drivers or service packs from a network location.

Safe Mode With Command Prompt This starts the computer in Safe Mode, but after you log in to Windows Server 2012 R2, only a command prompt is displayed. This mode does not provide access to the desktop. Experienced troubleshooters use this mode.

Enable Low-Resolution Video (640×480) This loads a standard VGA driver without starting the computer in Safe Mode. You might use this mode if you changed your video driver, did not test it, and tried to boot to Windows Server 2012 R2 with a bad driver that would not allow you to access video. The Enable VGA mode bails you out by loading a default driver, providing access to video so that you can properly install (and test!) the correct driver for your computer.

Safe Mode starts Windows Server 2012 R2 at a resolution of 800×600.

Last Known Good Configuration (Advanced) This boots Windows Server 2012 R2 by using the registry information that was saved the last time the computer was successfully booted. You would use this option to restore configuration information if you improperly configured the computer and did not successfully reboot it. When you use the *Last Known Good Configuration* option, you lose any system configuration changes that were made since the computer last successfully booted.

Directory Services Restore Mode This option is used for domain controllers only, and it is not relevant to Windows Server 2012 R2 unless it is a domain controller.

Debugging Mode This runs the Kernel Debugger, if it is installed. The Kernel Debugger is an advanced troubleshooting utility.

Disable Automatic Restart On System Failure This prevents Windows from restarting when a critical error causes Windows to fail. This option should be used only when Windows fails every time you restart so that you are not able to access the desktop or any configuration options.

Disable Driver Signature Enforcement This allows drivers to be installed even if they do not contain valid signatures.

Start Windows Normally This boots to Windows Server 2012 R2 in the default manner. This option is on the Advanced Boot Options menu in case you accidentally hit F8 during the boot process but really wanted to boot Windows Server 2012 R2 normally.

Windows Recovery Environment

When your Windows Server 2012 R2 machine fails to start, it will automatically enter into the *Windows Recovery Environment (Windows RE)*. This environment is an extensible recovery platform based on Windows Preinstallation Environment (Windows PE).

When your server starts in the Windows RE, the Startup Repair tool starts the diagnosis, and it will begin to help you repair the system. The Windows RE is also an environment in which you can use various tools to help you do a manual system recovery. The boot options for the Windows RE are as follows:

- Start recovery, troubleshooting, or diagnostic tools
- Boot from a device
- Access the Firmware menu
- Choose which operating system to boot, if multiple operating systems are installed on the same computer

Administrators also have the ability to configure a hardware button to run an alternate boot path that includes the Windows RE. This gives administrators the ability to help their users get to the Windows RE menus more easily, which allows your users to recover their PCs easily in the event of a corrupted system.

There are certain instances where Windows RE will automatically try to repair the system:

- Two successive failed attempts to start Windows
- Two successive unexpected shutdowns that occur within two minutes of boot completion
- A Secure Boot error (except for issues related to `Bootmgr.efi`)
- A BitLocker error on touch-only devices

Configure Site-Level Fault Tolerance

Disaster recovery is a key piece of maintaining a solid corporate infrastructure. Companies will rely heavily on the ability to configure fault tolerance, redundancy, and replication within the environment to ensure production uptime across the organization. Windows Server 2012 R2 has quite a few new features to help administrators accomplish these tasks in a failover clustered environment.

Hyper-V in Windows Server 2012 R2 gives you the power you need to be truly fault tolerant. Using the Hyper-V Replica feature, you can keep entire replicated copies of your virtual machines readily available to keep your production environment online when virtual machines fail. The nice thing about the replica VM is that it doesn't share storage with the primary VM like you are used to seeing with a traditional failover cluster. The replica starts off with a full cloned copy of the primary VM's virtual hard disk and then updates itself automatically through replication frequency from the primary VM. These automatic updates are configurable to occur anywhere from 30 seconds to 15 minutes.

To set up a Hyper-V replica properly, you must first configure the server-level replication settings for both physical Hyper-V hosts that will make up this failover configuration. One host will act as the primary, and the other will serve as the replica. You must enable replication on the replica host before you can replicate VMs from the primary host. These configuration settings are found in the Hyper-V Manager settings navigation pane under Replication Configuration. Check the box Enable This Computer As A Replica Server and then make your authentication, port, and storage selections, as shown in Figure 19.7. The authentication, port, and storage selections must be configured on both physical Hyper-V hosts.

FIGURE 19.7: `Hyper-V settings`

Once the Hyper-V hosts have been configured, you can enable replication on the VMs running on the primary Hyper-V host. Simply right-click a virtual machine running on the primary host and select the new Enable Replication option to start the Enable

Replication Wizard. Once you are finished configuring failover settings using the wizard, that VM is now considered to be fault tolerant between your two physical Hyper-V hosts. You should initiate a test failover action by launching the Hyper-V Manager on the replica host, right-clicking a replica VM, clicking Replication, and then clicking Test Failover. Testing failover is the only way you know for sure that your configuration settings are correct.

In addition to having the ability to create Hyper-V replicas, Windows Server 2012 R2 also has the ability to perform Hyper-V Extended Replication. Hyper-V Extended Replication is a new feature that allows administrators to extend the replication boundaries from the primary and replica hosts to an actual third site location. For example, you have a Hyper-V primary host in Denver replicating to a Hyper-V replica host in Tampa. Using Hyper-V Extended Replication, you can configure the Tampa replica host to replicate to a third Hyper-V host located at your London office. This feature gives you an added level of fault tolerance within your environment.

The component that manages how the cluster databases are updated within a failover cluster environment is known as the *Global Update Manager*. Whenever the state of the cluster changes, such as when a node goes down or offline, all of the other nodes in the cluster must acknowledge the change before those changes can be written to the cluster database. The Global Update Manager has three configurable settings available to you through Windows PowerShell using the following command:

```
(Get-Cluster).DatabaseReadWriteMode
```

The three configurable Global Update Manager settings are as follows:

0 = All (Write) And Local (Read) This is the default setting in Windows Server 2012 R2 for all cluster workloads except Hyper-V. It requires that all of the cluster nodes acknowledge the update before the change is committed to the database. Database reads occur on the local node.

1 = Majority (Read And Write) This is the default setting for Windows Server 2012 R2 Hyper-V failover clusters. It requires that only a majority of nodes acknowledge the update before the change is committed to the database. Database read involves comparing the most recent timestamp from the majority of available nodes and using the most recent data.

2 = Majority (Write) And Local (Read) This mode also requires that the majority of the cluster nodes acknowledge the update before committing the change to the database. The difference is that database read occurs on the local node, which means the data may be stale.

Microsoft recommends that you use mode 0 only when you have a requirement to make sure that the cluster database is consistent between all nodes in the cluster. For example, you would want to use mode 0 only when using availability groups in a Microsoft Exchange Server 2013 or Microsoft SQL Server 2012 environment to ensure that all of the cluster nodes acknowledge the change before the update is committed to the database. You cannot afford mismatched or stale data within a SQL or Exchange failover clustered environment. Having this situation could result in serious performance issues within the cluster.

Using the Startup Repair Tool

If your Windows Server 2012 R2 computer will not boot because of missing or corrupted system files, you can use the *Startup Repair tool* to correct these problems. Startup Repair cannot repair hardware failures. Additionally, Startup Repair cannot recover personal files that have been corrupted, damaged by viruses, or deleted. To ensure that you can recover your personal files, you should use the Backup utility previously discussed in this chapter.

To use the Startup Repair tool, follow these steps:

1. Boot your computer using the Windows Server 2012 R2 media.
2. When the Install Windows dialog box appears, select the language, the time and currency format, and the keyboard or input method. Click Next to continue.
3. The Install Now button appears in the center of the screen. Click Repair Your Computer in the lower-left corner.
4. Select the operating system to recover and click Next. If you do not see your operating system, you might need to load your hard disk drivers by clicking the Load Drivers button.
5. The System Recovery Options dialog box appears. You can choose one of the following options:
   - Startup Repair
   - System Restore
   - Windows Complete PC Restore
   - Windows Memory Diagnostic Tool
   - Command Prompt
   - Choose Startup Repair to continue.
6. Startup Repair checks your computer for problems and attempts to repair them. After Startup Repair has finished, click Shut Down or Restart.

If you were not provided the Windows Server 2012 R2 media when you purchased your computer, the computer manufacturer might have placed the files on a recovery partition—or they might have replaced the Startup Repair tool with one of their own. Check with the manufacturer for more information.

If Startup Repair is unable to correct the problem, you might have to reinstall Windows Server 2012 R2. This should be done as a last resort. This is a reason why you should always back up your Windows Server 2012 R2 machine.

Summary

In this chapter, you learned about the different ways to recover and protect your Windows Server 2012 R2 machine from hardware and software issues. I discussed using the Advanced Boot Options, such as Last Known Good Configuration, Safe Mode, debugging mode, and VGA mode. You can use these Advanced Boot Options for troubleshooting multiple software and hardware related issues within your environment.

Other important items that need to be completed on a Windows Server 2012 R2 machine are backups and restores. Backing up a Windows Server 2012 R2 machine protects it in the event of a hardware or software failure. Don't find yourself caught in the situation where a machine fails, and you don't have a fresh backup copy to restore data from. Take the time to back up all of the data that you care about.

Another way to protect data is by the use of shadow copies. Shadow copies allow you to keep previous versions of data and revert to that previous version in the event of a problem. Shadow copies are very convenient when you need to restore a file quickly.

Exam Essentials

Understand the various backup types available with the Windows Server 2012 R2 Backup utility. The Windows Server 2012 R2 Backup utility can perform full and incremental backup operations. Some third-party backup utilities also support differential and daily backups. You can use each of these operations as part of an efficient backup strategy.

Know how to back up Active Directory. The data within the Active Directory database on a domain controller is part of the system state data. You can back up the system state data to a file using the Windows Server 2012 R2 Backup utility.

Know how to restore Active Directory. Restoring the Active Directory database is considerably different from other restore operations. To restore some or the entire Active Directory database, you must first boot the machine into Directory Services Restore mode.

Understand the importance of an authoritative restore process. You use an authoritative restore when you want to restore earlier information from an Active Directory backup and you want the older information to be propagated to other domain controllers in the environment.

Understand offline maintenance using `ntdsutil`. The `ntdsutil` command-line tool is a primary method by which system administrators perform offline maintenance. Understand how to launch this tool by entering **`ntdsutil`** at a command prompt.

Review Questions

1. You need to ensure that you can recover your Windows Server 2012 R2 configuration and data if the computer's hard disk fails. What should you do?
   - **A.** Create a complete PC Backup.
   - **B.** Create a backup of all file categories.
   - **C.** Perform an automated system recovery (ASR) backup.
   - **D.** Create a system restore point.

2. After you update multiple drivers on your Windows Server 2012 R2 machine, the machine hangs at the logon screen, and you can't log into the machine. You need to get this computer up and running as quickly as possible. Which of the following repair strategies should you try first to correct your problem?
   - **A.** Restore your computer's configuration with your last backup.
   - **B.** Boot your computer with the Safe Mode option.
   - **C.** Boot your computer with the Last Known Good Configuration option.
   - **D.** Boot your computer to the recovery console and manually copy the old driver back to the computer.

3. You are the system administrator for a large organization that uses Windows Server 2012 R2 and Windows 8. You have a Windows 8 machine that needs to be configured with a normal backup schedule to restore sensitive data in the event of a catastrophic failure. At a worst case interval, you need to be able to perform a full restore from within the last 24 hours of a failure. What type of backup should you schedule?
   - **A.** Normal
   - **B.** Differential
   - **C.** Incremental
   - **D.** Daily

4. You are the network administrator for a small company. You manage the computers for the Marketing department, all of which are running the Windows Server 2012 R2 operating system. You are making several configuration changes to the manager's computer to enhance performance. Before you make any changes, you want to create a restore point that can be used if any problems arise. How do you manually create a restore point?
   - **A.** By using the System Restore utility
   - **B.** By using the Shadow Copies tab of the System Properties dialog box
   - **C.** By using the System Configuration utility
   - **D.** By using the Startup Repair tool

5. Your computer uses a SCSI adapter that supports a SCSI drive, which contains your Windows 8 system and boot partitions. After updating the SCSI driver, you restart your computer, but Windows 8 will not load. You need to get this computer up and running as quickly as possible. Which of the following repair strategies should you try first to correct your problem?
   - **A.** Restore your computer's configuration with your last backup.
   - **B.** Boot your computer with the Last Known Good Configuration.
   - **C.** Boot your computer with the Safe Mode option.
   - **D.** Boot your computer to the recovery console and manually copy the old driver back to the computer.

6. You enable the Boot Logging option on the Advanced Boot Options menu. Where can you find the log file that is created?
   - **A.** `\Windows\netlog.txt`
   - **B.** `\Windows\System32\netlog.txt`
   - **C.** `\Windows\ntbtlog.txt`
   - **D.** `\Windows\System32\netboot.log`

7. After you updated Will's computer, his system files became corrupted because of a virus and now need to be restored. Which of the following processes should you use to fix the problem?
   - **A.** Restore a backup.
   - **B.** Restore an image.
   - **C.** Use the Startup Repair tool.
   - **D.** Boot to Safe Mode.

8. You are unable to boot your Windows Server 2012 R2 computer, so you decide to boot the computer to Safe Mode. Which of the following statements regarding Safe Mode is false?
   - **A.** When the computer is booted to Safe Mode, there is no network access.
   - **B.** Safe Mode loads all of the drivers for the hardware that is installed on the computer.
   - **C.** When you run Safe Mode, boot logging is automatically enabled.
   - **D.** When you run Safe Mode, the screen resolution is set to 800×600.

9. You need to back up the existing data on a computer before you install a new application. You also need to ensure that you are able to recover individual user files that are replaced or deleted during the installation. What should you do?
   - **A.** Create a System Restore point.
   - **B.** Perform an automated system recovery (ASR) backup and restore.
   - **C.** In the Windows Server Backup utility, click the Backup Once link.
   - **D.** In the Backup And Restore Center window, click the Back Up Computer button.

10. Your data recovery strategy must meet the following requirements:

- Back up all data files and folders in `C:\Data`.
- Restore individual files and folders in `C:\Data`.
- Ensure that data is backed up to and restored from external media.

What should you do?

A. Use the Previous Versions feature to restore the files and folders.

B. Use the System Restore feature to perform backup and restore operations.

C. Use the NTBackup utility to back up and restore individual files and folders.

D. Use the Windows Server Backup to back up and restore files.

Chapter

20

Configure Advanced Network Services

THE FOLLOWING 70-412 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Implement an advanced Dynamic Host Configuration Protocol (DHCP) solution**

- Create and configure superscopes and multicast scopes
- Implement DHCPv6
- Configure high availability for DHCP including DHCP failover and split scopes
- Configure DHCP Name Protection
- Configure DNS registration

✓ **Implement an advanced DNS solution**

- Configure security for DNS including DNSSEC, DNS Socket Pool, and cache locking
- Configure DNS logging
- Configure delegated administration
- Configure recursion
- Configure netmask ordering
- Configure a GlobalNames zone
- Analyze zone level statistics

✓ **Deploy and manage IPAM**

- Provision IPAM manually or by using Group Policy
- Configure server discovery

- Create and manage IP blocks and ranges
- Monitor utilization of IP address space
- Migrate to IPAM
- Delegate IPAM administration
- Manage IPAM collections
- Configure IPAM database storage

In this chapter, you will take a deep dive into configuring network services using the new features and functionality provided by Windows Server 2012 R2. You should be familiar with the basics of both DNS and DHCP from Chapter 2, "Configure Network Services." Unlike the 70-410 exam, the 70-412 exam will require that you have the skills and knowledge to configure advanced network configurations beyond just their initial installations and setup.

This chapter will discuss and demonstrate some of the most common advanced network configuration options that you will see both on the exam and in the field. Once you have completed this chapter, you will have a better understanding of how to configure advanced network services surrounding DHCP, DNS, and IPAM in a Windows Server 2012 R2 environment.

Working with Advanced DHCP Configuration Options

DHCP makes the life of an administrator easy when it comes to managing the IP addresses of devices within an organization. Could you imagine having to keep track of each device and that device's IP manually? With Windows Server 2012 R2's DHCP high availability and load balancing options available, life gets even easier. The next few sections will cover how to implement advanced DHCP solutions in detail.

Create and Configure Superscopes

A *superscope* enables the DHCP server to provide addresses from more than one scope to clients on the same physical subnet. This is helpful when clients within the same subnet have more than one IP network and thus need IPs from more than one address pool. Microsoft's DHCP Management Console allows you to manage IP address assignment in the superscope, though you must still configure other scope options individually for each child scope. In Exercise 20.1 you will configure a superscope from two preexisting scopes.

NOTE

Remember that only one superscope can exist per server and that a superscope requires at least two preconfigured scopes.

EXERCISE 20.1

Creating a Superscope

1. Open the DHCP Management Console.
2. Right-click IPv4 and choose the New Superscope command to launch the New Superscope Wizard. Click Next.
3. On the Superscope Name page, name your superscope and click the Next button.
4. The Select Scopes page appears, listing all scopes on the current server. Select the two scopes you want to use for a superscope and then click the Next button.
5. The wizard's summary page appears. Click the Finish button to create your scope.
6. Verify that your new superscope appears in the DHCP Management Console to complete this exercise.

Deleting a Superscope

You can delete a superscope by right-clicking it and choosing the Delete command. A superscope is just an administrative convenience, so you can safely delete one at any time—it doesn't affect the "real" scopes that make up the superscope.

Adding a Scope to a Superscope

To add a scope to an existing superscope, find the scope you want to add, right-click it, and choose Action ➢ Add To Superscope. A dialog box appears, listing all of the superscopes known to this server. Pick the one to which you want the current scope appended and click the OK button.

Removing a Scope from a Superscope

To remove a scope from a superscope, open the superscope and right-click the target scope. The pop-up menu provides a Remove From Superscope command that will do the deed.

Activating and Deactivating Superscopes

Just as with regular scopes, you can activate and deactivate superscopes. The same restrictions and guidelines apply. You must activate a superscope before it can be used, and you must not deactivate it until you want all of your clients to lose their existing leases and be forced to request new ones.

To activate or deactivate a superscope, right-click the superscope name and select Activate or Deactivate, respectively, from the pop-up menu.

Create and Configure Multicast Scopes

Multicasting occurs when one machine communicates to a network of subscribed computers rather than specifically addressing each computer on the destination network.

It's much more efficient to *multicast* a video or audio stream to multiple destinations than it is to unicast it to the same number of clients, and the increased demand for multicast-friendly network hardware has resulted in some head scratching about how to automate the multicast configuration.

In the following sections, you will learn about MADCAP, the protocol that controls multicasting, and about how to build and configure a multicast scope.

Understanding the Multicast Address Dynamic Client Allocation Protocol

DHCP is usually used to assign IP configuration information for *unicast* (or one-to-one) network communications. With multicast, there's a separate type of address space assigned from 224.0.0.0 through 239.255.255.255. Addresses in this space are known as *Class D addresses*, or simply *multicast addresses*. Clients can participate in a multicast just by knowing (and using) the multicast address for the content they want to receive. However, multicast clients also need to have an ordinary IP address.

How do clients know what address to use? Ordinary DHCP won't help because it's designed to assign IP addresses and option information to one client at a time. Realizing this, the Internet Engineering Task Force (IETF) defined a new protocol: *Multicast Address Dynamic Client Allocation Protocol (MADCAP)*. MADCAP provides an analog to DHCP but for multicast use. A MADCAP server issues leases for multicast addresses only. MADCAP clients can request a multicast lease when they want to participate in a multicast.

DHCP and MADCAP have some important differences. First you have to realize that the two are totally separate. A single server can be a DHCP server, a MADCAP server, or both; no implied or actual relation exists between the two. Likewise, clients can use DHCP and/or MADCAP at the same time—the only requirement is that every MADCAP client has to get a unicast IP address from somewhere.

Remember that DHCP can assign options as part of the lease process, but MADCAP cannot. The only thing MADCAP does is to assign multicast addresses dynamically.

Building Multicast Scopes

Building a multicast scope is similar to building a unicast scope, but it requires a few different configuration settings when going through the wizard. Exercise 20.2 walks you through creating and activating a new multicast scope.

EXERCISE 20.2

Creating and Activating a New Multicast Scope

1. Open the DHCP Management Console.
2. Right-click IPv4 and choose New Multicast Scope to launch the New Multicast Scope Wizard. Click the Next button on the welcome page.

EXERCISE 20.2 *(continued)*

3. On the Multicast Scope Name page, provide a name and description for your multicast scope. Click Next.
4. The IP Address Range page appears. Enter a start IP address of **224.0.0.0** and an end IP address of **224.255.0.0**. Adjust the TTL to 1 to make sure no multicast packets escape your local network segment. Click Next.
5. On the Add Exclusions page of the wizard, add any IP Exclusions or leave this page blank. Click Next.
6. Keep the defaults on the Lease Duration page. Click Next.
7. Ensure the Activate Scope Now radio button is toggled to Yes. Click Finish to complete the creation and activation of your new multicast scope.
8. Verify that your new multicast scope appears in the DHCP Management Console to complete this exercise.

Setting Multicast Scope Properties

Once you create a multicast scope, you can adjust its properties by right-clicking the scope name and selecting Properties.

The Multicast Scope Properties dialog box has two tabs. The General tab (see Figure 20.1) allows you to change the scope's name, its start and end addresses, its Time To Live (TTL) value, its lease duration, and its description—in essence, all of the settings you provided when you created it in the first place.

FIGURE 20.1 General tab of the Multicast Scope Properties dialog box

The Lifetime tab (see Figure 20.2) allows you to limit how long your multicast scope will be active. By default, a newly created multicast scope will live forever, but if you're creating a scope to provide MADCAP assignments for a single event (or a set of events of limited duration), you can specify an expiration time for the scope. When that time is reached, the scope disappears from the server but not before making all of its clients give up their multicast address leases. This is a nice way to make sure the lease cleans up after itself when you're finished with it.

FIGURE 20.2 Lifetime tab of the Multicast Scope Properties dialog box

Implement DHCPv6

In Windows Server 2012 R2, administrators can create and manage both IPv4 and IPv6 DHCP scopes for their organization. Even though they are managed separately, they have the same capabilities of being able to configure reservations, exclusions, and other DHCP options. Unlike an IPv4 client, a DHCPv6 client uses a device unique identifier (DUID) instead of a MAC address to get an IP address from the DHCP server.

DHCPv6 supports both stateful address configuration and stateless address configuration. An easy way to think of the difference between a stateful configuration and a stateless configuration is that, with a stateful configuration, the DHCPv6 client receives its IPv6 address and its additional DHCP options from the DHCPv6 server. With a stateless configuration, the IPv6 client can automatically assign itself an IPv6 address without ever having to communicate with the DHCPv6 server. The stateless configuration process is also known as *DHCPv6 autoconfiguration*. Exercise 20.3 will walk you through the process of creating and activating a new DHCPv6 scope.

EXERCISE 20.3

Creating and Activating a New DHCPv6 Scope

1. Open the DHCP Management Console.
2. Right-click IPv6 and choose the New Scope command. The New Scope Wizard appears. Click the Next button.
3. On the Welcome to the New Scope Wizard page, click the Next button.
4. On the Scope Name page, provide a name and description for your new DHCPv6 scope. Click the Next button.
5. On the Scope Prefix page, input the corresponding prefix for your organization's IPv6 network settings. In the event that you have more than one DHCPv6 server, you can set a preference value that will indicate your server priority. The lower the preference value, the higher the server priority. Click Next.

6. On the Add Exclusions page of the wizard, you can configure either a single IP exclusion or a range of IPs to exclude from obtaining an address automatically. Exclusions should include any device or range of devices that have been manually set with a static IP on that particular scope. Click Next.

7. Keep the default selections on the Scope Lease page. Click Next.
8. Make sure the Activate Scope Now radio button is toggled to Yes. Click Finish to complete the creation and activation of your new DHCPv6 scope.

9. Verify that your new scope appears in the DHCP Management Console to complete this exercise.

Configure High Availability for DHCP Including DHCP Failover and Split Scopes

DHCP failover provides load balancing and redundancy for DHCP services, enabling administrators to deploy a highly resilient DHCP service for their organization. The idea is to share your DHCP IPV4 scopes between two Windows Server 2012 R2 servers so that if one of the failover partners goes down, then the other failover partner will continue providing DHCP services throughout the environment. DHCP failover supports large-scale DHCP deployments without the challenges of a split-scope DHCP environment.

Here are a few of the benefits that DHCP failover provides:

Multisite DHCP failover supports a deployment architecture that includes multiple sites. DHCP failover partner servers do not need to be located at the same physical site.

Flexibility DHCP failover can be configured to provide redundancy in hot standby mode; or, with load balancing mode, client requests can be distributed between two DHCP servers.

Seamless DHCP servers share lease information, allowing one server to assume the responsibility for servicing clients if the other server is unavailable. DHCP clients can keep the same IP address when a lease is renewed, even if a different DHCP server issues the lease.

Simplicity A wizard is provided to create DHCP failover relationships between DHCP servers. The wizard automatically replicates scopes and settings from the primary server to the failover partner.

Configuring DHCP Failover

One of the nice things about DHCP failover is that the configured scope is replicated between both clustered DHCP nodes whether or not you are running the cluster in hot standby or load balancing mode. If one server fails, the other can manage the entire pool of IP addresses on behalf of the environment. Exercise 20.4 provides step-by-step DHCP failover configuration in Windows Server 2012 R2.

EXERCISE 20.4

Configuring DHCP Failover

1. Open the DHCP Management Console.
2. Right-click IPv4 and choose the Configure Failover command to launch the Configure Failover Wizard. Click Next on the Introduction page.
3. On the Specify The Partner Server To Use For Failover page, select your partner DHCP server from the drop-down menu or by browsing the Add Server directory. Click Next.

4. On the Create A New Failover Relationship page, provide a relationship name, select the Load Balance mode from the drop-down, and provide a shared secret password that will be used to authenticate the DHCP failover relationship between the two servers in the failover cluster. Click Next.

EXERCISE 20.4 *(continued)*

5. Review your configuration settings and click the Finish button to configure your new DHCP failover configuration. Click Close upon successful completion.

6. After the wizard successfully completes on the primary DHCP server, verify that the new failover scope has been created and activated on the secondary DHCP server in the DHCP Management Console to complete this exercise.

You can always go back in and change the properties of the failover scope if you want. Test both hot standby and load balancing modes to decide which deployment configuration option best suits your organization's needs. Expect to see exam scenarios discussing both DHCP failover configuration modes and the differences between them.

DHCP Split Scopes

Even though you have the capabilities of DHCP failover in Windows Server 2012 R2, for exam purposes you will need to understand how DHCP split scopes work. Split scopes are configurable only on IPv4 IP addresses and cannot be configured on IPv6 scopes. The idea of DHCP split scopes is to have two stand-alone DHCP servers that are individually responsible for only a percentage of the IP addresses on a particular subnet.

For example, DHCP Server 1 would be responsible for 70 percent of the IP addresses, and DHCP Server 2 would be responsible for the other 30 percent of IP addresses. The two DHCP servers in a split-scope configuration do not share any lease information between one another, and they do not take over for one another in the event that one of the two DHCP servers fail. As you can see, a split-scope configuration is less fault tolerant than a full DHCP failover configuration. However, a split scope configuration does split the load of DHCP leases and renewals between two servers providing a basic level of native load balancing in a Windows Server 2012 R2 environment.

DHCP Allow and Deny Filtering

One of the nice things about DHCP is that administrators can use allow or deny filtering to control which devices get an IP address and which devices do not on your network. DHCP filtering is controlled by recording a client's MAC address in a list and then enabling either the Allow or Deny filter. One thing to keep in mind about DHCP filtering is that by enabling the allow list, you automatically deny DHCP addresses to any client computer not on the list. In Exercise 20.5, you will configure DHCP filtering by adding a client machine to the Deny filter by MAC address.

EXERCISE 20.5

Configuring DHCP Filtering

1. Open the DHCP Management Console.
2. Expand IPv4 until you reach the Deny filter object in your DHCP hierarchy.
3. Right-click the Deny filter object and select New Filter.
4. Enter the MAC address of the device you want to exclude from your network, provide a description such as **Unwanted Device**, click Add, and then click Close.

5. Right-click the Deny filter and select Enable to complete this exercise.

One of the good things about these filters is that you can move devices from one filter to the other quite easily at any time by right-clicking the device in the list and selecting either Move To Allow or Move To Deny. Test both Allow and Deny filters thoroughly while preparing for the exam. You will most likely see multiple scenarios surrounding DHCP filtering.

Configure DHCP Name Protection

DHCP name protection is an additional configuration option that administrators should consider when working DHCP within their environment. Name protection protects a DHCP leased machine's name from being overwritten by another machine with the same name during DNS dynamic updates so that you can configure a Windows 2012 R2 DHCP

server to verify and update the DNS records of a client machine during the lease renewal process. If the DHCP server detects that a machine's DNS A and PTR records already exist in the environment when a DHCP update occurs, then that DHCP update will fail on that client machine, making sure not to overwrite the existing server name. There are just a few simple steps needed in order to configure DHCP name protection. Exercise 20.6 will walk you through these steps.

EXERCISE 20.6

Enabling DHCP Name Protection

1. Open the DHCP Management Console.
2. Right-click IPv4 and select Properties.
3. The Server Properties dialog box appears. Click the DNS tab.
4. Verify that Enable DNS Dynamic Updates According To The Settings Below is checked, and verify that the radio button labeled Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients is selected.
5. Verify that Discard A And PTR Records When Lease Is Deleted is checked. If not, then check it.

6. Click Configure under Name Protection, and select Enable Name Protection.
7. Click OK twice to complete this exercise.

Configure DNS Registration

Another great feature of Windows Server 2012 R2 DHCP server is the ability to perform registration of DNS records with the DNS server on behalf of its clients. The DHCP server has the flexibility to register DNS clients based on Host A records only instead of being forced to use PTR records during DNS registration. This functionality reduces the number of registration failures that are directly due to the absence of suitable reverse and forward lookup zones on the DNS server.

In addition, you can now also create a DHCP policy that will register only certain clients that match a specific DNS suffix. Together, these new Windows Server 2012 R2 features further integrate DNS and DHCP so that administrators have cleaner control over how clients are registered on their networks. Exercise 20.7 will demonstrate disabling dynamic updates for DNS PTR records in DHCP.

EXERCISE 20.7

Disabling Dynamic Updates

1. Open the DHCP Management Console.
2. Right-click IPv4 and select Properties.
3. Navigate to the DNS tab.
4. Check the box Disable Dynamic Updates For DNS PTR Records.

5. Click Apply and OK to complete this exercise.

All of the new DHCP features provided to you by Windows Server 2012 R2 are worth examining. DHCP failover is a big win for administrators. I'm quite sure that many Windows customers will be changing their DHCP infrastructure from split scopes to a load balanced or hot standby configuration in the near future.

The Ins and Outs of DNS

You learned quite a bit about DNS in Chapter 2. This chapter will expand on what you have already learned over the course of the next few sections. It will focus on hardening your environment with DNS security options, DNS logging and analysis, and a few other advanced configuration options that you will most likely see on the 70-412 exam. DNS is a core network service about which every administrator should have a full understanding. Make it a point to be able to complete each lab from memory to prepare fully for your test.

DNS Security

Security is a main focal point for almost every organization. Since DNS is a core network service that has its hands in every piece of your infrastructure, it is extremely important that you take the time to make sure this environment's DNS is as secure as possible. Let's take a look at few major configuration options for securing DNS on your network.

DNSSEC

Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. DNSSEC works by securing a DNS zone with a process called *zone signing*. When a client machine queries a record in a zone that is signed by DNSSEC, the DNS server returns both the record and the record's digital signature. When you sign a DNS zone using DNSSEC, the following new resource records become available within the environment:

Resource Record Signature (RRSIG) Record This is the additional record that is returned to a client for validity upon a DNS query. This record is stored in the DNSSEC signed zone.

Next Secure (NSEC/NSEC3) Record This record provides proof that a queried record does not exist in the zone. If a client queries a nonexistent record, then the DNS server returns a NSEC record.

DNSKEY This record is used for cryptographic verification of the RRSIG records.

DNSSEC is usually used in high-security environments. The main security advantage of DNSSEC is that it prevents attacks where clients on your network are fed false DNS

information. In addition to the new resource records, when you deploy DNSSEC, the following cryptographic keys are created within the environment:

Zone Signing Key (ZSK) This cryptographic key is used to sign individual host records within a DNSSEC-implemented DNS zone.

Key Signing Key (KSK) This cryptographic key is used to sign all DNSKEY records.

Trust Anchor This cryptographic key is used to validate the DNSKEY record in a DNSSEC protected zone. The trust anchor is replicated to all domain controllers in the forest when you deploy DNSSEC with an Active Directory Integrated zone.

Together, these records and keys provide administrators with enhanced security on their DNS networks. The first DNS server within your environment that you implement with DNSSEC is referred to as the *DNSSEC key master*. It's the key master's job to generate and manage the keys that are signed within a DNSSEC protected zone. Using Group Policy, administrators can set client rules that will ensure that those clients will accept records only from a DNSSEC protected zone. In Exercise 20.8, you will use DNSSEC to sign a zone.

EXERCISE 20.8

Configuring DNSSEC

1. Open DNS Manager.
2. Right-click a forward lookup zone, scroll down to DNSSEC, and click Sign The Zone to launch the Zone Signing Wizard.
3. On the DNS Security Extensions (DNSSEC) page, click Next.
4. On the Signing Options page, select Use Default Settings To Sign The Zone and click Next.

5. On the DNS Security Extensions (DNSSEC) page, click Next.
6. On the Signing the Zone page, click Finish.
7. Verify that the new DNSSEC records and keys have been generated in the zone to complete this exercise.

DNS Socket Pool

DNS socket pooling is another great security technology that helps reduce cache-tampering and spoofing attacks by randomizing which source port is used when issuing DNS queries to remote DNS servers. Port randomization makes it difficult for an attacker to spoof the DNS server with an invalid record. By default, Windows Server 2012 R2 uses a socket pool of 2,500. The maximum configuration is 10,000. Administrators can use the `dnscmd` command-line utility to adjust the DNS socket pool size within their environment. The following is an example of expanding the pool to 5,000 via the command line. Make sure to restart the DNS service after making a change.

```
dnscmd /config /socketpoolsize 5000
```

DNS Cache Locking

DNS cache locking allows an administrator to control when the information stored in the DNS server's cache can be overwritten. When a DNS record is queried, that query is cached by the DNS server based on that record's Time To Live settings. If that same record is queried again before the TTL has expired, the cached information on the DNS server is overwritten. If DNS cache locking is enabled, the DNS server will not overwrite the cached information on new queries of the same record. The feature protects DNS from cache poisoning attacks.

DNS cache locking is configured as a percent value. For example, let's say you configure DNS cache locking at a defined value of 80 percent. This means the DNS server will not overwrite a record's cached information for 80 percent of the duration of that record's TTL. Just like DNS socket pools, DNS cache locking can be configured using the `dnscmd` command-line utility. By default, DNS cache locking is set to 100 percent. The following is an example of changing the default DNS cache locking percentage to 80 percent via the command line. Make sure and restart the DNS service after making a change.

```
dnscmd /config /cachelockingpercent 80
```

Having all of these additional DNS security tools at your disposal will greatly assist you in hardening your environment and making your network more secure overall.

Configure DNS Logging

Since DNS is such a crucial piece of every organization's infrastructure, it has a dedicated event log that tracks all of the actions that are completed by the DNS Server service, as shown in Figure 20.3. By default, in Windows Server 2012 R2, the DNS Server event logs automatically track audit events correlated to the DNS Server service. An audit event is logged each time DNS settings are changed. A few examples of audit events include zone transfers, zone signing, and dynamic updates.

Windows Server 2012 R2 comes with a new set of enhanced DNS Logging and Diagnostic Tools that provide administrators with Analytical and Debug logs in addition to the Audit logs enabled already. Analytical and Debug logs enable activity tracking that logs an event every time the DNS server sends or receives information. A few examples of Analytical log events include response success, response failure, and internal lookup CNAME.

To take full advantage of these additional tools, you must first install a Windows hotfix that will add change auditing and query logging to your DNS server. Analytical and Debug logs are not enabled by default. You can download and install the hotfix from the following location: `http://support.microsoft.com/kb/2956577`.

Once you have successfully installed the Windows hotfix, you can enable Analytical and Debug logs in the Window Event Viewer. Exercise 20.9 will demonstrate the process on enabling these additional DNS logs.

FIGURE 20.3 DNS Server Event Viewer log

EXERCISE 20.9

Enabling DNS Diagnostic Logging

1. Open Event Viewer.
2. Navigate to Applications And Services Logs ➢ Microsoft ➢ Windows ➢ DNS-Server.
3. Right-click and change your view to Show Analytic And Debug Logs. The Analytical log will be displayed.
4. Right-click the Analytical log and select Properties.
5. On the Log Properties page, select the Do Not Overwrite Events radio button, check the box to enable logging, and then click Apply.
6. Click OK to close log properties. You should now see detailed DNS Analytical events populate in the log.

EXERCISE 20.9 *(continued)*

7. Close the Event Viewer to complete this exercise.

DNS logging is a great way to manage and troubleshoot what DNS is doing on your network. Administrators can easily isolate and fix most DNS related issues by checking the event logs. It's even easier when you have the enhanced DNS diagnostic tools enabled.

Configure Delegated Administration

As you are well aware, DNS is highly integrated with Active Directory Domain Services (ADDS). Since the relationship between these two technologies is so close, Active Directory has a built-in security group called DNS Admins to help delegate DNS administration within an environment without having to expose full Domain Admins level privileges to a user account. An administrator would use this security group to separate roles and responsibilities between users.

For example, let's say you have an administrator who is required to manage DNS records, but it is not their responsibility to manage user accounts. Instead of just throwing that administrator in the Domain Admins security group and granting them permissions they don't need, place that administrator's user account in the DNSAdmins security group. This will ensure that you are managing environmental permissions properly, and it will eliminate the possibility of that administrator making changes to things not within their responsibility. You can then use the DNSAdmins group to restrict/allow access to DNS servers on your network just like any other security group.

Configure Recursion

DNS recursion is automatically configured by default in Windows Server 21012 R2. When a client asks a DNS server for a record that isn't stored in a zone that is hosted by that particular DNS server, the DNS server performs a recursive query by going out and finding the result of that query and passing it back to the client if it can be found. This is a nice service for the DNS server to perform, but unfortunately it leaves your network open to denial-of-service (DoS) attacks. In a DoS attack, false or invalid record requests are repeatedly sent to the DNS server, causing it to become increasingly slowed down and even crash completely if it gets too overburdened by requests. To avoid such attacks, it is recommended that DNS recursion be turned off. Exercise 20.10 will walk you through disabling DNS recursion on a DNS server.

EXERCISE 20.10

Disabling DNS Recursion

1. Open DNS Manager.
2. Right-click a DNS server of your choice and click Properties.
3. Navigate to the Advanced tab of the Properties window.
4. Check the box to disable recursion.

EXERCISE 20.10 *(continued)*

5. Click Apply and OK to complete this exercise.

Configure Netmask Ordering

Netmask ordering is another DNS feature that comes automatically enabled by default on Windows Server 2012 R2. Basically, this feature makes sure that if a client requests a host record from the DNS server, the DNS server will always return a host record from that client's subnet if one lives there. The DNS server will examine the first three octets of the client's IP address against the record request, assuming that the closest available response would come from that client's subnet.

DNS uses a round-robin rotation to load balance traffic between multiple server IP addresses that happen to share a single DNS name. For example, you have a hostname of `www.stellacon.com` that maps to three different servers across multiple subnets to help load-balance requests and improve performance within your environment. The IP addresses to each server are as follows:

172.100.10.10

172.100.20.10

172.100.30.10

A client machine with an IP of 172.100.10.150 submits a record request to the DNS server for a lookup on `www.stellacon.com`. Because of netmask ordering, the DNS server will return the IP of 172.100.10.10 for that client to use. Without netmask ordering enabled, the DNS server could have returned IPs for either of the other two servers, depending on where the next request would fall in this round-robin rotation.

Imagine if the other two servers in the previous example were physically located halfway around the world. Your client's connection could be severely degraded compared to the connection you would have on your local subnet. DNS netmask ordering ensures that your clients get the best possible connection available. Verifying that netmask ordering is enabled is done on the same advanced properties page as disabling DNS recursion (shown in Exercise 20.10).

Configure a GlobalNames Zone

A *GlobalNames zone* is a DNS zone in which the host records that live in that zone use short, single-labeled names instead of a fully qualified domain name (FQDN) to communicate on the network. This is similar to the way administrators use Windows Internet Name Service (WINS) as a name resolution protocol alternative to DNS. GlobalName zones are not intended to support peer-to-peer networks and workstation name resolution, and they don't support dynamic DNS updates. In Exercise 20.11, you will configure a DNS GlobalNames zone.

EXERCISE 20.11

Configuring a GlobalNames Zone

1. Open DNS Manager.
2. Right-click one of your DNS servers and click New Zone to start the New Zone Wizard.
3. Click Next on the Welcome page.
4. On the Zone Type page, make sure that Primary Zone and the Store Zone in Active Directory (available only if DNS server is a writeable domain controller) are selected and then click Next.
5. Click To All DNS Servers In This Forest and then click Next.
6. Click Forward Lookup Zone and then click Next.
7. In Zone Name, type **GlobalNames** and then click Next.
8. Click Do Not Allow Dynamic Updates and then click Next.
9. Click Finish to create the GlobalNames zone and complete this exercise.

Analyze Zone-Level Statistics

Windows Server 2012 R2 introduces a set of new features for gathering and analyzing DNS server statistics. Having this level of granularity for DNS statistics is useful for troubleshooting DNS-related issues. Using PowerShell, an administrator can now easily get the following statistics on every authoritative zone within the environment.

Zone Update Statistics Provides information on zone dynamic update transactions

- **DynamicUpdateReceived** The total number of dynamic update requests received by the DNS server
- **DynamicUpdateRejected** The total number of dynamic updates rejected by the DNS server

Zone Query Statistics Provides the following information

- **QueriesReceived** The number of queries received
- **QueriesResponded** The number of queries responded successfully (with a valid DNS response)
- **QueriesFailure** The number of queries not responded successfully
- **QueriesNameError** The number of queries that responded with an NXDOMAIN or EMPTY AUTH response

Zone Transfer Statistics Provides information about the zone transfer transactions

- **RequestReceived** The total number of zone transfer requests received by the DNS Server service when operating as a primary server for a specific zone
- **RequestSent** The total number of zone transfer requests sent by the DNS Server service when operating as a secondary server for a specific zone
- **ResponseReceived** The total number of zone transfer requests received by the DNS Server service when operating as a secondary server for a specific zone
- **SuccessReceived** The total number of zone transfers received by the DNS Server service when operating as a secondary server for a specific zone
- **SuccessSent** The total number of zone transfers successfully sent by the DNS Server service when operating as a master server for a specific zone

Use the following PowerShell syntax to analyze and view complete DNS zone-level statistics within your environment:

```
Get-DnsServerStatistics -ZoneName yourdomain.com
```

IPAM Administration 101

One of the great features of Windows Server 2012 R2 is the *IP Address Management (IPAM)* utility. IPAM is a built-in utility that allows an administrator to discover, monitor, audit, and manage the TCP/IP schema used on your network. IPAM provides an administrator with the ability to observe and administer the servers that are running the Dynamic Host Configuration Protocol (DHCP) and the Domain Name System. IPAM includes some of the following advantages:

Automatic IP Address Infrastructure Discovery IPAM has the ability to discover automatically the domain's DHCP servers, DNS servers, and domain controllers. IPAM can do the discovery for any of the domains you specify. Administrators also have the ability to enable or disable management of these servers using the IPAM utility.

Management of DHCP and DNS Services IPAM gives administrators the capability to monitor and manage Microsoft DHCP and DNS servers across an entire network using the IPAM console.

Custom IP Address Management Administrators now have the ability to customize the display of IP addresses and tracking and utilization data. IPAM allows the IP address space to be organized into IP address blocks, IP address ranges, and individual IP addresses. To help you organize the IP address space further, built-in or user-defined fields are also assigned to the IP addresses.

Auditing and Tracking of IP Address IPAM allows administrators to track and audit IP addresses through the use of the IPAM console. IPAM allows IP addresses to be tracked using DHCP lease events and user logon events. These events are collected from the Network Policy Server (NPS) servers, domain controllers, and DHCP servers. Administrators can track IP data by following the IP address, client ID, hostname, or username.

As an administrator, you should understand a few things before installing the IPAM feature. When setting up an IPAM server, you must *not* install IPAM on a domain controller. There are three main methods to deploy an IPAM server.

Distributed This method allows an IPAM server deployment at every site in an enterprise network.

Centralized This method allows only one IPAM server in an enterprise network.

Hybrid This method uses a central IPAM server deployment along with dedicated IPAM servers at each site in the enterprise network.

Remember, when installing IPAM in any of the scenarios mentioned, you cannot install the IPAM feature on an Active Directory domain controller.

Provision IPAM Manually or by Using Group Policy

If configured, IPAM automatically communicates on your domain. IPAM will try to locate your DNS servers, DHCP servers, and domain controllers as long as those servers are within the searching scope that you have configured. An administrator can configure whether the servers (DNS, DHCP, and domain controllers) are managed by IPAM or unmanaged. Please note that this will work only with Microsoft products; it won't find Infoblox or Unix-based DNS/DHCP.

If you want your servers to be managed by IPAM, you must make sure you set up the network and the servers properly. For example, you will need to configure the security settings and firewall ports properly on the servers (DNS, DHCP, and domain controllers) in order to allow IPAM to access these servers and perform its configuration and monitoring. You can configure these server settings in one of two ways: manually or automatically through the use of a Group Policy object (GPO).

Exercise 20.12 will show you how to install the IPAM feature. You will install and configure the IPAM feature using Server Manager. This exercise has to be done on a member server.

EXERCISE 20.12

Installing the IPAM Feature

1. Open Server Manager.
2. Click the number 2 link, Add Roles And Features.
3. Choose a role-based or feature-based installation and click Next.
4. Choose your server and click Next.
5. On the Roles screen, just click Next.
6. On the Features screen, click the box for the IP Address Management (IPAM) server. Click the Add Features button when the box appears. Click Next.
7. At the Confirmation screen, click the Install button.
8. Once the installation is complete, click the Close button.
9. While in Server Manager, click the IPAM link on the left side. This opens the IPAM Overview page.
10. Click number 2, Provision The IPAM Server.
11. Click Next at the Before You Begin screen.
12. Make your database selection on the Configure Database screen and click Next.
13. At the Select Provisioning Method screen, choose GPO and put in a GPO suffix name. I used IPAM1 for the GPO suffix name. This is a unique name to help identify the IPAM.

14. At the Summary screen, click the Apply button.
15. Once the process is completed, click the Close button.
16. Under Manage on the IPAM overview screen, choose Add Server.

EXERCISE 20.12 *(continued)*

17. In the Add Servers box, click the DNS tab. In the search box, type the name of your DNS server and click the magnifying glass.

18. Under Name, double-click the server name. The server will be added to the right-side box. Click OK. Close Server Manager.

Configure Server Discovery

Once you have successfully installed and provisioned the IPAM feature on your Windows Server 2012 R2 machine, you can begin server discovery. One of the great things about IPAM is that you can define multiple domains within the same forest to be managed by a single IPAM server. Once initiated, server discovery will automatically search for all of the machines running on the specified domain. Administrator privileges are required for the domain against which you are running server discovery. Exercise 20.13 will walk you through the server discovery process.

EXERCISE 20.13

Configuring IPAM Server Discovery

1. Open Server Manager and select IPAM.
2. On the IPAM Overview page, select option 3, Configure Server Discovery.
3. On the Configure Server Discovery page, select and add the domains you want to discover and click OK.

4. On the IPAM Overview page, select option 4, Start Server Discovery. The task will run in the background. You will receive notification once server discovery has completed.
5. On the IPAM home page, select Server Inventory to review the now-completed server discovery of the requested domain. Servers found by server discovery will be in a blocked status until those servers have applied the GPO configured from Exercise 20.12.

Create and Manage IP Blocks and Ranges

In IPAM, IP address space is divided into addresses, ranges, and blocks. Blocks are groups of ranges, and ranges are groups of IPs. Here you will find a breakdown of each IP Management space found within IPAM:

IP Addresses Individual IP addresses map to a single IP address range. When you map an IP address to a range, it enables actions to be taken on a range that affect all IP addresses in the range, such as adding, updating, or deleting IP address fields.

IP Address Ranges IP address ranges are smaller chunks of IP addresses that typically correspond to a DHCP scope. IP address ranges are contained within, or "mapped to," IP address blocks. IP address ranges cannot map to multiple IP address blocks, and ranges that map to the same block cannot overlap.

IP Address Blocks IP address blocks are large chunks of IP addresses that are used to organize address space at a high level. For example, you might use one IP address block for all private IP addresses in your organization and another block for public IP addresses. You can think of IP address blocks as containers that hold IP address ranges. IP address blocks are not deployed and managed on the network like IP address ranges or individual IP addresses.

When you have an IPAM managed DHCP server, the IP address ranges found within the scopes of that DHCP server are automatically entered into the IPAM database during the discovery process. Individual IP addresses and IP blocks are not automatically added to the IPAM database. Exercise 20.14 will demonstrate how to add an IP address space manually.

EXERCISE 20.14

Manually Add IPAM IP Address Space

1. Open Server Manager and select IPAM.
2. Select IP Address Inventory.
3. Right-click IPv4 and select Add IP Address.
4. Enter the IP address of the device that is to be managed by IPAM. Keep all other defaults.
5. Click Apply.
6. On the Summary page, verify that the task completed successfully.

7. Click OK to complete this exercise. Your new IP address is now managed by IPAM. You can now both create and delete DHCP reservations and DNS records for this IP address space from inside the IPAM management console. Similar steps are used to create IP address ranges and blocks. Find the wizard for each under the Tasks menu in the IPAM navigation window.

Monitor Utilization of IP Address Space

It is essential for network administrators to be able to monitor and manage their IP address infrastructure well. This grows increasingly difficult as your network gets bigger and becomes more complex. Unfortunately, quite a few administrators still rely on spreadsheets and basic database applications for IP tracking and usage. The problem is that manual tracking is time-consuming and prone to error.

IPAM tracks the service status of the DNS and DHCP servers on the network. By aggregating multiple DHCP servers, the multiserver management (MSM) module enables an administrator to perform editing and configuration of important properties on multiple DHCP servers and scopes. It also facilitates surveillance and tracking of DHCP service status and utilization of DHCP scopes. IPAM allows for monitoring the condition of a DNS zone on multiple DNS servers by exposing the collected status of a zone across all authoritative DNS servers.

IPAM also comes with its own event catalog that allows administrators to track both DHCP and DNS correlated events. The nice thing about this event log is that you can easily search by client hostname, client ID, username, or IP address for a full list of both DNS- and DHCP-related events on that client. You can also export these event logs to an Excel workbook. The Event Catalog is found toward the bottom of the IPAM hierarchical navigation window, as shown in Figure 20.4.

FIGURE 20.4 IPAM event catalog

Migrate to IPAM

The situation may arise in which you must migrate your IPAM database infrastructure either from a Windows Internal Database (WID) to a Microsoft SQL database or from one SQL server to another. New to Windows Server 2012 R2, IPAM comes with the functionality to migrate an IPAM database via PowerShell. The `Move-IpamDatabase` cmdlet is used to complete this operation. When this cmdlet is run, a new IPAM schema is created, and then all of the IP address information is copied over. You can also use the `Get-IpamDatabase` cmdlet to review and compare pre- and postdatabase configuration settings during an IPAM database migration.

Delegate IPAM Administration

The delegation of IPAM administration is similar to the delegation of DNS. When IPAM is installed and provisioned, new security groups become available to administrators to configure role-based administration within your IPAM infrastructure. The five new security groups for IPAM administration are as follows:

IPAM Administrators Members of this group have full permissions to manage and administer an IPAM infrastructure.

IPAM IP Audit Administrators Members of this group can perform common IPAM management tasks and can carry out IPAM audits.

IPAM ASM Administrators Members of this group can perform tasks related to IP address space management (ASM) functionality.

IPAM MSM Administrator Members of this group can perform tasks across multiple IPAM servers through the IPAM multiserver management (MSM) functionality.

IPAM Users Members of this group can only view information about server discovery, ASM, and MSM in IPAM. They can also view operational events, but they have no access to tracking or auditing information.

In addition to these new security groups, IPAM comes with a new Access Control feature, which allows administrators to get even more granular with IPAM permissions by using up to eight different preconfigured roles. You can also create your own custom IPAM administration roles for full IPAM permissions flexibility within your environment. Figure 20.5 illustrates the new Access Control panel for IPAM delegation of administration. Take the time to add and remove users from each of these groups and roles to get used to IPAM permission sets.

FIGURE 20.5 IPAM Access Control

Manage IPAM Collections

In IPAM, server groups are logical groups used to organize managed DHCP and DNS servers. Servers are members of a server group based on values of custom fields that are assigned to the server. Having servers of the same type sorted into their own IPAM collections makes it easier to manage your server lists within the IPAM Management Console. Drop-down menus will allow you to filter server and task lists by IPAM service categories such as DNS or DHCP servers.

Configure IPAM Database Storage

There are two possible IPAM database storage solutions. An administrator can use either a Windows Internal Database (WID) or a dedicated Microsoft SQL Server Instance for their IPAM configuration. For smaller networks, a WID back end will work just fine for the initial IPAM deployment. If in the future the need arises to expand past a WID to a SQL database, then you already know that IPAM comes with migration functionality just for that situation. The database configuration options are chosen during the provisioning steps of an IPAM deployment.

Fully deploy and test the capabilities of the IPAM feature set to help track and forecast IP address utilization within your organization. IPAM is great way to discover, monitor, and manage all of the TCP/IP devices on your network.

Summary

This chapter talked about the advanced configuration options of DHCP, DNS, and IPAM. You learned step-by-step how to configure core network services and features. These features allow administrators to manage network devices easily in a large or complex environment. Understanding how DHCP, DNS, and IPAM all work together is essential for ensuring success when taking the exam. Focus your attention on completing the labs found within the chapter and learning the ins and outs of each management console for DHCP, DNS, and IPAM administration.

Exam Essentials

Understand DHCP Failover DHCP failover (and load sharing) is one of the hottest new features in Windows Server 2012 R2. It is easy to deploy, and it provides an added level of redundancy when compared to using a DHCP split-scope configuration.

Know How to Configure DHCP Name Protection DHCP name protection protects DNS Host A records from being overwritten by other client's Host A records during DNS dynamic updates. DHCP name protection is configured using the DHCP Management Console.

Understand IP Address Management IPAM allows administrators to track and audit IP addresses through the use of the IPAM console. IPAM allows IP addresses to be tracked using DHCP lease events and user logon events.

Know How to Provision IPAM and Configure Server Discovery IPAM is managed and monitored in Server Manager. Know that there are two separate provisioning models—manual and GPO—and know how to configure each. Know how to configure IPAM server discovery.

Understand Security for DNS Hardening your DNS infrastructure is important. Know how to configure and use DNSSEC, socket pooling, and cache locking to make your network more secure.

Know How to Configure and Use DNS Logging DNS logging gives administrators a more granular inside view at what DNS is actually doing on the network. DNS logging helps administrators troubleshoot DNS issues within the environment.

Know How to Analyze DNS Zone-Level Statistics Administrators can use PowerShell to troubleshoot DNS-related issues further. You can generate and export multiple reports that will help you analyze DNS queries, requests, and dynamic updates.

Know How to Delegate Both DNS and IPAM Administration Active Directory has specific security groups for delegating DNS administration, and IPAM has its own internal delegation of administration. A user does not need to be a member of the Domain Admins group in order to manage these services.

Review Questions

1. You are the network administrator for a midsize computer company. You have a single Active Directory forest, and you have a requirement to implement DHCP for the organization. You need to ensure that your DHCP deployment configuration is both fault-tolerant and redundant. Out of the options provided, which is the most reliable DHCP configuration that you could implement?
   - **A.** DHCP split scope
   - **B.** DHCP multicast scope
   - **C.** DHCP failover
   - **D.** DHCP super scope

2. You are a systems administrator for a large computer company. You have a multidomain Active Directory forest, and you have a requirement to implement advanced DNS security options for the organization. Which three security options could you configure to make DNS more secure on your network? (Choose three.)
   - **A.** DNSSEC
   - **B.** DNS registration
   - **C.** DNS cache locking
   - **D.** DNS socket pooling

3. You are the network administrator for a software development company. Your DNS infrastructure consists of multiple DNS servers that are geographically disparate. You need to ensure that when clients perform DNS queries, those queries will always be sent to the closest DNS server for lookup services. What must be enabled for this to take place on your network?
   - **A.** DNS logging
   - **B.** DNS delegated administration
   - **C.** DNS recursion
   - **D.** DNS netmask ordering

4. You are an IT manager for an enterprise storage solutions company. You have just hired a new team member to your network staff with the primary responsibility of managing DNS for your organization. It will not be this administrator's responsibility to manage any other active directory services for the company. Which security group would best fit this administrator's responsibilities?
   - **A.** Domain Admins
   - **B.** Enterprise Admins
   - **C.** Schema Admins
   - **D.** DNSAdmins

5. You are the network administrator for a toy company. Your DHCP infrastructure includes the use of DNS dynamic updates. You need to ensure that DNS host A records are not overwritten by new DNS devices with the same hostname during DNS dynamic updates. Which DHCP configuration option would fulfill this requirement?
   - **A.** Configure DNS Registration
   - **B.** Configure DHCP Name Protection
   - **C.** Configure DHCP High Availability
   - **D.** Implement A DHCPv6 Scope

6. You are the infrastructure team lead for a high-tech hardware development company. You need to delegate some of the teams IPAM administration responsibilities between team members. You decide that Noelle will be managing IPAM address spaces, but she will not be managing IP address tracking and auditing. Which IPAM security group would best fit Noelle's new responsibilities?
   - **A.** IPAM Administrators
   - **B.** IPAM Users
   - **C.** IPAM ASM Administrators
   - **D.** IPAM MSM Administrators

7. You are the network administrator for a large communications company. You have recently decided to implement IPAM within your organization with the release of Windows Server 2012 R2. You want to set up your IPAM infrastructure so that one primary server can manage your entire enterprise. Which IPAM deployment method would fulfill this requirement?
   - **A.** Isolated
   - **B.** Centralized
   - **C.** Hybrid
   - **D.** Distributed

8. You are the systems administrator for an advanced space exploration research facility. Your DNS infrastructure needs to accommodate the use of short, single-labeled DNS hostnames instead of the usual FQDN. Which advanced network configuration option would accommodate this requirement?
   - **A.** Configure DNS Recursion
   - **B.** Configure DHCP Name Protection
   - **C.** Configure IPAM Server Discovery
   - **D.** Configure A GlobalNames Zone

9. You are the lead network administrator for a web hosting company. You have recently made the decision to implement IPAM within your organization. You have already installed and provisioned the IPAM feature on your dedicated Windows Server 2012 R2 server. What is the next logical step in your IPAM deployment?

A. Create a new IP block

B. Delegate IPAM administration

C. Configure server discovery

D. Create a new IP range

10. You are a systems administrator for the Stellacon Corporation. Because of the unusual growth of TCP/IP devices on your corporate network over the last year, you need to scale out your IPAM database capabilities. You are currently using a Windows Internal Database (WID) for your IPAM infrastructure, and you want to migrate your IPAM database to a Microsoft SQL Server. Which PowerShell cmdlet would you use to verify current IPAM database configuration settings?

A. `Get-IpamDatabase`

B. `Show-IpamDatabaseConfig`

C. `Show-IpamStatistics`

D. `Get-IpamMigrationSettings`

Chapter

21

Configure the Active Directory Infrastructure

THE FOLLOWING 70-412 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure a forest or a domain**

- Implement multi-domain and multi-forest Active Directory environments including interoperability with previous versions of Active Directory
- Upgrade existing domains and forests including environment preparation and functional levels
- Configure multiple user principal name (UPN) suffixes

✓ **Configure Trusts**

- Configure external, forest, shortcut, and realm trusts
- Configure trust authentication
- Configure SID filtering
- Configure name suffix routing

✓ **Configure Sites**

- Configure sites and subnets
- Create and configure site links
- Manage site coverage
- Manage registration of SRV records
- Move domain controllers between sites

✓ **Manage Active Directory and SYSVOL replication**

- Configure replication to Read-Only Domain Controllers (RODCs)
- Configure Password Replication Policy (PRP) for RODCs
- Monitor and manage replication
- Upgrade SYSVOL replication to Distributed File System Replication (DFSR)

Microsoft has designed Active Directory to be an enterprise-wide solution for managing network resources. In previous chapters, you saw how to create Active Directory objects based on an organization's logical design. Domain structure and organizational unit (OU) structure, for example, should be designed based primarily on an organization's business needs.

Now it's time to learn how Active Directory can map to an organization's *physical* requirements. Specifically, you must consider network connectivity between sites and the flow of information between domain controllers (DCs) under less-than-ideal conditions. These constraints determine how domain controllers can work together to ensure that the objects within Active Directory remain synchronized no matter how large and geographically dispersed the network.

Fortunately, through the use of the Active Directory Sites and Services administrative tool, you can quickly and easily create the various components of an Active Directory replication topology. Using this tool, you can create objects called *sites*, place servers in sites, and create connections between sites. Once you have configured Active Directory replication to fit your current network environment, you can sit back and allow Active Directory to make sure that information remains consistent across domain controllers.

This chapter covers the features of Active Directory, which allow system administrators to modify the behavior of replication based on their physical network design. Through the use of sites, system and network administrators will be able to leverage their network infrastructure best to support Windows Server 2012 R2 and Active Directory.

So far, you have learned the steps necessary to install the Domain Name System (DNS) and to implement the first Active Directory domain. Although I briefly introduced multidomain Active Directory structures earlier, I focused on only a single domain and the objects within it.

Many businesses find that using a single domain provides an adequate solution to meet their business needs. By working with *trees* and *forests*, however, large organizations can use multiple domains to organize their environments better.

Overview of Network Planning

Before I discuss sites and replication, you need to understand some basic physical and network concepts.

The Three Types of Networks

When designing networks, system and network administrators use the following terms to define the types of connectivity between locations and servers:

Local Area Networks A *local area network (LAN)* is usually characterized as a high-bandwidth network. Generally, an organization owns all of its LAN network hardware and software. Ethernet is by far the most common networking standard. Ethernet speeds are generally at least 10Mbps and can scale to multiple gigabits per second. Currently, the standard for Ethernet is the 10 Gigabit Ethernet, which runs at 10 times the speed of Gigabit Ethernet (1GB). Several LAN technologies, including routing and switching, are available to segment LANs and to reduce contention for network resources.

Wide Area Networks The purpose of a *wide area network (WAN)* is similar to that of a LAN, that is, to connect network devices. Unlike LANs, however, WANs are usually leased from third-party telecommunications carriers and organizations known as *Internet service providers (ISPs)*. Although extremely high-speed WAN connections are available, they are generally costly for organizations to implement through a distributed environment. Therefore, WAN connections are characterized by lower-speed connections and, sometimes, nonpersistent connections.

The Internet The *Internet* is a worldwide public network infrastructure based on the *Internet Protocol (IP)*. Access to the Internet is available through Internet service providers (ISPs). Because it is a public network, there is no single "owner" of the Internet. Instead, large network and telecommunications providers constantly upgrade the infrastructure of this network to meet growing demands.

Organizations use the Internet regularly to sell and market their products and services. For example, it's rare nowadays to see advertisements that don't direct you to one website or another. Through the use of technologies such as *virtual private networks (VPNs)*, organizations can use encryption and authentication technology to enable secure communications across the Internet.

Exploring Network Constraints

In an ideal situation, a high-speed network would connect all computers and networking devices. In such a situation, you would be able to ensure that any user of your network, regardless of location, would be able to access resources quickly and easily. When you are working in the real world, however, you have many other constraints to keep in mind, including network bandwidth and network cost.

Network Bandwidth

Network bandwidth generally refers to the amount of data that can pass through a specific connection in a given amount of time. For example, in a WAN situation, a T1 may have 1.544Mbps (megabits per second), while a DSL might have a bandwidth of 56Kbps or 57.6Kbps (kilobits per second) or more. On the other hand, your LAN's Ethernet connection may have a bandwidth of 100Mbps. Different types of networks work at

different speeds. Therefore, it's imperative that you always consider network bandwidth when thinking about how to deploy domain controllers in your environment.

Network Cost

Cost is perhaps the single largest factor in determining a network design. If cost were not a constraint, organizations would clearly elect to use high-bandwidth connections for all of their sites. Realistically, trade-offs in performance must be made for the sake of affordability. Some factors that can affect the cost of networking include the distance between networks and the types of technology available at locations throughout the world. In remote or less-developed locations, you may not even be able to get access through an ISP or telecom beyond a satellite connection or dial-up, and what is available can be quite costly. Network designers must keep these factors in mind, and they must often settle for less-than-ideal connectivity.

You have considered the monetary value of doing business. Now let's consider another aspect of cost. When designing and configuring networks, you can require certain devices to make data-transport decisions automatically based on an assigned network cost. These devices are commonly known as *routers*, and they use routing protocols to make routing decisions. One of the elements a router uses to configure a routing protocol is its ability to adjust the cost of a route. For example, a router may have multiple ways to connect to a remote site, and it may have multiple interfaces connected to it, each with different paths out of the network to which it is connected locally. When two or more routes are available, you can set up a routing protocol that states that the route with the lower cost is automatically used first.

Another cost is personnel. Do you have the personnel to do the job, or do you need to hire a consultant? Remember that even if you use individuals already on staff, they will be spending time on these projects. When your IT team is working on a project, this is a cost because they cannot also be working on day-to-day tasks.

All of these factors play an important role when you make your Active Directory implementation decisions.

Overview of Active Directory Replication and Sites

Now I need to address two topics that not only are covered heavily on the Microsoft exams but are two areas that all IT administrators should understand. Understanding Active Directory replication and sites can help you fine-tune a network to run at peak performance.

Replicating Active Directory

Regardless of the issues related to network design and technological constraints, network users have many different requirements and needs that must be addressed. First, network resources, such as files, printers, and shared directories, must be made available.

Similarly, the resources stored within Active Directory, and its security information in particular, are required for many operations that occur within domains.

With these issues in mind, take a look at how you can configure Active Directory to reach connectivity goals using replication.

Active Directory was designed as a scalable, distributed database that contains information about an organization's network resources. In previous chapters, you saw how you can create and manage domains and how you can use domain controllers to store Active Directory databases.

Even in the simplest of network environments, you generally need more than one domain controller. The major reasons for this are *fault tolerance* (if one domain controller fails, others can still provide services as needed) and performance (the workload can be balanced between multiple domain controllers). Windows Server 2012 R2 domain controllers have been designed to contain read-write copies as well as read-only copies of the Active Directory database. However, the domain controllers must also remain current when objects are created or modified on other domain controllers.

To keep information consistent between domain controllers, you use *Active Directory replication*. Replication is the process by which changes to the Active Directory database are transferred between domain controllers. The result is that all of the domain controllers within an Active Directory domain contain up-to-date information and achieve convergence. Keep in mind that domain controllers may be located very near to each other (for example, within the same server rack), or they may be located across the world from each other. Although the goals of replication are quite simple, the real-world constraints of network connections between servers cause many limitations that you must accommodate. If you have a domain controller on your local LAN, you may find that you have Gigabit Ethernet, which runs at 1000Mbps between your server connections, whereas you may have a domain controller on the other side or a WAN where the network link runs at a fraction of a T1, 56Kbps. Replication traffic must traverse each link to ensure convergence no matter what the speed or what bandwidth is available.

Throughout this chapter, you will study the technical details of Active Directory replication. You will also learn how to use the concept of sites and site links to map the logical structure of Active Directory to a physical network topology to help it work efficiently, no matter the type of link with which you are working.

Understanding Active Directory Site Concepts

One of the most important aspects of designing and implementing Active Directory is understanding how it allows you to separate the logical components of the directory service from the physical components.

The logical components—Active Directory domains, OUs, users, groups, and computers—map to the organizational and business requirements of a company.

The physical components, on the other hand, are designed based on the technical issues involved in keeping the network synchronized (that is, making sure that all parts of the network have the same up-to-date information). Active Directory uses the concept of sites to map to an organization's physical network. Stated simply, a *site* is a collection of well-connected subnets. The technical implications of sites are described later in this chapter.

It is important to understand that no specified relationship exists between Active Directory domains and Active Directory sites. An Active Directory site can contain many domains. Alternatively, a single Active Directory domain can span multiple sites. Figure 21.1 illustrates this very important characteristic of domains and sites.

FIGURE 21.1 Potential relationships between domains and sites

There are two main reasons to use Active Directory sites: service requests and replication.

Service Requests

Clients often require the network services of a domain controller. One of the most common reasons for this is that they need the domain controller to perform network authentication. If your Active Directory network is set up with sites, clients can easily connect to the domain controller that is located closest to them. By doing this, they avoid many of the inefficiencies associated with connecting to distant domain controllers or to those that are located on the other side of a slow network connection. For example, by connecting to a local domain controller, you can avoid the problems associated with a saturated network link that might cause two domain controllers to be out of sync with each other.

Replication

As mentioned earlier, the purpose of Active Directory replication is to ensure that the information stored on all domain controllers within a domain remains synchronized. In environments with many domains and domain controllers, multiple communication paths usually connect them, which makes the synchronization process more complicated. A simple method of transferring updates and other changes to Active Directory involves all of the servers communicating directly with each other as soon as a change occurs; they can all update with the change and reach convergence again. This is not ideal, however, because it places high requirements on network bandwidth and is inefficient for many network environments that

use slower and more costly WAN links, especially if all environments update at the same time. Such simultaneous updating could cause the network connection at the core of your network to become saturated and decrease the performance of the entire WAN.

Using sites, Active Directory can automatically determine the best methods for performing replication operations. Sites take into account an organization's network infrastructure, and Active Directory uses these sites to determine the most efficient method for synchronizing information between domain controllers. System administrators can make their physical network design map to Active Directory objects. Based on the creation and configuration of these objects, the Active Directory service can then manage replication traffic in an efficient way.

Whenever a change is made to the Active Directory database on a domain controller, the change is given an update sequence number. The domain controller can then propagate these changes to other domain controllers based on replication settings.

Windows Server 2012 R2 uses a feature called *linked value replication* that is active only when the domain is in the Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 domain functional level. With linked value replication, only the group member is replicated. This greatly enhances replication efficiency and cuts down on network traffic utilization. Linked value replication is automatically enabled in Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 functional-level domains.

Planning Your Sites

Much of the challenge of designing Active Directory is related to mapping a company's business processes to the structure of a hierarchical data store. So far, you've seen many of these requirements. What about the existing network infrastructure, however? Clearly, when you plan for and design the structure of Active Directory, you must take into account your LAN and WAN characteristics. Let's see some of the ways that you can use Active Directory sites to manage replication traffic.

Synchronizing Active Directory is extremely important. To keep security permissions and objects within the directory consistent throughout the organization, you must use replication. The Active Directory data store supports *multimaster replication*; that is, data can be modified at any domain controller within the domain because replication ensures that information remains consistent throughout the organization.

Ideally, every site within an organization has reliable, high-speed connections with the other sites. A much more realistic scenario, however, is one in which bandwidth is limited and connections are sometimes either sporadically available or completely unavailable.

Using sites, network and system administrators can define which domain controllers are located on which areas of the network. These settings can be based on the bandwidth available between the areas of the network. Additionally, these administrators can define *subnets*—logically partitioned areas of the network—between areas of the network. Subnets are designed by subdividing IP addresses into usable blocks for assignment, and they are also objects found within the Sites and Services Microsoft Management Console (MMC) in the Administrative Tools folder. Windows Server 2012 R2 Active Directory services use this information to decide how and when to replicate data between domain controllers.

Directly replicating information between all domain controllers might be a viable solution for some companies. For others, however, this might result in a lot of traffic traveling over slow or undersized network links. One way to synchronize data efficiently between sites that have slow connections is to use a *bridgehead server*. Bridgehead servers are designed to accept traffic between two remote sites and then to forward this information to the appropriate servers. Figure 21.2 provides an example of how a bridgehead server can reduce network bandwidth requirements and improve performance. Reduced network bandwidth requirements and improved performance can also be achieved by configuring replication to occur according to a predefined schedule if bandwidth usage statistics are available.

FIGURE 21.2 Using a bridgehead server

Bridgehead servers do not fit a normal hub-and-spoke WAN topology. Such a topology usually involves a core site (for example, company headquarters) with remote sites as links one off from the core. However, you can use a bridgehead server design to fit a distributed star, where you have a hub-and-spoke topology design with additional spokes coming out of the first set of spokes. Doing so would make some of your spoke sites into smaller core sites. It is at these sites that you would place your bridgehead servers. In Figure 21.2, you can see that your Asia headquarters site is also where you can connect to India, China, and Hong Kong, thus making the Asia headquarters the ideal site for the bridgehead server.

In addition to managing replication traffic, sites offer the advantage of allowing clients to access the nearest domain controller. This prevents problems with user authentication across slow network connections, and it can help find the shortest and fastest path to resources such as files and printers. Therefore, Microsoft recommends that you place at least one domain controller at each site that contains a slow link. Preferably, this domain controller also contains a copy of the global catalog so that logon attempts and resource search queries do not occur across slow links. The drawback, however, is that deploying more copies of the global catalog to servers increases replication traffic.

Through proper planning and deployment of sites, organizations can best use the capabilities of the network infrastructure while keeping Active Directory synchronized.

Understanding Distributed File System Replication

DFS Replication (DFSR) was created to replace the File Replication Service (FRS) that was introduced in the Windows 2000 Server operating systems. DFSR is a state-based, multimaster replication engine that supports replication scheduling and bandwidth throttling. DFSR has the ability to detect insertions, removals, and rearrangements of data in files. This allows DFS Replication to replicate only the changed file blocks when files are updated.

The DFS Replication component uses many different processes to keep data synchronized on multiple servers. To understand the DFSR process, it is helpful to understand some of the following concepts:

- DFSR is a multimaster replication engine, and changes that occur on one of the members are then replicated to all of the other members of the replication group.
- DFSR uses the update sequence number (USN) journal to detect changes on the volume, and then DFSR replicates the changes only after the file is closed.
- Before sending or receiving a file, DFSR uses a staging folder to stage the file.
- When a file is changed, DFSR replicates only the changed blocks and not the entire file. The RDC protocol is what helps determine the blocks that have changed in the file.
- One of the advantages of DFSR is that it is self-healing and can automatically recover from USN journal wraps, USN journal loss, or loss of the DFS Replication database.
- Windows Server 2012 R2 DFSR includes the ability to add a failover cluster as a member of a replication group.
- Windows Server 2012 R2 DFSR allows for read-only replicated folders on a particular member in which users cannot add or change files.
- In Windows Server 2012 R2, it is possible to make changes to the `SYSVOL` folder of an RODC.

The `Dfsrdiag.exe` command-line tool includes three Windows Server 2012 R2 command-line switches that provide enhanced diagnostic capabilities for DFSR:

`Dfsrdiag.exe ReplState` When you use the `ReplState` switch, a summary of the replication status across all connections on the specified replication group member is provided. The `ReplState` switch takes a snapshot of the internal state of the DFSR service, and the updates that are currently being processed (downloaded or served) by the service are shown in a list.

`Dfsrdiag.exe IdRecord` When replicating a file or folder, the DFSR service creates an ID record, and an administrator can use this ID record to determine whether a file has replicated properly to a specific member. The `IdRecord` switch returns the DFSR ID record for the file or folder that you specify by using its path or its unique identifier (UID).

`Dfsrdiag.exe FileHash` The `FileHash` switch, when used against a particular file, will compute and display the hash value that is generated by the DFSR service. An administrator can then look at the hash values to compare two files. If the hash values for the two files are the same, then the two files are the same.

Implementing Sites and Subnets

Now that you have a good idea of the goals of replication, take a look at the following quick overview of the various Active Directory objects that are related to physical network topology.

The basic objects that are used for managing replication include the following:

Subnets A *subnet* is a partition of a network. As I started to discuss earlier, subnets are logical IP blocks usually connected to other IP blocks through the use of routers and other network devices. All of the computers that are located on a given subnet are generally well connected with each other.

It is extremely important to understand the concepts of TCP/IP and the routing of network information when you are designing the topology for Active Directory replication. TCP/IP is covered in detail in Chapter 8, "Configure TCP/IP."

Sites An Active Directory site is a logical object that can contain servers and other objects related to Active Directory replication. Specifically, a *site* is a grouping of related subnets. Sites are created to match the physical network structure of an organization. Sites are primarily used for slow WAN links. If your network is well connected (using fiber optics, Category 5 Ethernet, and so on), then sites are not needed.

Site Links A *site link* is created to define the types of connections that are available between the components of a site. Site links can reflect a relative cost for a network connection and can also reflect the bandwidth that is available for communications.

All of these components work together to determine how information is used to replicate data between domain controllers. Figure 21.3 provides an example of the physical components of Active Directory.

FIGURE 21.3 Active Directory replication objects

Many issues are related to configuring and managing sites, and all of them are covered in this chapter. Overall, using sites allows you to control the behavior of Active Directory replication between domain controllers. With this background and goal in mind, let's look at how you can implement sites to control Active Directory replication so that it is efficient and in sync.

If you do not have replication set up properly, after a while you will experience problems with your domain controllers. An example of a common replication problem is Event Log event ID 1311, which states that the Windows NT Directory Services (NTDS) Knowledge Consistency Checker (KCC) has found (and reported) a problem with Active Directory replication. This error message states that the replication configuration information in Active Directory does not accurately reflect the physical topology of the network. This error is commonly found on ailing networks that have replication problems for one reason or another.

Creating Sites

The primary method for creating and managing Active Directory replication components is to utilize the Active Directory Sites and Services tool or the MMC found within the `Administrative Tools` folder. Using this administrative component, you can graphically create and manage sites in much the same way that you create and manage OUs.

Exercise 21.1 walks you through the process of creating Active Directory sites. For you to complete this exercise, the local machine must be a domain controller. Also, this exercise assumes that you have not yet changed the default domain site configuration.

Do not perform any testing on a production system or network. Make sure you test site configuration in a lab setting only.

EXERCISE 21.1

Creating Sites

1. Open the Active Directory Sites and Services tool from the Administrative Tools program group.
2. Expand the `Sites` folder.
3. Right-click the Default-First-Site-Name item and choose Rename. Rename the site **CorporateHQ**.
4. Create a new site by right-clicking the `Sites` object and selecting New Site.

5. In the New Object – Site dialog box, type **Farmington** for the site name. Click the DEFAULTIPSITELINK item, and an information screen pops up. Then click OK to create the site. Note that you cannot include spaces or other special characters in the name of a site.

EXERCISE 21.1 *(continued)*

6. Notice that the Farmington site is now listed under the `Sites` object.

7. Create another new site and name it **Portsmouth**. Again, choose the DEFAULTIPSITE-LINK item. Notice that the new site is listed under the `Sites` object.

8. When you have finished, close the Active Directory Sites and Services tool.

Creating Subnets

Once you have created the sites that map to your network topology, it's time to define the subnets that define the site boundaries.

Subnets are based on TCP/IPv4 or TCP/IPv6 address information. For example, the IPv4 address may be 10.10.0.0, and the subnet mask may be 255.255.0.0. This information specifies that all of the TCP/IP addresses that begin with the first two octets are part of the same TCP/IP subnet. All of the following TCP/IP addresses would be within this subnet:

- 10.10.1.5
- 10.10.100.17
- 10.10.110.120

The Active Directory Sites and Services tool expresses these subnets in a somewhat different notation. It uses the provided subnet address and appends a slash followed by the number of bits in the subnet mask. In the example in the previous paragraph, the subnet would be defined as 10.1.0.0/16.

Remember that sites typically represent distinct physical locations, and they almost always have their own subnets. The only way for a domain controller in one site to reach a DC in another site is to add subnet information about the remote site. Generally, information regarding the definition of subnets for a specific network environment will be available from a network designer. Exercise 21.2 walks you through the steps that you need to take to create subnets and assign subnets to sites. To complete the steps in this exercise, you must have completed Exercise 21.1.

EXERCISE 21.2

Creating Subnets

1. Open the Active Directory Sites and Services tool from the Administrative Tools program group.
2. Expand the `Sites` folder. Right-click the `Subnets` folder and select New Subnet.
3. In the New Object – Subnet dialog box, you are prompted for information about the IPv4 or IPv6 details for the new subnet. For the prefix, type **10.10.1.0/24** (you are staying with the more commonly used IPv4). This actually calculates out to 10.10.1.0 with the mask of 255.255.255.0. Click the Farmington site and then click OK to create the subnet.
4. In the Active Directory Sites and Services tool, right-click the newly created 10.10.1.0/24 subnet object and select Properties.
5. On the subnet's Properties dialog box, type **Farmington 100MB LAN** for the description. Click OK to continue.

EXERCISE 21.2 *(continued)*

6. Create a new subnet using the following information:

   Address: **160.25.0.0/16**

   Site: **Portsmouth**

   Description: **Portsmouth 100Mbit LAN**

7. Finally, create another subnet using the following information:

   Address: **176.33.0.0/16**

   Site: **CorporateHQ**

   Description: **Corporate 100Mbit switched LAN**

8. When finished, close the Active Directory Sites and Services tool.

So far, you have created the basic components that govern Active Directory sites and subnets. You also linked these two components by defining which subnets belong in which sites. These two steps—creating sites and creating subnets—form the basis of mapping the physical network infrastructure of an organization to Active Directory. Now look at the various settings that you can make for sites.

Configuring Sites

Once you have created Active Directory sites and have defined which subnets they contain, it's time to make some additional configuration settings for the site structure. Specifically, you'll need to assign servers to specific sites and configure the site-licensing options. By placing servers in sites, you tell Active Directory replication services how to replicate information for various types of servers. Later in this chapter, you'll examine the details of working with replication within and between sites.

In Exercise 21.3, you will add servers to sites and configure CorpDC1 options. To complete the steps in this exercise, you must have completed Exercise 21.1 and Exercise 21.2.

EXERCISE 21.3

Configuring Sites

1. Open the Active Directory Sites and Services tool from the Administrative Tools program group.
2. Expand the `Sites` folder and click and expand the Farmington site.
3. Right-click the Servers container in the Farmington site and select New ➢ Server. Type **FarmingtonDC1** for the name of the server and then click OK.

EXERCISE 21.3 *(continued)*

4. Create a new Server object within the CorporateHQ site and name it **CorpDC1**. Note that this object also includes the name of the local domain controller.
5. Create two new Server objects within the Portsmouth site and name them **PortsmouthDC1** and **PortsmouthDC2**.
6. Right-click the CorpDC1 server object and select Properties. On the General tab of the CorpDC1 Properties box, select SMTP in the Transports Available For Inter-site Data Transfer box and click Add to make this server a preferred IP bridgehead server. Click OK to accept the settings.
7. When you have finished, close the Active Directory Sites and Services tool.

With the configuration of the basic settings for sites out of the way, it's time to focus on the real details of the site topology—creating site links and site link bridges.

Configuring Replication

Sites are generally used to define groups of computers that are located within a single geographic location. In most organizations, machines that are located in close physical proximity (for example, within a single building or branch office) are well connected. A typical example is a LAN in a branch office of a company. All of the computers may be connected using Ethernet, and routing and switching technology may be in place to reduce network congestion.

Often, however, domain controllers are located across various states, countries, and even continents. In such a situation, network connectivity is usually much slower, less reliable, and more costly than that for the equivalent LAN. Therefore, Active Directory replication must accommodate this situation accordingly. When managing replication traffic within Active Directory sites, you need to be aware of two types of synchronization:

Intrasite *Intrasite replication* refers to the synchronization of Active Directory information between domain controllers that are located in the same site. In accordance with the concept of sites, these machines are usually well connected by a high-speed LAN.

Intersite *Intersite replication* occurs between domain controllers in different sites. Usually, this means there is a WAN or other type of low-speed network connection between the various machines. Intersite replication is optimized for minimizing the amount of network traffic that occurs between sites.

In the following sections, you'll look at ways to configure both intrasite and intersite replication. Additionally, you'll see features of Active Directory replication architecture that you can use to accommodate the needs of almost any environment.

Intrasite Replication

Intrasite replication is generally a simple process. One domain controller contacts the others in the same site when changes to its copy of Active Directory are made. It compares the update sequence numbers in its own copy of Active Directory with those of the other domain controllers; then the most current information is chosen by the DC in question, and all domain controllers within the site use this information to make the necessary updates to their database.

Because you can assume that the domain controllers within an Active Directory site are well connected, you can pay less attention exactly to when and how replication takes place. Communications between domain controllers occur using the *Remote Procedure Call (RPC) protocol*. This protocol is optimized for transmitting and synchronizing information on fast and reliable network connections. The RPC protocol provides for fast replication at the expense of network bandwidth, which is usually readily available because most LANs today are running on Fast Ethernet (100Mbps) at a minimum.

Intersite Replication

Intersite replication is optimized for low-bandwidth situations and network connections that have less reliability. Intersite replication offers several features that are tailored toward these types of connections. To begin with, two different protocols may be used to transfer information between sites:

RPC over IP When connectivity is fairly reliable, IP is a good choice. IP-based communications require you to have a live connection between two or more domain controllers in different sites and let you transfer Active Directory information. RPC over IP was originally designed for slower WANs in which packet loss and corruption may often occur.

Simple Mail Transfer Protocol *Simple Mail Transfer Protocol (SMTP)* is perhaps best known as the protocol that is used to send and receive email messages on the Internet. SMTP was designed to use a store-and-forward mechanism through which a server receives a copy of a message, records it to disk, and then attempts to forward it to another email server. If the destination server is unavailable, it holds the message and attempts to resend it at periodic intervals.

This type of communication is extremely useful for situations in which network connections are unreliable or not always available. For example, if a branch office in Peru were connected to the corporate office through a dial-up connection that is available only during certain hours, SMTP would be a good choice for communication with that branch.

SMTP is an inherently insecure network protocol. Therefore, if you would like to ensure that you transfer replication traffic securely and you use SMTP for Active Directory replication, you must take advantage of Windows Server 2012's Certificate Services functionality.

Other intersite replication characteristics are designed to address low-bandwidth situations and less-reliable network connections. These features give you a high degree of flexibility in controlling replication configuration. They include the following:

- Compression of Active Directory information. This compression is helpful because changes between domain controllers in remote sites may include a large amount of information and also because network bandwidth tends to be less available and more costly.
- Site links and site link bridges help determine intersite replication topology.
- Replication can occur based on a schedule defined by system administrators.

You can configure intersite replication by using the Active Directory Sites and Services tool. Select the name of the site for which you want to configure settings. Then right-click the NTDS Site Settings object in the right window pane and select Properties. By clicking the Change Schedule button in the NTDS Site Settings Properties dialog box, you'll be able to configure how often replication occurs between sites (see Figure 21.4).

FIGURE 21.4 Configuring intersite replication schedules

NOTE You will see how to set the replication schedule in Exercise 21.4.

In the following sections, you will see how to configure site links and site link bridges as well as how to manage connection objects and bridgehead servers.

Creating Site Links and Site Link Bridges

The overall topology of intersite replication is based on the use of site links and site link bridges. *Site links* are logical connections that define a path between two Active Directory sites. Site links can include several descriptive elements that define their network characteristics. *Site link bridges* are used to connect site links so that the relationship can be transitive. Figure 21.5 provides an example of site links and site link bridges.

FIGURE 21.5 An example of site links and site link bridges

Both of these types of logical connections are used by Active Directory services to determine how information should be synchronized between domain controllers in remote sites. The Knowledge Consistency Checker (KCC) uses this information, which forms a replication topology based on the site topology created. The KCC service is responsible for determining the best way to replicate information within sites.

When creating site links for your environment, you'll need to consider the following factors:

Transporting Information You can choose to use either RPC over IP or SMTP for transferring information over a site link. You will need to determine which is best based on your network infrastructure and the reliability of connections between sites.

Assigning a Cost Value You can create multiple site links between sites and assign site links a cost value based on the type of connection. The system administrator determines the cost value, and the relative costs of site links are then used (by the system) to determine the optimal path for replication. The lower the cost, the more likely the link is to be used for replication.

For example, a company may primarily use a T1 link between branch offices, but it may also use a slower and circuit-switched dial-up ISDN connection for redundancy (in case the T1 fails). In this example, a system administrator may assign a cost of 25 to the T1 line and a cost of 100 to the ISDN line. This ensures that the more reliable and higher-bandwidth T1 connection is used whenever it's available but that the ISDN line is also available.

Determining a Replication Schedule Once you've determined how and through which connections replication will take place, it's time to determine when information should be replicated. Replication requires network resources and occupies bandwidth. Therefore, you need to balance the need for consistent directory information with the need to conserve bandwidth. For example, if you determine that it's reasonable to have a lag time of six hours between when an update is made at one site and when it is replicated to all others, you might schedule replication to occur once in the morning, once during the lunch hour, and more frequently after normal work hours.

Based on these factors, you should be able to devise a strategy that allows you to configure site links.

Exercise 21.4 walks you through the process of creating site links and site link bridges. To complete the steps in this exercise, you must have completed Exercises 21.1, 21.2, and 21.3.

EXERCISE 21.4

Creating Site Links and Site Link Bridges

1. Open the Active Directory Sites and Services tool from the Administrative Tools program group.
2. Expand the Sites, Inter-site Transports, and IP objects. Right-click the DEFAULTIPSITE-LINK item in the right pane and select Rename. Rename the object **CorporateWAN**.
3. Right-click the CorporateWAN link and select Properties. In the General tab of the CorporateWAN Properties dialog box, type **T1 Connecting Corporate and Portsmouth Offices** for the description. Remove the Farmington site from the link by highlighting Farmington in the Sites In This Site Link box and clicking Remove. For the Cost value, type **50** and specify that replication should occur every **60** minutes. To create the site link, click OK.
4. Right-click the `IP` folder and select New Site Link. In the New Object – Site Link dialog box, name the link **CorporateDialup**. Add the Farmington and CorporateHQ sites to the site link and then click OK.
5. Right-click the CorporateDialup link and select Properties. In the General tab of the CorporateDialup Properties dialog box, type **ISDN Dialup between Corporate and Farmington** for the description. Set the Cost value to **100** and specify that replication should occur every **120** minutes. To specify that replication should occur only during certain times of the day, click the Change Schedule button.

6. In the Schedule For Corporate Dialup dialog box, highlight the area between 8:00 a.m. and 6:00 p.m. for the days Monday through Friday and click the Replication Not Available option. This will ensure that replication traffic is minimized during normal work hours.
7. Click OK to accept the new schedule and then click OK again to create the site link.
8. Right-click the IP object and select New Site Link Bridge. In the New Object – Site Link Bridge dialog box, name the site link bridge **CorporateBridge**. Note that the CorporateDialup and CorporateWAN site links are already added to the site link bridge. Because there must be at least two site links in each bridge, you will not be able to remove these links. Click OK to create the site link bridge.
9. When finished, close the Active Directory Sites and Services tool.

Creating Connection Objects

Generally, it is a good practice to allow Active Directory's replication mechanisms to schedule and manage replication functions automatically. In some cases, however, you may want to have additional control over replication. Perhaps you want to replicate certain changes on demand (for example, when you create new accounts). Or you may want to specify a custom schedule for certain servers.

Connection objects provide you with a way to set up these different types of replication schedules. You can create connection objects with the Active Directory Sites and Services tool by expanding a server object, right-clicking the NTDS Settings object, and selecting New Active Directory Domain Services Connection (see Figure 21.6).

FIGURE 21.6 Creating a new Active Directory Domain Services connection

Within the properties of the connection object, which you can see in the right pane of the Active Directory Sites and Services tool, you can specify the type of transport to use for replication (RPC over IP or SMTP), the schedule for replication, and the domain controllers that participate in the replication. Additionally, you can right-click the connection object and select Replicate Now.

Moving Server Objects between Sites

Using the Active Directory Sites and Services tool, you can easily move servers between sites. To do this, simply right-click the name of a domain controller and select Move. You can then select the site to which you want to move the domain controller object.

Figure 21.7 shows the Move Server dialog box. After the server is moved, all replication topology settings are updated automatically. If you want to choose custom replication settings, you'll need to create connection objects manually (as described earlier).

FIGURE 21.7 Choosing a new site for a specific server

In Exercise 21.5, you move a server object between sites. To complete the steps in this exercise, you must have completed the previous exercises in this chapter.

EXERCISE 21.5

Moving Server Objects Between Sites

1. Open the Active Directory Sites and Services administrative tool.
2. Right-click the server named PortsmouthDC1 and select Move.
3. In the Move Server dialog box, select the Farmington site and then click OK. This moves this server to the Farmington site.
4. To move the server back, right-click PortsmouthDC1 (now located in the Farmington site) and then click Move. Select Portsmouth for the destination site.
5. When finished, close the Active Directory Sites and Services administrative tool.

Creating Bridgehead Servers

By default, all of the servers in one site communicate with all of the servers in another site. You can, however, further control replication between sites by using bridgehead servers. As mentioned earlier in the chapter, using bridgehead servers helps minimize replication traffic, especially in larger distributed star network topologies, and it allows you to dedicate machines that are better connected to receive replicated data. Figure 21.8 provides an example of how bridgehead servers work.

FIGURE 21.8 A replication scenario using bridgehead servers

You can use a bridgehead server to specify which domain controllers are preferred for transferring replication information between sites. Different bridgehead servers can be selected for RPC over IP and SMTP replication, thus allowing you to balance the load. To create a bridgehead server for a site, simply right-click a domain controller and select Properties, which brings up the bridgehead server's Properties dialog box (see Figure 21.9). To make the server a bridgehead server, just select one or both replication types (called *transports*) from the left side of the dialog box and click the Add button to add them to the right side of the dialog box.

FIGURE 21.9 Specifying a bridgehead server

RODCs and Replication

I have talked quite a bit about read-only domain controllers (RODCs) throughout the book. It's important that you understand that since RODCs don't actually commit changes against the Active Directory Domain Services (ADDS) database within your environment, then replication to and from your primary domain controller (PDC) and your RODCs can occur only one way. This is referred to as *unidirectional replication*. Any writable domain controller that serves as a replication partner to one of your RODCs will never pull changes from that RODC by design. This helps ensure that no malicious or corrupt changes that are made from an RODC are replicated throughout your entire forest. The RODC performs normal inbound replication for AD DS and Sysvol changes. Any other shares on an RODC that you configure to replicate using DFS Replication would still use bidirectional replication.

RODCs come with additional configuration settings like the *Password Replication Policy (PRP)*. The PRP is used to determine which user's credentials can be cached locally on a specific RODC. By default, an RODC will not cache an Active Directory user's credentials. That would defeat the purpose of an RODC. When a user wants to authenticate to an RODC, the authentication request is forwarded to a writable domain controller for authentication. If the request succeeds, it is then passed back to the RODC, and then that user will be able to log in to the domain.

Nonetheless, it is possible to allow certain user credentials to be cached on an RODC by configuring the PRP. Once a user has been added to the Allowed RODC Password Replication group, then that user's credentials will be cached, and that RODC would be able to authenticate that user locally again in the future. Because the RODC maintains only a subset of user credentials, if the RODC is compromised or stolen, only the user accounts that had been cached on the RODC must have their passwords changed. To configure an RODC PRP, open the properties of an RODC computer object in Active Directory and select the Password Replication Policy tab.

Configuring Server Topology

When you are using environments that require multiple sites, you must carefully consider where you place your servers. In doing so, you can greatly improve performance and end user experience by reducing the time they must spend performing common operations, such as authentication or searching Active Directory for resources.

There are two main issues to consider when you are designing a distributed Active Directory environment. The first is how you should place domain controllers within the network environment. The second is how to manage the use of global catalog servers. Finding the right balance between servers, server resources, and performance can be considered an art form for network and system administrators. In the following sections, you'll look at some of the important considerations that you must take into account when you design a replication server topology.

Placing Domain Controllers

Microsoft highly recommends that you have at least two domain controllers in each domain of your Active Directory environment. As mentioned earlier in this chapter, using additional domain controllers provides the following benefits:

- Increased network performance:
  - The servers can balance the burden of serving client requests.
  - Clients can connect to the server closest to them instead of performing authentication and security operations across a slow WAN link.
- Fault tolerance (in case one domain controller fails, the other still contains a valid and usable copy of the Active Directory database).
- In Windows Server 2012 R2, RODCs help increase security when users connect to a domain controller in an unsecured remote location.

Placing Global Catalog Servers

A *global catalog (GC)* server is a domain controller that contains a copy of all of the objects contained in the forest-wide domain controllers that compose the Active Directory database. Making a domain controller a GC server is simple, and you can change this setting quite easily. That brings us to the harder part—determining which domain controllers should also be GC servers.

Where you place domain controllers and GC servers and how many you deploy are important network planning decisions. Generally, you want to make GC servers available in every site that has a slow link. This means the most logical places to put GC servers are in every site and close to the WAN link for the best possible connectivity. However, having too many GC servers is a bad thing. The main issue is associated with replication traffic—you must keep each GC server within your environment synchronized with the other servers. In a very dynamic environment, using additional GC servers causes a considerable increase in network traffic. Therefore, you will want to find a good balance between replication burdens and GC query performance in your own large multidomain environment.

To create a GC server, simply expand the Server object in the Active Directory Sites and Services tool, right-click NTDS Settings, and select Properties to bring up the NTDS Settings Properties dialog box (see Figure 21.10). To configure a server as a GC server, simply place a check mark in the Global Catalog box.

FIGURE 21.10 Enabling the global catalog on an Active Directory domain controller

Real World Scenario

Accommodating a Changing Environment

You're a system administrator for a medium-sized business that consists of many offices located throughout the world. Some of these offices are well connected because they use high-speed, reliable links, while others are not so fortunate. Overall, things are going well until your CEO announces that the organization will be merging with another large company and that the business will be restructured. The restructuring will involve opening new offices, closing old ones, and transferring employees to different locations. Additionally, changes in the IT budget will affect the types of links that exist between offices. Your job as the system administrator is to ensure that the network environment and, specifically, Active Directory keep pace with the changes and ultimately outperform them.

An important skill for any technical professional is the ability to adapt quickly and efficiently to a changing organization. When a business grows, restructures, or forms relationships with other businesses, often many IT-related changes must also occur. You may have to create new network links, for example.

Fortunately, Active Directory was designed with these kinds of challenges in mind. For example, you can use the Active Directory Sites and Services administrative tool to reflect physical network changes in Active Directory topology. If a site that previously had 64Kbps of bandwidth is upgraded to a T1 connection, you can change those characteristics for the site link objects. Conversely, if a site that was previously well connected is reduced to a slow, unreliable link, you can reconfigure the sites, change the site link transport mechanisms (perhaps from IP to SMTP to accommodate a nonpersistent link), and create connection objects (which would allow you to schedule replication traffic to occur during the least busy hours).

Suppose further that many of your operations move overseas to a European division. This might call for designating specific domain controllers as preferred bridgehead servers to reduce the amount of replication traffic over costly and slow overseas links.

Sweeping organizational changes inevitably require you to move servers between sites. For example, an office may close and its domain controllers may move to another region of the world. Again, you can accommodate this change by using Active Directory administrative tools. You may change your OU structure to reflect new logical and business-oriented changes, and you can move server objects between sites to reflect physical network changes.

Rarely can the job of mapping a physical infrastructure to Active Directory be "complete." In most environments, it's safe to assume that you will always need to make changes based on business needs. Overall, however, you should feel comfortable that the physical components of Active Directory are at your side to help you accommodate these changes.

Using Universal Group Membership Caching

To understand how Universal Group Membership Caching (UGMC) works, you must first understand how authentication works. When a user tries to authenticate with a domain controller, the first action that takes place is that the domain controller checks with the global catalog to see to which domain the user belongs.

If the domain controller (the one to which the user is trying to authenticate) is not a GC, then the domain controller sends a request to the GC to verify the user's domain. The GC responds with the user's information, and the domain controller authenticates the user (if the user belongs to the same domain as the domain controller).

There are two ways to speed up the authentication process. First, you can make all of the domain controllers global catalogs. But then you end up with a lot of GC replication traffic. This becomes even more of an issue if you have multiple sites. Now replication traffic can be too large for your site link connections.

Thus, if you have a slower site link connection or multiple domains, you can use Universal Group Membership Caching. If you are using UGMC, after a domain controller communicates with the global catalog, the domain controller will then cache the user's credentials for eight hours by default. Now if the user logs off the domain and then logs back into the domain, the domain controller will use the cached credentials and not ask the global catalog. The downside to using UGMC is that it is for authentication only. Global catalogs help speed up Active Directory searches, and they work with Directory Service–enabled applications (applications that have to work with Active Directory) such as Exchange and SQL.

Domain Controller Cloning

Throughout the book, I have talked about why so many organizations are switching to virtualization in their server rooms. Virtualization allows an administrator to take one physical server and turn it into multiple virtual servers by using Windows Server 2012 R2.

In Windows Server 2012 R2, administrators can now easily and safely create replica domain controllers by copying an existing virtual domain controller. Before Windows Server 2012, an administrator would have to deploy a server image that they prepared by using `sysprep.exe`. After going through the process of using `sysprep.exe`, the administrator would have to promote this server to a domain controller and then complete additional configuration requirements for deploying each replica domain controller.

Domain controller cloning allows an administrator to deploy rapidly a large number of domain controllers. To set up domain controller cloning, you must be a member of the Domain Admins group or have the equivalent permissions. The administrator must then run Windows PowerShell from an elevated command prompt.

Only Windows Server 2012 or Windows Server 2012 R2 domain controllers that are hosted on a VM-compatible hypervisor can be used as a source for cloning. You should also make sure that the domain controller that you choose to clone is in a healthy state (use computer management to see the computer's state).

The following example is used to create a clone domain controller named TestClone with a static IP address of 10.0.0.5 and a subnet mask of 255.255.0.0. This command also configures the DNS Server and WINS server configurations.

```
New-ADDCCloneConfigFile -CloneComputerName "TestClone" -Static -IPv4Address
"10.0.0.5" -IPv4DNSResolver "10.0.0.1" -IPv4SubnetMask "255.255.0.0" -
PreferredWinsServer "10.0.0.1" -AlternateWinsServer "10.0.0.2"
```

When you are ready to clone a domain controller, I recommend you visit Microsoft's TechNet site for all of the PowerShell commands needed to complete this entire process.

Monitoring and Troubleshooting Active Directory Replication

For the most part, domain controllers handle the replication processes automatically. However, system administrators still need to monitor the performance of Active Directory replication because failed network links and incorrect configurations can sometimes prevent the synchronization of information between domain controllers.

You can monitor the behavior of Active Directory replication and troubleshoot the process if problems occur.

About System Monitor

The Windows Server 2012 R2 System Monitor administrative tool was designed so that you can monitor many performance statistics associated with using Active Directory. Included within the various performance statistics that you can monitor are counters related to Active Directory replication.

Troubleshooting Replication

A common symptom of replication problems is that information is not updated on some or all domain controllers. For example, a system administrator creates a user account on one domain controller, but the changes are not propagated to other domain controllers. In most environments, this is a potentially serious problem because it affects network security and can prevent authorized users from accessing the resources they require.

You can take several steps to troubleshoot Active Directory replication. These steps are discussed in the following sections.

Verifying Network Connectivity

For replication to work properly in distributed environments, you must have network connectivity. Although ideally all domain controllers would be connected by high-speed LAN links, this is rarely the case for larger organizations. In the real world, dial-up connections and slow connections are common. If you have verified that your replication

topology is set up properly, you should confirm that your servers are able to communicate. Problems such as a failed dial-up connection attempt can prevent important Active Directory information from being replicated.

Verifying Router and Firewall Configurations

Firewalls are used to restrict the types of traffic that can be transferred between networks. They are mainly used to increase security by preventing unauthorized users from transferring information. In some cases, company firewalls may block the types of network access that must be available for Active Directory replication to occur. For example, if a specific router or firewall prevents data from being transferred using SMTP, replication that uses this protocol will fail.

Examining the Event Logs

Whenever an error in the replication configuration occurs, the computer writes events to the Directory Service and File Replication Service event logs. By using the Event Viewer administrative tool, you can quickly and easily view the details associated with any problems in replication. For example, if one domain controller is unable to communicate with another to transfer changes, a log entry is created.

Verifying That Information Is Synchronized

It's often easy to forget to perform manual checks regarding the replication of Active Directory information. One of the reasons for this is that Active Directory domain controllers have their own read-write copies of the Active Directory database. Therefore, if connectivity does not exist, you will not encounter failures while creating new objects.

It is important to verify periodically that objects have been synchronized between domain controllers. This process might be as simple as logging on to a different domain controller and looking at the objects within a specific OU. This manual check, although it might be tedious, can prevent inconsistencies in the information stored on domain controllers, which, over time, can become an administration and security nightmare.

Verifying Authentication Scenarios

A common replication configuration issue occurs when clients are forced to authenticate across slow network connections. The primary symptom of the problem is that users complain about the amount of time it takes them to log on to Active Directory (especially during a period when there's a high volume of authentications, such as at the beginning of the workday).

Usually, you can alleviate this problem by using additional domain controllers or reconfiguring the site topology. A good way to test this is to consider the possible scenarios for the various clients that you support. Often, walking through a configuration, such as "A client in Domain1 is trying to authenticate using a domain controller in Domain2, which is located across a slow WAN connection," can be helpful in pinpointing potential problem areas.

Verifying the Replication Topology

The Active Directory Sites and Services tool allows you to verify that a replication topology is logically consistent. You can quickly and easily perform this task by right-clicking NTDS Settings within a Server object and choosing All Tasks ➢ Check Replication. If any errors are present, a dialog box alerts you to the problem.

Another way to verify replication is by using the command-line utility `Repadmin`. Table 21.1 shows some of the `Repadmin` commands.

TABLE 21.1 `Repadmin` commands

Command	Description
`Repadmin Bridgeheads`	Lists the bridgehead servers for a specified site.
`Repadmin dsaguid`	Returns a server name when given a GUID.
`Repadmin failcache`	Shows a list of failed replication events.
`Repadmin istg`	Returns the server name of the Inter-Site Topology Generator (ISTG) server for a specified site. The ISTG manages the inbound replication connection objects for the bridgehead servers in a site.
`Repadmin kcc`	Forces the Knowledge Consistency Checker (KCC) to recalculate replication topology for a specified domain controller. The KCC modifies data in the local directory in response to system-wide changes.
`Repadmin latency`	Shows the amount of time between replications.
`Repadmin queue`	Shows tasks waiting in the replication queue.
`Repadmin querysites`	Uses routing information to determine the cost of a route from a specified site to another specified site or to other sites.
`Repadmin replicate`	Starts a replication event for the specified directory partition between domain controllers.
`Repadmin replsummary`	Displays the replication state and relative health of a forest.
`Repadmin showrepl`	Displays replication partners for each directory partition on a specified domain controller.

Reasons for Creating Multiple Domains

Before you look at the steps that you must take to create multiple domains, become familiar with the reasons an organization might want to create them.

In general, you should always try to reflect your organization's structure within a single domain. By using organizational units (OUs) and other objects, you can usually create an accurate and efficient structure within one domain. Creating and managing a single domain is usually much simpler than managing a more complex environment consisting of multiple domains.

That being said, you should familiarize yourself with some real benefits and reasons for creating multiple domains and some drawbacks of using them.

Reasons for Using Multiple Domains

You might need to implement multiple domains for several reasons. These reasons include the following considerations:

Scalability Although Microsoft has designed Active Directory to accommodate millions of objects, this may not be practical for your current environment. Supporting thousands of users within a single domain requires more disk space, greater central processing unit (CPU) usage, and additional network burdens on your domain controllers (computers containing Active Directory security information). To determine the size of the Active Directory domain your network can support, you need to plan, design, test, and analyze within your own environment.

Reducing Replication Traffic All of the domain controllers in a domain must keep an up-to-date copy of the entire Active Directory database. For small to medium-sized domains, this is generally not a problem. Windows Server 2012 R2 and Active Directory manage all of the details of transferring the database behind the scenes. Other business and technical limitations might, however, affect Active Directory's ability to perform adequate replication. For example, if you have two sites that are connected by a slow network link (or a sporadic link or no link at all), replication is not practical. In this case, you would probably want to create separate domains to isolate replication traffic. Sporadic coverage across the wide area network (WAN) link would come from circuit-switching technologies such as Integrated Services Digital Network (ISDN) technologies. If you didn't have a link at all, then you would have a service provider outage or some other type of disruption. Separate domains mean separate replication traffic, but the amount of administrative overhead is increased significantly.

Because it's common to have WAN links in your business environment, you will always need to consider how your users authenticate to a domain controller (DC). DCs at a remote site are commonly used to authenticate users locally to their local area network (LAN). The most common design involves putting a DC at each remote site to keep authentication

traffic from traversing the WAN. If it is the other way around, the authentication traffic may cause users problems if WAN utilization is high or if the link is broken and no other way to the central site is available. The design you are apt to see most often is one in which each server replicates its database of information to each other's server so that the network and its systems converge.

However, it's important to realize that the presence of slow WAN links alone is *not* a good reason to break an organization into multiple domains. The most common solution is to set up site links with the Sites and Services Microsoft Management Console (MMC). When you use this MMC, you can manage replication traffic and fine-tune independently of the domain architecture.

You would want to use a multidomain architecture, such as when two companies merge through an acquisition, for the following reasons:

Meeting Business Needs Several business needs might justify the creation of multiple domains. Business needs can be broken down even further into organizational and political needs.

One of the organizational reasons for using multiple domains is to avoid potential problems associated with the Domain Administrator account. At least one user needs to have permissions at this level. If your organization is unable or unwilling to trust a single person to have this level of control over all business units, then multiple domains may be the best answer. Because each domain maintains its own security database, you can keep permissions and resources isolated. Through the use of trusts, however, you can still share resources.

A political need for separate domains might arise if you had two companies that merged with two separate but equal management staffs and two sets of officers. In such a situation, you might need to have Active Directory split into two separate databases to keep the security of the two groups separate. Some such organizations may need to keep the internal groups separate by law. A multidomain architecture provides exactly this type of pristinely separate environment.

Many Levels of Hierarchy Larger organizations tend to have complex internal and external business structures that dictate the need for many different levels of organization. For example, two companies might merge and need to keep two sets of officers who are managed under two different logical groupings. In Chapter 5, "Administer Active Directory," I showed you that you can use OUs to help group different branches of the company so that you can assign permissions, delegations, or whatever else you can think of without affecting anyone else. Managing data becomes much easier when you're using OUs, and if you design them correctly, OUs will help you control your network right from one console. You may need only one level of management—your company may be small enough to warrant the use of the default OU structure you see when Active Directory is first installed. If, however, you find that you need many levels of OUs to manage resources (or if large numbers of objects exist within each OU), it might make sense to create additional domains. Each domain would contain its own OU hierarchy and serve as the root of a new set of objects.

Decentralized Administration Two main models of administration are commonly used: a centralized administration model and a decentralized administration model. In the centralized administration model, a single IT organization is responsible for managing all of the users, computers, and security permissions for the entire organization. In the decentralized administration model, each department or business unit might have its own IT department. In both cases, the needs of the administration model can play a significant role in whether you decide to use multiple domains.

Consider, for example, a multinational company that has a separate IT department for offices in each country. Each IT department is responsible for supporting only the users and computers within its own region. Because the administration model is largely decentralized, creating a separate domain for each of these major business units might make sense from a security and maintenance standpoint.

Multiple DNS or Domain Names Another reason you may need to use a multidomain architecture is if you want or plan to use multiple DNS names within your organization. If you use multiple DNS names or domain names, you must create multiple Active Directory domains. Each AD domain can have only one *fully qualified domain name (FQDN)*. An FQDN is the full name of a system that consists of a local host, a second-level domain name, and a top-level domain (TLD). For example, `corp.stellacon.com` is an FQDN, `.com` is the TLD, `www` is the host, and `stellacon` is the second-level domain name.

Legality One final reason you may need to use a multidomain architecture is legality within your organization. Some corporations have to follow state or federal regulations and laws. For this reason, they may need to have multiple domains.

Drawbacks of Multiple Domains

Although there are many reasons why it makes sense to have multiple domains, there are also reasons why you should not break an organizational structure into multiple domains, many of which are related to maintenance and administration. Here are some of the drawbacks to using multiple domains:

Administrative Inconsistency One of the fundamental responsibilities of most system administrators is implementing and managing security. When you are implementing Group Policy and security settings in multiple domains, you want to be careful to ensure that the settings are consistent. In Windows Server 2012 R2, security policies can be different between and within the same domains. If this is what the organization intended, then it is not a problem. However, if an organization want to make the same settings apply to all users, then each domain requires a separate GPO with similar security settings.

Increased Management Challenges Managing servers, users, and computers can become a considerable challenge when you are also managing multiple domains because many more administrative units are required. In general, you need to manage all user, group, and computer settings separately for the objects within each domain. The hierarchical structure provided by OUs, on the other hand, provides a much simpler and easier way to manage permissions.

Decreased Flexibility Creating a domain involves the *promotion* of a DC to the new domain. Although the process is quite simple, it is much more difficult to rearrange the domain topology within an Active Directory environment than it is simply to reorganize OUs. When planning domains, you should ensure that the domain structure will not change often, if at all.

Now that you have examined the pros and cons related to creating multiple domains, it is time to see how to create trees and forests.

Creating Domain Trees and Forests

So far, this chapter has covered some important reasons for using multiple domains in a single network environment. Now it's time to look at how to create multidomain structures such as domain trees and domain forests.

Regardless of the number of domains you have in your environment, you always have a tree and a forest. This might surprise those of you who generally think of domain trees and forests as belonging only to Active Directory environments that consist of multiple domains. However, recall that when you install the first domain in an Active Directory environment, that domain automatically creates a new forest and a new tree.

In the following sections, you will learn how to plan trees and forests and how to promote domain controllers to establish a tree and forest environment.

Planning Trees and Forests

You have already seen several reasons why you might want to have multiple domains within a single company. What you haven't yet seen is how multiple domains can be related to each other and how their relationships can translate into domain forests and trees.

A fundamental commonality between the various domains that exist in trees and forests is that they all share the same Active Directory global catalog (GC). This means that if you modify the Active Directory schema, these changes must be propagated to all of the domain controllers in all of the domains. This is an important point because adding and modifying the structure of information in the GC can have widespread effects on replication and network traffic. Also, you need to ensure that any system you use in the GC role can handle it—you might need to size up the system's hardware requirements. This is especially true if there are multiple domains.

Every domain within an Active Directory configuration has its own unique name. For example, even though you might have a sales domain in two different trees, the complete names for each domain will be different (such as `sales.stellacon1.com` and `sales.stellacon2.com`).

In the following sections, you'll look at how you can organize multiple Active Directory domains based on business requirements.

Using a Single Tree

The concept of domain trees was created to preserve the relationship between multiple domains that share a common contiguous namespace. For example, you might have the following DNS domains (based on Internet names):

- `mycompany.com`
- `sales.mycompany.com`
- `engineering.mycompany.com`
- `europe.sales.mycompany.com`

Note that all of these domains fit within a single contiguous namespace. That is, they are all direct or indirect children of the `mycompany.com` domain. In this case, `mycompany.com` is called the *root domain*. All of the direct children (such as `sales.mycompany.com` and `engineering.mycompany.com`) are called *child domains*. Finally, *parent domains* are the domains that are directly above one domain. For example, `sales.mycompany.com` is the parent domain of `europe.sales.mycompany.com`. Figure 21.11 provides an example of a domain tree.

FIGURE 21.11 A domain tree

To establish a domain tree, you must first create the root domain for the tree. Then you can add child domains off this root. These child domains can then serve as parents for further subdomains. Each domain must have at least one domain controller, and domain

controllers can participate in only one domain at a time. However, you can move a domain controller from one domain to another. To do this, you must first demote a domain controller to a member server and then promote it to a domain controller in another domain.

You will learn how to demote a domain controller later in this chapter in the section "Demoting a Domain Controller."

Domains are designed to be logical boundaries. The domains within a tree are, by default, automatically bound together using a two-way transitive trust relationship, which allows resources to be shared among domains through the use of the appropriate user and group assignments. Because trust relationships are transitive, all of the domains within the tree trust each other. Note, however, that a trust by itself does not automatically grant any security permissions to users or objects between domains. Trusts are designed only to *allow* resources to be shared; you must still go through the process of sharing and managing them. Enterprise administrators must explicitly assign security settings to resources before users can access resources between domains.

Using a single tree makes sense when your organization maintains only a single contiguous namespace. Regardless of the number of domains that exist within this environment and how different their security settings are from each other, they are related by a common name. Although domain trees make sense for many organizations, in some cases the network namespace may be considerably more complicated. You'll look at how forests address these situations next.

Using a Forest

Active Directory forests are designed to accommodate multiple noncontiguous namespaces. That is, they can combine domain trees into logical units. An example might be the following tree and domain structure:

- Tree: `Organization1.com`
  - `Sales.Organization1.com`
  - `Marketing.Organization1.com`
  - `Engineering.Organization1.com`
  - `NorthAmerica.Engineering.Organization1.com`
- Tree: `Organization2.com`
  - `Sales.Organization2.com`
  - `Engineering.Organization2.com`.

Figure 21.12 provides an example of how multiple trees can fit into a single forest. Such a situation might occur in the acquisition and merger of companies or if a company is logically divided into two or more completely separate and autonomous business units.

FIGURE 21.12 A single forest consisting of multiple trees

All of the trees within a forest are related through a single forest root domain. This is the first domain that was created in the Active Directory environment. The root domain in each tree creates a transitive trust with the forest root domain. The result is a configuration in which all of the trees within a domain and all of the domains within each tree trust each other. Again, as with domain trees, the presence of a trust relationship does not automatically signify that users have permissions to access resources across domains. It allows only objects and resources to be shared. Authorized network administrators must set up specific permissions.

All of the domains within a single Active Directory forest have the following features in common:

Schema The *schema* is the Active Directory structure that defines how the information within the data store is structured. For the information stored on various domain controllers to remain compatible, all of the domain controllers within the entire Active Directory environment must share the same schema. For example, if you add a field for an employee benefit plan number, all domain controllers throughout the environment need to recognize this information before you can share information among them.

Global Catalog One of the problems associated with working in large network environments is that sharing information across multiple domains can be costly in terms of network and server resources. Fortunately, Active Directory uses the global catalog (GC), which serves as a repository for information about a subset of all objects within *all* Active Directory domains in a forest. System administrators can determine what types of information should be added to the defaults in the GC. Generally, they decide to

store commonly used information, such as a list of all of the printers, users, groups, and computers. In addition, they can configure specific domain controllers to carry a copy of the GC. Now if you have a question about where to find all of the color printers in the company, for example, all you need to do is to contact the nearest GC server.

Configuration Information Some roles and functions must be managed for the entire forest. When you are dealing with multiple domains, this means that you must configure certain domain controllers to perform functions for the entire Active Directory environment. I will discuss some specifics of this later in this chapter.

The main purpose of allowing multiple domains to exist together is to allow them to share information and other resources. Now that you've seen the basics of domain trees and forests, take a look at how domains are actually created.

The Promotion Process

A domain tree is created when a new domain is added as the child of an existing domain. This relationship is established during the promotion of a Windows Server 2012 R2 computer to a domain controller. Although the underlying relationships can be quite complicated in larger organizations, the Server Manager's Active Directory Installation Wizard makes it easy to create forests and trees.

Using the Active Directory Installation Wizard, you can quickly and easily create new domains by promoting a Windows Server 2012 R2 stand-alone server or a member server to a domain controller. When you install a new domain controller, you can choose to make it part of an existing domain, or you can choose to make it the first domain controller in a new domain. In the following sections and exercises, you'll become familiar with the exact steps you need to take to create a domain tree and a domain forest when you promote a server to a domain controller.

Creating a Domain Tree

In previous chapters, you learned how to promote the first domain controller in the first domain in a forest, also known as the root. If you don't promote any other domain controllers, then that domain controller simply controls that one domain and only one tree is created. To create a new domain tree, you need to promote a Windows Server 2012 R2 computer to a domain controller. In the Active Directory Installation Wizard, you select the option that makes this domain controller the first machine in a new domain that is a child of an existing domain. As a result, you will have a domain tree that contains two domains—a parent and a child, or two trees if you don't create a child domain.

Before you can create a new child domain, you need the following information:

- The name of the parent domain (for the exercises, you'll use the one you created in the previous chapter.)
- The name of the child domain (the one you are planning to install)
- The file system locations for the Active Directory database, logs, and shared system volume

- DNS configuration information
- The NetBIOS name for the new server
- A domain administrator username and password

Exercise 21.6 walks you through the process of creating a new child domain using Server Manager. This exercise assumes you have already created the parent domain and you are using a server in the domain that is not a domain controller.

EXERCISE 21.6

Creating a New Subdomain

1. Open Server Manager.
2. Click item 2, Add Roles And Features.

3. Make sure that the Role-Based Or Feature-Based Installation button is selected and click Next.
4. At the Select Destination screen, click Next.

5. At the Select Server Roles screen, check the Active Directory Domain Services check box. A box will appear stating that you need to install additional roles. Click the Add Features button. Then click Next.

EXERCISE 21.6 *(continued)*

6. At the Add Roles And Features Wizard screen, click Next.
7. At the Confirmation screen, click the Install button.
8. When the installation is complete, click the Close button.
9. Close Server Manager and restart the machine.
10. Log in and restart Server Manager.
11. In the Roles And Server Groups area, click the AD DS link.

12. In the Servers section, click the More link next to Configuration Required For Active Directory Domain Services.
13. At the All Servers Task Details screen, click the Promote This Server To A Domain Controller link.

14. At the Deployment Configuration screen, click the radio button Add A New Domain To An Existing Forest. In the Select Domain Type drop-down, chose Child Domain and then choose your parent domain. In the New Domain Name box, type in the name of your new domain. I used NewHampshire. Click the Next button.

EXERCISE 21.6 *(continued)*

15. At the Domain Controller Options screen, I set the following options:

    Domain Functional Level: Windows Server 2012 R2

    Domain Name System (DNS) Server: Checked

    Global Catalog (GC): Checked

    Site Name: CorporateHQ

    Password: **P@ssw0rd**

    Click Next.

16. At the DNS screen, click Next.
17. At the Additional Options screen, accept the default NetBIOS domain name and click Next.
18. At the Paths screen, accept the default file locations and click Next.
19. At the Review Options screen, verify your settings and click Next.
20. At the Prerequisites Check screen, click the Install button (as long as there are no errors).

21. After the installation completes, the machine will automatically reboot. Log in as the administrator.
22. Close Server Manager.

Joining a New Domain Tree to a Forest

A *forest* is one or more trees that do not share a contiguous namespace. For example, you could join the `organization1.com` and `organization2.com` domains together to create a single Active Directory environment.

Any two trees can be joined together to create a forest, as long as the second tree is installed after the first and the trees have noncontiguous namespaces. (If the namespaces were contiguous, you would actually need to create a new domain for an existing tree.) The process of creating a new tree to form or add to a forest is as simple as promoting a server to a domain controller for a new domain that does *not* share a namespace with an existing Active Directory domain.

NOTE

The command-line tool `adprep.exe` is used to prepare a Microsoft Windows 2003, 2008, or 2008 R2 forest or a Windows 2003, 2008, or 2008 R2 domain for the installation of Windows Server 2012 R2 domain controllers.

To add a new domain to an existing forest, you must already have at least one other domain, which is the root domain. Keep in mind that the entire forest structure is destroyed if the original root domain is ever removed entirely. Therefore, you should have at least two domain controllers in the Active Directory root domain; the second serves as a backup in case you have a problem with the first, and it can also serve as a backup solution for disaster recovery and fault tolerance purposes. Such a setup provides additional protection for the entire forest in case one of the domain controllers fails.

Adding Additional Domain Controllers

In addition to the operations you've already performed, you can use the Active Directory Installation Wizard to create additional domain controllers for any of your domains. There are two main reasons to create additional domain controllers:

Fault Tolerance and Reliability You should always consider the theory of *disaster recovery (DR)* and have a plan, sometimes referred to as a *disaster recovery plan (DRP)*. If you're part of one of those organizations that rely upon their network directory services infrastructures, you need Active Directory to provide security and resources for all users.

For this reason, downtime and data loss are very costly. Through the use of multiple domain controllers, you can ensure that if one of the servers goes down, another one is available to perform the necessary tasks, such as user authentication and resource browsing. Additionally, data loss (perhaps from hard disk drive failure) will not result in the loss or unavailability of network security information because you can easily recover Active Directory information from the remaining, still-functional domain controller.

Performance The burden of processing login requests and serving as a repository for security permissions and other information can be quite extensive, especially in larger businesses. By using multiple domain controllers, you can distribute this load across multiple systems. Additionally, by strategically placing domain controllers, you can greatly increase response times for common network operations, such as authentication and browsing for resources.

As a rule of thumb, you should always plan and design your infrastructure to have at least two domain controllers per domain. For many organizations, this provides a good balance between the cost of servers and the level of reliability and performance. For larger or more distributed organizations, however, additional domain controllers greatly improve performance.

Demoting a Domain Controller

In addition to being able to promote member servers to domain controllers, the Active Directory Installation Wizard can do the exact opposite, that is, demote domain controllers.

You might choose to demote a domain controller for a couple of reasons. First, if you have determined that the role of a server should change (for example, from a domain controller to a member or stand-alone server that you might make into a web server), you can easily demote it to make this happen. Another common reason to demote a domain

controller is if you want to move the machine from one domain to another. You cannot do this in a single step: First you need to demote the existing domain controller to remove it from the current domain and then promote it into a new domain. The result is that the server is now a domain controller for a different domain.

To demote a domain controller, you simply access the Active Directory Installation Wizard. The wizard automatically notices that the local server is a domain controller, and it asks you to verify each step you take, as with most things you do in Windows. You are prompted to decide whether you really want to remove this machine from the current domain. Note that if the local server is a global catalog server, you will be warned that at least one copy of the GC must remain available so that you can perform logon authentication.

By default, at the end of the demotion process, the server is joined as a member server to the domain for which it was previously a domain controller. If you demote the last domain controller in the domain, the server becomes a stand-alone server.

Real World Scenario

Planning for Domain Controller Placement

You are the senior system administrator for a medium-sized Active Directory environment. Currently the environment consists of only one Active Directory domain. Your company's network is spread out over 40 different sites throughout North America. Recently, you've received complaints from users and other system administrators about the performance of Active Directory–related operations. For example, users report that it takes several minutes to log on to their machines between 9 a.m. and 10 a.m., when activity is at its highest. Simultaneously, system administrators complain that updating user information within the OUs for which they are responsible can take longer than expected.

Fortunately, Active Directory's distributed domain controller architecture allows you to optimize performance for this type of situation without making dramatic changes to your environment. You decide that the quickest and easiest solution is to deploy additional domain controllers throughout the organization. The domain controllers are generally placed within areas of the network that are connected by slow or unreliable links. For example, a small branch office in Des Moines, Iowa, receives its own domain controller. The process is quite simple: You install a new Windows Server 2012 R2 computer and then run the Active Directory Installation Wizard in Server Manager to make the new machine a domain controller for an existing domain. Once the initial directory services data is copied to the new server, it is ready to service requests and updates of your domain information.

Note that there are potential drawbacks to this solution; for instance, you have to manage additional domain controllers and the network traffic generated from communications between the domain controllers. It's important that you monitor your network links to ensure that you've reached a good balance between replication traffic and overall Active Directory performance. In later chapters, you'll see how you can configure Active Directory sites to map Active Directory operations better to your physical network structure.

Removing a domain from your environment is not an operation that you should take lightly. Before you plan to remove a domain, make a list of all of the resources that depend on the domain and the reasons why the domain was originally created. If you are sure that your organization no longer requires the domain, then you can safely continue. If you are not sure, think again, because the process cannot be reversed, and you could lose critical information!

Managing Multiple Domains

You can easily manage most of the operations that must occur *between* domains by using the Active Directory Domains and Trusts administrative tool. On the other hand, if you want to configure settings *within* a domain, you should use the Active Directory Users and Computers tool. In the following sections, you'll look at ways to perform two common domain management functions with the tools just mentioned: managing *single-master operations* and managing *trusts*. You'll also look at ways to manage UPN suffixes in order to simplify user accounts, and you'll examine GC servers in more detail.

Managing Single-Master Operations

For the most part, Active Directory functions in what is known as *multimaster* replication. That is, every domain controller within the environment contains a copy of the Active Directory database that is both readable and writable. This works well for most types of information. For example, if you want to modify the password of a user, you can easily do this on *any* of the domain controllers within a domain. The change is then automatically propagated to the other domain controllers.

However, some functions are not managed in a multimaster fashion. These operations are known as *operations masters*. You must perform single-master operations on specially designated domain controllers within the Active Directory forest. There are five main single-master functions: two that apply to an entire Active Directory forest and three that apply to each domain.

Forest Operations Masters

You use the Active Directory Domains and Trusts tool to configure forest-wide roles. The following single-master operations apply to the entire forest:

Schema Master Earlier you learned that all of the domain controllers within a single Active Directory environment share the same schema. This ensures information consistency. However, developers and system administrators can modify the Active

Directory schema by adding custom information. A trivial example might involve adding a field to employee information that specifies a user's favorite color.

When you need to make these types of changes, you must perform them on the domain controller that serves as the *Schema Master* for the environment. The Schema Master is then responsible for propagating all of the changes to all of the other domain controllers within the forest.

Domain Naming Master The purpose of the *Domain Naming Master* is to keep track of all of the domains within an Active Directory forest. You access this domain controller whenever you need to add/remove new domains to a tree or forest.

Domain Operations Masters

You use the Active Directory Users and Computers snap-in to administer roles within a domain. Within each domain, at least one domain controller must fulfill each of the following roles:

Relative ID (RID) Master Every security object within Active Directory must be assigned a unique identifier so that it is distinguishable from other objects. For example, if you have two OUs named IT that reside in different domains, you must have some way to distinguish easily between them. Furthermore, if you delete one of the IT OUs and then later re-create it, the system must be able to determine that it is not the same object as the other IT OU. The unique identifier for each object consists of a domain identifier and a relative identifier (RID). RIDs are always unique within an Active Directory domain and are used for managing security information and authenticating users. The *RID Master* is responsible for creating these values within a domain whenever new Active Directory objects are created.

PDC Emulator Master Within a domain, the *PDC Emulator Master* is responsible for maintaining backward compatibility with Windows 95, 98, and NT clients. It is also responsible for processing account lockouts, performing password changes, and validating failed logon authentications within the domain. If a user's logon authentication fails to a bad password on a domain controller, then that domain controller passes the authentication request to the PDC Emulator Master to check and see whether the password that was used matches the password that is most current for that user.

The PDC Emulator Master serves as the default domain controller to process authentication requests if another domain controller is unable to do so. The PDC Emulator Master also receives preferential treatment whenever domain security changes are made.

Infrastructure Master Whenever a user is added to or removed from a group, all of the other domain controllers should be made aware of this change. The role of the domain controller that acts as an *Infrastructure Master* is to ensure that group membership information stays synchronized within an Active Directory domain.

Unless there is only one domain controller, you should not place the Infrastructure Master on a global catalog server. If the Infrastructure Master and global catalog are on the same domain controller, the Infrastructure Master will not function. If you have only one domain, then all DCs are GCs.

Another service that a server can control for the network is the Windows Time service. The Windows Time service uses a suite of algorithms in the Network Time Protocol (NTP). This helps ensure that the time on all computers throughout a network is as accurate as possible. All client computers within a Windows Server 2012 R2 domain are synchronized with the time of an authoritative computer.

Assigning Single-Master Roles

Now that you are familiar with the different types of single-master operations, take a look at Exercise 21.7. This exercise shows you how to assign these roles to servers within the Active Directory environment. In this exercise, you will assign single-master operations roles to various domain controllers within the environment. To complete the steps in this exercise, you need one Active Directory domain controller.

EXERCISE 21.7

Assigning Single-Master Operations

1. Open the Active Directory Domains and Trusts administrative tool.
2. Right-click Active Directory Domains And Trusts and choose Operations Masters.
3. In the Operations Masters dialog box, note that you can change the operations master by clicking the Change button. If you want to move this assignment to another computer, first you need to connect to that computer and then make the change. Click Close to continue without making any changes.
4. Close the Active Directory Domains and Trusts administrative tool.
5. Open the Active Directory Users and Computers administrative tool.
6. Right-click the name of a domain and select Operations Masters. This brings up the RID tab of the Operations Masters dialog box.

   Notice that you can change the computer that is assigned to the role. To change the role, first you need to connect to the appropriate domain controller. Notice that the PDC and Infrastructure roles have similar tabs. Click Close to continue without making any changes.
7. When you have finished, close the Active Directory Users and Computers tool.

Remember that you manage single-master operations with three different tools. You use the Active Directory Domains and Trusts tool to configure the Domain Name Master role, while you use the Active Directory Users and Computers snap-in to administer roles within a domain. Although this might not seem intuitive at first, it can help you remember which roles apply to domains and which apply to the whole forest. The third tool, the Schema Master role, is a bit different from these other two. To change the Schema Master role, you must install the Active Directory Schema MMS snap-in and change it there.

Managing Trusts

Trust relationships make it easier to share security information and network resources between domains. As was already mentioned, standard transitive two-way trusts are automatically created between the domains in a tree and between each of the trees in a forest. Figure 21.13 shows an example of the default trust relationships in an Active Directory forest.

FIGURE 21.13 Default trusts in an Active Directory forest

When configuring trusts, you need to consider two main characteristics:

Transitive Trusts By default, Active Directory trusts are *transitive trusts*. The simplest way to understand transitive relationships is through this example: If Domain A trusts Domain B and Domain B trusts Domain C, then Domain A implicitly trusts Domain C. If you need to apply a tighter level of security, trusts can be configured as intransitive.

One-Way vs. Two-Way Trusts can be configured as one-way or two-way relationships. The default operation is to create *two-way trusts* or *bidirectional trusts*. This makes it easier to manage trust relationships by reducing the trusts you must create. In some cases, however, you might decide against two-way trusts. In one-way relationships, the trusting domain allows resources to be shared with the trusted domain but not the other way around.

When domains are added together to form trees and forests, an automatic transitive two-way trust is created between them. Although the default trust relationships work well for most organizations, there are some reasons you might want to manage trusts manually:

- You may want to remove trusts between domains if you are absolutely sure you do not want resources to be shared between domains.
- Because of security concerns, you may need to keep resources isolated.

In addition to the default trust types, you can configure the following types of special trusts:

External Trusts You use *external trusts* to provide access to resources on a Windows NT 4 domain or forest that cannot use a forest trust. Windows NT 4 domains cannot benefit from the other trust types that are used in Windows Server 2012 R2. Thus, in some cases, external trusts could be your only option. External trusts are always nontransitive, but they can be established in a one-way or two-way configuration.

Default SID Filtering on External Trusts When you set up an external trust, remember that it is possible for hackers to compromise a domain controller in a trusted domain. If this trust is compromised, a hacker can use the security identifier (SID) history attribute to associate SIDs with new user accounts, granting themselves unauthorized rights (this is called an *elevation-of-privileges attack*). To help prevent this type of attack, Windows Server 2012 R2 automatically enables SID filter quarantining on all external trusts. SID filtering allows the domain controllers in the trusting domain (the domain with the resources) to remove all SID history attributes that are not members of the trusted domain.

Realm Trusts *Realm trusts* are similar to external trusts. You use them to connect to a non-Windows domain that uses Kerberos authentication. Realm trusts can be transitive or nontransitive, one-way or two-way.

Cross-Forest Trusts *Cross-forest trusts* are used to share resources between forests. They have been used since Windows Server 2000 domains and cannot be nontransitive, but you can establish them in a one-way or a two-way configuration. Authentication requests in either forest can reach the other forest in a two-way cross-forest trust. If you want one

forest to trust another forest, you must set it (at a minimum) to at least the forest function level of Windows Server 2003.

Selective Authentication vs. Forest-wide Authentication Forest-wide authentication on a forest trust means that users of the trusted forest can access all of the resources of the trusting forest. Selective authentication means that users cannot authenticate to a domain controller or resource server in the trusting forest unless they are explicitly allowed to do so. Exercise 21.8 will show you the steps necessary to change forest-wide authentication to selective authentication.

Shortcut Trusts In some cases, you may actually want to create direct trusts between two domains that implicitly trust each other. Such a trust is sometimes referred to as a *shortcut trust*, and it can improve the speed at which resources are accessed across many different domains. Let's say you have a forest, as shown in Figure 21.14.

FIGURE 21.14 Example of a forest

Users in the `NY.us.stellacon.com` domain can access resources in the `London.uk.stellacon.com` domain, but the users have to authenticate using the parent domains to gain access (`NY.us.stellacon.com` to `us.stellacon.com` to `stellacon.com` to `uk.stellacon.com` to finally reach `London.uk.stellacon.com`). This process can be slow.

An administrator can set up a one-way trust from `London.uk.stellacon.com` (trusting domain) to `NY.us.stellacon.com` (trusted domain) so that the users can access the resources directly.

Perhaps the most important aspect to remember regarding trusts is that creating them only *allows* you to share resources between domains. The trust does not grant any permissions between domains by itself. Once a trust has been established, however, system administrators can easily assign the necessary permissions.

Exercise 21.8 walks you through the steps necessary to manage trusts. In this exercise, you will see how to assign trust relationships between domains. To complete the steps in this exercise, you must have domain administrator access permissions.

EXERCISE 21.8

Managing Trust Relationships

1. Open the Active Directory Domains and Trusts administrative tool.
2. Right-click the name of a domain and select Properties.
3. Select the Trusts tab. You will see a list of the trusts that are currently configured. To modify the trust properties for an existing trust, highlight that trust and click Properties.
4. The Properties window for the trust displays information about the trust's direction, transitivity, and type along with the names of the domains involved in the relationship. Click Cancel to exit without making any changes.
5. To create a new trust relationship, click the New Trust button on the Trusts tab. The New Trust Wizard appears. Click Next to proceed with the wizard.
6. On the Trust Name page, you are prompted for the name of the domain with which the trust should be created. Enter the name of the domain and click Next.
7. On the Trust Type page, you would normally choose the Trust With A Windows Domain option if you know that the other domain uses a Windows domain controller. Choose Realm Trust. Click Next when you have finished.
8. On the Transitivity Of Trust page, you choose whether the trust is transitive or nontransitive. Choose the Nontransitive option and click Next to continue.
9. On the Direction Of Trust page, you select the direction of the trust. If you want both domains to trust each other, you select the Two-Way option. Otherwise, you select either One-Way: Incoming or One-Way: Outgoing, depending on where the affected users are located. For the sake of this exercise, choose One-Way: Incoming and then click Next.

10. On the Trust Password page, you need to specify a password that should be used to administer the trust. Type **P@ssw0rd** and confirm it. Note that if there is an existing trust relationship between the domains, the passwords must match. Click Next to continue.
11. Now you see the Trust Selections Complete page that recaps the selections you have made. Because this is an exercise, you don't actually want to establish this trust. Click Cancel to cancel the wizard without saving the changes.
12. Exit the trust properties for the domain by clicking Cancel.

To Enable Selective Authentication

1. In the console tree, right-click the name of a domain and select Properties.
2. Select the Trusts tab. Under either Domains Trusted By This Domain (Outgoing Trusts) or Domains That Trust This Domain (Incoming Trusts), click the forest trust that you want to administer and then click Properties.
3. On the Authentication tab, click Selective Authentication and then click OK.

Managing UPN Suffixes

User principal name (UPN) suffixes are the part of a user's name that appears after the `@` symbol. For example, the UPN suffix of `wpanek@stellacon.com` would be `stellacon.com`. By default, the UPN suffix is determined by the name of the domain in which the user is created. In this example, the user wpanek was created in the domain `stellacon.com`, so the two pieces of the UPN logically fit together. However, you might find it useful to provide an alternative UPN suffix to consolidate the UPNs forest wide.

For instance, if you manage a forest that consists of `stellacon.com` and `stellacon2.com`, you might want all of your users to adopt the more generally applicable `stellacon.com` UPN suffix. By adding additional UPN suffixes to the forest, you can easily choose the appropriate suffix when it comes time to create new users. Exercise 21.9 shows you how to add additional suffixes to a forest.

EXERCISE 21.9

Adding a UPN Suffix

1. Open the Active Directory Domains and Trusts administrative tool.
2. Right-click Active Directory Domains And Trusts in the left side of the window and select Properties.
3. On the UPN Suffixes tab of the Active Directory Domains And Trusts Properties dialog box, enter an alternative UPN suffix in the Alternative UPN Suffixes field. Click the Add button to add the suffix to the list.
4. To remove a UPN suffix, select its name in the list and click the Remove button.

Name Suffix Routing

Name Suffix Routing is a mechanism that is used to manage how authentication requests are routed across Active Directory forests that are joined together by forest trusts. To simplify the administration of authentication requests, when you create a forest trust, all unique name suffixes are routed by default. A *unique name suffix* is a name suffix within a forest, such as a user principal name (UPN) suffix, service principal name (SPN) suffix, or Domain Name System forest, or a domain tree name that is not subordinate to any other name suffix. Name Suffix Routing is managed from the Active Directory Domains and Trusts Administrative Console.

Managing Global Catalog Servers

One of the best features of a distributed directory service like Active Directory is that you can store different pieces of information in different places within an organization. For example, a domain in Japan might store a list of users who operate within a company's Asian operations business unit, while one in New York would contain a list of users who operate within its North American operations business unit. This architecture allows system administrators to place the most frequently accessed information on domain controllers in different domains, thereby reducing disk space requirements and replication traffic.

However, you may encounter a problem when you deal with information that is segmented into multiple domains. The issue involves querying information stored within Active Directory. For example, what would happen if a user wanted a list of all the printers available in all domains within the Active Directory forest? In this case, the search would normally require information from at least one domain controller in each of the domains within the environment. Some of these domain controllers may be located across slow WAN links or may have unreliable connections. The result would include an extremely long wait while retrieving the results of the query, that is, if any results came up without the query timing out.

Fortunately, Active Directory has a mechanism that speeds up such searches. You can configure any number of domain controllers to host a copy of the GC. The GC contains all of the schema information and a subset of the attributes for all domains within the Active Directory environment. Although a default set of information is normally included with the GC, system administrators can choose to add additional information to this data store if it is needed. To help reduce replication traffic and to keep the GC's database small, only a limited subset of each object's attributes is replicated. This is called the *partial attribute set (PAS)*. You can change the PAS by modifying the schema and marking attributes for replication to the GC.

Servers that contain a copy of the GC are known as *GC servers*. Now whenever a user executes a query that requires information from multiple domains, they need only contact the nearest GC server for this information. Similarly, when users must authenticate across domains, they do not have to wait for a response from a domain controller that may be located across the world. The result is that the overall performance of Active Directory queries improves.

Exercise 21.10 walks you through the steps that you need to take to configure a domain controller as a GC server. Generally, GC servers are useful only in environments that use multiple Active Directory domains.

EXERCISE 21.10

Managing GC Servers

1. Open the Active Directory Sites and Services administrative tool.
2. Find the name of the local domain controller within the list of objects, typically under Default First Site Name ➢ Servers, and expand this object. Right-click NTDS Settings, and select Properties.
3. In the NTDS Settings Properties dialog box, type **Primary GC Server for Domain** in the Description field. Note that there is a check box that determines whether this computer contains a copy of the global catalog. If the box is checked, then this domain controller contains a subset of information from all other domains within the Active Directory environment. Select the Global Catalog check box and then click OK to continue.
4. When you have finished, close the Active Directory Sites and Services administrative tool.

Managing Universal Group Membership Caching

Many networks run into problems with available network bandwidth and server hardware limitations. For this reason, it may not be wise to install a GC in smaller branch offices. Windows Server 2012 R2 can help these smaller sites by deploying domain controllers that use *Universal Group Membership Caching (UGMC)*.

Once enabled, Universal Group Membership Caching stores information locally when a user attempts to log on for the first time. With the use of a GC, the domain controller retains the universal group membership for that logged-on user.

The next time that user attempts to log on, the authenticating domain controller running Windows Server 2012 R2 will obtain the universal group membership information from its local cache without the need to contact a GC. By default, the universal group membership information is retained on the domain controller for eight hours.

There are several advantages of using Universal Group Membership Caching:

Faster Logon Times Because the domain controller does not need to contact a global catalog, logon authentication is faster.

Reduced Network Bandwidth The domain controller does not have to handle object replication for all of the objects located in the forest.

Ability to Use Existing Hardware There is no need to upgrade hardware to support a GC.

Exercise 21.11 shows you the steps necessary to configure Universal Group Membership Caching.

EXERCISE 21.11

Managing Universal Group Membership Caching

1. Open the Active Directory Sites and Services administrative tool.
2. Click Sites and then click `CorporateHQ`. In the right pane, right-click NTDS Settings and choose Properties.
3. In the NTDS Site Settings Properties dialog box, check the box Enable Universal Group Membership Caching and then click OK to continue.
4. When you have finished, close the Active Directory Sites and Services administrative tool.

Upgrading Existing Domains and Forests

Now that you have a new operating system to which you can upgrade, it's important that you take some time to talk about the different ways you can get your infrastructure up-to-date. There are quite a few upgrade paths to consider. Table 21.2 illustrates the most commonly used in-place upgrade paths for upgrading your domain controllers from Windows Server 2008 to Windows Server 2012 R2. The in-place upgrades hold true only for 64-bit versions of Server 2008 to Server 2012 R2. You cannot in-place upgrade domain controllers that run either Windows Server 2003 or a 32-bit version of Windows Server 2008. If your current environmental configurations fall outside of the possibility of an in-place upgrade, then you will need to install new domain controllers on the most up-to-date Windows Server OS and then delete the old ones.

TABLE 21.2 Supported domain controller in-place upgrade paths

If you are running these editions...	You can upgrade to these editions...
Windows Server 2008 Standard with SP2 or Windows Server 2008 Enterprise with SP2	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter
Windows Server 2008 Datacenter with SP2	Windows Server 2012 R2 Datacenter
Windows Web Server 2008	Windows Server 2012 R2 Standard

Windows Server 2008 R2 Standard with SP1 or Windows Server 2008 R2 Enterprise with SP1	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter
Windows Server 2008 R2 Datacenter with SP1	Windows Server 2012 R2 Datacenter
Windows Web Server 2008 R2	Windows Server 2012 Standard

When preparing for your domain controller upgrade, make sure you make a full backup of your Active Directory environment prior to the performing the task. If you have never actually performed a full backup and restore of your Active Directory environment, then I recommend doing so by following the instructions in Chapter 19 of this book. You never know if a backup actually works until you perform the restore, and you should never make infrastructure changes without a backup of your current configuration.

In addition to knowing the proper upgrade path and having full backups of your environment, you will also want to take into account domain and forest functional levels. Windows Server 2012 R2 requires a forest functional level of at least Windows Server 2003. This essentially means you cannot add a Windows Server 2012 R2 domain controller to a forest that contains a Windows 2000 machine. You would need to upgrade or eliminate any Windows 2000 machine and then raise the forest functional level to at least Windows Server 2003 in order to accommodate a Windows Server 2012 R2 domain controller. It may seem old, but you'd be surprised how many government organizations still have Windows Server 2000 and Windows Server 2003 running legacy applications in a production environment. You will notice that the issue is far less frequent in commercial settings.

Summary

In this chapter, I discussed the purpose of Active Directory replication. As you have learned, replication is used to keep domain controllers synchronized, and it is important in Active Directory environments of all sizes. Replication is the process by which changes to the Active Directory database are transferred between domain controllers.

This chapter also covered the concepts of sites, site boundaries, and subnets. In addition to learning how to configure them, you learned that subnets define physical portions of your network environment and that sites are defined as collections of well-connected IP subnets. Site boundaries are defined by the subnet or subnets that you include in your site configuration.

I also covered the basics of replication and the differences between intrasite and intersite replication. Additionally, I covered the purpose and use of bridgehead servers in depth. Although replication is a behind-the-scenes type of task, the optimal configuration of sites

in distributed network environments results in better use of bandwidth and faster response by network resources. For these reasons, you should be sure you thoroughly understand the concepts related to managing replication for Active Directory.

I covered the placement of domain controllers and global catalog servers in the network and how, when placed properly, they can increase the performance of Active Directory operations.

I also showed how to monitor and troubleshoot replication. The Windows Server 2012 R2 System Monitor administrative tool was designed so that you can monitor many performance statistics associated with using Active Directory.

The chapter also covered the basics of linking multiple domains in trees and forests. You now know why you would want to plan for them and the benefits and drawbacks of using only one domain or of having a multidomain environment. For example, you might decide to have multiple domains if you have an acquisitions-and-mergers situation where you need to keep multiple administrators. In addition, by using multiple domains, organizations can retain separate security databases; however, in such cases, they are also able to share resources between domains.

You can use multiple domains to provide two major benefits for the network directory services—security and availability. These benefits are made possible through Active Directory and the administrative tools that can be used to access it.

System administrators can simplify operations while still ensuring that only authorized users have access to their data. Multiple domains can interact to form Active Directory trees and forests, and you can use the Active Directory Installation Wizard to create new Active Directory trees and forests.

Exam Essentials

Understand the reasons for using multiple domains. There are seven primary reasons for using multiple domains: They provide additional scalability, they reduce replication traffic, they help with political and organizational issues, they provide many levels of hierarchy, they allow for decentralized administration, they preserve legality, and they allow for multiple DNS or domain names.

Understand the drawbacks of using multiple domains. With multiple domains, maintaining administrative consistency is more difficult. The number of administrative units multiplies as well, which makes it difficult to keep track of network resources. Finally, it is much more difficult to rearrange the domain topology within an Active Directory environment than it is simply to reorganize OUs.

Know how to create a domain tree. To create a new domain tree, you need to promote a Windows Server 2012 R2 computer to a domain controller, select the option that makes this domain controller the first machine in a new domain, and make that domain the first domain of a new tree. The result is a new domain tree.

Know how to join a domain tree to a forest. Creating a new tree to form or add to a forest is as simple as promoting a server to a domain controller for a new domain that does *not* share a namespace with an existing Active Directory domain. To add a domain to an existing forest, you must already have at least one other domain. This domain serves as the root domain for the entire forest.

Understand how to manage single-master operations. Single-master operations must be performed on specially designated machines within the Active Directory forest. There are five main single-master functions: two that apply to an entire Active Directory forest (Schema Master and Domain Naming Master) and three that apply to each domain (RID Master, PDC Emulator Master, and Infrastructure Master).

Understand how to manage trusts. When configuring trusts, you'll need to consider two main characteristics: transitivity and direction. The simplest way to understand transitive relationships is through this example: If Domain A trusts Domain B and Domain B trusts Domain C, then Domain A implicitly trusts Domain C. Trusts can be configured as nontransitive so that this type of behavior does not occur. In one-way relationships, the trusting domain allows resources to be shared with the trusted domain. In two-way relationships, both domains trust each other equally. Special trusts include external trusts, realm trusts, cross-forest trusts, and shortcut trusts.

Understand how to manage UPN suffixes. By default, the name of the domain in which the user is created determines the UPN suffix. By adding additional UPN suffixes to the forest, you can easily choose more manageable suffixes when it comes time to create new users.

Understand how to manage global catalog servers. You can configure any number of domain controllers to host a copy of the global catalog. The GC contains all of the schema information and a subset of the attributes for all domains within the Active Directory environment. Servers that contain a copy of the GC are known as GC servers. Whenever a user executes a query that requires information from multiple domains, they need only contact the nearest GC server for this information. Similarly, when users must authenticate across domains, they will not have to wait for a response from a domain controller that may be located across the world. The result is increased overall performance of Active Directory queries.

Understand universal group membership caching. You can enable a domain controller as a Universal Group Membership Caching server. The Universal Group Membership Caching machine will then send a request for the logon authentication of a user to the GC server. The GC will then send the information back to the Universal Group Membership Caching server to be cached locally for eight hours (by default). The user can then authenticate without the need to contact the GC again.

Understand the purpose of Active Directory replication. Replication is used to keep domain controllers synchronized, and it is important in Active Directory environments of all sizes. Replication is the process by which changes to the Active Directory database are transferred between domain controllers.

Understand the concept of sites, site boundaries, and subnets. Subnets define physical portions of your network environment. Sites are defined as collections of well-connected IP subnets. Site boundaries are defined by the subnet or subnets that you include in your site configuration.

Understand the differences between intrasite and intersite replication. Intrasite replication is designed to synchronize Active Directory information to machines that are located in the same site. Intersite replication is used to synchronize information for domain controllers that are located in different sites.

Understand the purpose of bridgehead servers. Bridgehead servers are designed to accept traffic between two remote sites and then to forward this information to the appropriate servers. One way to synchronize data between sites efficiently that are connected with slow connections is to use a bridgehead server.

Implement site links, site link bridges, and connection objects. You can use all three of these object types to finely control the behavior of Active Directory replication and to manage replication traffic. Site links are created to define the types of connections that are available between the components of a site. Site links can reflect a relative cost for a network connection and can reflect the bandwidth that is available for communications. You can use site link bridges to connect site links so that the relationship can be transitive. Connection objects provide you with a way to set up special types of replication schedules such as immediate replication on demand or specifying a custom schedule for certain servers.

Configure replication schedules and site link costs. You can create multiple site links between sites, and you can assign site links a cost value based on the type of connection. The system administrator determines the cost value, and the relative costs of site links are then used to determine the optimal path for replication. The lower the cost, the more likely the link is to be used for replication. Once you've determined how and through which connections replication will take place, it's time to determine *when* information should be replicated. Replication requires network resources and occupies bandwidth. Therefore, you need to balance the need for consistent directory information with the need to conserve bandwidth.

Determine where to place domain controllers and global catalog servers based on a set of requirements. Where you place domain controllers and global catalog servers can positively affect the performance of Active Directory operations. However, to optimize performance, you need to know the best places to put these servers in a network environment that consists of multiple sites.

Monitor and troubleshoot replication. The Windows Server 2012 R2 System Monitor administrative tool is designed so that you can monitor many performance statistics associated with using Active Directory. In addition to this monitoring, you should always verify basic network connectivity and router and firewall connections and also examine the event logs.

Review Questions

1. You need to deactivate the UGMC option on some of your domain controllers. At which level in Active Directory would you deactivate UGMC?
   - **A.** Server
   - **B.** Site
   - **C.** Domain
   - **D.** Forest

2. You work for an organization with a single domain forest. Your company has one main location and two branch locations. All locations are configured as Active Directory sites, and all sites are connected with the DEFAULTIPSITELINK object. Your connections are running slower than company policy allows. You want to decrease the replication latency between all domain controllers in the various sites. What should you do?
   - **A.** Decrease the Replication interval for the DEFAULTIPSITELINK object.
   - **B.** Decrease the Replication interval for the site.
   - **C.** Decrease the Replication schedule for the site.
   - **D.** Decrease the Replication schedule for all domain controllers.

3. You need to enable three of your domain controllers as global catalog servers. Where would you configure the domain controllers as global catalogs?
   - **A.** Forest, NTDS settings
   - **B.** Domain, NTDS settings
   - **C.** Site, NTDS settings
   - **D.** Server, NTDS settings

4. Daniel is responsible for managing Active Directory replication traffic for a medium-sized organization that has deployed a single Active Directory domain. Currently, the environment is configured with two sites and the default settings for replication. Each site consists of 15 domain controllers. Recently, network administrators have complained that Active Directory traffic is using a large amount of available network bandwidth between the two sites. Daniel has been asked to meet the following requirements:
   - Reduce the amount of network traffic between domain controllers in the two sites.
   - Minimize the amount of change to the current site topology.
   - Require no changes to the existing physical network infrastructure.

   Daniel decides that it would be most efficient to configure specific domain controllers in each site that will receive the majority of replication traffic from the other site. Which of the following solutions meets the requirements?
   - **A.** Create additional sites that are designed only for replication traffic and move the existing domain controllers to these sites.
   - **B.** Create multiple site links between the two sites.
   - **C.** Create a site link bridge between the two sites.
   - **D.** Configure one server at each site to act as a preferred bridgehead server.

5. Which of the following does not need to be created manually when you are setting up a replication scenario involving three domains and three sites?
   - **A.** Sites
   - **B.** Site links
   - **C.** Connection objects
   - **D.** Subnets

6. Which of the following services of Active Directory is responsible for maintaining the replication topology?
   - **A.** File Replication Service
   - **B.** Knowledge Consistency Checker
   - **C.** Windows Internet Name Service
   - **D.** Domain Name System

7. A system administrator for an Active Directory environment that consists of three sites wants to configure site links to be transitive. Which of the following Active Directory objects is responsible for representing a transitive relationship between sites?
   - **A.** Additional sites
   - **B.** Additional site links
   - **C.** Bridgehead servers
   - **D.** Site link bridges

8. You have configured your Active Directory environment with multiple sites and have placed the appropriate resources in each of the sites. You are now trying to choose a protocol for the transfer of replication information between two sites. The connection between the two sites has the following characteristics:
   - The link is generally unavailable during certain parts of the day because of an unreliable network provider.
   - The replication transmission must be attempted whether the link is available or not. If the link was unavailable during a scheduled replication, the information should automatically be received after the link becomes available again.
   - Replication traffic must be able to travel over a standard Internet connection.

   Which of the following protocols meets these requirements?
   - **A.** IP
   - **B.** SMTP
   - **C.** RPC
   - **D.** DHCP

9. A system administrator suspects that there is an error in the replication configuration. How can the system administrator look for specific error messages related to replication?

A. By using the Active Directory Sites and Services administrative tool

B. By using the Computer Management tool

C. By going to Event Viewer ➢ System Log

D. By going to Event Viewer ➢ Directory Service Log

10. Christina is responsible for managing Active Directory replication traffic for a medium-sized organization. Currently, the environment is configured with a single site and the default settings for replication. The site contains more than 50 domain controllers, and the system administrators are often making changes to the Active Directory database. Recently, network administrators have complained that Active Directory traffic is consuming a large amount of network bandwidth between portions of the network that are connected by slow links. Ordinarily, the amount of replication traffic is reasonable, but recently users have complained about slow network performance during certain hours of the day.

Christina has been asked to alleviate the problem while meeting the following requirements:

- Be able to control exactly when replication occurs.
- Be able to base Active Directory replication on the physical network infrastructure.
- Perform the changes without creating or removing any domain controllers.

Which two of the following steps can Christina take to meet these requirements? (Choose two.)

A. Create and define Connection objects that specify the hours during which replication will occur.

B. Create multiple site links.

C. Create a site link bridge.

D. Create new Active Directory sites that reflect the physical network topology.

E. Configure one server at each of the new sites to act as a bridgehead server.

Chapter

22

Configure Access and Information Protection Solutions

THE FOLLOWING 70-412 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Install and configure Active Directory Certificate Services (AD CS)**

- Describe and explain the new features in Windows Server 2012 Active Directory Certificate Services
- Install and configure Active Directory Certificate Services using Server Manager and Windows PowerShell
- Manage Active Directory Certificate Services using management consoles and Windows PowerShell
- Configure CRL distribution points
- Install and configure Online Responder
- Implement administrative role separation
- Configure CA Disaster recovery
- Manage certificates
- Manage certificate templates
- Implement and manage certificate deployment, validation, and revocation
- Manage certificate renewal
- Manage certificate enrollment and renewal to computers and users using Group Policies
- Configure and manage key archival and recovery

- Manage trust between organizations including Certificate Trust List (CTL)
- Managing Cross certifications and bride CAs
- Monitoring CA Health

✓ **Install and Configure Active Directory Federation Services (AD FS)**

- Implement claims-based authentication including Relying Party Trusts
- Configure authentication policies
- Configure Workplace Join
- Configure multi-factor authentication

✓ **Install and configure Active Directory Rights Management Services (AD RMS)**

- Install a licensing or certificate AD RMS server
- Manage AD RMS Service Connection Point (SCP)
- Manage RMS templates
- Configure Exclusion Policies
- Backup and restore AD RMS

In this chapter, I will discuss certificate services and the importance of securing the corporate *public key infrastructure (PKI)* environment. The Windows 2012 PKI implementation resides in Active Directory Certificate Services. PKI is the collection of technology, protocols, services, standards, and policies that control the issuing and management of public and private keys using digital certificates, which are the core of PKI. Encryption is used to protect data messages. While certificates provide a certain level of security, they are still vulnerable.

Next, I will cover federation services and how to set up relying party trusts with certificates. Finally, I will discuss rights management, which Microsoft created to further protect documents, email, and web pages from unauthorized copying, printing, forwarding, editing, deleting, and so forth.

What's New in Windows Server 2012 R2 with Active Directory Certificate Services?

Active Directory Certificate Services is a server role included in Windows Server 2012 R2. AD CS allows administrators to customize, issue, and manage public key certificates. AD CS issues digital certificates for authentication, encryption and decryption, and signing.

The following are the new features regarding Active Directory Certificate Services (AD CS) in Windows Server 2012 R2:

Server Core and Minimal Server Interface Support You can install and deploy any of the six AD CS role services to any version of Windows Server 2012 R2, including Server Core and Minimal Server Interface. The Minimal Server Interface looks and feels like a Server Core installation with most of the GUI management utilities intact. Windows Server 2012 R2 Minimal Server Interface reduces the attack surface and lowers the footprint by removing components such as Windows Explorer and Internet Explorer and their supporting libraries.

Site-Aware Certificate Enrollment Windows 8/8.1 and Windows Server 2012 R2 computers default to using certificate authorities within their sites when requesting certificates. However, you must configure site information on the certificate authorities' objects within Active Directory for the site-awareness feature to be worthwhile. Once

configured, computers running Windows 8/8.1 and Windows Server 2012 R2 request certificates from a certificate authority running in the same site as the computer.

Automatic Certificate Renewal for Non-Domain-Joined Computers Certificate Enrollment Web Services (CES) allows non-domain-joined computers and computers not directly connected to the corporate network to request and retrieve certificates. AD CS in Windows Server 2012 R2 includes the ability for these clients to renew certificates automatically for non-domain-joined computers.

Enforcement of Certificate Renewal with the Same Key In earlier versions of Windows, clients that received certificates from templates that were configured for renewal with the same key had to renew their certificates using the same key, or renewal would fail.

With Windows 8/8.1 or Windows Server 2012 R2, you can continue this behavior, or you can configure certificate templates to give higher priority to Trusted Platform Module (TPM)–based KSPs for generating keys. Moreover, using renewal with the same key, administrators can rest assured that the key remains on TPM after renewal.

This feature allows you to enforce renewal with the same key, which can reduce administrative costs (when keys are renewed automatically) and increase key security (when keys are stored using TPM-based KSPs).

Internationalized Domain Names (IDNs) International languages often contain characters that cannot be represented using ASCII encoding, which limits the function of these languages when enrolling for a certificate. Windows Server 2012 R2 now includes support for international domain names.

Default Security Increased on the Certificate Authority Role Service Certificate authorities running on Windows Server 2012 R2 include increased RPC security. Increased RPC security on the CA requires that all clients must encrypt the RPC communication between themselves and the CA when requesting certificates.

Active Directory Certificate Services Roles

The Active Directory Certificate Services role provides six role services to issue and manage public key certificates in an enterprise environment. These roles are listed in Table 22.1 and described in the following sections.

TABLE 22.1 AD CS roles

Role service	Description
Certificate Authority (CA)	The CA service includes root and subordinate CAs for issuing certificates to users, computers, and services. This role service also manages certificate validity.
Web Enrollment	This is a web-based interface to enable users to enroll, request, and retrieve certificates as well as retrieve certificate revocation lists from a CA using a web browser.

Online Responder (OCSP)	The Online Responder service retrieves revocation status requests for specific certificates and the status of these certificates, and it returns a signed response with the requested certificate status information.
Network Device Enrollment Service (NDES)	NDES enables routers and other non-domain-joined network devices to acquire certificates.
Certificate Enrollment Policy Web Server (CEP)	CEP enables users and computers to inquire about certificate enrollment policy information.
Certificate Enrollment Web Services (CES)	CES enables users and computers to enroll for certificates with the HTTPS protocol. CEP and CES can be used together to support certificate enrollment for non-domain-joined computers and computers not directly connected to the corporate network.

Planning the Certificate Authority Hierarchy

A *certification authority (CA)* is a trusted server designed to grant certificates to individuals, computers, or organizations to certify the identity and other attributes of the certificate subject.

A CA receives a certificate request, verifies the requester's identity data according to the policy of the CA, and uses its private key to apply its digital signature to the certificate. The CA issues the certificate to the subject of the certificate as a security credential within a PKI environment. A CA is also responsible for revoking certificates and publishing a *certificate revocation list (CRL)*.

A CA can be a third-party issuer, such as VeriSign, or you can create your own CA by installing Active Directory Certificate Services. Every CA also has a certificate confirming its identity, issued by another trusted CA or root CAs.

Cryptography

The Cryptography options for a certificate authority provide increased deployment flexibility to those with a more advanced understanding of cryptography. You can implement cryptographic options by using cryptographic service providers (CSPs) or key storage providers (KSPs).

CSPs are hardware and software components of Windows operating systems that provide generic cryptographic functions. CSPs can provide a variety of encryption and signature algorithms. Key storage providers can provide strong key protection on computers running Windows Server 2012/2012 R2, Windows Server 2008/2008 R2, Windows Vista, Windows 7, or Windows 8. Figure 22.1 shows some of the Cryptography options in the AD CS installation.

FIGURE 22.1 Cryptography for CA screen

Here are the options:

Select a Cryptographic Provider Windows Server 2012 R2 provides many CSPs and KSPs, and you can install additional CSPs or KSPs provided by third parties. In Windows Server 2012 R2, the algorithm name is listed in the provider list. All providers with a number sign (#) in the name are cryptography next-generation (CNG) providers. CNG providers can support multiple asymmetric algorithms. CSPs implement only a single algorithm.

Key Length Each CSP and KSP supports different character lengths for cryptographic keys. Configuring a longer key length hardens against an attack by a hacker to decrypt the key and also degrades the performance of cryptographic operations.

Select The Hash Algorithm For Signing Certificates Used By This CA The CA uses hash algorithms to sign CA certificates and issues certificates to ensure that an external identity has not tampered with a certificate. Each CSP can support different hash algorithms.

NOTE

Make sure that your applications, your devices, and all operating systems that may request certificates from this certificate authority support the selected hash algorithm.

Allow Administrator Interaction When The Private Key Is Accessed By The CA Use this option to help secure the CA and its private key by requiring an administrator to enter a password before every cryptographic operation.

Exercise caution with this setting because this requires user interaction each time the certificate authority accesses the private key. A certificate authority signs each issued certificate. To sign the issued certificate, the certificate authority must access the private key.

Private Key

A certificate authority uses its assigned certificate to generate and issue certificates. The certificate used by the CA includes a public key and a private key. The private key should be available only to the owner. The public key is publicly available to other entities on the network.

For example, a user's public key can be published within a certificate in a folder so that it is accessible to other people in the organization. The sender of a message can retrieve the user's certificate from Active Directory Domain Services, obtain the public key from the certificate, and then encrypt the message by using the recipient's public key.

Data encrypted with a public key can be decrypted only with the mathematically paired private key. Certificate authorities use their private key to create a digital signature in the certificate when issuing certificates.

Enterprise Certificate Authorities

Enterprise certificate authorities (CAs) publish certificates and CRLs to Active Directory. Enterprise CAs access domain data stored in Active Directory. Enterprise CAs engage certificate templates when issuing certificates. The enterprise CA uses default configuration data in the certificate template to create a certificate with the appropriate attributes for that certificate type.

If you want to enable automatic certificate approval and automatic user certificate enrollment, use enterprise CAs to issue certificates. These features are available only when the CA infrastructure is integrated with Active Directory. Additionally, only enterprise CAs can issue certificates that enable smart card logon because this process requires the CA to map the user account in Active Directory to the smart card certificates.

A *root CA*, sometimes called a *root authority*, is the most trusted CA type in an organization's PKI. The root CA is the only CA that signs its own certificate. The physical security and the certificate issuance policy of a root CA should be tightly reinforced. If the root CA is compromised or if it issues a certificate to an unauthorized identity, any certificate-based security in your organization is compromised by the exposed private key. The best practice is to deploy a second PKI tier to issue certificates from other CAs, called *subordinate CAs* (see Figure 22.2).

FIGURE 22.2 Two-tier PKI hierarchy model

A *subordinate CA* is one that has received its signing certificate by a root CA, third-party CA, or stand-alone CA in your organization. Subordinate CAs normally issue certificates for specific purposes, such as secure email, SSL, Wireless 801.x security, or smart card authentication. Subordinate CAs can also issue certificates to other, more subordinate CAs. A root CA, the subordinate CAs certified by the root, and subordinate CAs certified by other subordinate CAs form a certification hierarchy.

Stand-alone certificate authorities are not integrated into Active Directory and do not support certificate templates. If you deploy stand-alone CAs, you must include all the information about the requested certificate type in the certificate request. By default, all submitted certificate requests to a stand-alone CA are placed in a pending queue, awaiting a CA administrator's approval. Stand-alone CAs can issue certificates automatically upon request, but this is not recommended because the requests are not authenticated.

Because stand-alone CAs are not Active Directory integrated, a stand-alone CA would seem like a less appropriate choice for an enterprise. However, stand-alone root CAs offer a layer of protection when a powered-down stand-alone CA is less likely to be compromised and does not have a footprint in Active Directory. More organizations are deploying *offline stand-alone root CAs* that are brought online only temporarily for re-issuing signing certificates to subordinate CAs. Some organizations permanently keep the offline stand-alone root CA disconnected from the network and distribute signing certificates only via removable media such as CDs, DVDs, or USB flash drives. Offline root CAs have the following characteristics:

- Deployed as a stand-alone root CA
- Deployed on a non-domain-joined server to avoid being offline or powered down for long periods without requiring computer password synchronizations

Real World Scenario

Protect the Offline Root CA

Best practice strongly recommends you securely store and back up the offline stand-alone root CA. A large Medical center implemented their offline stand-alone root CA solution by installing their root CA on a laptop. They routinely kept the laptop in the datacenter until a new administrator discovered and returned laptop to the help desk for repurposing. Needless to say, the laptop was re-imaged, and the entire PKI infrastructure was wiped out. No one was aware until the subordinate CA's certificate had expired a year later and certificates could no longer be issued. You can avoid this catastrophic scenario by securely storing and backing up the offline stand-alone CA.

Two-Tier and Three-Tier Models

It's acceptable for a single enterprise to have multiple PKIs. Multiple PKIs result in one root CA for each PKI and possibly multiple subordinate CAs that chain to their respective roots.

Organizations also may choose a third-tier CA hierarchy model, which involves adding a CA policy server. CA policy servers are designed to implement specific certificate policies that can include certificate life cycle, encryption type, key length, and some approval workflow.

Validity Period

All certificates issued by a certification authority have a validity period. The *validity period* is a time range that specifies how long PKI clients can accept the certificate as an authoritative credential based on the identity stated in the subject of the certificate. This assertion presumes the certificate is not revoked before the validity period ends and the issuing CA remains trusted. The validity period limits the time in which an issued certificate is exposed to the possibility of being compromised (`http://technet.microsoft.com/en-us/library/cc740209(v=WS.10).aspx`).

All CAs have an expiration date based on its CA certificate's validity ending period. This rule affects the CA's ability to issue certificates and not the validity period of its CA certificate. Because of this rule, organizations must plan for the renewal of every certificate issued to a CA in the certification hierarchy to ensure the existing trust chains and to extend the lifetimes of CAs.

Active Directory Certificate Services enforces a rule that a CA never issues a certificate past the expiration date of its own certificate. Because of this behavior, when a CA's certificate reaches the end of its validity period, all certificates issued by the CA will also expire. Certificates issued by the now-expired CA will not be honored as valid security credentials.

Active Directory Certificate Services allows for the maximum validity periods shown in Table 22.2, which are based on the type of certificate. You configure these validity periods using certificate templates.

TABLE 22.2 AD CS maximum validity periods

Certificate type	Maximum validity period
Root certificate authority	Determined during CA deployment
Subordinate CA Internet Protocol Security Enrollment agent Domain controller	Up to five years, but never more than the root CA's or the issuing CA's validity period
All other certificates	One year, but never more than the root CA's or issuing CA's validity period

Certificate Validation

PKI trust requires a certificate to be validated for both for its expiration and its overall chain of trust. When a certificate user leaves the company, you will want to make sure that no one can use that certificate for authentication and revoke the certificate. Revocation checking is one of the key components of PKI.

Certificate revocation uses certificate revocation lists. CRLs contain a list of certificates that are no longer valid, and the CRL can become large. To solve this, you can access a delta CRL that contains changes or new revocations.

CRLs are accessed through *CRL distribution points (CDPs)*, which are part of a CA role in Windows Server 2012. HTTP, FTP, LDAP, or file-based addresses may be used as URLs. Only newly issued certificates will recognize new changes in the CRL URL; old certificates will use the old URL for revocation list operations.

Online Responders

When a new certificate is issued, the computer queries the issuing CA to find out whether the certificate has been revoked. Traditionally, certificate revocation checking can be done by retrieving certificate revocation lists that are published in Lightweight Directory Access Protocol (LDAP) or Hypertext Transfer Protocol (HTTP) or by using a newer HTTP method named the Online Certificate Status Protocol (OCSP).

OCSP is a lightweight HTTP protocol that responds faster and more efficiently than downloading a traditional CRL. An *online responder* is a trusted server that receives and responds to individual client requests for the status of a certificate. An OCSP responder retrieves CRLs and provides digitally signed real-time certificate revocation status responses to clients based on a given certificate authority's CRL. The amount of data retrieved per request remains constant regardless of the number of revoked certificates.

Online responders process certificate status requests more efficiently than direct access to CRLs in several scenarios (`http://technet.microsoft.com/en-us/library/cc725958.aspx`):

- When clients have slow VPN connections or do not have the high-speed connections required to download large CRLs
- When network utilization peaks because revocation-checking activity is high, such as when large numbers of users log on or send signed email simultaneously
- When revocation data for certificates is needed from a non-Microsoft certification authority
- When revocation data is needed to verify individual certificate status requests rather than all revoked or suspended certificates

Installing AD CS

Server Manager provides a graphical user interface to install Active Directory Certificate Services on local and remote computers running Windows Server 2012 R2. The Remote Server Administration Tools for Windows Server 2012 R2 also includes Server Manager, which allows you to run Server Manager on a computer running Windows 8/8.1. In Exercise 22.1, you'll install an AD CS role on the local computer using Server Manager.

EXERCISE 22.1

Installing AD CS Through Server Manager

1. Start Server Manager.
2. Click Manage and click Add Roles And Features
3. The Add Roles And Features Wizard shows the Before You Begin screen. Click Next.
4. Click Role-Based Or Feature-Based Installation on the Select Installation Type screen. Click Next.
5. Click the server on which you want to install Active Directory Certificate Services from the Server Pool list on the Select Destination Server screen. Click Next.
6. Select the Active Directory Certificate Services check box on the Select Server Roles screen.

Server Manager prompts you to add more features associated with this role, such as management tools. Leave the default selections. Click Add Features to close the dialog. Click Next on the Select Server Roles screen.

7. Click Next on the Select Features screen.
8. Server Manager displays the Active Directory Certificate Services screen. This screen provides a simple role introduction and noteworthy information, such as that the name of the certificate authority cannot be changed. Click Next.
9. From the Select Role Services screen, select the check boxes next to the AD CS role services you want to install on the computer. Click Next.
10. Read the Confirm Installation Selections screen. This screen provides a list of roles, role services, and features that the current installation prepares on the computer. Click Install to start the installation.

Installation Using Windows PowerShell

A major benefit gained from basing Windows Server 2012 R2's Server Manager on Windows PowerShell is consistency of installation. Server Manager relies on its Windows PowerShell foundation as the underlying engine responsible for installing any of the Active Directory Certificate Services role services. However, you cannot use Server Manager to install roles and features on a Windows Server 2012 R2 core installation.

The Server Manager module for Windows PowerShell provides cmdlets to install, view, and remove features and roles included in Windows Server 2012 R2. You can use these cmdlets on any installation of Windows Server 2012 R2 because it provides Windows PowerShell in all installation types. Also, these cmdlets can install, view, and uninstall Active Directory Certificate Services role services from remote computers running Windows Server 2012 R2.

To view the installation state of Active Directory Certificate Services using Windows PowerShell, follow these steps:

1. Open an elevated Windows PowerShell console. (On Server Core installations, type **`PowerShell`** in the command console.)
2. In the Windows PowerShell console, type the following command and press Enter:

```
Get-WindowsFeature | where {$_.name -like "adcs*" -or $_.name -like "ad-c*"}
```

The Windows PowerShell cmdlet outputs three columns of information: Display Name, Name, and Install State. The Display Name column is a user-friendly name that describes the feature or service role's use. The Name column represents the name of the component. You use this name with the `Install-WindowsFeature` and `Remove-WindowsFeature` cmdlets. Use the Install State column to determine the installation state of the role or service role.

Typically, the Install State column shows one of three install states: Removed, Available, and Installed. The Removed install state designates that its associated role or feature is not included in the current installation of Windows. You cannot install the associated role or feature without the installation media or Internet connectivity to Windows Update if the feature or role is removed. The Available installation state indicates that the role or feature is staged in the current installation of Windows; however, it is currently not installed.

The Installed installation state indicates that the role or feature is installed on the current installation of the computer and is ready, or it has been deployed or configured.

The Active Directory Certificate Services entry from the cmdlet's output represents the parent role. Six child role services appear underneath the parent role. A lowercase *x* appears between the opening and closing square brackets in the parent role if any of the six child role services are installed. The cmdlet also places a lowercase *x* between the opening and closing square brackets for any installed child role service. You should interpret entries without a lowercase *x* between the opening and closing square brackets as not installed. Check the install state to determine whether the role or role service is staged on your installation of Windows.

To install Active Directory Certificate Services using Windows PowerShell, follow these steps:

1. Open an elevated Windows PowerShell console.
2. Use the `Get-WindowsFeature` cmdlet to ensure the Active Directory Certificate Services role's installation state is Available.
3. In the Windows PowerShell console, type the following command and press Enter:

   ```
   Install-WindowsFeature adcs-cert-authority -IncludeManagementTools
   ```

4. Use the `Get-WindowsFeature` cmdlet to verify the installation (see Figure 22.1).

The preceding command instructs the Server Manager module of Windows PowerShell to take the staged binaries for the Certificate Authority role service and install them to the current computer.

It's important to remember the `-IncludeManagementTools` argument when installing a feature using Windows PowerShell. The Server Manager module for Windows PowerShell does not install a feature or role management tool by default. The `Install-WindowsFeature` cmdlet does not install the role management tool without this argument. The Server Manager GUI automatically selects installing the role management tool for you, and it gives you a choice of not to install it before completing the installation.

You can install any of the other child role services using the `Install-WindowsFeature` cmdlet simply by replacing the `adcs-cert-authority` argument with the associated name of the child role service. The following example installs the Active Directory Certificate Services Web Enrollment role service:

```
Install-WindowsFeature adcs-web-enrollment -IncludeManagementTools
```

The role and feature installation experience is consistent on Windows Server 2012 R2 using the Server Manager module for Windows PowerShell. You can use the same syntax to install a feature or role listed using `Get-WindowsFeature`.

Configuring Active Directory Certificate Services

You begin the Active Directory Certificate Services deployment by starting the AD CS Configuration Wizard (Exercise 22.2). To start the wizard, click the Configure Active Directory Certificate Services On The Destination Server link shown in the Action Flag dialog. The wizard shows the current destination for the role deployment in the Destination Server portion of the screen.

EXERCISE 22.2

Configuring AD CS Through Server Manager

1. After the AD CS installation is successful, click the Configure Active Directory Certificate Services On The Destination Server link.

2. The Credentials screen of the AD CS Configuration Wizard displays the required credentials to perform specific AD CS role services deployment. The wizard shows your current credentials in the Credentials portion of the screen. Click Change if your current credentials do not match the credentials needed for the current role service deployment. Otherwise, continue by clicking Next.
3. Select the check boxes for the Certification Authority and Online Responder role services.
4. The Setup Type screen of the AD CS Configuration Wizard shows the two types of certificate authorities you can configure with Active Directory Certificate Services: enterprise or stand-alone. An enterprise certificate authority must run on domain-joined computers and typically remains online to issue certificates or certificate policies. Select Enterprise and click Next.
5. In the Setup Type dialog box, select Enterprise CA and click Next.
6. In the CA Type dialog box, click Root CA and click Next.
7. In the Private Key dialog box, verify that Create A New Private Key is selected and click Next.
8. Select the RSA# Microsoft Software Key Storage Provider.
9. Windows Server 2012 includes a number of CSPs and KSPs, and you can install additional CSPs or KSPs provided by third parties. In Windows Server 2012 R2, the provider

EXERCISE 22.2 *(continued)*

list includes the name of the algorithm. All providers with a number sign (#) in the name are CNG providers. CNG providers can support multiple asymmetric algorithms. CSPs implement only a single algorithm.

10. Select a key length of 2048.
11. Each CSP and KSP supports different character lengths for cryptographic keys. Configuring a longer key length can enhance security by making it more difficult for a hacker or disgruntled employee to decrypt the key, but it can also slow down the performance of cryptographic operations.
12. Select the SHA1 hash algorithm and click Next.
13. Enter a name for the root CA Server and click Next.
14. In the Certificate Request dialog box, verify that Save A Certificate Request To File On The Target Machine is selected and click Next.
15. In the CA Database dialog box, verify the location for the log files in the Certificate Database Log Location box and click Next.
16. In the Confirmation dialog box, click Configure.
17. In the Results dialog box, click Close.

The CA uses hash algorithms to sign CA certificates and issues certificates to ensure that an external identity has not tampered with a certificate. Each CSP can support different hash algorithms. Make sure your applications, devices, and all operating systems that may request certificates from this certificate authority support the selected hash algorithm.

Use the Create A New Private Key option when creating or reinstalling a certificate authority.

Certificate Authority Name

Names for CAs cannot exceed 64 characters in length. You can create a name by using any Unicode character, but you might want the ANSI character set if interoperability is a concern.

In Active Directory Domain Services (AD DS), the name you specify when you configure a server as a CA (Figure 22.3) becomes the common name of the CA, and this name is reflected in every certificate the CA issues. Because of this behavior, it is important that you do not use the fully qualified domain name (FQDN) for the common name of the CA. Hackers can acquire a copy of a certificate and use the FQDN of the CA to compromise security.

FIGURE 22.3 Specifying the name of the CA

The CA name does not have to be the computer's name. Changing the name after installing Active Directory Certificate Services (AD CS) will invalidate every certificate issued by the CA.

Group Policy Certificate Auto-enrollment

Many certificates can be distributed without the client interaction. These can include most types of certificates issued to computers and services, as well as many certificates issued to users.

To enroll clients automatically for certificates in a domain environment, you must do the following:

- Configure a certificate template with auto-enroll permissions
- Configure an auto-enrollment policy for the domain

Membership in Domain Admins or Enterprise Admins, or equivalent, is the minimum required to complete this procedure. In Exercise 22.3 we are going to configure a group policy to support the auto-enrollment feature.

EXERCISE 22.3

Configure an Auto-enrollment Group Policy for a Domain

1. On a domain controller running Windows Server 2008 R2 or Windows Server 2008, click Start ➢ Administrative Tools ➢ Group Policy Management.
2. In the console tree, double-click Group Policy Objects in the forest and domain containing the Default Domain Policy Group Policy object (GPO) that you want to edit.
3. Right-click the Default Domain Policy GPO and click Edit.
4. In the Group Policy Management Console (GPMC), go to User Configuration ➢ Windows Settings ➢ Security Settings and click Public Key Policies.
5. Double-click Certificate Services Client – Auto-Enrollment.
6. Select the Enroll Certificates Automatically check box to enable auto-enrollment. If you want to block auto-enrollment from occurring, select the Do Not Enroll Certificates Automatically check box.
7. If you are enabling certificate auto-enrollment, you can select the following check boxes:

   "Renew expired certificates, update pending certificates, and remove revoked certificates enables auto-enrollment for certificate renewal, issuance of pending certificate requests, and the automatic removal of revoked certificates from a user's certificate store."

   "Update certificates that use certificate templates enables auto-enrollment for issuance of certificates that supersede issued certificates."
8. Click OK to accept your changes.

Key-Based Renewal for Non-Domain-Joined Computers

Windows Server 2012 R2 combines automatic certificate renewal with AD CS Certificate Enrollment Web Services to enable non-domain-joined computers to renew their certificates automatically before they expire like Internet-facing web servers.

Many organizations and service providers maintain servers that require SSL certificates. These servers are not typically joined to the same domain as an issuing certificate authority, and they do not have identity records or accounts in the organization's Active Directory. This means they cannot benefit from today's automatic certificate renewal, which is based on secured certificate templates in Active Directory. As a result, these organizations manage and renew SSL certificates manually, a time-intensive and error-prone process. Neglecting to renew a single SSL certificate can cause a massive and costly system outage.

Currently, Certificate Enrollment Web Services supports three types of server-side authentication modes:

- Windows integrated (Kerberos)
- Certificate-based
- Username and password

These authentication mode options, however, are not viable choices when the client is not joined to a domain and the enterprise certificate authority makes authorization decisions using templates that are based on the Active Directory group membership of the requestor.

Consider the following authentication options for automatic renewal:

Windows Integrated This authentication option is not suitable for auto renewal because the two domains to which the certificate authority and the requesting server belong do not have a trust relationship between them or the requesting server is not joined to any domain.

Certificate-Based The initially enrolled server certificate is not suitable for authentication because it contains no identity information within it that can be mapped to a directory account object.

Username And Password Usernames and passwords can be cached within the system's identity vault and used for authentication to the enrollment server. However, passwords usually have shorter lifetimes than server SSL certificates. (Both default and recommended settings for passwords are shorter than the default and recommended certificate lifetime.) Thus, by the time renewal happens, the password will likely have changed.

Anonymous This authentication option is not suitable since MS CEP and CES do not support this option, making automatic renewal impossible for these targeted server systems.

Enforcement of Certificate Renewal with Same Key

Windows 8/8.1 and Windows Server 2012 R2 provide an efficient mechanism to increase the security of renewing hardware-based certificates. This is accomplished by enforcing the certificate renewal to occur for the same key. This guarantees the same assurance level for the key throughout its life cycle. Additionally, Windows Server 2012 R2's Certificate

Template Management Console supports CSP/KSP ordering that clients may choose for generating a private/public key pair. This way, you can give a higher priority to hardware-based keys (Trusted Platform Module or smart card) over software-based keys.

Cryptographic Service Provider/Key Service Provider Ordering

Another problem addressed in Windows Server 2012 R2 is GUI support for CSP/KSP ordering. With increased interest in the deployment of Trusted Platform Module in enterprise scenarios, providing a mechanism for prioritizing TPM-based keys over other types of keys has become a "must-have" for certificate enrollment based on certificate templates. This is important from the client perspective when enrolling for a non-exportable key. You want to have assurance that the non-exportable keys are generated in the TPM and are not software-based (assuming that no malware is involved and the user is not malicious).

Currently this prioritization is captured as an attribute of a certificate template object in Active Directory; however, a user interface does not exist for modifying such properties, and Microsoft does not support it. Windows Server 2012 R2's Certificate Template Management Console fully supports CSP/KSP ordering.

Managing Certificate Authority: Certificate Templates Overview

Enterprise certificate authorities issue certificates from certificate templates, a preconfigured list of certificate settings. This allows administrators to enroll users and computers for certificates without the need to create complex certificate requests. Windows Server 2012 AD CS does include a minor user interface change and the Active Directory Certificate Services Administration module for Windows PowerShell. The new Compatibility tab in the Certificate Templates Management Console lets you identify incompatible certificate template settings between different versions of Windows-based certificate recipients and the certificate authority. The AD CS Administration module for Windows PowerShell lets you manage common AD CS management tasks using Windows PowerShell.

Certificate Template Compatibility

Multiple versions of certificate templates have been released for the family of Windows Server products. New certificate template versions include settings that control the features relevant to each new certificate authority. However, not all features are compatible with all certificate authorities and certificate requests. Therefore, it can be difficult to determine which certificate templates are compatible with different versions of certificate authorities and different Windows-based certificate requestors.

Version 2 certificate templates are customizable certificate templates that are supported with Windows Server 2008 Enterprise CAs or Windows Server 2003 Enterprise edition CAs. Version 2 certificate templates enable advanced CA features, such as key archiving and recovery and certificate auto-enrollment.

To use version 2 templates, Active Directory must be upgraded to support Windows Server 2008 or Windows Server 2003 schema changes. Standard editions of Windows Server 2008 and Windows Server 2003 support only version 1 certificate templates, which are not customizable and do not support key archival or automatic enrollment.

Version 3 certificate templates were new to Windows Server 2008. Version 3 certificate templates function similarly to version 2 templates, and they support new Active Directory Certificate Services features available in Windows Server 2008. These features include CNG, which introduces support for Suite B cryptographic algorithms such as elliptic curve cryptography (ECC).

The Windows Server 2012 R2 Certificate Template Management Console includes a new certificate template Compatibility tab that lets you select the Windows operating system of the certificate authority and the Windows operating system of the certificate recipient. The Certificate Template Management Console determines incompatible settings between the selections and shows a list of template settings that the management console adds or removes from template selection.

You view the compatibility table from the Certificate Template Management Console. You can launch the Certificate Template Management Console by typing **`certtmpl.msc`** in the Run dialog or on the Start screen and pressing Enter.

Creating Certificate Templates

When creating a new certificate template, you copy an existing template similar to the configuration defaults needed for your particular application. It is best to review the default list of certificate template and find the template that best matches your application's requirements.

The Request Handling tab (Figure 22.4) in the Certificate Templates Management console has the Renew With Same Key Certificate Template Configuration option. This certificate template option becomes visible in the user interface when you configure the Certification Authority and the Certificate Recipient options to Windows Server 2012 R2 and Windows 8/8.1, respectively.

You will create an example certificate template in Exercise 22.4.

EXERCISE 22.4

Creating a Certificate Template

1. Start the Certificate Templates snap-in, read through the certificate templates titles, and choose the Computer Template.
2. In the details pane, right-click an existing certificate and click Duplicate Template.
3. Choose to duplicate the template as a Windows Server 2008–based template.
4. On the General tab, enter the template display name and the template name and click OK.
5. Define any additional attributes for the newly created certificate template.

FIGURE 22.4 Request Handling tab of the Certificate Templates Management console

Publishing the Certificate Template

After creating a certificate template and applying the proper security permissions, you will want to deploy the new certificate template by publishing to the Active Directory where it can be shared with other Enterprise CAs. The following exercise will take us through the steps to perform the task.

In Exercise 22.5, you will deploy a certificate template.

EXERCISE 22.5

Publishing a Certificate Template

1. In Server manager, click Tools and then Certification Authority
2. In the Certification Authority MMC, expand the CA Server Name
3. Select the Certificate Templates container.
4. Right-click Certificate Templates container and then click New Certificate Template To Issue.
5. In the Enable Certificate Templates dialog box, select the certificate template or templates that you want the CA server to issue and click OK. The newly selected certificate template or templates should appear in the right side details pane.

If a certificate template is not displayed in the Enable Certificate Templates dialog box, the replication of the certificate template may not have finished on all domain controllers in the forest.

Certificate Revocation

Revocation renders a certificate invalid and lists the revoked certificate in the CRL. You can revoke a certificate in the Certificate Authority snap-in with the steps shown in Exercise 22.6.

EXERCISE 22.6

Revoking a Certificate

1. Start the Certification Authority snap-in.
2. In the console tree, click the Issuing certificate container.
3. In the right pane, select and right-click the target certificate.
4. Select All Tasks.
5. Select Revoke Certificate.
6. In Certificate Revocation dialog box, you must select one of the following reason codes:

   Unspecified: Default reason code. This lacks information during future audits.
   Key Compromise: Select this when you think the key has been compromised.
   CA Compromise: Select this when you suspect the issuing CA of being compromised.
   Change of Affiliation: Select this when the person has exited the organization or changed roles.
   Superseded: Select this when issuing a new certificate to replace an existing certificate.
   Cease of Operation: Select this when the issuing device or server has been decommissioned.
   Certificate Hold: Select this to suspend an existing certificate temporarily.
7. Click OK.

Display the Current Site Name for Certificate Authorities

Enter the following command to display current site names for one or more certificate authorities:

```
Certutil -ping caDnsName, [caDnsName, …]
```

The command utilizes the `DsGetSiteName` API on each named certificate authority. After determining the site for all the certificate authorities, `certutil.exe` uses the `DsQuerySitesByCost` API to obtain the client's site costs for all the name certificate authorities.

CA Policy Auditing

PKI auditing logging is not enabled on the Windows 2012 R2 CA server by default. After the auditing is enabled, all the events will be logged in the Security log.

Exercise 22.7 covers the steps that the CA administrator must complete to enable auditing.

EXERCISE 22.7

Configuring CA Policy Auditing

1. Enable Object Access/Success Auditing in the CA machine's local security policy.
   a. Start `mmc.exe`.
   b. Add the snap-in Group Policy Object Editor and select the Local Computer GPO.
   c. Under the path `Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy`, enable success auditing for Object Access.
2. Enable auditing on the CA.
   a. Start the CA Management snap-in.
   b. Open the CA Properties dialog.
   c. On the Auditing tab, check the Change CA Configuration and Change CA Security Settings options.

Backing Up the Certificate Authority Server

The AD CS certificate authority deployment creates a database. The CA records certificates issued by the CA, private keys archived by the CA, revoked certificates, and all certificate requests to the database regardless of issuance status.

Configure the database location on an NTFS partition on the server's disk drives to provide the best security possible for the database file. Specify the location for the database in the Certificate Database Location box. By default, the wizard configured the database location to `systemroot\system32\certlog`. The name of the database file uses the CA's name, with an `.edb` extension.

The certificate database uses a transaction log to ensure the integrity of the database. The CA records its transactions in its configured log files. The CA then commits each transaction from the log file into the database. The CA then updates the last committed transaction in the database, and the process continues.

The CA database logs are selected when restoring the CA from a backup. If a CA is restored from a backup that is one month old, then the CA database can be updated with more recent activity recorded in the log to restore the database to its most current state. When you back up a CA, the existing certificate database logs are truncated in size because they are no longer needed to restore the certificate database to its most current state.

The recommended method to back up a CA is to leverage the native Backup utility (included with the operating system) to back up the entire server, including the system state, which contains the CA's data. However, the Certificate Authority snap-in can be used to back up and restore the CA, but this backup method is intended only in cases where you want to migrate CA data to different server hardware. The public key and private key are backed up or restored using the PKCS #12 PFX format.

The Backup Or Restore Wizard will ask you to supply a password when backing up the public and private keys and CA certificates. This password will be needed to restore the CA.

Start the Certificate Authority snap-in for Exercise 22.8, which explains how to back up a CA.

EXERCISE 22.8

Backing Up the Certificate Authority Server

1. Start the Certification Authority MMC.
2. In the left pane, right-click the name of the server; then choose All Tasks > Back Up CA.
3. When the Certification Authority Backup Wizard appears, click Next.
4. At the Items To Back Up screen, click the Private Key And CA Certificate check box. Next to the Back Up To This Location field, click the Browse button. Choose a location for your backup and click OK. Click Next.
5. At the Select A Password screen, enter and confirm a password. For this exercise, enter `P@ssw0rd`. Click Next.

Configuring and Managing Key Archive and Recovery

The key archive stores a certificate's subject name, public key, private key, and supported cryptographic algorithms in its CA database. This procedure can be performed manually or automatically, depending on the configuration. If the certificate template requires key archiving, then the process requires no manual intervention. However, key archiving can also be performed manually if the private key is exported and then sent to an administrator for import into the CA database.

There is also a Key Recovery Agent template available in the standard templates within Active Directory Certificate Services. The Key Recovery Agent template enables Domain Admins and Enterprise Admins to export private keys. Additionally, you can add other accounts and groups to have the necessary permissions (Read and Enroll) through the Security tab of the template.

The Key Recovery Agent template also needs to be enabled, as with other certificate templates, through the Certification Authority tool by selecting Certificate Template To Issue. See "Publishing a Certificate Template" earlier in this chapter for more details on enabling a certificate template on a CA.

With the Key Recovery Agent template in place, the following process must take place for key archiving and recovery:

1. Request a key recovery agent certificate using the Certificates snap-in.
2. Issue the key recovery agent certificate using the Certification Authority tool.
3. Retrieve the enrolled certificate using the Certificates snap-in.
4. Configure the CA for key archiving and recovery.

The final step, configuring the CA for key archiving and recovery, takes place in the Properties dialog box of each CA that will need to archive and recover keys. Specifically, the Recovery Agents tab configures the behavior of the CA when a request includes key archiving.

Each Key Recovery Agent certificate should be added using the Add button on the Recovery Agents tab.

Implement Active Directory Federation Services

Active Directory Federation Services (AD FS) demands a great deal of preparation and planning to ensure a successful implementation. The type of certificate authority used to sign the AD FS server's certificate must be planned. The SSL encryption level must be negotiated with the partnering organization. For instance, how much Active Directory information should be shared with the partnering organization? What should the DNS structure look like to support federation communications? You must explore all of these questions before implementing AD FS. In this section, I will discuss how to deploy AD FS and the configurations used to set up a federated partnership between businesses.

What Is a Claim?

A *claim* is an identifiable element (email address, username, password, and so on) that a trusted source asserts about an identity, for example, the SID of a user or computer. An identity can contain more than one claim, and any combination of those claims can be used to authorize access to resources.

Windows Server 2012 R2 extends the authorization identity beyond using the SID for identity and enables administrators to configure authorization based on claims published in Active Directory.

Today, the claims-based identity model brings us to cloud-based authentication. One analogy to the claim-based model is the old airport check-in procedure.

1. You first check in at the ticket counter.
2. You present a suitable form of ID (driver's license, passport, credit card, and so on). After verifying that your picture ID matches your face (authentication), the agent pulls up your flight information and verifies that you've paid for a ticket (authorization).
3. You receive a boarding pass (token). The boarding pass lets the gate agents know your name and frequent flyer number (authentication and personalization), your flight number and seating priority (authorization), and more. The boarding pass has bar-code information (certificate) with a boarding serial number proving that the boarding pass was issued by the airline and not a (self-signed) forgery.

Active Directory Federation Service is Microsoft's claims-based identity solution providing browser-based clients (internal or external to your network) with transparent access to one or more protected Internet-facing applications.

When an application is hosted in a different network than the user accounts, users are occasionally prompted for secondary credentials when they attempt to access the application. These secondary credentials represent the identity of the users in the domain where the application is hosted. The web server hosting the application usually requires these credentials to make the most proper authorization decision.

AD FS makes secondary accounts and their credentials unnecessary by providing trust relationships that send a user's digital identity and access rights to trusted partners. In a federated environment, each organization continues to manage its own identities, but each organization can also securely send and accept identities from other organizations. This seamless process is referred to as *single sign-on (SSO)*.

Windows Server 2012 R2 AD FS federation servers can extract Windows authorization claims from a user's authorization token that is created when the user authenticates to the AD FS federation server. AD FS inserts these claims into its claim pipeline for processing. You can configure Windows authorization claims to pass through the pipeline as is, or you can configure AD FS to transform Windows authorization claims into a different or well-known claim type.

Claims Provider

A *claims provider* is a federation server that processes trusted identity claims requests. A federation server processes requests to issue, manage, and validate security tokens. Security tokens consist of a collection of identity claims, such as a user's name or role or an anonymous identifier. A federation server can issue tokens in several formats. In addition, a federation server can protect the contents of security tokens in transmission with an X.509 certificate.

For example, when a Stellacon Corporation user needs access to Fabrikam's web application, the Stellacon Corporation user must request claims from the Stellacon Corporation AD FS server claim provider. The claim is transformed into an encrypted security token, which is then sent to Fabrikam's AD FS server.

Relying Party

A *relying party* is a federation server that receives security tokens from a trusted federation partner claims provider. In turn, the relying party issues new security tokens that a local relying party application consumes. In the prior example, Fabrikam is the relying party that relies on the Stellacon's claim provider to validate the user's claim. By using a relying-party federation server in conjunction with a claims provider, organizations can offer web single sign-on to users from partner organizations. In this scenario, each organization manages its own identity stores.

Endpoints

Endpoints provide access to the federation server functionality of AD FS, such as token issuance, information card issuance, and the publishing of federation metadata. Based on the type of endpoint, you can enable or disable the endpoint or control whether the endpoint is published to AD FS proxies.

Table 22.3 describes the property fields that distinguish the various built-in endpoints that AD FS exposes. The table includes the types of endpoints and their methods of client authentication. Table 22.4 describes the AD FS security modes.

TABLE 22.3 AD FS Endpoints

Name	Description
WS-Trust 1.3	An endpoint built on a standard Simple Object Access Protocol (SOAP)–based protocol for issuing security tokens.
WS-Trust 2005	An endpoint built on a prestandard, SOAP-based protocol for issuing security tokens.
WS-Federation Passive/ SAML Web SSO	An endpoint published to support protocols that redirect web browser clients to issue security tokens.
Federation Metadata	A standard-formatted endpoint for exchanging metadata about a claims provider or a relying party.
SAML Artifact Resolution	An endpoint built on a subset of the Security Assertion Markup Language (SAML) version 2.0 protocol that describes how a relying party can access a token directly from a claims provider.
WS-Trust WSDL	An endpoint that publishes WS-Trust Web Services Definition Language (WSDL) containing the metadata that the federation service must be able to accept from other federation servers.
SAML Token (Asymmetric)	The client accepts a SAML token with an asymmetric key.

TABLE 22.4 AD FS Security Modes

Name	Description
Transport	The client credentials are included at the transport layer. Confidentiality is preserved at the transport layer (Secure Sockets Layer [SSL]).
Mixed	The client credentials are included in the header of a SOAP message. Confidentiality is preserved at the transport layer (SSL).
Message	The client credentials are included in the header of a SOAP message. Confidentiality is preserved by encryption inside the SOAP message.

Claim Descriptions

Claim descriptions are claim types based on an entity's or user's attribute like a user's email address, common name or UPN. AD FS publishes these claims types in the federation metadata and most common claim descriptions are pre-configured in the AD FS Management snap-in.

The claim descriptions are published to federation metadata which is stored in the AD FS configuration database. The claim descriptions include a claim type URI, name, publishing state, and description.

Claim Rules

Claim rules define how AD FS processes a claim. The most common rule is using a user's email address as a valid claim. The email address claim is validated through the partner's Active Directory email attribute for the user's account. If there is a match, the claim is accepted as valid.

Claim rules can quickly evolve into more complex rules with more attributes such as a user's employee ID or department. The key goal of claim rules is to process the claim in a manner that validates the user's claim and to assemble a user's profile information based on a sufficient number of attributes to place the user into a role or group.

The Attribute Store

Attribute stores are the repositories containing claim values. AD FS natively supports Active Directory by default as an attribute store. SQL Server, AD LDS, and custom attribute stores are also supported.

AD FS Role Services

The AD FS server role includes federation, proxy, and web agent services. These services enable the following:

- Web SSO
- Federated web-based resources

- Customizing the access experience
- Managing authorization to access applications

Based on your organization's requirements, you can deploy servers running any one of the following AD FS role services:

Active Directory Federation Service Microsoft federation solution for accepting and issuing claims based token for users to experience a single sign-on to a partnered web application.

Federation Service Proxy The Federation Service Proxy forwards user claims over the internet or DMZ using WS-Federation Passive Requestor Profile (WS-F PRP) protocols to the internal ADFS farm. Only the user credential data is forwarded to the Federation Service. All other datagram packets are dropped.

Claims-Aware Agent The claims-aware agent resides on a web server with a claims-aware application to enable the Microsoft ASP.NET application to accept AD FS security token claims.

Windows Token-Based Agent The Windows token-based agent resides on a web server with a Windows NT token-based application to translate an AD FS security token to an impersonation-level Windows NT token-based authentication.

What's New for AD FS in Windows Server 2012 R2?

The Active Directory Federation Services role in Windows Server 2012 R2 introduces the following new features:

- HTTP.SYS
- Server Manager integration
- AD FS deployment cmdlets in the AD FS module for Windows PowerShell
- Interoperability with Windows authorization claims
- Web proxy service

HTTP.SYS

Prior AD FS versions relied on IIS components for the AD FS claim functions. Microsoft has improved the overall claims handling performance and SSO customization by building the AD FS 3.0 code on top of the standard kernel mode driver—HTTP.SYS. This approach also avoids the huge security "no-no" of hosting IIS on a domain controller.

The classic `netsh` HTTP command can be entered to query and configure HTTP.SYS. AD FS proxy server introduces interesting deployment nuisances and "gotchas" with HTTP.SYS, which I will discuss in the "Web Proxy Service" section.

Improved Installation Experience

The installation experience for Active Directory Federation Services 3.0 was cumbersome, requiring multiple hotfixes, as well as .NET Framework 3.5, Windows PowerShell, and the

Windows Identity Foundation SDK. Windows Server 2012 R2's AD FS role includes all of the software you need to run AD FS for an improved installation experience.

Web Proxy Service

The kernel mode (HTTP.SYS) in Windows Server 2012 R2 includes server name indication (SNI) support configuration. I strongly recommend verifying that your current load balancer/reverse proxy firmware supports SNI. This prerequisite is a sore spot for most AD FS 3.0 upgrade projects in the field. Therefore, it's worthwhile checking the following:

- Your preferred load balancer/device needs to support SNI.
- Clients and user agents need to support SNI and should not become locked out of authentication.
- All SSL termination endpoints vulnerable to the recent heartbleed bug (`http://heartbleed.com`) need to be patched, exposing OpenSSL libraries and certificates.

AD FS Dependency Changes in Windows Server 2012 R2

Active Directory Federation Services was built on a claim-based identity framework called *Windows Identity Foundation (WIF)*. Prior to Windows Server 2012 R2, WIF was distributed in a software development kit and the .NET runtime. WIF is currently integrated into version 4.5 of the .NET Framework, which ships with Windows Server 2012 R2.

Windows Identity Foundation

WIF is a set of .NET Framework classes; it is a framework for implementing claims-based identity for applications. Any web application or web service that uses .NET Framework version 4.5 or newer can run WIF.

New Claims Model and Principal Object

Claims are at the core of .NET Framework 4.5. The base claim classes (`Claim`, `ClaimsIdentity`, `ClaimsPrincipal`, `ClaimTypes`, and `ClaimValueTypes`) all live directly in `mscorlib`. Interfaces are no longer necessary to plug claims in the .NET identity system. `WindowsPrincipal`, `GenericPrincipal`, and `RolePrincipal` now inherit from `ClaimsPrincipal`, `WindowsIdentity`, and `GenericIdentity`, and `FormsIdentity` now inherit from `ClaimsIdentity`. In short, every principal class will now serve claims. The integration classes and interfaces (`WindowsClaimsIdentity`, `WindowsClaimsPrincipal`, `IClaimsPrincipal`, and `IClaimsIdentity`) have thus been removed. The `ClaimsIdentity` object model also contains various improvements, which makes it easier to query the identity's claims collection.

As you climb further up "Mount Federation," you will realize that not all vendor SAML flavors are compatible, and configuration challenges can bring even the most seasoned system integrators to their knees. SAML deserves an entire book, so to avoid this chapter reaching encyclopedia size, I will touch on just a few pointers.

AD FS negotiates SAML authentication in order of security strength from the weakest to the strongest, as shown in Table 22.5. The default mode, Kerberos, is considered the strongest method. The authentication precedence can be tuned by executing the PowerShell command `Set-AD FSProperties -AuthenticationContextOrder` to select an order to meet your organization's security requirements.

TABLE 22.5 SAML-supported authentication methods

Authentication method	Authentication context class URI
Username/password	`urn:oasis:names:tc:SAML:3.0:ac:classes:Password`
Password-protected transport	`urn:oasis:names:tc:SAML:3.0:ac:classes:PasswordProtectedTransport`
Transport Layer Security (TLS) Client	`urn:oasis:names:tc:SAML:3.0:ac:classes:TLSClient`
X.509 certificate	`urn:oasis:names:tc:SAML:3.0:ac:classes:X509`
Integrated Windows authentication	`urn:federation:authentication:windows`
Kerberos	`urn:oasis:names:tc:SAML:3.0:classes:Kerberos`

Active Directory Federation Services Installation

This section describes how to install and deploy Active Directory Federation Services roles on computers running Windows Server 2012 R2 (see Exercise 22.9). You will learn about the following:

- Deploying AD FS role services using Windows PowerShell
- Supporting upgrade scenarios for AD FS

EXERCISE 22.9

Installing the AD FS Role on a Computer Using Server Manager

1. Start Server Manager.
2. Click Manage and click Add Roles And Features. Click Next.
3. The Add Roles And Features Wizard shows the Before You Begin screen. Click Next.
4. Click Role-Based Or Feature-Based Installation on the Select Installation Type screen. Click Next.

5. Click the server on which you want to install Active Directory Federation Services from the Server Pool list on the Select Destination Server screen. Click Next.
6. Select the Active Directory Federation Services check box on the Select Server Roles screen. Server Manager will prompt you to add other features associated with this role, such as management tools. Leave the default selections. Click Add Features to close the dialog.
7. Click Next on the Select Server Roles screen.
8. Click Next on the Select Features screen.
9. Server Manager shows the Active Directory Federation Services screen. This screen displays simple role introduction and important AD FS configuration information. Click Next.
10. From the Select Server Roles screen, select the check box next to the AD FS role services to install on the computer. Click Next.

11. Server Manager prompts you to add other features associated with this role, such as management tools. Leave the default selections. Click Add Features to close the dialog.
12. Read the Confirm Installation Selections screen. This screen provides a list of roles, role services, and features that the current installation prepares on the computer. Click Install to begin the installation.

Role Installation Using Windows PowerShell

To view the installation state of AD FS using Windows PowerShell, open an elevated Windows PowerShell console, type the following command, and press Enter:

```
Get-WindowsFeature "adfs*","*fed*"
```

Upgrading to Windows AD FS 2012 R2

Windows Server 2012 R2's AD FS role supports upgrading version 3.0 of Active Directory Federation Services. You cannot upgrade versions of AD FS prior to version 3.0 using Windows Server 2012 R2.

Table 22.6 represents the support upgrade matrix for the AD FS role in Windows Server 2012 R2.

TABLE 22.6 Support upgrade matrix for the AD FS role in Windows Server 2012 R2

AD FS and operating system version	Windows Server 2012 R2 upgrade supported
AD FS 3.0 running on Windows Server 2008	Yes
AD FS 3.0 running on Windows Server 2008 R2	Yes
AD FS 3.0 Proxy running on Windows Server 2008	Yes
AD FS 3.0 Proxy running on Windows Server 2008 R2	Yes
AD FS 1.1 running on Windows Server 2008	No
AD FS 1.1 running on Windows Server 2008 R2	No
AD FS 1.1 Proxy running on Windows Server 2008	No
AD FS 1.1 Proxy running on Windows Server 2008 R2	No
AD FS 1.1 Web Agents on Windows Server 2008 or Windows Server 2008 R2	Yes

Configuring Active Directory Federation Services

Windows Server 2012 R2 delineates role installation and role deployment. Role installations make staged role services and features available for deployment. Role deployment enables you to configure the role service, which enables the role service in your environment. AD FS in Windows Server 2012 R2 uses the same deployment tools as AD FS 3.0. However, an entry point to start these tools is included in Server Manager. Server Manager indicates that one or more role services are eligible for deployment by showing an exclamation point inside a yellow triangle on the Action Flag notification. Click the action flag to show the role services you can deploy (see Figure 22.5).

FIGURE 22.5 Alert for role services eligible for deployment in Server Manager

AD FS Graphical Deployment

The Run The AD FS Management snap-in link in Windows Server 2012 R2 Server Manager is how you perform the initial configuration for the AD FS roles using the graphical interface. Alternatively, you can start the AD FS management console using the AD FS Management tile on the Start screen. The Start screen tile points to the `Microsoft.IdentityServer.msc` file located in the `c:\windows\adfs` folder.

To configure AD FS, select Start ➢ Run and type **`FsConfigWizard.exe`**; alternatively, click the `FsConfigWizard.exe` file located in the `c:\windows\adfs` folder.

Exercise 22.10 uses the AD FS Federation Server Configuration Wizard. To complete this exercise, you'll need an active SSL certificate assigned to the server and a managed service account for AD FS service.

EXERCISE 22.10

Configuring the AD FS Role on the Computer Using Server Manager

1. Select Create The First Federation Server In The Federation Server Farm.
2. Select the administrative account with permissions to configure the AD FS server and click Next.
3. Select the server certificate from the SSL certificate drop-down list.
4. Select the AD FS service name from the drop-down list.
5. Type **`ADFS-Test`** in the federation service's Display Name field and click Next.
6. Select Create A Database On This Server Using Windows Internal Database and click Next.

EXERCISE 22.10 *(continued)*

7. Click Next on the Review Options screen.
8. If the prerequisites check is successful, click Configure on the Prerequisite Check screen.
9. If the Result screen displays "This Server was successfully configured," you can click Close.

Deployment Using Windows PowerShell

Windows Server 2012 R2 includes the Active Directory Federation Services module for Windows PowerShell when you install the AD FS role using Server Manager. The AD FS module for Windows PowerShell includes five new cmdlets to deploy the AD FS role.

- `Add-AdfsProxy`
- `Add-AdfsFarmNode`
- `Export-AdfsDeploymentSQLScript`
- `Install-AdfsStand-alone`
- `Install-AdfsFarm`

These AD FS cmdlets provide the same functionality as the command-line version of the AD FS Federation Server Configuration Wizard, `fsconfig.exe`. The AD FS role in Windows Server 2012 R2 includes `fsconfig.exe` to remain compatible with previously authored deployment scripts. New deployments should take advantage of the deployment cmdlets included in the AD FS module for Windows PowerShell.

Add-AdfsProxy Configures a server as a federation server proxy.

FederationServiceName Specifies the name of the federation service for which a server proxies requests.

FederationServiceTrustCredentials Specifies the credentials of the Active Directory identity that is authorized to register new federation server proxies. By default, this is the account under which the federation service runs or an account that is a member of the Administrators group on the federation server.

ForwardProxy Specifies the DNS name and port of an HTTP proxy that this federation server proxy uses to obtain access to the federation service.

Add-AdfsFarmNode Adds this computer to an existing federation server farm.

CertificateThumbprint Specifies the value of the certificate thumbprint of the certificate that should be used in the SSL binding of the default website in IIS. This value should match the thumbprint of a valid certificate in the Local Computer certificate store.

OverwriteConfiguration Must be used to remove an existing AD FS configuration database and overwrite it with a new database.

SQLConnectionString Specifies the SQL Server database that will store the AD FS configuration settings. If not specified, AD FS uses Windows Internal Database to store configuration settings.

ServiceAccountCredential Specifies the Active Directory account under which the AD FS service runs. All nodes in the farm must have the same service account.

PrimaryComputerName Specifies the name of the primary federation server in the farm that this computer will join.

PrimaryComputerPort Specifies the value of the HTTP port that this computer uses to connect with the primary computer in order to synchronize configuration settings. Specify a value for this parameter only if the HTTP port on the primary computer is not 80.

Active Directory Federation Services Certificates

There are three types of certificates used by an AD FS implementation:

- Service communications
- Token decrypting
- Token signing

The service communications certificate is required for communication with web clients over SSL and with web application proxy services using Windows Communication Foundation (WCF) components. This certificate is specified at configuration time for AD FS.

The token decrypting certificate is required to decrypt claims and tokens received by the federation service. The public key for the decrypting certificate is usually shared with relying parties and others to encrypt the claims and tokens using the certificate.

The token signing certificate is required to sign all claims and tokens created by the server. You can have multiple token encrypting and signing certificates for an implementation, and new ones can be added within the AD FS management tool, shown in Figure 22.6.

FIGURE 22.6 Active Directory Federation Certificate Console screen

Relying-Party Trust

The federation service name originates from the SSL certificate used for AD FS. The SSL certificate can be template-based and needs to be enrolled and used by IIS.

The next step in setting up AD FS is to configure a relying-party trust. A relying-party trust can be configured with a URL acquired from the relying party. The URL contains the federation metadata used to complete the federation trust configuration. The federation metadata may also be exported to a file that can then be imported into the relying-party trust. There is also a manual option for configuring a relying-party trust.

See Table 22.7 for the Federation Metadata fields.

TABLE 22.7 Federation Metadata Fields

Field	Description
Display Name	This is the friendly display name given to this relying party trust.
Profile	Select AD FS Profile for the standard Windows Server 2012 AD FS, or select AD FS 1.0 And 1.1 Profile for AD FS configurations that need to work with older versions of AD FS.
Certificate	This is the optional certificate file from the relying party for token encryption.
URL	This is the URL for the relying party. WS-Federation Passive Protocol URL or SAML 2.0 WebSSO protocols are supported.
Identifiers	This is the unique identifier used for this trust.
Authorization Rules	Selecting this permits all users to access the relying party or denies all users access to the relying party, depending on the needs of this trust.

Configuring Claims Provider and Transform Claims Rules

Claims provider trust rules are configured within the AD FS management console and are configured on a per-trust basis. Planning claims rules involves determining what claims are needed by the relying party to complete the authentication and authorization process and which users will need access to the relying-party trust. The relying party determines what claims need to be received and trusted from the claims provider.

Trust rules start with templates as the basis for the rule. There are different types of claims templates depending on the type of rule being used. The claims rule templates for transforms are described in Table 22.8.

TABLE 22.8 Transform claims rule templates

Template	Description
Send LDAP Attributes as Claims	Attributes found in an LDAP directory (such as Active Directory) can be used as part of the claim.
Send Group Membership as Claim	The group memberships of the logged-in user are sent as part of the claim.
Transform an Incoming Claim	This is used for configuring a rule to change an incoming claim. Changes include both the type and the value of an incoming claim.
Pass Through or Filter an Incoming Claim	This performs an action such as pass-through or filter on an incoming claim based on certain criteria, as defined in the rule.
Send Claims Using a Custom Rule	This creates a rule that's not covered by a predefined template, such as an LDAP attribute generated with a custom LDAP filter.

Defining Windows Authorization Claims in AD FS

Windows Server 2012 R2 stores information that describes Windows authorization claims in the configuration partition of Active Directory. Windows refers to this information as *claim types*; however, Active Directory Federation Services typically refers to this information as claim descriptions (see Figure 22.7). There are more than 40 new claims descriptions available in the AD FS Windows Server 2012 R2 release.

The Active Directory Federation Services role included in Windows Server 2012 R2 lets you configure AD FS to include Windows authorization claims in the AD FS claim pipeline. To simplify this configuration, you can create *claim descriptions* in AD FS. Claim types in Windows authorization claims are analogous to claim descriptions in AD FS. The Windows authorization claim ID maps to the AD FS claim description's claim identifier (see Figure 22.8).

To simplify AD FS configuration using Windows authorization claims, create a claim description in AD FS for each Windows authorization claim you intend to deploy in AD FS.

Create Claim Pass-Through and Transformation Rules

You need to configure a claim rule with the Active Directory Claims Provider Trusts Wizard to insert Windows authorization claims into the AD FS claims pipeline.

Creating a claim description makes it easier to select the incoming claim type. Alternatively, you can type the claim type ID directly in the Incoming Claim Type list. A *pass-through claim rule* enables the Windows authorization claim to enter the AD FS claim

FIGURE 22.7 AD FS claim descriptions

FIGURE 22.8 Adding a claim description

pipeline. A pass-through claim leaves the claim type ID intact. Therefore, the pass-through claim ID begins with `ad://ext`, whereas most claim description URIs begin with `http://`. In addition, you can create a claim transformation claim rule on the Active Directory Claim Provider Trust Wizard to transform a Windows authorization claim into a well-known claim description (see Figure 22.9).

FIGURE 22.9 Claim transformation claim rule

Creating a claim provider trust claim rule enables the Windows authorization claim to enter the AD FS claim pipeline. However, this does not ensure that AD FS sends the Windows authorization claim. AD FS claim processing begins with the claim provider. This allows the claim to enter the pipeline. Claim processing continues for the targeted relying party—first with the issuance authorization rules and then with the issuance transform rules.

You can configure Windows authorization claims in claims rules configured on a relying party. By default, a relying party does not have any issuance transform rules. Therefore, AD FS drops all claims in the pipeline destined for a relying party when the relying party does not have any rules that pass incoming claims. Additionally, issuance authorization rules determine whether a user can receive claims for a relying party and, therefore, access the relying party.

Choose the claims types from the list of inbound rules created in the Active Directory claim provider trust that you want to send to the designated relying party. Then create rules that continue to pass the selected claim types through the pipeline to the relying party. Alternatively, you can create a rule that passes all the inbound claims to the relying party (see Figure 22.10).

FIGURE 22.10 Editing the claims rules

The AD FS role in Windows Server 2012 R2 cannot provide claim information when the incoming authentication is not Kerberos. Clients must authenticate to AD FS using Kerberos authentication. If Windows authorization claims are not entering the AD FS claim pipeline, then make sure the client authenticates to AD FS using Kerberos and the correct service principal name is registered on the computer/service account.

Enabling AD FS to Use Compound Authentication for Device Claims: Compound Authentication

Windows Server 2012 R2 enhances Kerberos authentication by introducing compound authentication. Compound authentication enables a Kerberos TGS request to include two identities: the identity of the user and the identity of the user's device. Windows accomplishes compound authentication by extending Kerberos Flexible Authentication Secure Tunneling (FAST) or Kerberos armoring.

During normal Kerberos authentication, the Kerberos client requesting authentication for a service sends the ticket-granting service (TGS) a request for that service. Using Kerberos armoring, the TGS exchange is armored using the user's ticket-granting ticket (TGT). Prior to sending the ticket-granting service reply (TGS-REP) to the client, the KDC checks the 0x00020000 bit in the value of the `msDS-SupportedEncryptionTypes` attribute of the security principal's object running the service. An enabled bit means that the service can accept compound authentication. The KDC sends the TGS-REP, which includes the service's ability to support compound authentication.

The Kerberos client receives the ticket-granting service TGS-REP that includes compound authentication information. The Kerberos client then sends another ticket-granting service request (TGS-REQ), with the difference being that this TGS-REQ is armored with the device's TGT rather than the user. This allows the KDC to retrieve authentication information about the principal and the device.

The Active Directory Federation Services role included in Windows Server 2012 R2 automatically enables compound authentication when creating an AD FS web farm. During the creation of the first node in the farm, the AD FS configuration wizard enables the compound authentication bit on the `msDS-SupportedEncryptionTypes` attribute on the account that you designate to run the AD FS service. If you change the service account, then you must manually enable compound authentication by running the `Set-ADUser -compoundIdentitySupported:$true` Windows PowerShell cmdlet.

In Exercise 22.11, you will learn how to configure multifactor authentication.

EXERCISE 22.11

Configuring Multifactor Authentication

1. In the AD FS Management Console, traverse to Trust Relationships And Relying Party Trusts.
2. Select the relying party trust that represents your sample application (claimapp) and then either by using the Actions pane or by right-clicking this relying party trust, select Edit Claim Rules.
3. In the Edit Claim Rules For Claimapp window, select the Issuance Authorization Rules tab and click Add Rule.
4. In the Add Issuance Authorization Claim Rule Wizard, on the Select Rule Template screen, select Permit Or Deny Users Based On An Incoming Claim Rule Template and click Next.

5. On the Configure Rule screen, complete all of the following tasks and click Finish.
   a. Enter a name for the claim rule, for example **`TestRule`**.
   b. Select Group SID As Incoming Claim Type.
   c. Click Browse, type in **`Finance`** for the name of your AD test group, and resolve it for the Incoming Claim Value field.
   d. Select the Deny Access To Users With This Incoming Claim option.
   e. In the Edit Claim Rules For Claimapp window, make sure to delete the Permit Access To All Users rule that was created by default when you created this relying party trust.

Verify Multifactor Access Control Mechanism

In this phase, you will verify the multifactor access control policy that you set up in the previous phase. You can use the following procedure to verify that a test AD user can access your sample application because the test account belongs to the Finance group. Conversely, you will use the procedure to verify that AD users who do not belong to the Finance group cannot access the sample application.

1. On your client computer, open a browser window and navigate to your sample application: `https://webserv1.contoso.com/claimapp`. This action automatically redirects the request to the federation server, and you are prompted to sign in with a username and password.
2. Type in the credentials of a test AD account to be granted access to the application.
3. Type in the credentials of another test AD account that does not belong to the Finance group.

At this point, because of the access control policy that you set up in the previous steps, an access denied message is displayed for an AD account that does not belong to the Finance group. The default message text is "You are not authorized to access this site. Click here to sign out, and sign in again or contact your administrator for permissions." However, this text is fully customizable.

Workplace Join

Today's employees are mobile and remote, working across a plethora of consumer platforms. The age of bring your own device (BYOD) is here to stay. CIOs, IT security workers, and administrators cringe at the idea of storing company data on unmanaged devices. The Workplace Join feature adds a safety measure to ensure that only registered devices have access to company data.

For Workplace Join to work, a certificate is placed on the mobile device. AD FS challenges the device as a claims-based authentication to applications or other resources without requiring administrative control of the device.

Device Registration Service

Workplace Join is supported by the Device Registration Service (DRS) included with the Active Directory Federation Services role in Windows Server 2012 R2. When a device is set up with Workplace Join, the DRS registers a device as an object in Active Directory and sets a certificate on the consumer device that is used to represent the device identity. The DRS is meant to be both internal and external facing.

DRS requires at least one global catalog server in the forest root domain. The global catalog server is needed to run the PowerShell cmdlet `-Initialize-ADDeviceRegistration` during AD FS authentication.

Workplace Join Your Device

For Workplace Join to succeed, the client computer must trust the AD FS SSL certificate. It must also be able to access and validate revocation information for the certificate from the CRL.

In Exercise 22.12, you will configure the DRS.

EXERCISE 22.12

Workplace Joining a Device

1. Start a Windows PowerShell command window and type **`Initialize-ADDevice Registration`**.
2. When prompted for a service account, type **`contoso\fsgmsa$`**. Now run the Windows PowerShell cmdlet.

   ```
   Enable-AdfsDeviceRegistration
   ```

3. On the AD FS server, in the AD FS Management console, navigate to the Authentication Policies tab. Select Edit Global Primary Authentication. Select the Enable Device Authentication check box and click OK.

   Finally, you will need to make sure you have the following DNS records for the DRS.

Entry	Type	Address
adfs1	A	IP address of the AD FS server
enterpriseregistration	Alias (CNAME)	adfs1.contoso.com

4. Log on to the client with your Microsoft account.
5. On the Start screen, start the Charms bar and then select the Settings charm. Select Change PC Settings.
6. On the PC Settings screen, select Network and click Workplace.

7. In the Enter Your UserID To Get Workplace Access Or Turn On Device Management box, type the user's UPN or email address—for example, **`RobertM@contoso.com`**—and click Join.
8. When prompted for credentials, type the user's UPN or email address—for example, **`roberth@contoso.com`**—and a password such as **`P@ssword`**. Click OK.
9. You should now see the message "This device has joined your workplace network."

Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS), included with Microsoft Windows Server 2012 R2, helps safeguard sensitive information created and distributed using AD RMS–enabled applications such as Word, Outlook, or InfoPath, similar to Adobe Acrobat's permissions for print, save, fill-form, and copy functions. Unlike traditional file permission methods, RMS rights stay with the content and ensure exclusive access to the intended recipient.

Application developers may enable their applications to work with RMS extensions. AD RMS uses policies managed from the RMS server to provide a consistent experience for users across the enterprise.

You can enforce AD RMS usage policy templates directly to protect confidential information. You can install AD RMS easily using Server Manager, and you can administer it through the MMC snap-in. These three new administrative roles allow you to delegate AD RMS responsibilities:

- AD RMS Enterprise Administrators
- AD RMS Template Administrators
- AD RMS Auditors

AD RMS integrates with AD FS, which allows two organizations to share information without requiring AD RMS in both organizations.

Self-enrollment AD RMS server enrollment allows for the creation and signing of a server licensor certificate (SLC). This SLC enables the AD RMS server to issue certificates and licenses whenever required.

Considerations and Requirements for AD RMS

Before installing Active Directory Rights Management Services on Windows Server 2012 R2 for the first time, you must meet several requirements:

AD RMS Server Install the AD RMS server as a member server in the same Active Directory domain as the user accounts that will be using rights-protected content.

AD RMS Service Account Create a domain user account that has no additional permissions that can be used as the AD RMS service account. I recommend using a group-managed service account to ensure that the account password is managed by Active Directory and that it does not require a manual password change by an administrator.

If you are registering the AD RMS service connection point during installation, the user account installing AD RMS must be a member of the AD DS Enterprise Admins group or equivalent.

Which database AD RMS Will Store Configuration Data Microsoft SQL Server 2008 or newer and WID are supported databases for the AD RMS configuration data. Windows Internal Database is more suitable for small and/or test environments. If you are using an external SQL database server for the AD RMS databases, the user account installing AD RMS must have the right to create new databases.

AD RMS URL Reserve a URL for the AD RMS cluster that will be available throughout the lifetime of the AD RMS installation. Make sure the reserved URL differs from the computer name.

Cryptographic Mode Mode 1 is composed of RSA 1024-bit keys and SHA-1 hashes. Mode 2 includes RSA 2048-bit keys and SHA-256 hashes for a more secure and recommended option.

Location for Cluster Key Storage By default, the cluster key is stored within AD RMS. You may also deploy a cryptographic service provider to store the cluster key. However, you will have to distribute the key manually when installing additional AD RMS servers.

Cluster Key Password The Cluster Key password helps to encrypt the cluster key, and it must be provided when adding AD RMS servers to the cluster. The Cluster Key password must also be provided when recovering an AD RMS cluster from backup.

Cluster Name Choose the fully qualified domain name to be hosted on the AD RMS server. An SSL certificate should be configured with the FQDN of the AD RMS server. The cluster address and port cannot be changed after AD RMS is deployed. A non-SSL address can be configured, but you will lose the AD RMS with Identity Federation functionality.

AD RMS Add-on for Internet Explorer

The Windows Rights Management Add-on (RMA) for Internet Explorer enables rights-protected content to be viewed only. Because you can only view and not alter these restricted files, this prevents sensitive documents, web-based information, and email messages from being forwarded, edited, or copied by unauthorized individuals. For you to run RMA for Internet Explorer successfully, you must first install the Windows Rights Management (RM) client. The Extensible Rights Markup Language (XrML) is the XML verbiage used by AD RMS to express usage rights for rights-protected content.

AD RMS Requirements

AD RMS requires an AD RMS–enabled client. Windows Vista, Windows 7, and Windows 8/8.1 include the AD RMS client by default. If you are not using Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2, you can download the AD RMS client for previous versions of Windows from Microsoft's Download Center.

File System: The NTFS file system is recommended.

Messaging: Message Queuing.

Web Services: Internet Information Services (IIS). ASP.NET must be enabled.

Active Directory Domain Services

AD RMS must be installed in an Active Directory domain in which the domain controllers are running Windows Server 2008, Windows Server 2008 R2, or Windows Server 2008 R2. All users and groups that use AD RMS to acquire licenses and publish content require an email address configured in Active Directory.

Database Server: AD RMS requires a SQL database server. Microsoft SQL Server 2005, 2008, and 2012 are supported SQL versions.

The new AD RMS administrative roles are as follows:

AD RMS Service Group When the AD RMS role is installed onto a server, a local AD RMS service account is created and added to the local AD RMS service group. The server uses the service account to start services at system startup and cannot be the same account used to install the service.

AD RMS Enterprise Administrators The AD RMS policies and settings are managed by members of the local AD RMS Enterprise Administrators group. When AD RMS is installed onto the server, the user account installing the role is added to the AD RMS Enterprise Administrators group. Only administrators who manage RMS should be added to this group.

AD RMS Template Administrators Users who belong to the local AD RMS Templates Administrators group are allowed to manage rights policy templates. AD RMS template administrators have the rights to read cluster data, list rights policy templates, create new rights policy templates, modify existing rights policy templates, and export rights policy templates.

AD RMS Auditors The local AD RMS Auditors role allows administrators who have this right to manage logs and reports. The AD RMS Auditors role is a read-only role that is restricted to running reports available on the AD RMS cluster, reading cluster information, and reading logging settings.

Installing AD RMS

AD RMS deployment is described as a root cluster, which is not used in terms of failover or network balancing clustering. An AD RMS root cluster manages all of the AD RMS licensing and certificate provisions for the forest. There can be only one AD RMS root cluster per AD forest. After a root cluster is deployed, there is the option of installing additional licensing-only clusters, which issue licenses to clients for publishing their content.

Now that you have a basic understanding of AD RMS, let's take the next step and install it. In Exercise 22.13, you will install AD RMS using the Server Manager MMC.

EXERCISE 22.13

Installing an AD RMS Role on the Local Computer Using Server Manager

1. Start Server Manager. Click Manage and then click Add Roles And Features.
2. The Add Roles And Features Wizard shows the Before You Begin screen. Click Next.
3. Select the Active Directory Rights Management Services Role and click Next.

4. Add the required Active Directory Rights Management Services by default and click Add Features.
5. Click Next.

6. On the screen that explains ADRMS, click Next.
7. On the Select Role Services screen, by default Active Directory Rights Management Server is selected. Identity Federation Support uses AD FS federated trust between organizations to establish user identities and provide access to the RMS-protected content across the federation. Click Next.
8. Click Next on the Web Server (IIS) screen.
9. At the confirmation screen, click Install.
10. Once the installation is complete, click Close.
11. While still in Server Manager, click the AD RMS link on the left side.
12. Click the More About The AD RMS Service Account link next to Configuration Required For Active Directory Rights Management Service.
13. Under Action, click the Perform Additional Configuration link.
14. At the AD RMS introduction screen, click Next.
15. On the Create Or Join An AD RMS Cluster screen, choose Create A New AD RMS Cluster. (The other choice will not be available because you are installing the first AD RMS server and must start the cluster.) Click Next.
16. AD RMS uses a database to store configuration and policy information. At the Select Configuration Database screen, choose Use Windows Internal Database on this server. (The other option is to use a third-party database engine or MSSQL.) Click Next.

EXERCISE 22.13 *(continued)*

17. On the Specify Service Account screen, choose the service account that AD RMS will use. Click the Specify button and type in an administrator account and password other than the ones with which you are currently logged in. Click Next.
18. At the Cryptographic Mode screen, choose Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes) and click Next.
19. At the Configure AD RMS Cluster Key Storage screen, choose Use AD RMS Centrally Managed Key Storage and click Next.

20. Next you will be asked to enter a password in the AD RMS Cluster Key Password field. The AD RMS cluster key password is used to encrypt the AD RMS cluster key that is stored in the AD RMS database. Type **P@ssw0rd**, confirm it, and click Next.
21. On the Select Website screen, click default website and click Next. AD RMS needs to be hosted in IIS. This will set up a default website for AD RMS.
22. On the Specify Cluster Address screen, choose whether to use a secure or a nonsecure website. Choose the Use An SSL-Encrypted Connection (`https://`) check box. In the Internal Address box, type in the server name and click the Validate button. After the address is verified, click Next.

23. The Choose A Server Authentication Certificate For SSL Encryption screen appears. If you receive a message stating the certificate for this server is already created, just click Next. If the message doesn't appear, choose one of your certificates and click Next.
24. The Name The Server Licensor Certificate screen appears. Accept the default server and click Next.
25. You have the option to register AD RMS now or later. If you register the server now, AD RMS will take effect immediately. If you register the server later, AD RMS will not work until you register. You will not register during this exercise. Choose Register Later and click Next.
26. At the Configure Identity Federation Support screen, specify the name of the web server that Identity Federation will use and click the Validate button. The Next button will become available once the server is validated. If an error appears during validation, it will not affect this exercise. Click Next.
27. At the Confirm Installation Selections screen, verify all of your settings and click Install.
28. The install progress screen appears. When the install is complete, click Close.
29. Close the Server Manager MMC.

Managing AD RMS: AD RMS Service Connection Point

The *service connection point (SCP)* is used to store the URL of the AD RMS cluster. The SCP is stored as an object in Active Directory. The SCP can be configured when AD RMS is being installed or later through the Active Directory Rights Management Services console. Only one SCP can exist in an Active Directory forest.

The AD RMS SCP can be registered automatically during AD RMS installation, or it can be registered after installation has finished. To register the SCP, you must be a member of the local AD RMS Enterprise Administrators group and the Active Directory Domain Services (AD DS) Enterprise Admins group, or you must have been given the appropriate authority.

Managing the SCP is accomplished on the SCP tab of the AD RMS cluster's Properties dialog box.

If a client computer is not located within the Active Directory forest, you must use registry keys to point the AD RMS client to the AD RMS cluster. These registry keys are created in `HKEY_Local_Machine\Software\Microsoft\MSDRM\ServiceLocation`. Create a key called `Activation` with the value of `http(s)://<your_cluster>/_wmcs/certification`, where `<your_cluster>` is the URL of the root cluster used for certification.

AD RMS Templates

As you know, a template is a mold that you can use over and over again. AD RMS templates are no different. Before you start creating AD RMS templates, you must first create a shared directory where the templates can be stored. An administrator can then create AD RMS rights policy templates on the AD RMS cluster and export those templates to the shared directory. If your users are connected to the company intranet and they are using AD RMS–enabled applications, they can access the AD RMS templates right from the shared directory as long as they have read access to the shared folder. If your users are not connected to the company intranet, just copy the template to their computers, and this will allow AD RMS–enabled applications to continue to function properly.

When publishing protected content, the author selects the rights policy template to apply from the templates that are available on the local computer. Visibility of the templates is controlled via NTFS permissions. If the user does not have NTFS read access, the respective template will not be visible in an RMS-aware application.

When a user attempts to use protected content, the RMS-enabled application obtains the latest version of the rights policy template that was used to publish the content from the configuration database. The RMS-enabled application then applies its settings to the content. When the rights policy template is modified on the RMS server, RMS updates the template accordingly, in both the configuration database and the shared folder.

If a rights policy template is deleted, it is removed from the configuration database and also from the shared folder (that is specified as the file location for storing copies of templates) location when the template is deleted.

When working with rights policy templates, perform the following tasks:

1. Create and edit rights policy templates.
2. When creating a rights policy template, define the users and rights that apply. Also define how the rights policy template is to be applied to content.
3. Edit the rights policy templates later when they need to be updated.
4. Create as many rights policy templates as are required to manage rights in the organization, but consider that some applications are limited in the number of templates that can be displayed in the application's user interface. If more than a few templates are created in a cluster, you might want to scope the different templates to different groups of users by modifying NTFS permissions.
5. When a template is no longer appropriate, archive the rights policy template and update the distribution of the rights policy templates to the clients so that users do not try to protect content with the retired template. Users attempting to use content protected with the template will still be able to do so because the archived template is still accessible to the RMS servers issuing licenses.
6. If usage of all documents protected with a template is no longer desired, you can delete the template instead of archiving it. If users attempt to use content that was published by using the deleted rights policy template, they will not be issued licenses to do so.

See Table 22.9 for a description of the RMS template rights.

TABLE 22.9 Description of rights in RMS templates

Right	Description
Full control	If established, this right enables a user to exercise all rights in the license, whether or not the rights are specifically established to that user.
View	If this right is established, the AD RMS client enables protected content to be decrypted. Usually, when this right is established, the RMS-aware application will allow the user to view protected content.
Edit	If this right is established, the AD RMS client enables protected content to be decrypted and re-encrypted by using the same content key. Usually, when this right is established, the RMS-aware application will allow the user to change protected content and then save it to the same file. This right is effectively identical to the Save right.
Save	If this right is established, the AD RMS client enables protected content to be decrypted and then re-encrypted by using the same content key. Usually, when this right is established, the RMS-aware application will allow the user to change protected content and then save it to the same file. This right is effectively identical to the Edit right.
Export (Save As)	If this right is established, the AD RMS client enables protected content to be decrypted and then re-encrypted by using the same content key. Usually, when this right is established, the RMS-aware application will allow the user to use the Save As feature to save protected content to a new file.
Print	Usually when this right is established, the RMS-aware application will allow the user to print protected content.
Forward	Usually when this right is established, the RMS-aware application will allow an email recipient to forward a protected message.
Reply	Usually when this right is established, the RMS-aware application will allow an email recipient to reply to a protected message and include a copy of the original message.
Reply All	Usually when this right is established, the RMS-aware application will allow an email recipient to reply to all recipients of a protected message and include a copy of the original message.
Extract	Usually when this right is established, the RMS-aware application will allow the user to copy and paste information from protected content.
Allow Macros	Usually when this right is established, the RMS-aware application will allow the user to run macros in the document or use an editor to modify macros in the document.
View Rights	If this right is established, the AD RMS client enables a user to view the user rights that are assigned by the license.
Edit Rights	If this right is established, the AD RMS client enables a user to edit the user rights that are assigned by the license.

Backing Up AD RMS

Follow these steps to allow you to recover from any AD rights management server failure:

1. Record your cluster key password and store it in a safe manner.
2. Export the trusted publishing domain (see Exercise 22.18).
3. Create database backups.

Record and Store Your Cluster Key Password

During installation, take note of the cluster key password and securely store it. If you inherited the AD RMS server and the cluster key password hasn't been documented, you should change it before backup. To accomplish this, start the Active Directory Rights Management Services console under ServerName ➢ Security Policies ➢ Cluster Key Password. Click Change Cluster Key Password.

Create a Backup of the AD RMS Database

AD RMS uses three databases in the database server:

Configuration Database This is a critical component of an AD RMS installation. The database stores, shares, and retrieves all configuration data and other data that the service requires to manage account certification, licensing, and publishing services for a whole cluster.

Directory Services Database This contains information about users, identifiers (such as email addresses), security IDs, group membership, and alternate identifiers. This information is a cache of directory services data.

Logging Database This is all of the historical data about client activity and license acquisition. For each root or licensing-only cluster, by default AD RMS installs a logging database in the same database server instance hosting the configuration database.

In Exercise 22.14, we will perform a backup of the RMS database.

EXERCISE 22.14

Backing Up an AD RMS Database

1. Log on to the SQL server.
2. Click Start ➢ All Programs ➢ Microsoft SQL Server 2008 or 2012 and select SQL Server Management Studio. The Connect To Server dialog box will appear. Verify the server name is correct and that authentication is set for Windows Authentication.
3. Click Connect.
4. Expand the Databases node.
5. Right-click DRMS_Config_rms_domain_com_443, select Tasks, and then select Back Up.

6. Click Add in the Destination section and select the location.
7. Click OK to finish the backup.
8. Repeat these steps to back up the logging and directory services cache database.

If you cannot restore the configuration database, you can recover your AD RMS infrastructure with the exported TPD and the cluster key password.

AD RMS Trust Policies

Trust policies are implemented to define how content licensing requests are processed throughout the enterprise, including rights-protected content from other AD RMS clusters. Trust policies are defined as follows:

Trusted User Domains A trusted user domain (TUD) is the boundary mechanism for the AD RMS root cluster to process client licensor certificates or use licenses from users whose rights account certificates (RACs) were issued by another AD RMS root cluster. You must import the server licensor certificate of the AD RMS cluster to be trusted, to define your TUD.

Trusted Publishing Domains A trusted publishing domain (TPD) is another boundary type for one AD RMS cluster to issue licenses against publishing licenses issued by another AD RMS cluster. You must also import the server licensor certificate and private key of the server to be trusted, to define the TPD.

Windows Live ID Microsoft offers an online RMS service for an AD RMS user to send rights-protected content to another user with their Windows Live ID. The Windows Live ID recipient is then able to read rights-protected content from the originating AD RMS cluster registered through Microsoft's online RMS service. This extended AD RMS implantation does not allow the Windows Live ID user to create rights-protected content from the on-premise AD RMS cluster.

Federated Trust With a federated trust established between AD forests, users from one organization can share rights-protected content with another organization without requiring AD RMS implementation on both sides of the trust.

Microsoft Federation Gateway Microsoft also offers federated trust through the Microsoft Federation Gateway, which is essentially a trusted broker between organizations. Microsoft Federation Gateway handles all of the identity verifications with all participating Microsoft federated organizations. Microsoft federated organizations can take advantage of this gateway by filtering lists to select which domains can receive certificates or licenses from the on-premise AD RMS cluster.

Managing Trusted User Domains Trusted user domains enable trust between domains running AD RMS, and they are often used to connect users between forests. TUD

management is accomplished in the AD RMS Management console. TUD information is exported to a `.bin` file and then subsequently imported using the Import Trusted User Domain dialog box.

Adding a Trusted User Domain By default, Active Directory Rights Management Services (AD RMS) will not process requests from users whose rights account certificate was issued by a different AD RMS installation. However, you can add user domains to the list of trusted user domains, which allows AD RMS to process such requests.

For each TUD, you can also add and remove specific users or groups of users. In addition, you can remove a TUD; however, you cannot remove the root cluster for this Active Directory forest from the list of TUDs. Every AD RMS server trusts the root cluster in its own forest. In Exercise 22.15 we'll add a TUD into the test domain.

EXERCISE 22.15

Adding a Trusted User Domain

Before getting started, the TUD of the AD RMS installation should already be exported and available.

1. Start the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand Trust Policies and click Trusted User Domains.
3. In the Actions pane, click Import Trusted User Domain.
4. In the Trusted User Domain File dialog box, type the path to the exported server licensor certificate of the user domain to trust or click Browse to locate it.
5. In Display Name, type a name to identify this trusted user domain. If you would like to extend this trust to federated users, select Extend Trust To Federated Users Of The Imported Server.
7. Click Finish.

Exporting the Trusted User Domain

TUDs allow an AD RMS cluster to issue licenses to users whose rights account certificate was established by another server in an AD RMS cluster. Exporting a TUD's key and importing it into another AD RMS cluster allows the cluster to process requests for use licenses from users whose rights account certificates are in a different cluster.

Membership in the local **AD RMS Enterprise Admins group**, or equivalent, is the minimum required to complete this procedure. In Exercise 22.16, we will export the TUD and store the data in a location you provide.

EXERCISE 22.16

Exporting the Trusted User Domain

1. Start the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand Trust Policies and click Trusted User Domains.
3. In the Actions pane, click Export Trusted User Domain.
4. The Save As dialog box appears. I recommend you modify the `.bin` file name to include the name of your server, such as `ADRMS_Cluster1_LicensorCert.bin`.
5. Click Save to save the file with the name and location you specified.

Exporting the Trusted Publishing Domain

Unlike a trusted user domain, a trusted publishing domain enables an AD RMS cluster to issue licenses as if it was a different AD RMS cluster. To accomplish this, both the certificate and the private key need to be imported. This is different from a TUD scenario, where only the certificate is imported.

Importing a TPD is accomplished within the AD RMS Management console using the Import Trusted Publishing Domain dialog box. Saving a copy of the trusted publishing domain can be done from within the AD RMS administration console. In the Exercise 22.17, we will export the TPD.

EXERCISE 22.17

Exporting the Trusted Publishing Domain

1. Start the AD RMS administration console.
2. In the console tree view, select Trusted Publishing Domains node.
3. In the details pane on the right, select Export Trusted Publishing Domain. The Export Trusted Publishing Domain dialog box will appear.
4. From the Export Trusted Publishing Domain dialog box, click Save As. The Export Trusted Publishing Domain File Save As dialog box will appear. On the left pane, select the folder you want to save the trusted publishing domain.
5. In File Name enter a filename; then verify the XML File (`*.xml`) type is selected for Save As Type.
6. Click Save. This will close the Export Trusted Publishing Domain As dialog box.
7. In the ExportTrusted Publishing Domain dialog box, enter a password in the Password box.
8. Enter a password again in the Confirm Password dialog box.
9. Click Finish.

Adding a Trusted Publishing Domain

Exercise 22.18 assumes you have exported the trusted publishing domain of another AD RMS cluster (as described in the preceding section). Membership in the local AD RMS Enterprise Admins group, or equivalent, is the minimum required to complete this procedure.

EXERCISE 22.18

Adding the Trusted Publishing Domain

1. Start the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand Trust Policies and click Trusted Publishing Domains.
3. In the Actions pane, click Import Trusted Publishing Domain.
4. In the Trusted Publishing Domain File dialog box, type the path to the trusted publishing domain file or click Browse to locate it. This file contains the licensor certificate, private key (if the key is stored in software), and rights policy templates. This file is encrypted.
5. In Password, type the password required to decrypt this file.
6. In Display Name, type a name to identify this trusted user domain.
7. Click Finish.

Managing Distributed and Archived Rights Policy Templates

Rights policy templates are managed in the AD RMS Management console. Planning and overviews of rights policies are available here:

`http://technet.microsoft.com/en-us/library/ee221094`

`http://technet.microsoft.com/en-us/library/dd996658`

You can designate the location for the templates as well as set whether the templates can be exported by using the properties of the Rights Policy Template tab.

Summary

In this chapter, I discussed the certificate authority role and some of the new features in Microsoft Windows Server 2012 R2, including additional management options, new certificate templates, and better support for globalized organizations with limited IDN support. I also covered the details of the same-key certificate renewal requirement and the effects of the new increased default security settings on the CA role service.

I also discussed Active Directory Federation Services, which provides Internet-based clients with a secure identity access solution that works on both Windows and non-Windows operating systems.

Finally, I talked about Active Directory Rights Management Services. I explained that AD RMS is included with Microsoft Windows Server 2012 R2 and discussed how it allows administrators or users to determine what access to give other users in an organization.

Exam Essentials

Understand the concepts behind certificate authority. Certificate authority servers manage certificates. Make sure you understand why companies use certificate servers and how they work.

Understand certificate enrollment. You need to understand the many different ways to issue certificates to users and computers. You also need to understand the differences between installing certificates using GPOs, auto-enrollment, and web enrollment.

Understand Active Directory Federation Service. Active Directory Federation Service gives users the ability to do a single sign-on and access applications on other networks without needing a secondary password. Organizations can set up trust relationships with other trusted organizations so that a user's digital identity and access rights can be accepted without a secondary password.

Know how to install Active Directory Rights Management Services. Active Directory Rights Management Services, included with Microsoft Windows Server 2012 R2, allows administrators and users to determine what access (open, read, modify, and so on) they give to other users in an organization. This access can be used to secure email messages, internal websites, and documents.

Review Questions

1. Channel Fishing Company wants to configure a CA server in the DMZ to issue certificates to remote users. How would you accomplish this? (Choose all that apply.)
   - **A.** You should consider having the Certificate Enrollment Policy Web Server role included in the solution.
   - **B.** You should consider having the online responder included in the solution.
   - **C.** You should consider having the Network Device Enrollment Service included in the solution.
   - **D.** You should consider having the web service included in the solution.
   - **E.** You should consider having the Certificate Enrollment Web Service included in the solution.
   - **F.** You should consider having the Web Enrollment service included in the solution.

2. The certificate revocation list (CRL) polling begins to consume bandwidth. What steps should you consider to reduce network traffic?
   - **A.** You should consider implementing the Certificate Enrollment Policy Web Server role and Certificate Enrollment Web Services role.
   - **B.** You should consider implementing an online responder.
   - **C.** You should consider implementing an online issuing CA and a root CA.
   - **D.** You consider publishing more CRLs.

3. ABC Industries wants configuration modifications of the Certification Authority role service to be logged. How would you implement this? (Choose all that apply.)
   - **A.** You should consider enabling auditing of system events.
   - **B.** You should consider enabling logging.
   - **C.** You should consider enabling auditing of object access.
   - **D.** You should consider enabling auditing of privilege use.
   - **E.** You should consider enabling auditing of process tracking.

4. Federation proxy services are installed through which of the following?
   - **A.** Separate Active Directory Federation Proxy install download
   - **B.** Server Manager ➢ Remote Access ➢ Web Proxy
   - **C.** Server Manager ➢ Active Directory Federation Services ➢ Active Directory Proxy services
   - **D.** Windows PowerShell ➢ Install-Windows-Feature Web Proxy

5. The new Workplace Join feature supports which of following? (Choose all that apply.)
   - **A.** Federates an iPhone to the corporate intranet
   - **B.** Allows Windows 8 clients to process claim-based trusts
   - **C.** Allows Windows 8 clients to form claim-based trusts automatically with the home domain
   - **D.** None of the above

6. You install and configure four Windows Server 2012 R2 servers as an AD FS server farm. The AD FS configuration database is stored in a Microsoft SQL Server 2012 database. You need to ensure that AD FS will continue to function in the event of an AD FS server failure. You also need to ensure that all four servers in the AD FS farm will actively perform AD FS functions. What should you include in your solution?
   - **A.** Windows Failover Clustering
   - **B.** Windows Identity Foundation 3.5
   - **C.** Network Load Balancing
   - **D.** Web Proxy Server

7. Your network contains an Active Directory domain named contoso.com. You plan to deploy a Windows 2012 R2 Active Directory Federation Services (AD FS) farm that will contain eight federation servers. You need to identify which technology or technologies must be deployed on the network before you install the federation servers. Which technology or technologies should you identify? (Choose all that apply.)
   - **A.** Network Load Balancing
   - **B.** Microsoft Forefront Identity Manager 2010
   - **C.** Windows Internal Database feature
   - **D.** Microsoft SQL Server 2012 R2
   - **E.** The Windows Identity Foundation 3.5 feature

8. You are the system administrator at JavaCup, which hosts a web RMS-aware application that the JavaCup forest and Boston Tea Company forest users need to access. You deploy a single AD FS server in the JavaCup forest. Which of the following is a true statement about your AD FS implementation? (Choose all that apply.)
   - **A.** You will configure a relying-party server on the JavaCup AD FS server.
   - **B.** The AD FS server in the Boston Tea Company forest functions as the claims provider.
   - **C.** The AD FS server in the Boston Tea Company forest functions as the relying-party server.
   - **D.** You will configure a claims provider trust on the JavaCup AD FS server.

9. You store AD FS servers in an OU named Federation Servers. You want to auto-enroll the certificates used for AD FS. Which certificates should you add to the GPO?

A. The CA certificate of the forest

B. The third-party (VeriSign, Entrust) CA certificate

C. The SSL certificate assigned to the AD FS servers

D. The Token Signing certificate assigned to the AD FS Servers

10. You plan to implement Active Directory Rights Management Services (AD RMS) across the enterprise. You need to plan the AD RMS cluster installations for the forest. Users in all domains will access AD RMS–protected documents. You need to minimize the number of AD RMS clusters. Which of the following will help you determine how many AD RMS root clusters you require?

A. You need at least one AD RMS root cluster for the enterprise.

B. You need at least one AD RMS root cluster per forest.

C. You need at least one AD RMS root cluster per domain.

D. You need at least one AD RMS root cluster per Active Directory site.

E. An AD RMS root cluster is not required.

Appendix A

Answers to Review Questions

Chapter 1: Install Windows Server 2012 R2

1. B. Windows Server 2012 R2 Server Core is a more secure, slimmed-down version of Windows Server. Web versions of Windows Server 2012 R2 are not available. You would use Windows Server 2012 R2 Standard as a web server.

2. C. One of the new advantages of Windows Server 2012 R2 is that you can convert Server Core and GUI versions without the need to reinstall the operating system files completely.

3. B. Microsoft recommends that you upgrade your Windows Server 2008 or Windows Server 2008 R2 web server to Windows Server 2012 R2 Standard.

4. A. Windows Server 2012 R2 Datacenter was designed for organizations that are seeking to migrate to a highly virtualized, private cloud environment. Windows Server 2012 R2 Datacenter has full Windows Server functionality with unlimited virtual instances.

5. D. Windows Server 2012 R2 Foundation was designed for smaller companies that need a Windows Server experience for as few as 15 users. Windows Server 2012 R2 Foundation is general-purpose server with basic server functionality and no virtualization rights.

6. C. Windows Server 2012 R2 Essentials is ideal for small businesses that have as many as 25 users and 50 devices. It has a simple interface, preconfigured connectivity to cloud-based services, and no virtualization rights.

7. A, B, C and D. All four answers are advantages of using Windows Server 2012 R2 Server Core. Server Core is a smaller installation of Windows Server, and therefore all four answers apply.

8. B. Windows Server 2012 R2 Features On Demand allows an administrator not only to disable a role or feature but also to remove the role or feature's files completely from the hard disk.

9. D. New to Windows Server 2012 R2, an administrator has the ability to turn a Windows GUI installation into a Server Core installation.

10. C. Windows Server 2012 R2 has a type of domain controller called a read-only domain controller (RODC). This gives an organization the ability to install a domain controller in an area or location (onsite or offsite) where security is a concern.

Chapter 2: Configure Network Services

1. B. Because of the `.(root)` zone, users will not be able to access the Internet. The DNS forwarding option and DNS root hints will not be configurable. If you want your users to access the Internet, you must remove the `.(root)` zone.

2. C. Active Directory Integrated zones store their records in Active Directory. Because this company has only one Active Directory forest, it's the same Active Directory that both DNS servers are using. This allows ServerA to see all of the records of ServerB and ServerB to see all the records of ServerA.

3. D. The Secure Only option is for DNS servers that have an Active Directory Integrated zone. When a computer tries to register with DNS dynamically, the DNS server checks Active Directory to verify that the computer has an Active Directory account. If the computer that is trying to register has an account, DNS adds the host record. If the computer trying to register does not have an account, the record gets tossed away, and the database is not updated.

4. A. If you need to complete a zone transfer from Microsoft DNS to a BIND (Unix) DNS server, you need to enable BIND secondaries on the Microsoft DNS server.

5. B. Conditional forwarding allows you to send a DNS query to different DNS servers based on the request. Conditional forwarding lets a DNS server on a network forward DNS queries according to the DNS domain name in the query.

6. B. On a Windows Server 2012 R2 DNS machine, debug logging is disabled by default. When it is enabled, you have the ability to log DNS server activity, including inbound and outbound queries, packet type, packet content, and transport protocols.

7. D. Active Directory Integrated zones give you many benefits over using primary and secondary zones including less network traffic, secure dynamic updates, encryption, and reliability in the event of a DNS server going down. The Secure Only option is for dynamic updates to a DNS database.

8. A. Windows Server 2012 R2 DNS supports two features called DNS Aging and DNS Scavenging. These features are used to clean up and remove stale resource records. DNS zone or DNS server aging and scavenging flags old resource records that have not been updated in a certain amount of time (determined by the scavenging interval). These stale records will be scavenged at the next cleanup interval.

9. C. The `dnscmd /zoneexport` command creates a file using the zone resource records. This file can then be given to the Compliance department as a copy.

10. D. Stub zones are useful for slow WAN connections. These zones store only three types of resource records: NS records, glue host (A) records, and SOA records. These three records are used to locate authoritative DNS servers.

Chapter 3: Plan and Install Active Directory

1. B, C and D. The forest and function levels have to be Windows 2003 or newer to install an RODC.

2. B. A domain controller can contain Active Directory information for only one domain. If you want to use a multidomain environment, you must use multiple domain controllers configured in either a tree or a forest setting.

3. D. NTFS has file-level security, and it makes efficient usage of disk space. Since this machine is to be configured as a domain controller, the configuration requires at least one NTFS partition to store the Sysvol information.

4. A and D. To convert the system partition to NTFS, you must first use the `CONVERT` command-line utility and then reboot the server. During the next boot, the file system will be converted.

5. B and E. The use of LDAP and TCP/IP is required to support Active Directory. TCP/IP is the network protocol favored by Microsoft, which determined that all Active Directory communication would occur on TCP/IP. DNS is required because Active Directory is inherently dependent on the domain model. DHCP is used for automatic address assignment and is not required. Similarly, NetBEUI and IPX/SPX are not available network protocols in Windows Server 2012 R2.

6. A and C. The Sysvol directory must be created on an NTFS partition. If such a partition is not available, you will not be able to promote the server to a domain controller. An error in the network configuration might prevent the server from connecting to another domain controller in the environment.

7. B and C. You need to run the `Adprep` command when installing your first Windows Server 2012 R2 domain controller onto a Windows Server 2008 R2 domain. `Adprep /rodcprep` actually gets the network ready to install a read-only domain controller and not a GUI version.

8. A. You'll need to use Active Directory Federation Services (AD FS) in order to implement federated identity management. Federated identity management is a standards-based and information technology process that will enable distributed identification, authentication, and authorization across organizational and platform boundaries. The AD FS solution in Windows Server 2012 R2 helps administrators address these challenges by enabling organizations to share a user's identity information securely.

9. B. The HOSTS file is a text-file-based database of mappings between hostnames and IP addresses. It works like a file-based version of DNS. DNS resolves a hostname to an IP address.

10. A. You only need to give them rights to the `Stellacon.com` zone using the DNS snap-in. If they do not have any rights to the `Stellatest.com` zone, they will not be able to configure this zone in any way.

Chapter 4: Configure Windows Server 2012 R2

1. C. You need to publish shares in the directory before they are available to the users of the directory. If NetBIOS is still enabled on the network, the shares will be visible to the NetBIOS tools and clients, but you do not have to enable NetBIOS on shares. Although replication must occur before the shares are available in the directory, it is unlikely that the replication will not have occurred by the next day. If this is the case, then you have other problems with the directory as well.

2. A. The Sharing tab contains a check box that you can use to list the printer in Active Directory.

3. A and C. A printer may not show up within Active Directory if the printer has not been shared or if the client does not have permission to view the printer. The printer will appear as an object in Active Directory even if it is offline or malfunctioning.

4. B. Offline files give you the opportunity to set up files and folders so that users can work on the data while outside the office.

5. A, B, C and D. Improved security, quotas, compression, and encryption are all advantages of using NTFS over FAT32. These features are not available in FAT32. The only security you have in FAT32 is shared folder permissions.

6. E. By giving Moe Modify on the NTFS security setting, you're giving him just enough to do his job. You could also give Sales or Finance the Modify permission, but then everyone in those groups would be able to delete, change, and do more than they all need to do. Also, Moe does not need Full Control to change or delete files.

7. B. Disk quotas allow you to limit the amount of space on a volume or partition. You can set an umbrella quota for all users and then implement individual users' quotas to bypass the umbrella quota.

8. C and E. The Admin group needs Full Control on the NTFS security and shared permission settings in order to do their job. To be able to give other users permissions, you must have the Full Control permission.

9. A and C. Windows Remote Management and Windows PowerShell allow an administrator to configure a Windows Server 2012 R2 machine remotely. The command prompt is used locally on a Windows Server 2012 R2 Server Core system, and there is no application called Microsoft Remote Admin (MRA).

10. D. File servers are used for storage of data, especially for users' home folders. Home folders are folder locations for your users to store data that is important and that needs to be backed up.

Chapter 5: Administer Active Directory

1. A. A computer account and the domain authenticate each other by using a password. The password resets every 30 days. Since the machine has not connected to the domain for 16 weeks, the computer needs to be rejoined to the domain.

2. C. Checking the box Account Never Expires will prevent this user's account from expiring again.

3. D. The `dsadd` command allows you to add an object (user's account) to the Active Directory database.

4. A. Distribution groups are for emails only, and distribution groups cannot be assigned rights and permissions to objects.

5. A. Inheritance is the process by which permissions placed on parent OUs affect child OUs. In this example, the permissions change for the higher-level OU (Texas) automatically caused a change in permissions for the lower-level OU (Austin).

6. B and E. Enabling the Advanced Features item in the View menu will allow Isabel to see the `LostAndFound` and `System` folders. The `LostAndFound` folder contains information about objects that could not be replicated among domain controllers.

7. A. Through the use of filtering, you can choose which types of objects you want to see using the Active Directory Users and Computers tool. Several of the other choices may work, but they require changes to Active Directory settings or objects.

8. A. To allow the junior admin to do backups, their account needs to be part of the Backup Operators local group. To add their account to the local group, you need to use Computer Management.

9. A, B, C and D. All of the options listed are common tasks presented in the Delegation of Control Wizard.

10. D. The Delegation of Control Wizard is designed to allow administrators to set up permissions on specific Active Directory objects.

Chapter 6: Manage GPOs

1. A and B. If you want your clients to be able to edit domain-based GPOs by using the ADMX files that are stored in the ADMX Central Store, you must be using Windows Vista, Windows 7, Windows 8, or Windows Server 2003/2008/2008 R2/2012/2012 R2.

2. D. If you assign an application to a user, the application does not get automatically installed. To have an application installed automatically, you must assign the application to the computer account. Since Finance is the only OU that should receive this application, you would link the GPO to Finance only.

3. C. The Resultant Set of Policy (RSoP) utility displays the exact settings that apply to individual users, computers, OUs, domains, and sites after inheritance and filtering have taken effect. Desktop wallpaper settings are under the User section of the GPO, so you would run the RSoP against the user account.

4. B. The Enforced option can be placed on a parent GPO, and this option ensures that all lower-level objects inherit these settings. Using this option ensures that Group Policy inheritance is not blocked at other levels.

5. A. If the data transfer rate from the domain controller providing the GPO to the computer is slower than what you have specified in the slow link detection setting, the connection is considered to be a slow connection and the application will not install properly.

6. D. To disable the application of Group Policy on a security group, you should deny the Apply Group Policy option. This is particularly useful when you don't want GPO settings to apply to a specific group, even though that group may be in an OU that includes the GPO settings.

7. A. GPOs at the OU level take precedence over GPOs at the domain level. GPOs at the domain level, in turn, take precedence over GPOs at the site level.

8. B. The Block Policy Inheritance option prevents group policies of higher-level Active Directory objects from applying to lower-level objects as long as the Enforced option is not set.

9. A, B, C and D. GPOs can be set at all of the levels listed. You cannot set GPOs on security principals such as users or groups.

10. D and E. Administrative templates are used to specify the options available for setting Group Policy. By creating new administrative templates, Ann can specify which options are available for the new applications. She can then distribute these templates to other system administrators in the environment.

Chapter 7: Manage Security

1. B, C and E. The Account Lockout Duration setting states how long an account will be locked out if the password is entered incorrectly. Account Lockout Threshold is the number of bad password attempts, and Account Lockout Counter is the time in which the bad password attempts are made. Once the Account Lockout Counter value reaches 0, the number of bad password attempts returns to 0.

2. B. Account logon events are created for domain account activity. For example, you have a user who logs onto a server so that they can access files; the act of logging onto the server creates this audit event.

3. B, E and F. The first step is to enable auditing. With auditing enabled, Alexis can specify which actions are recorded. To give permissions to the Audit user account, she can use the Delegation of Control Wizard.

4. B, E, G and H. The Active Directory Users and Computers tool allows system administrators to change auditing options and to choose which actions are audited. At the file system level, Crystal can specify exactly which actions are recorded in the audit log. She can then use Event Viewer to view the recorded information and provide it to the appropriate managers.

5. B. Account logon events are created for domain account activity. For example, you have a user who logs on to a server so that they can access files; the act of logging on to the server creates this audit event.

Chapter 8: Configure TCP/IP

1. D. To calculate the network mask, you need to figure out which power number (2^x) is greater than or equal to the number you need. Since you are looking for 1000, $2^{10} = 1024$. You then add the power (10) to the current network mask (53 + 10 = 63).

2. A. When you look at an IPv6 address, the first sections tell you the IPv6 address space prefix. Fd00:: /8 is the unique local unicast prefix, and this allows the server to communicate with all local machines within your intranet.

3. C. The unique local address can be FC00 or FD00, and it is used like the private address space of IPv4. Unique local addresses are not expected to be routable on the global Internet, but they are used for private routing within an organization.

4. A. A Class B address with a default subnet mask of 255.255.0.0 will support up to 65,534 hosts. To increase the number of networks that this network will support, you need to subnet the network by borrowing bits from the host portion of the address. The subnet mask 255.255.252.0 uses 6 bits from the host's area, and it will support 64 subnets while leaving enough bits to support 1,022 hosts per subnet. The subnet mask 255.255.248.0 uses 5 bits from the hosts and will support 32 subnetworks while leaving enough bits to support 2,046 hosts per subnet. 255.255.252.0 is the better answer because it leaves quite a bit of room for further growth in the number of networks while still leaving room for more than 1,000 hosts per subnet, which is a fairly large number of devices on one subnet. The subnet mask 255.255.254.0 uses 7 bits from the host's area and will support more than 120 networks, but it will leave only enough bits to support 500 hosts per subnet. The subnet mask 255.255.240.0 uses 4 bits from the hosts and will support only 16 subnetworks, even though it will leave enough bits to support more than 4,000 hosts per subnet.

5. A. The network mask applied to an address determines which portion of that address reflects the number of hosts available to that network. The balance with subnetting is always between the number of hosts and individual subnetworks that can be uniquely represented within one encompassing address. The number of hosts and networks that are made available depends on the number of bits that can be used to represent them. This scenario requires more than 35 networks and fewer than 1,000 workstations on each network. If you convert

the subnet masks as described in the chapter, you will see that the mask in option A allows for more than 60 networks and more than 1,000 hosts. All of the other options are deficient in either the number of networks or the number of hosts that they represent.

6. A. The subnet mask 255.255.255.192 borrows 2 bits from the hosts, which allows you to build four separate networks that you can route through the Windows server. This will allow you to have 62 hosts on each segment. A mask of 255.255.255.128 would have been even better, with two subnets of 126 hosts each, but that wasn't an option, and this solution gives you room for growth in the number of subnets. The subnet mask 255.255.255.224 borrows 3 bits from the hosts. This allows you to create 8 networks, which you don't need, and it leaves only enough bits for 30 hosts. The subnet mask 255.255.255.252 borrows 6 bits from the hosts. This allows you to create more than 60 networks, which you don't need, and it leaves only enough bits for 2 hosts. The subnet mask 255.255.255.240 borrows 4 bits from the hosts. This allows you to create 16 networks, which you don't need, and it leaves only enough bits for 14 hosts per subnet.

7. B, C and D. When you add up the locations that currently need to be given a network address, the total is 3,150, and the maximum number of hosts at any one of these locations is fewer than 1,000. The subnet masks need to support those requirements. Assuming that you choose the Class A private address space 10.0.0.0/8, the subnet masks given in options B, C, and D will provide the address space to support the outlined requirements. The subnet mask 255.255.240.0 supports more than 4,000 subnets and more than 4,000 hosts. The subnet mask 255.255.248.0 supports more than 8,000 subnets and more than 2,000 hosts. The subnet mask 255.255.252.0 supports more than 16,000 subnets and more than 1,000 hosts. Although each of these subnet masks will work, at the rate that this company is growing, 255.255.252.0 is probably the best mask to prepare for the future. It's unlikely that there will ever be more than 1,000 hosts on any given network. In fact, that number would probably cause performance problems on that subnet. Therefore, it's better to have more subnets available to deploy as the company grows. The subnet mask 255.255.224.0 supports more than 2,000 subnets—an insufficient number to cover the locations. The subnet mask 255.255.254.0 supports more than 32,000 subnets, but only 500 hosts per subnet, which are not enough hosts to cover all of the locations.

8. C. The CIDR /27 tells you that 27 1s are turned on in the subnet mask. Twenty-seven 1s equals 11111111.11111111.11111111.11100000. This would then equal 255.255.255.224.

The network address 192.168.11.192 with a subnet mask of 255.255.255.224 is perfect for Subnet A because it supports up to 30 hosts. The network address 192.168.11.128 with a subnet mask of 255.255.255.192 is perfect for Subnet B because it supports up to 62 hosts. The network address 192.168.11.0 with a subnet mask of 255.255.255.128 is perfect for Subnet C because it supports up to 126 hosts.

9. A. Microsoft's `jetpack.exe` utility allows you to compact a JET database. Microsoft JET databases are used for WINS and DHCP databases.

10. B and D. If the first word of an IPv6 address is FE80 (actually the first 10 bits of the first word yields `1111 1110 10` or FE80`:: /10`), then the address is a link-local IPv6 address. If it's in EUI-64 format, then the MAC address is also available (unless it's randomly generated). The middle FF:FE is the filler and indicator of the EUI-64 space, with the MAC address being 00:03:FF:11:02:CD. Remember also the 00 of the MAC becomes 02 in the link-local IPv6 address, flipping a bit to call it local.

Chapter 9: Use Virtualization in Windows Server 2012

1. B and D. Hyper-V can be installed on the Standard or Datacenter Editions of Windows Server 2012 R2. Itanium, x86, and Web Editions are not supported.

2. C. The external virtual network type will allow the virtual machine to communicate with the external network as it would with the Internet, so A is wrong. The internal-only network type allows communication between the virtual machines and the host machine. Because the question says that only communication between the virtual machines should be allowed, the only valid answer is private virtual machine network. The last option, public virtual machine network, does not exist in Hyper-V.

3. A. This question focuses on the fact that you cannot change the memory if the virtual machine is running, paused, or saved. The only valid answer is to shut it down and then change the memory.

4. A. The only virtual hard disk that increases in size is the dynamically expanding disk. Thus, this is the only valid answer to this question. The fixed-size disk creates a disk of the size you specify, the differencing disk is a special disk that stores only the differences between it and a parent disk, and the physical disk uses a physical drive and makes it available to the virtual machine.

5. C. Physical hard disks cannot be configured using the Virtual Hard Disk Wizard, the Edit Virtual Hard Disk Wizard, or the New Virtual Machine Wizard. You can configure and attach a physical disk only by using the virtual machine's settings.

6. B. Hyper-V is not supported on Itanium-based systems; thus, he cannot install it.

7. A, B and C. The minimum CPU requirement for running Hyper-V is a x64-based processor (Itanium is not supported), hardware Data Execution Protection must be enabled, and hardware-assisted virtualization must be enabled. There is no minimum requirement for a dual-core processor.

8. C. This question relates to the setup command used to install the Hyper-V server role on a Windows Server 2008 Server Core machine. It's important to remember that these commands are case sensitive and that the correct command is `start /wocsetup Microsoft-Hyper-V`, which is option C. All of the other commands will fail to install Hyper-V on a Server Core machine. If you were using a Windows Server 2012 R2 machine, you would use the `DISM` command.

9. A and D. The Hyper-V Manager is available only for Windows Server 2008, Windows 7, and Windows 8. There is no version available that runs on Windows Server 2003 or on Windows XP SP3.

10. C. The virtual network type in which the machines communicate with each other and with the host machine is called *internal only*. In a private virtual network, the virtual machines can communicate only with each other, not with the network or the host machine. The external network type defines a network where the virtual machines can communicate with each other, with the host machine, and with an external network like the Internet.

Chapter 10: Manage and Maintain Servers

1. D. All of the applications that are running on the Windows Server 2012 R2 machine will show up on the Details tab. Right-click the application and end the process.

2. A. If you use MBSA from the command-line utility `mdsacli.exe`, you can specify several options. You type **`mdsacli.exe/hf`** (from the folder that contains `mdsacli.exe`) and then customize the command execution with an option such as *`/ixxxx.xxxx.xxxx.xxxx`*, which specifies that the computer with the specified IP address should be scanned.

3. B and E. You can set the registry key `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer` to 0 to use the public Windows Update server, or you can set it to 1, which means that you will specify the server for Windows Update in the `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate` key. The WUServer key sets the Windows Update server using the server's HTTP name, for example, `http://intranetSUS`.

4. C. Server Manager is the one place where you install all roles and features for a Windows Server 2012 R2 system.

5. C. All options are valid steps to complete the configuration except option C because SERVERB cannot automatically draw updates from whichever sources are on SERVERA.

6. B, D, and F. Option A schedules the updates to occur at a time when the computers are generally not connected to the corporate network. Options C and E require more user interaction than would be considered minimal. By setting updates to occur with no user interaction at noon, you satisfy the requirements.

7. D. You can recover system state data from a backup, which always includes the Active Directory database. In this case, Event Viewer and System Monitor wouldn't help you recover the database, but they might help you determine why the hard drive crashed in the first place.

8. D. By using the Network Monitor, you can view all of the network packets that are being sent to or from the local server. Based on this information, you can determine the source of certain types of traffic, such as pings. The other types of monitoring can provide useful information, but they do not allow you to drill down into the specific details of a network packet, and they don't allow you to filter the data that has been collected based on details about the packet.

9. A. Microsoft Baseline Security Analyzer is a free download that you can get from Microsoft's website.

10. C. The Update Source And Proxy Server option allows you to specify where you will be receiving your updates (from Microsoft or another WSUS server) and your proxy settings if a proxy server is needed.

Chapter 11: Manage File Services

1. C. You need to publish shares in the directory before they are available to the users of the directory. If NetBIOS is still enabled on the network, the shares will be visible to the NetBIOS tools and clients, but you do not have to enable NetBIOS on shares. Although replication must occur before the shares are available in the directory, it is unlikely that the replication will not have occurred by the next day. If this is the case, then you have other problems with the directory as well.

2. A. The Sharing tab contains a check box that you can use to list the printer in Active Directory.

3. B, E, G and H. The Active Directory Users and Computers tool allows system administrators to change auditing options and to choose which actions are audited. At the file system level, Isabel can specify exactly which actions are recorded in the audit log. She can then use Event Viewer to view the recorded information and provide it to the appropriate managers.

4. B. Offline files give you the opportunity to set up files and folders so that users can work on the data while outside the company walls. Offline files allows a user to work on files while at home without the need to be logged into the network.

5. A, B, C and D. Improved security, quotas, compression, and encryption are all advantages of using NTFS over FAT32. These features are not available in FAT32. The only security you have in FAT32 is shared folder permissions.

6. A. Encrypting File System (EFS) allows a user or administrator to secure files or folders by using encryption. Encryption employs the user's security identification (SID) number to secure the file or folder. Encryption is the strongest protection that Windows provides.

7. B. Disk quotas allow you to limit the amount of space on a volume or partition. You can set an umbrella quota for all users and then implement individual users' quotas to bypass the umbrella quota.

8. B. Cipher is a command-line utility that allows you to configure or change EFS files and folders.

9. B. The Distributed File System (DFS) Namespace service in Windows Server 2012 R2 offers a simplified way for users to access geographically dispersed files. DFS allows you to set up a tree structure of virtual directories to allow users to connect to shared folders throughout the entire network.

10. D. File servers are used for storage of data, especially for users' home folders. Home folders are folder locations for your users to store data that is important and that needs to be backed up.

Chapter 12: Configure DNS

1. B. Because of the `.(root)` zone, users will not be able to access the Internet. The DNS forwarding option and DNS root hints will not be configurable. If you want your users to access the Internet, you must remove the `.(root)` zone.

2. C. Active Directory Integrated zones store their records in Active Directory. Because this company has only one Active Directory forest, it's the same Active Directory that both DNS servers are using. This allows ServerA to see all of the records of ServerB and allows ServerB to see all the records of ServerA.

3. D. The Secure Only option is for DNS servers that have an Active Directory Integrated zone. When a computer tries to register with DNS dynamically, the DNS server checks Active Directory to verify that the computer has an Active Directory account. If the computer that is trying to register has an account, DNS adds the host record. If the computer trying to register does not have an account, the record gets tossed away and the database is not updated.

4. A. If you need to complete a zone transfer from Microsoft DNS to a BIND (Unix) DNS server, you need to enable BIND Secondaries on the Microsoft DNS server.

5. B. Conditional forwarding allows you to send a DNS query to different DNS servers based on the request. Conditional forwarding lets a DNS server on a network forward DNS queries according to the DNS domain name in the query.

6. B. On a Windows Server 2012 R2 DNS machine, debug logging is disabled by default. When it is enabled, you have the ability to log DNS server activity, including inbound and outbound queries, packet type, packet content, and transport protocols.

7. D. Active Directory Integrated zones give you many benefits over using primary and secondary zones including less network traffic, secure dynamic updates, encryption, and reliability in the event of a DNS server going down. The Secure Only option is for dynamic updates to a DNS database.

8. A. Windows Server 2012 R2 DNS supports two features called DNS Aging and DNS Scavenging. These features are used to clean up and remove stale resource records. DNS zone or DNS server aging and scavenging flags old resource records that have not been updated in a certain amount of time (determined by the scavenging interval). These stale records will be scavenged at the next cleanup interval.

9. C. The `dnscmd /zoneexport` command creates a file using the zone resource records. This file can then be given to the Compliance department as a copy.

10. D. Stub zones are useful for slow WAN connections. These zones store only three types of resource records: NS records, glue host (A) records, and SOA records. These three records are used to locate authoritative DNS servers.

Chapter 13: Configure Routing and Remote Access

1. B. The boot threshold for an interface controls how long the relay agent will wait before forwarding DHCP requests it hears on that interface.

2. B. Multilink PPP has nothing to do with encryption of data. Multilink is easy to set up, relatively low in cost, and it makes the connection faster.

3. C and E. MS-CHAPv2 provides encrypted and mutual authentication between the respective RRAS locations. MPPE works with MS-CHAPv2 and provides encryption for all of the data between the locations. CHAP provides encrypted authentication, but MS-CHAPv2 is needed for MPPE to work. PAP is the lowest level of authentication providing passwords, but it sends passwords in cleartext, which is not the most secure solution. L2TP needs to team up with IPsec to provide the data encryption for the secure transfer of information between the locations.

4. B. MS-CHAPv2 authentication allows you to create VPN connections with a stand-alone server using PPTP and MPPE. MPPE employs keys that are created via MS-CHAPv2 or EAP-TLS authentication. EAP-TLS is not the correct answer because only domain controllers or member servers support EAP-TLS. Stand-alone servers support only MPPE. Neither PAP nor CHAP is supported with MPPE.

5. A and C. L2TP connections can be used to authenticate both sides of the VPN. L2TP needs IPsec to provide the encryption for the connection. These two together will provide the secure and authenticated transmission of data across the Internet between the two sites. PPTP connections provide encryption using only MPPE, but they don't provide authentication between the machines. RADIUS is a service that provides dial-in connectivity. MS-CHAPv2 is an authentication protocol for clients accessing the network.

6. B. L2TP and IPsec each has its own negotiation procedure for making a connection. If you remove the IPsec portion of the connection and the problem is alleviated, it is likely that IPsec is the problem, and you can then focus on IPsec. If the problem remains, you can work on the L2TP portion of the connection. IPsec has two modes: tunnel mode and transport mode. But because L2TP is a tunneling protocol, there is no sense in using IPsec tunneling. IPsec transport mode is used with L2TP and should be set aside for troubleshooting, as discussed. The L2TP implementation in Windows Server 2012 R2 doesn't support MPPE.

7. C. The default configuration for RRAS supports 5 PPTP ports and 5 L2TP ports. There are up to 150 sales reps trying to connect to the server, but only the first 10 will be able to connect. You can increase the number of ports available, up to 1,000, by using the Ports Properties dialog box. The Windows 8 clients are, by default, ready to support VPNs; they will first try L2TP and then switch over to PPTP if ports are unavailable.

8. C, E and G. Because the communication is not a continuous or frequent occurrence, it doesn't make sense to have the line always available, so RRAS with demand-dial will be less expensive than ISDN, which is always up. MS-CHAPv2 provides encryption and

a mutual authentication process. The MPPE provides the encryption of the actual data that travels across the connection. PAP is a cleartext authentication method, and CHAP provides only one-way authentication. L2TP doesn't provide any encryption by itself.

9. C. When you use Windows accounting, the local Windows account logs are found in the `systemroot\System32\LogFiles` folder. These logs can be stored in one of two formats for later analysis—Open Database Connectivity (ODBC) or Internet Authentication Service. The Performance Monitor utility that came with Windows NT has been replaced with the system event log. This keeps track of global service errors such as initialization failures and service starts and stops. There is no RRAS authentication log. You do have RADIUS logging available; when it's used, the log files are stored on the RADIUS servers. This is useful when you have multiple RRAS servers because you can centralize RRAS authentication requests. Active Directory is not used to log events from the various services in Windows Server 2012 R2.

10. B. The Server Status node in the RRAS snap-in shows you a summary of all the RRAS servers known to the system. Each server entry displays whether the server is up, what kind of server it is, how many ports it has, how many ports are currently in use, and how long the server has been up.

Chapter 14: Configure a Network Policy Server Infrastructure

1. B and E. By setting the Network Policy Server, you can force your DHCP users to use NAP on all of the DHCP scopes. This ensures that client systems meet minimum requirements to connect to a domain network.

2. D. Servers that are running Network Policy Server (NPS) are required to have a certificate installed on the NPS server.

3. B. One advantage of using NAP for DHCP is that you can set up user classes so that specific machines (for example, noncompliant DHCP systems) can get specific rules or limited access to the network.

4. D. Logman creates and manages Event Trace Session and Performance logs, and it allows an administrator to monitor many different applications through the use of the command line.

5. D. The higher the RADIUS priority number, the less that the RADIUS server gets used. To make sure that RADIUS ServerD is used only when ServerB and ServerC is unavailable, you would set the RADIUS priority from 1 to 10. This way it will get used only when ServerB and ServerC are having issues or are unresponsive.

6. C. The NPS snap-in allows you to set up RADIUS servers and specify which RADIUS server would accept authentication from other RADIUS servers. You can do your entire RADIUS configuration through the NPS snap-in.

7. C. NPS allows you to set up policies on how your users could log into the network. NPS allows you to set up policies that systems needs to follow, and if they don't follow these policies or rules, they will not have access to the full network.

8. C. Windows Server 2012 R2 comes with Extensible Authentication Protocol with Transport Level Security (EAP-TLS). This EAP type allows you to use public key certificates as an authenticator. TLS is similar to the familiar Secure Sockets Layer (SSL) protocol used for web browsers and 802.1X authentication. When EAP-TLS is turned on, the client and server send TLS-encrypted messages back and forth. EAP-TLS is the strongest authentication method you can use; as a bonus, it supports smart cards. However, EAP-TLS requires your NPS server to be part of the Windows Server 2012 R2 domain.

9. B and D. PEAP-MS-CHAP v2 is an EAP-type protocol that is easier to deploy than Extensible Authentication Protocol with Transport Level Security (EAP-TLS). It is easier because user authentication is accomplished by using password-based credentials (username and password) instead of digital certificates or smart cards. Both PEAP and EAP both use certificates with their protocols.

10. C. One advantage of NPS is that you can use the accounting part of NPS so that you can keep track of what each department does on your NPS server. This way, departments pay for the amount of time they use on the SQL server database.

Chapter 15: Configure and Manage Active Directory

1. A. Using images allows you to back up and restore your entire Windows Server 2012 R2 machine instead of just certain parts of data.

2. C. The Backup Once link allows you to start a backup on the Windows Server 2012 R2 system.

3. D. If you need to back up and restore your Windows Server 2012 R2 machine, you need to use the Windows Server Backup MMC.

4. C. To create multiple password policies, you would use ADSI Edit (or `adsiedit.msc`).

5. D. Universal security groups, global groups, and domain local groups are all available when you are running a Windows 2008 and Windows 2012 domain functional level.

6. B, C and E. The Account Lockout Duration setting states how long an account will be locked out if the password is entered incorrectly. The Account Lockout Threshold setting is the number of bad password attempts, and the Account Lockout Counter setting is the time in which the bad password attempts are made. Once Account Lockout Counter reaches 0, the number of bad password attempts returns to 0.

7. D. When resources are made available to users who reside in domains outside the forest, foreign security principal objects are automatically created. These new objects are stored within the `Foreign Security Principals` folder.

8. B. The primary method by which systems administrators create and manage application data partitions is through the `ntdsutil` tool.

9. A and E. To meet the requirements, Robert should use the normal backup type to create a full backup every week and the incremental backup type to back up only the data that has been modified since the last full or incremental backup operation.

10. B and D. You would need to transfer the two forestwide operations master roles: Schema Master and Domain Naming Master. This means that there can only be one Schema Master and only one Domain Naming Master per forest. The PDC Emulator Master, RID Master, and Infrastructure Master are all domain-based operations master roles. (Each domain in the forest must have a domain controller with these three roles installed.)

Chapter 16: Configure and Manage Group Policy

1. C. The Delegation of Control Wizard can be used to allow other system administrators permission to add GPO links.

2. C. The system administrator can specify whether the application will be uninstalled or whether future installations will be prevented.

3. B. You would use `GPUpdate.exe /force`. The `/force` switch forces the GPO to reapply all policy settings. By default, only policy settings that have changed are applied.

4. A. You would use the Windows PowerShell `Invoke-GPUpdate` cmdlet. This PowerShell cmdlet allows you to force the GPO to reapply the policies immediately.

5. D. DVD Present Targeting is not one of the options that you may consider when using item-level targeting.

6. A and B. If you want your clients to be able to edit domain-based GPOs by using the ADMX files that are stored in the ADMX Central Store, you must be using Windows Vista, Windows 7, Windows 8, or Windows Server 2003/2008/2008 R2/2012/2012 R2.

7. D. If you assign an application to a user, the application does not get automatically installed. To have an application automatically installed, you must assign the application to the computer account. Since Finance is the only OU that should receive this application, you would link the GPO to Finance only.

8. C. The Resultant Set of Policy (RSoP) utility displays the exact settings that apply to individual users, computers, OUs, domains, and sites after inheritance and filtering have taken effect. Desktop wallpaper settings are under the User section of the GPO, so you would run the RSoP against the user account.

9. B. The Enforced option can be placed on a parent GPO, and this option ensures that all lower-level objects inherit these settings. Using this option ensures that Group Policy inheritance is not blocked at other levels.

10. A. If the data transfer rate from the domain controller providing the GPO to the computer is slower than what you have specified in the slow link detection setting, the connection is considered to be a slow connection, and the application will not install properly.

Chapter 17: Configure and Manage High Availability

1. A, B and D. Only the Standard, Datacenter, and Hyper-V editions of Windows Server 2012 R2 can participate in a failover cluster.

2. A, B and D. All versions of Windows Server 2012 R2 can participate in an NLB cluster except for the Windows Server 2012 R2 Hyper-V edition.

3. D. A Windows Server 2012 R2 cluster can contain up to 64 nodes.

4. B. Drainstop is the function that allows the current session to end before stopping the cluster on the node. Evict is used to remove a node completely from a failover cluster. Pause is used to keep resources from failing over to a failover cluster node. Stop will immediately end the cluster service on the NLB cluster node, not allowing the current sessions to complete.

5. D. A Windows Server 2012 R2 NLB cluster can contain up to 32 nodes.

6. A and C. SQL Server and Exchange Server are supported only on failover clusters. Websites and VPN services are network-based services, so they are better suited for NLB clusters.

7. B and D. Websites and Terminal Services are all designed to work with NLB clusters. Database servers such as SQL Server do not work on NLB clusters.

8. B. To use unicast communication between NLB cluster nodes, each node must have a minimum of two network adapters.

9. B. Up to two votes can be lost before quorum can no longer be achieved. These votes can come from the file share witness or a cluster node.

10. B. In a three-node cluster, only one node can be offline before quorum is lost; a majority of the votes must be available to achieve quorum.

Chapter 18: Configure File and Storage Solutions

1. B, E, G and H. The Group Policy Management Console allows system administrators to change auditing options and to choose which actions are audited. At the file system level, LaDonna can specify exactly which actions are recorded in the audit log. She can then use Event Viewer to view the recorded information and provide it to the appropriate managers.

2. A. The iSCSI default port is TCP 3260. Port 3389 is used for RDP, port 1433 is used for Microsoft SQL, and port 21 is used for FTP.

3. C. Account logon events are created for domain account activity. For example, you have a user who logs onto a server so that they can access files; the act of logging onto the server creates this audit event.

4. A. File servers are used for storage of data, especially for users' home folders. Home folders are folder locations for your users to store data that is important and that needs to be backed up.

5. A, B, C and D. Improved security, quotas, compression, and encryption are all advantages of using NTFS over FAT32. These features are not available in FAT32. The only security you have in FAT32 is shared folder permissions.

6. D. The `iscsicli addisnsserver server_name` command manually registers the host server to an iSNS server. `refreshisnsserver` refreshes the list of available servers. `removeisnsserver` removes the host from the iSNS server. `listisnsservers` lists the available iSNS servers.

7. A. Windows Server 2012 R2 Features On Demand allows an administrator not only to disable a role or feature but also to remove the role or feature's files completely from the hard disk.

8. D. The iSNS feature is used to provide for the automatic discovery of iSCSI targets that are available on the network. This is a useful feature within a larger environment. Note that without iSNS DHCP configured, iSNS clients must be registered manually with the `iscsicli` command.

9. A. After generating hashes on the Colorado Springs file server that will be preloading Tampa's file server cache with file share data, the next logical step is to run `Export-BCCachePackage` to get the data to FS02 from FS01.

10. B. Since there is a classification rule that is currently configured and applied to company resources, you will be unable to delete the Contains Personal Information classification property manually because the Classification Rule controls the property. In this case, you have to delete the Classification Rule in order to be able to delete the classification property.

Chapter 19: Implement Business Continuity and Disaster Recovery

1. A. Using images allows you to back up and restore your entire Windows Server 2012 R2 machine instead of just certain parts of data.

2. C. If you need to get a stalled computer up and running as quickly as possible, you should start with the Last Known Good Configuration option. This option is used when you've made changes to your computer's hardware configuration and are having problems restarting but have not logged into the machine. Last Known Good Configuration will revert to the configuration used the last time the computer was successfully booted.

3. D. Daily backups back up all of the files that have changed during a single day. This operation uses the file time/date stamps to determine which files should be backed up and does not mark the files as having been backed up.

4. B. To create a restore point manually or to restore your computer to a previous restore point, you use the Shadow Copies tab of the System Properties dialog box. Although System Restore uses restore points, you do not use the System Restore utility to create a restore point.

5. B. You should start with the Last Known Good Configuration option. This option is used when you've made changes to your computer's hardware configuration and are having problems restarting. The Last Known Good Configuration will revert to the configuration used the last time the computer was successfully booted. Although this option helps overcome configuration errors, it will not help when there are hardware errors.

6. C. When you enable boot logging, the file created is `\Windows\ntbtlog.txt`. This log file is used to troubleshoot the boot process.

7. C. To repair the system files quickly, you can use the Startup Repair tool. You can restore an image by using the Backup and Repair Center, but it is faster to use the Startup Repair tool. Additionally, you will not lose any personal files by using the Startup Repair tool. Alternatively, you could try to use System Restore to go back to a previous checkpoint.

8. B. When you run your computer in Safe Mode, you simplify your Windows Server 2012 R2 configuration. Only the drivers that are needed to get the computer up and running are loaded.

9. C. The Backup Once link allows you to start a backup on the Windows Server 2012 R2 system.

10. D. If you need to back up and restore your Windows Server 2012 R2 machine, you need to use the Windows Server Backup MMC.

Chapter 20: Configure Advanced Network Services

1. C. Out of the possible answers provided, the only DHCP configuration option that would be both fault-tolerant and redundant is DHCP failover.

2. B, C and D. DNS registration is an advanced DHCP configuration. All three other options provide additional security for DNS on your network.

3. D. DNS netmask ordering is the only way to ensure that clients will get the closest DNS server to their subnet when performing DNS queries on your network. If DNS netmask ordering were not enabled, requests would go through a round-robin approach from all of the DNS servers available to provide lookup services. You could end up with a poor connection depending on which DNS server responds to your client's requests.

4. D. The DNSAdmins security group is the best fit for this administrator's responsibilities. If you were to place this administrator in either the Domain Admins or Enterprise Admins security group, that individual would have too many unnecessary permissions granted within the environment, making their Active Directory account a security vulnerability. The Schema Admins group does not pertain to this question.

5. B. DHCP name protection ensures that DNS host A records are never overwritten during DNS dynamic updates. The other three possible answers would not fulfill this question's requirements.

6. C. The IPAM ASM Administrators group is specifically designed for the delegation of IPAM Address Space Management. The IPAM Administrators group would give her domain account way to much access within the environment, and the other two possible answers would not provide her with enough permissions to perform her required responsibilities.

7. B. Out of the three real possible deployment methods—Distributed, Centralized, and Hybrid—only the Centralized deployment method allows one primary IPAM server to manage the entire enterprise. The Distributed method places an IPAM server at each site location, and the Hybrid method uses a primary server with an additional IPAM server at each site location within the enterprise.

8. D. The only way to accommodate the use of short, single-labeled host names within your DNS infrastructure is to implement a GlobalNames zone.

9. C. After you have successfully installed and provisioned your IPAM server, the next logical step in the IPAM deployment configuration is to configure and run server discovery. Be sure to follow the step-by-step configuration guide found on the IPAM Overview page in Server Manager when going through your IPAM test deployment.

10. A. The proper PowerShell syntax to display current IPAM database configuration settings is `Get-IpamDatabase`. The other possible answers are not valid PowerShell cmdlets.

Chapter 21: Configure the Active Directory Infrastructure

1. B. The NTDS settings for the site level are where you would activate and deactivate UGMC.

2. A. By decreasing the Replication interval for the DEFAULTIPSITELINK object, you will decrease the replication latency for all sites using the DEFAULTIPSITELINK.

3. D. In the Active Directory Sites and Services console, the Server NTDS settings are where you would activate and deactivate global catalogs.

4. D. Preferred bridgehead servers receive replication information for a site and transmit this information to other domain controllers within the site. By configuring one server at each site to act as a preferred bridgehead server, Daniel can ensure that all replication traffic between the two sites is routed through the bridgehead servers and that replication traffic will flow properly between the domain controllers.

5. C. By default, connection objects are automatically created by the Active Directory replication engine. You can choose to override the default behavior of Active Directory replication topology by manually creating connection objects, but this step is not required.

6. B. The Knowledge Consistency Checker (KCC) is responsible for establishing the replication topology and ensuring that all domain controllers are kept up-to-date.

7. D. Site link bridges are designed to allow site links to be transitive. That is, they allow site links to use other site links to transfer replication information between sites. By default, all site links are bridged. However, you can turn off transitivity if you want to override this behavior.

8. B. Simple Mail Transfer Protocol was designed for environments in which persistent connections may not always be available. SMTP uses the store-and-forward method to ensure that information is not lost if a connection cannot be made.

9. D. The Directory Service event log contains error messages and information related to replication. These details can be useful when you are troubleshooting replication problems.

10. A and D. By creating new sites, Christina can help define settings for Active Directory replication based on the environment's network connections. She can use connection objects to define further the details of how and when replication traffic will be transmitted between the domain controllers.

Chapter 22: Configure Access and Information Protection Solutions

1. A and E. Certificate Enrollment Web Service with the Certificate Enrollment Policy Web Server role is the preferred Microsoft solution for issuing certificates through the internet.

2. B. The online responder uses a lightweight HTTP protocol that responds faster and more efficiently than downloading a traditional CRL.

3. B and C. To enable AD FS 3.0 auditing, you must check the boxes for Success Audits and Failure Audits on the Events tab of the Federation Service Properties dialog box. You must also enable Object Access Auditing in Local Policy or Group Policy.

4. B. Federation Proxy Services are installed under Remote Access as a web application proxy server in Windows Server 2012.

5. A, B and C. By using Workplace Join, information workers can join their personal devices with their company's workplace computers to access company resources and services. When you join your personal device to your workplace, it becomes a known device and provides seamless second-factor authentication and single sign-on to workplace resources and applications. Windows Server 2012 R2, Windows 8.1, and iOS devices can be joined by using Workplace Join.

6. C. Network Load Balancing (NLB) is the only support Microsoft solution for providing high availability across an ADFS server farm. Windows Failover Clustering does not currently support ADFS as one master server is allowed to write to the configuration database per farm.

7. D. The AD FS configuration database stores all of the configuration data. It contains information that a federation service requires to identify partners, certificates, attribute stores, claims, and so forth. You can store this configuration data in either a Microsoft SQL Server 2005 or newer database or the Windows Internal Database feature that is included with Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 R2. The Windows Internal Database supports only up to five federation servers in a farm.

8. A and B. The relying-party server is a member of the Active Directory forest that hosts resources that a user in the partner organization wants to access. In this case, the relying party server should be the JavaCup AD FS server. A claims provider provides users with claims. These claims are stored within digitally encrypted and signed tokens. In this case, Boston Tea Party is the claims provider.

9. A. The Forest CA certificate is the only certificate that is automatically trusted, does not require user interaction and digital signature does not change in this scenario.

10. B. Licensing Server/Cluster is the component in charge of delivering publishing and use licenses. Several clusters can be installed per forest depending on the technical needs (servers' workload and bandwidth constraints).

Appendix B

About the Additional Study Tools

IN THIS APPENDIX:

- Additional Study Tools
- System requirements
- Using the Study Tools
- Troubleshooting

Additional Study Tools

The following sections are arranged by category and summarize the software and other goodies you'll find from the companion website. If you need help with installing the items, refer to the installation instructions in the "Using the Study Tools" section of this appendix.

NOTE

The additional study tools can be found at `www.sybex.com/go/mcsawin2012r2`. Here, you will get instructions on how to download the files to your hard drive.

Sybex Test Engine

The files contain the Sybex test engine, which includes two bonus practice exams, as well as the Assessment Test and the Chapter Review Questions, which are also included in the book itself.

Electronic Flashcards

These handy electronic flashcards are just what they sound like. One side contains a question, and the other side shows the answer.

PDF of Glossary of Terms

We have included an electronic version of the Glossary in `.pdf` format. You can view the electronic version of the Glossary with Adobe Reader.

Adobe Reader

We've also included a copy of Adobe Reader so you can view PDF files that accompany the book's content. For more information on Adobe Reader or to check for a newer version, visit Adobe's website at `www.adobe.com/products/reader/`

System Requirements

Make sure your computer meets the minimum system requirements shown in the following list. If your computer doesn't match up to most of these requirements, you may have problems using the software and files. For the latest and greatest information, please refer to the ReadMe file located in the downloads.

- A PC running Microsoft Windows 98, Windows 2000, Windows NT4 (with SP4 or later), Windows Me, Windows XP, Windows Vista, or Windows 7
- An Internet connection

Using the Study Tools

To install the items, follow these steps:

1. Download the `.ZIP` file to your hard drive, and unzip to an appropriate location. Instructions on where to download this file can be found here: `www.sybex.com/go/mcsawin2012r2`
2. Click the `Start.EXE` file to open up the study tools file.
3. Read the license agreement, and then click the Accept button if you want to use the study tools.

The main interface appears. The interface allows you to access the content with just one or two clicks.

Troubleshooting

Wiley has attempted to provide programs that work on most computers with the minimum system requirements. Alas, your computer may differ, and some programs may not work properly for some reason.

The two likeliest problems are that you don't have enough memory (RAM) for the programs you want to use or you have other programs running that are affecting installation or running of a program. If you get an error message such as "Not enough memory" or "Setup cannot continue," try one or more of the following suggestions and then try using the software again:

Turn off any antivirus software running on your computer. Installation programs sometimes mimic virus activity and may make your computer incorrectly believe that it's being infected by a virus.

Close all running programs. The more programs you have running, the less memory is available to other programs. Installation programs typically update files and programs; so if you keep other programs running, installation may not work properly.

Have your local computer store add more RAM to your computer. This is, admittedly, a drastic and somewhat expensive step. However, adding more memory can really help the speed of your computer and allow more programs to run at the same time.

Customer Care

If you have trouble with the book's companion study tools, please call the Wiley Product Technical Support phone number at (800) 762-2974. 74, or email them at `http://sybex.custhelp.com/`

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A

A (host) records
  addressing space, 60
  format, **88**, **585**
  IPv6 addresses, 425
  stub zones, 76, 574
A Recursive Query To Other DNS Servers option, 105, 602
AAAA records
  format, 88, 585
  IP addresses, 60
  IPv6 addresses, 425
AAS (application assignment scripts), 330, 790
Access-Based Enumeration (ABE)
  description, **212**
  DFS, 540
access control entries (ACEs)
  delegating, 254
  description, **369**, *369*, **712**, *712*
access control for networks, **667–668**
access control lists (ACLs), **369**, *369*, **712**, *712*
Access-Denied Assistance remediation, **887–889**, *888–889*
access rules and policies in DAC, **881–884**, *882–883*
Account Lockout Duration option, 373, 720
Account Lockout Threshold option, 373, 720
Account Operators group, 363, 706
Account tab for user templates, 274
accounts
  AD RMS, 1092
  audit policies for, 545
  computer, **283–284**, *359*, 703
  managed service and virtual, **708–709**
Accounts: Rename Administrator Account option, 373, 720
acknowledge messages in DORA process, 117
Action screen for BranchCache, 864–865, *864*
Activate instance %s command in ntdsutil, 743
Activate Scope page, 134, *135*
activating
  DHCPv6 scopes, **944–945**, *944–945*
  IPv4 scopes, 134, *135*, **149–151**
  superscopes, **940**
Active Directory, **166**
  account integration, 377
  AD CS. *See* Active Directory Certificate Services (AD CS)
  AD Delegation, 314, 771
  AD DS, 4, 8, 700, 741, 915
  AD FS. *See* Active Directory Federation Services (AD FS)
  AD LDS, 8, **178**, 741, 915
  AD RMS. *See* Active Directory Rights Management Services (AD RMS)
  administrative tools, **192–193**
  application data partitions, **195–200**, *197*, *200*
  authorizing DHCP for, **126–128**, ***127–128***
  backups. *See* backups
  command prompt commands, **290–291**
  domains. *See* domains
  Event Viewer, **190–192**

Active Directory (*continued*)
exam essentials, **203**, **747**, **1038–1040**
file system verification, **166–171**, *167*, *170–171*
forests. *See* forests
GPOs linked to, **309**, **764**
installing, **179–190**, *181–189*
network connectivity, **171–174**
objects. *See* objects in Active Directory
OUs. *See* organizational units (OUs)
recycle bin, **741–742**, **914–915**
replication. *See* replicas and replication
review questions, **204–206**, **748–750**, **1041–1043**
security. *See* security
sites. *See* sites
subnets
creating, **991–993**, *992*
description, **987–988**, *987*
summary, **203**, **746**, **1037–1038**
testing, **193–195**, *194*
trees
creating, **1017–1023**, *1018–1023*
joining to forests, **1023–1024**
planning, **1013**
single, **1014–1015**, *1015*
WSUS clients, **498**
Active Directory Administrative Center
DAC, 878, *878*, 880, *880*, 882, 885
description, **193**
working with, **289–290**, *289*
Active Directory Certificate Services (AD CS), **7–8**
CAs. *See* certificate authorities (CAs)
certificates. *See* certificates
configuring, **1059–1061**, *1059–1060*
cryptography, **1049–1051**, *1050*
description, 4, 700
installing, **1055–1058**, *1056*
new features, **1047–1048**
roles, **1048–1049**
Active Directory Claims Provider Trusts Wizard, 1084, 1086
Active Directory Delegation (AD Delegation), 314, 771
Active Directory-detached failover clusters, 852
Active Directory Domain Services (AD DS), 8
description, 4, 700
recycle bin, 741, 915
Active Directory Domains and Trusts tool
description, 193
name suffix routing, 1034
single-master operations, 728, 1028–1029
trust management, 1032
UPN suffixes, 1033
Active Directory Federation Services (AD FS), **1070**
attribute stores, **1073**
certificates, **1082**, *1082*
claims. *See* claims in AD FS
compound authentication, **1088–1089**
configuring, **1078–1082**, *1079–1080*
description, 8
endpoints, **1072–1073**
exam essentials, **1105**
federated identity management, **177**
installing, **1076–1078**, *1077*
new features, **1074–1076**
relying parties, **1072**, **1083**
review questions, **1106–1108**
services, **1074**
summary, **1104–1105**
upgrading, **1078**
Active Directory Installation Wizard
DNS servers, 180
domain controllers, 1024–1025
promotion process, 1017
trees, 1017
Active Directory Integrated DNS, **74–75**, *74*, **201–202**, *202*, **572–573**, *572*
Active Directory Lightweight Directory Services (AD LDS)
description, 8
forests, **178**
recycle bin, 741, 915

Active Directory Migration Tool (ADMT)
functions, **274–275**
OUs, 253
Active Directory Module for PowerShell, 193
Active Directory Object Type page, 264
Active Directory Rights Management Services (AD RMS), 9
backups, **1100–1101**
connection points, **1097**
considerations, **1091–1093**
description, 4–5, 700
encryption, 372, 719
exam essentials, **1105**
installing, **1094–1097**, *1094–1096*
overview, **1091**
requirements, **1093**
review questions, **1106–1108**
summary, **1104–1105**
templates, **1098–1099**, **1104**
trusts, **1101–1104**
Active Directory Service Interfaces (ADSI), **197**
Active Directory Service Interfaces Editor (ADSI Edit), 723, *724*, **745**, **917–918**
Active Directory Sites and Services tool
connection objects, 999–1000, *999*
description, 193
global catalog servers, 1004, 1035
intersite replication, 996
replication topology, 1009
sites
configuring, 993
creating, 988–990, *989–990*
links, 998
moving objects between, 1000–1001, *1000*
subnets, 991
UGMC, 1036
Active Directory Users and Computers tool
applications, 334, 795, 804
audit logs, 873
audit policies, 546
computer accounts, 283
delegating control, 370–371, 717–718, 770
description, 193, *194*
dial-in access, 680
file sharing, 211
filtering, 280–281, *281*
foreign security principals, 367, *367*, 710, *710*
GPOs, 312–313, 769
groups, 280, 361, 704
objects
creating, **270–273**, *271*
finding, 287–288
moving, 282
properties, 277
sections, 268
OUs, 253, 255, 257, 263, 714–716, *715*
passwords, 725
permissions, 368, 711
queries, 287
RSoP, 345, 805
shared folders, 287, 549
single-master operations, 728, 1028–1029
user templates, 717
ActiveX controls in Performance Monitor, 501
activity retries in Windows PowerShell, 236
AD CS. *See* Active Directory Certificate Services (AD CS)
AD CS Configuration Wizard, 1059, *1060*
AD Delegation (Active Directory Delegation), 314, 771
AD DS (Active Directory Domain Services), 8
description, 4, 700
recycle bin, 741, 915
AD FS. *See* Active Directory Federation Services (AD FS)
ad hoc mode in wireless access, 663–664

AD LDS (Active Directory Lightweight Directory Services)
  description, 8
  forests, **178**
  recycle bin, 741, 915
AD RMS. *See* Active Directory Rights Management Services (AD RMS)
Add-AdfsFarmNode cmdlet, 1081
Add-AdfsProxy cmdlet, 1081
Add-BCDataCacheExtension cmdlet, 867
Add Counters dialog box, 503–504, *503*
Add Exclusion dialog box, 144, *145*
Add Exclusions page
  DHCPv6 scopes, 944
  IP scopes, 138, *138*, 152
  multicast scopes, 942
Add Exclusions And Delay page, 130, *131*, 135
Add Features screen
  DNS, 92, 591
  failover clusters, 835
  RDC, 543
  Remote Access role, 634
  SNMP, 522
Add Group Or User dialog box, 313, *314*, 770, *770*
Add IP Address dialog box, 968, *969*
Add Issuance Authorization Claim Rule Wizard, 1088
Add New Quota Entry dialog box, 225
Add Node Wizard, 840
Add Printer page, 227
Add Printer Wizard, 226, 285, *285*
Add Roles And Features Wizard
  AD CS, 1056, *1056*
  AD FS, 1076
  AD RMS, 1094, *1094*
  Backup utility, 736, *737*, 910, *910–911*
  BitLocker, 536, *536–537*
  BranchCache, 865, *866*
  DFS, 540
  DHCP, 122, *123*
  failover clusters, 835–837, *835*
  FSRM, 531
  Hyper-V, 448, *448–449*
  IPAM, 964, *965*
  iSNS, 47, *47*, 893, *893*
  MPIO, 42, *42*
  NFS data store, 859
  NLB nodes, 825, *825*
  Remote Access role, 633, *633*
  roles, 7, *8*
  SNMP, 522
  trees, 1018–1020, *1019*
  Windows Server Migration Tools, 11
  WSUS servers, 489–490, *489–490*
Add Roles Wizard for Hyper-V, 447, *447*
Add Servers dialog box, 966, *966*
Add ShadowStorage command in vssadmin.exe, 217, 924
Add Storage Wizard, 861, *861*
Add To Superscope option, 940
Add Upgrade Package dialog box, 336, 797
Add-WdsDriverPackage cmdlet, 481
Add-WindowsFeature cmdlet, 189
Additional Options screen for trees, 1022
additive permissions, 222
address pools in DHCP, **121**
Address Resolution Protocol (ARP), 390
address space in IPv6 addresses, **423**
addresses. *See* IP addresses
adjunct policies, 673
administration
  Active Directory tools, **192–193**
  delegating control of, **253–254**
  WDS, 479
administrative templates, 299–300, 754–755
Administrative Tools window, 185–186
Administrator accounts, 365, 707
administrator password, 24
Administrators group, 363–364, 706
ADMT (Active Directory Migration Tool)
  functions, **274–275**
  OUs, 253

ADMX Central Store, **300**, **756**
adprep command
  description, 180
  forests, 1023
  recycle bin, 741, *915*
  user attributes, **179**
ADSI (Active Directory Service Interfaces), **197**
ADSI Edit (Active Directory Service Interfaces Editor), 723, *724*, **745**, **917–918**
Adsiedit.msc tool, 745, 918
Advanced Attributes dialog box, 732, *732*, 906, *906*
Advanced Audit Policy settings, 377, 548, 874
Advanced Boot Options screen, 925, *925*
Advanced Deployment dialog box, 339, *339*, 799, *800*
Advanced Encryption Standard (AES), 663
Advanced Policies tab for resources, 849–850, *850*
Advanced Security Settings dialog box, 649
Advanced Sharing dialog box, 551
Advanced Sharing page, 224
Advanced tab
  DHCP scope, 149
  DNS recursion, *959*, *960*
  IPv4 server properties, 141, *142*
  IPv6 server properties, 143, *144*
  netmask ordering, 85
  printers, 230–231, *231*
  queries, 288, *288*
advertising in Microsoft Windows Installer, **328–329**, **789**
AES (Advanced Encryption Standard), 663
AGDLP acronym, **280**
aging in DNS, **103–104**, **600–601**
alerts in Graph tab, **509–510**
alias records, **89**, **586**
all-1s broadcasts, *396*
All Servers Task Details screen, 1020
All Servers Task Details And Notifications screen, 491, *491*
allocate-on-write transactional model, 168
Allow Administrator Interaction When The Private Key Is Accessed By The CA option, 1051
allow filtering in DHCP, **950**, *950*
Allow Macros right, 1099
Allow The Connection option, 864
Allow These Protocols option, 649
Allow Users To Continue To Use The Software, But Prevent New Installations option, 341, 803
Allow Zone Transfers option, 98, *595*
Allowed EAP Types attribute, 672
Allowed RODC Password Replication group, 366, 710
Always Callback To option, 669
Always Dynamically Update DNS A And PTR Records option, 154, 613
Always Install With Elevated Privileges option, 804
Analytical logs, 956–957
ANI information, 667
anonymous authentication, 1063
AnonymousAddress value, 429
anycast addresses
  DHCP scope, 137
  IPv6 addresses, 428–429
Appearance tab in Performance Monitor, 508–509, *509*
application assignment scripts (AAS), 330
application data partitions
  creating, **196–198**, *197*
  ntdsutil for, **197–200**, *200*
  overview, **195–196**
  replicas, **198**
Application layer in TCP/IP model, 390, *391*
Application Server, 9

applications
assigning, 331, 334–335, 791–792, 794–796
categories, **340**, *341*, **801–802**, *801*
compatibility, 168
failover clustering, **841–843**, *842–843*
legacy, 370
publishing, **651–652**
repairing, **328**, **789**
virtualization, 441
applications and services logs, 518, *518*
AppLocker feature, **333**, **794**
Apply Static Routes option, **669–670**
Approve-WdsClient cmdlet, 481
ARP (Address Resolution Protocol), 390
Assign Drive Letter Or Path page, 35
Assign Memory page, 462
Assign Static IP Addresses option, **669**
assigning applications, **331**, **334–335**, **791–792**, **794–796**
Attribute Editor tab
passwords, 725
user principal names, 272
attribute stores, **1073**
au domain, 62, 560
Audit Directory Service Access Properties dialog box, 375, 545, 872
Audit Log File Path setting, 141
audit policies and auditing, **373–374**, **543**
`Auditpol.exe` command, **376**, **873–874**
certificate authority policies, **1068**
description, 701
enhanced features, **874**
features, 376–377, 547–548, 874–875
implementing, **374–375**, **544–545**, **871–872**
overview, **374**, **544**, **870–871**
viewing information, **546–547**, **873**
Auditors role, 1093
`Auditpol.exe` utility
commands, **376**, **546–547**, **873–874**
GPOs, **306**, **760–761**
authentication
AD FS, **1076**, **1088–1089**
domain controllers, **1006**
key-based renewal, **1063**
multiple domains, **1031**, 1033
networks, **664–666**, **689–690**
pass-through, **652**
RADIUS, **688**
remote access profiles, **681–682**, *681*
verifying, **1008**
VPN clients, 649
Windows, **689**
Workplace Join feature, 1090
Authentication Methods pane, **681–682**, *681*
Authentication Type attribute, 672
Authoritative restore command in ntdsutil, 743
authoritative restores, **740**, **913–914**
authorization
AD FS claims, **1084**, *1085*
DHCP, 126–128, *127–128*
relying-party trusts, 1083
Authorization Rules field, 1083
auto-enrollment for group policy certificates, **1062**
autoconfiguration in DHCPv6, 943
automated failure recovery, 236
automated installations, **328**, **789**
Automatic Approvals option, 492
automatic certificate renewal, 1048
automatic stop and start in virtual machines, 465
automatic updates, **485–486**
configuring, **486**, *486–487*
for software, **337**, **798**
WSUS clients, 498
Automatic Virtual Machine Activation (AVMA), 442–443
Automatically Use My Windows Logon Name And Password (And Domain If Any) option, 649

availability
high. *See* high availability
Resilient File System, 168
Storage Spaces, 36
AVMA (Automatic Virtual Machine Activation), 442–443
AXFR (full zone transfers), 78, *575*

B

Background Intelligent Transfer Services (BITS) technology, 485–486
background zone loading in DNS, **81**, **579**
backup intervals in database files, **157**
Backup Once Wizard, 738–739, *738–739*, 911, *911–912*
Backup Operators group, 364, 706
Backup Or Restore Wizard, 1069
Backup utility, **731–732**, **736–739**, *737–739*, **903–906**, **910–912**, *910–912*
backup vaults in Windows Azure, **920–921**
backups
Active Directory, **903–904**
Backup utility, **731–732**, **736–739**, *737–739*, **905–906**, 910–912, *910–912*
bare-metal, **734–735**, **907–908**
database compaction, **744**, **917**
Group Policy objects, **735–736**, **909**
offline maintenance, **742–744**, **915–917**
replication, **744–745**, **917**
restoring, **735**, **739–741**, **908–909**, **913–915**
scheduling, **735**, **908**
setting up, **736–739**, *737–739*, **909–912**, *910–912*
system state data, **733–734**, **906–907**
types, **732–733**, **905–906**, *906*
AD RMS, **1100–1101**
ADSI Edit, **745**, **917–918**
certificate authorities, **1068–1069**
GPOs, **782–783**
wbadmin command, **745–746**, **918**
Windows Azure, **919–921**
bandwidth
networks, **980–981**
UGMC, 1035
Bandwidth Allocation Control Protocol (BACP), 631
Bandwidth Allocation Protocol (BAP), 631, **683**
bare-metal operating systems, 858
bare-metal restores (BMRs), **734–735**, **907–908**
basic disks, configuring, **32–34**, *33*
Basic Encryption (MPPE 40-Bit) option, 683–684
Basic Resource Health Check Interval option, 850
BCD (Boot Configuration Data), **52**, **909**
bcdedit utility, 52, **909**
Berkeley Internet Name Domain (BIND), 562
BGP (Border Gateway Protocol) routing protocol, 633
bidirectional trusts, 1030
BIND (Berkeley Internet Name Domain), 562
BIOS for virtual machines, 464
BitLocker Drive Encryption
description, 5
features, **533–536**
working with, **532–533**
BITS (Background Intelligent Transfer Services) technology, 485–486
Block Policy Inheritance option, **304**, **758–759**
blocks of IP addresses, **968–969**, *969*
BMRs (bare-metal restores), **734–735**, **907–908**
Boot Configuration Data (BCD), **52**, **909**

boot environment in Windows Deployment Services, 479
boot files, backing up, 733, 907
boot.ini file, 52
`Bootcfg.exe` utility, 909
booting
advanced options, **925**, *925*
boot logging, **926–928**, *927*
menu modes, **928–929**
Safe Mode, **925–926**
from VHD, **52**
Windows Recovery Environment, **928**
Border Gateway Protocol (BGP) routing protocol, 633
BranchCache technology
description, 5
distributed cache mode, **862–865**, *863–864*
enhanced features, **868**
hosted mode, **865–866**, *866*
PowerShell for, **866–867**
storage, **862**
bridgehead servers
creating, **1001–1002**, *1001–1002*
working with, **985**, *985*
bring your own device (BYOD) applications, 652, 1089
broadcast addresses, 396, 425
browsing for connectivity tests, **174**
Built-In container, 268
built-in domain local groups, **363–365**, *363*, *365*, **705–707**, *706*, *708*
business continuity. *See* disaster recovery (DR)
business needs, multiple domains for, **1011**
BYOD (bring your own device) applications, 652, 1089

C

CA Database dialog box, 1060
ca domain, 62, 560
CA Type dialog box, 1059
cache locking in DNS, **83**, **580–581**, **956**
caches
BranchCache, 868
DNS, **70**, **567–568**
UGMC, 361, 704, **1006**
caching-only servers, **94–95**, *94*, **591–592**, *592*
Callback Control Protocol (CBCP)
PPP, 623
remote access, 666–667
Callback Options settings, **669**
Called Station Id attribute, 672
Caller ID, 667
Calling Station Id attribute, 672
canonical name (CNAME) records, **89**, **586**
CAs. *See* certificate authorities (CAs)
categories for applications, **340**, *341*, **801–802**, *801*
CAU (Cluster-Aware Updating), **851**
CBCP (Callback Control Protocol)
PPP, 623
remote access, 666–667
CCP (Compression Control Protocol), 623, 631
CDPs (CRL distribution points), 1055
Central Policy tab, 885, *885*
CEP (Certificate Enrollment Policy Web Server), 1049
Cert Publishers group, 366, 709
certificate authorities (CAs)
description, **1048**
enterprise, **1051–1052**, *1052*
functions, 320, 776
hierarchy, **1049–1051**
names, **1061–1062**, *1061*
policy auditing, **1068**
private keys, **1051**
server backups, **1068–1069**
site names, **1068–1069**
subordinate, 1051–1052, *1052*
Certificate Enrollment Policy Web Server (CEP), 1049
Certificate Enrollment Web Services (CES), 1049

Certificate field, 1083
Certificate Publishers, 320, 776
Certificate Request dialog box, 1060
Certificate Revocation dialog box, 1067
certificate revocation lists (CRLs), 1049, 1054–1055
Certificate Service DCOM Access group, 364, 707
Certificate Template Management Console, 1065, *1066*
certificates
  AD CS, 1059
  AD FS, **1082**, *1082*
  auto-enrollment, **319–321**, *321*, **776–778**, *778*, **1062**
  CAs. *See* certificate authorities (CAs)
  CSP/KSP ordering, **1064**
  key archive and recovery, **1069–1070**
  key-based renewal, **1063**
  online responders, **1055**
  relying-party trusts, 1083
  renewal enforcement, **1063–1064**
  revocation, 1054–1055, **1067**
  templates
    compatibility, **1064–1065**
    creating, **1065**, *1066*
    description, 777
    overview, **1064**
  validation, **1054–1055**
  validity periods, **1054**
CertificateThumbprint option, 1081
CES (Certificate Enrollment Web Services), 1049
chained installation for Windows Update, 485
Challenge Handshake Authentication Protocol (CHAP), 44, 623
Change service account command in ntdsutil, 743
child domains, 1014, *1014*
Choose A Local Or Network Printer page, 285
Choose A Printer Port page, 227, 285
Choose A Server Authentication Certificate For SSL Encryption screen, 1097
Choose Classifications screen, 495
Choose Disk Format screen, 458
Choose Disk Type page, 458
Choose Upstream Server screen, 494
CIDR (Classless Inter-Domain Routing), 395, **419–420**
Cipher command, **538–539**
circular logging in Performance Monitor, 510
claims-aware agents, 1074
claims in AD FS
  authorization, **1084**, *1085*
  descriptions, **1073**
  model, **1075–1076**
  overview, **1070–1071**
  providers, **1071**
  rules
    description, **1073**
    pass-through, **1084–1087**, *1085–1087*
    transform, **1083–1084**
Class A networks, subnetting, **417–418**, **420**
Class B networks, subnetting, **415–416**, **420**
Class C networks, subnetting, **410–415**, **419–420**
Class D addresses, **941**
Class D networks, 151
classes
  DHCP clients, **147–149**
  IP addresses, **395–398**
  resource records, 86, 584
Classification tab, 884, *884*
classifications
  DAC, 884, *884*
  FSRM, 530, 869
Classless Inter-Domain Routing (CIDR), 395, **419–420**
Clear-BCCache cmdlet, 867
Clear-History cmdlet, 237
Client Friendly Name attribute, 672
Client IP Address attribute, 672
Client Vendor attribute, 672

clients
Active Directory testing from, **193–195**, *194*
connectivity tests, 172
DHCP scope, 147
DNS, *65*, *563*
DNSSEC, **84**, **582**
forcing GPO updates, **765–766**
PPP, 623
preparation in WDS, **29**, **483–484**
RADIUS, **677**
VPNs, **644–650**, *645–646*, *648*, *650–651*
WSUS, **496–499**
cloning
databases, **542**
domain controllers, **1006–1007**
CLR (common language runtime), 235
Cluster-Aware Updating (CAU), **851**
Cluster Shared Volumes (CSV), **850**
clustered applications, 830
clusters
AD RMS, 1092, 1100
failover. *See* failover clustering
NLB nodes, **826–829**, *826–828*
cmdlets, 235, 240
CNAME (canonical name) records, **89**, **586**
collections in IPAM, **972**
Color Management tab, 232
COM+ class registration database, backing up, 734, 907
com domain, 62, 560
Comment field for printers, 228
common language runtime (CLR), 235
Common Name screen, 723
communities in SNMP, 522
compacting
databases, **158**, **744**, **917**
virtual hard disks, 460
compatibility in certificate templates, **1064–1065**
Compatibility tab, 1064
Completing The New Scope Wizard page, 138, *139*
compound authentication, **1088–1089**
Compression Control Protocol (CCP), 623, 631
compression in NTFS file system, 218, *218*
computer accounts
resetting, **283–284**
security, 359, 703
computer certificates in GPOs, **319–321**, *321*, **776–778**, *778*
Computer Management
dial-in access, 680
differencing hard disks, 457–458
disk configuration, 171
dynamic disks, 33
initializing files, 32
network adapters, 172
shadow copies, 216, 922, *922*
SNMP, 522
volume sets, 34
computer names, 77, *575*
Computer Network Options settings, 318, *775*
Computer Selection page, 345, *345*, 806, *806*
computers and computer objects
description, 269
Group Policy, **300**, 754
offline domain joins, **275**
properties, **278**
WSUS servers, 492
Computers container, 268
conditional forwarding in DNS, 102, *599*
conditions in DAC, 877
configSDDL command in WinRM, 235
configurable settings command in ntdsutil, 743
configuration database in AD RMS, 1100
Configure A Service Or Application Wizard, 842, 844

Configure AD RMS Cluster Key Storage screen, 1096
Configure Authentication Methods page, 675, 686
Configure Automatic Updates Properties dialog box, 498
Configure Constraints page, 675, 686
Configure Device - WAN Miniport (PPTP) dialog box, 636, *636*
Configure DHCP Options page, 131, *132*, 135
Configure Disk page, 458
Configure Failover Wizard, 946, *947–948*
Configure Identity Federation Support screen, 1097
Configure Networking page, 462
Configure Rule screen, 1089
Configure Server Discovery page, 967, *967*
Configure Settings page
  network access policies, 676
  VPN access policies, 686
configuring Windows Server, **208**
  disk quotas, **224–225**
  exam essentials, **242–243**
  file servers. *See* file servers
  print services, **226–233**, *227–232*
  remote management, **233–240**, *241*
  review questions, **244–246**
  summary, **241–242**
Confirm Installation Selections page, 41
Conflict Detection Attempts option, 141
Connect To Server dialog box, 1100
Connect To Upstream Server screen, 494
connection command in `ntdsutil.exe`, 199
Connection Manager, 686–687
Connection Settings dialog box, 723
connections
  AD RMS, **1097**
  creating, **999–1000**, *999*
  network security, **666–667**
  remote access, 686–687
  virtual machines, **465–466**, *466*
connectivity
  client tests, 194
  networks, **171–174**
consistency
  multiple domains, **1011**
  performance monitoring, **500–501**
contact objects, 269
Content Location Selection screen, 490
Context-Sensitive Buttons Provide Quick Access to Key Features option, 466
Control Access permission, 368, 712
Convert action for virtual hard disks, 460
Convert To Dynamic Disk dialog box, 34
CONVERT utility, 170
converting
  basic disks to dynamic, **33–34**, *33*, 460
  FAT partitions to NTFS, 170
copy backups, 733, 906
copy on write model, 168
Copy-WdsInstallImage cmdlet, 481
copying GPOs, **783**
costs, network, **981**
Counter logs in Performance Monitor, 510
counters in Performance Monitor, **503**
CPU requirements in Hyper-V, 447
Create A New Failover Relationship page, 947
Create A New Private Key option, 1060
Create Child permission, 368, 712
Create Claim Type dialog box, 878, *878*
create command
  ntdsutil, 199
  WinRM, 234
Create Or Join An AD RMS Cluster screen, 1095
Create Shadow command in `vssadmin.exe`, 217, 924
Create Virtual Switches screen, 448
Credentials screen, 1059
CRL distribution points (CDPs), 1055
CRLs (certificate revocation lists), 1049, 1054–1055

cross-forest trusts, 1030–1031
cryptographic mode in AD RMS, 1092, 1096
Cryptographic Mode screen, 1096
Cryptographic Operators group, 364, 707
Cryptographic Service Provider/Key Service Provider (CSP/KSP) ordering, **1064**
cryptographic service providers (CSPs), 1049–1050
cryptography in AD CS, **1049–1051**, *1050*. *See also* encryption
CSV (Cluster Shared Volumes), **850**
`csvde.exe` utility, 274, 290
custom views in Event Viewer, 518–519, *518*
Customize Message For Access Denied Errors dialog box, 888, *888*

D

DAC. *See* Dynamic Access Control (DAC)
daily backups, 733, 906
dashboard, cluster, 853
Data Collector Sets in Performance Monitor, **502**
data integrity in Resilient File System, 168
Data Protection Manager (DPM) application, **919–921**
data store, backing up, 733, 907
Data tab in Performance Monitor, 507, *508*
database mounting tool, **744**, **916**
databases
  AD RMS, **1100–1101**
  compacting, **158**, **744**, **917**
  DFS, **542–543**
  DHCP, **156–158**
  DNS zones, **72–73**, **570–571**
  IPAM, **972**
Day And Time Restrictions attribute, 672
Dcdiag command, 290
DCM (Desired Configuration Manager), 823
DDNS (Dynamic DNS) standard, **65–66**, *67*, **563–565**, *564*
  database population, **67**, *68*, *565–566*, *565*
  DHCP integration with, **153–155**, *155*, **612–614**
deactivating
  DHCP scopes, **149–151**
  superscopes, **940**
Debug Logging tab, 106, *107*, 602, *603*
Debug logs, *956–957*
Debugging Mode option, 928
decentralized administration, multiple domains for, **1012**
decimal points (.) in IP addresses, *59*, *557*
Default Domain policy, 723
Default Package Location setting, 339, *799*
Default Routing class, 149
Default Stores screen, 449
defaults
  gateways, 132, *133*
  packages, **338–340**, *338–339*, **799–800**, *799–800*
  subnet masks, 403
defragmentation of databases, **744**, **917**
defunct schema classes and attributes, 177
delay in DHCP scope, 130, *131*
Delegated Domain Name page, 101, *598*
delegation of control
  administrative, **253–254**
  DNS, **959**
  DNS zones, **100–101**, **597–598**
  GPOs, **313–314**, *314*, **770–771**, *770*
  IPAM, **971**, *972*
  OUs, **263–267**, *264–266*
  Storage Spaces, 36
  users and groups, **370–371**, **717–719**
  zones, **571–572**
Delegation of Control Wizard, **263–266**, *264–266*, 370, 717–718
Delete Child permission, 368, 712
delete command
  ntdsutil, 199
  WinRM, 234

Delete Shadows command in `vssadmin.exe`, 217, 924
Delete ShadowStorage command in `vssadmin.exe`, 217, 924
Delete Tree permission, 369, 712
deleting
  objects, 278, **282–283**
  OUs, **260–261**, *260–261*
  superscopes, 150, **940**
  virtual machines, **465**, *465*
deletions, backups for, 903–904
Demand-Dial Routing Connections (Inbound And Outbound) option, 637
demoting domain controllers, **1024–1025**
Denied RODC Password Replication group, 366, 710
deny filtering in DHCP, **950**, *950*
Deny-WdsClient cmdlet, 481
dependencies
  in AD FS, **1075**
  in failover clustering, **847–848**, *848*
dependency viewers, 846–847, *847*
Deploy Software dialog box, 335, 795
Deployment Configuration screen, 183
Deployment tab for software, 338–339, *339*, 799–800, *799*
deprecated features, **12–15**
deprovisioning objects, 278
descriptions for organizational units, 252
Desired Configuration Manager (DCM), 823
desktop virtualization, 441
Details tab
  RSoP, 347, *348*, 808, *809*
  Task Manager, 513, *513*
device claim types in DAC, **875–879**, *876–879*
Device Registration Service (DRS), 1090
device unique identifiers (DUIDs), 943
devolution in DNS, **84**, **582**
DFS. *See* Distributed File System (DFS)
DFS Replication (DFSR), **986**
`Dfsrdiag.exe` tool, **986**
DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
DHCP Management Console
  DHCP failover, 946
  DHCPv6 scopes, 944–945
  DNS registration, 952
  filtering, 950
  multicast scopes, 941
  name protection, 950
  superscopes, 940
dhcp.mdb database, 157
dhcp.tmp file, 157
DHCP User Classes dialog box, 148
dial-in access, restricting, **680**
Dial-In tab, 668, *669*
Dial-Up Networking (DUN)
  infrastructure, **621–623**
  overview, **621**
  Point-to-Point Protocol, **623–624**
Dialing Options settings, **647**
differencing virtual hard disks, 457
differential backups, 733, 906
digital certificates. *See* certificates
DirectAccess technology, **653**
  infrastructure, **655–656**
  operation, **655**
  prerequisites, **654**
  vs. virtual private networks, **653**
directed broadcasts, 396
Direction Of Trust page, 1032
directory services database, 1100
Directory Services Restore Mode (DSRM), 735, 908
Directory Services Restore Mode option, 928
Disable Automatic Restart On System Failure option, 928
Disable-BC cmdlet, 867
Disable-BCDowngrading cmdlet, 867
Disable Driver Signature Enforcement option, 929
Disable Dynamic Updates For DNS PTR Records option, 952

Disable-WdsBootImage cmdlet, 481
Disable-WdsDriverPackage cmdlet, 482
Disable-WdsInstallImage cmdlet, 482
Disabled option in Group Policy, 299, 754
disabling objects, 278
disaster recovery (DR), 730, 821, **902**
  backups. *See* backups
  boot options, **925–929**, *925*, *927*
  domain controllers for, 1024
  exam essentials, **933**
  review questions, **934–936**
  shadow copies, 921–924, *922–924*
  site-level fault tolerance, **929–931**, *931*
  Startup Repair tool, **932**
  summary, **933**
  system protection, **902–903**
disaster recovery plans (DRPs), 1024
Discard A And PTR Records When Lease Is Deleted option, 154–155, 613, 950
Disconnect-WdsMulticastClient cmdlet, 482
discover step in DORA process, 116
Discovery tab, 891, *891–892*
Discovery Domain Sets tab, 48, *49*
Discovery Domains tab, 48, 894, *894*
Discretionary Access Control List (DACL) option, 784
disk drives
  configuring, **32–34**, *33*
  encrypting
    BitLocker, **532–537**, *536–537*
    Encrypting File System, **537–539**
  Hyper-V, 447
  initializing, **31–32**
  virtual machines, 464. *See also* virtual hard disks (VHDs)
Disk Management program
  disk conversions, 33–34
  Hyper-V, 458, *458*
  initializing disk drives, 32
  mount points, 40
  NTFS partitions, 171
  shadow copies, 216, 922
  VDS, 51
  volume sets, 34–35, 39, *40*
disk mirroring, **36–37**
disk quotas, **168–169**, **224–225**
disk striping with parity, **37**
DiskPart command, 51, *51*
DiskRAID command, 51
Disks To Convert dialog box, 34
`Dism.exe` utility, 30
Display Name field, 1083
Display Progress While Connecting option, 647
distributed cache mode in BranchCache, **862–865**, *863–864*
Distributed File System (DFS), **539**
  advantages, **539–540**
  databases
    cloning, **542**
    recovering, **542–543**
  optimizing, **543**
  replication, **540–542**, **986**
  types, **540–541**, *541*
distribution groups
  description, 279
  security, **359–360**, **703**
Djoin command, 291
DNS. *See* Domain Name System (DNS)
DNS Manager
  DNSSEC, 954–955, *955*
  GlobalName zones, 961
  recursion, 959
DNS Notify, **78**, *79*, **576**, *577*
DNS screen, 185
DNSCmd utility, **113–114**, **610**
DNSKEY records, 953–954
DNSLint utility, **111–112**, **608–609**
DNSSEC (Domain Name System Security Extensions), **83–84**, **581–582**, **953–955**, *954–955*
DnsUpdateProxy group, **85**, **582–583**
Do Not Enroll Certificates Automatically option, 1062
Do Not Log Any Events option, 640

Do Not Use A Migration Table option, 784
Domain Admins group, 366, 709
Domain Computers group, 366, 709
Domain Controller: Allow Server Operators To Schedule Tasks option, 373, 721
Domain Controller Options screen, 1022
domain controllers
  adding, **1024**
  authentication, **1006**
  cloning, **1006–1007**
  demoting, **1024–1025**
  placing, **1003**, **1025–1026**
  RODCs, 20
    DNS, **82**, **580**
    local groups, 366, 710
    replication, **1002–1003**
Domain Controllers group, 268, 366, 709
Domain Guests group, 366, 709
domain local groups
  built-in, **363–365**, *363*, *365*, **705–707**, *706*, *708*
  description, 279
  security, **361**, **704**
Domain Name And DNS Servers page, 132, *133*, 136
Domain Name System (DNS), **58–59**
  Active Directory integration, **74–75**, *74*, **201–202**, *202*, **572–573**, *572*
  advantages, **80–86**, **578–583**
  aging and scavenging, **103–104**, **600–601**
  cache locking, **83**, **580–581**, **956**
  caching-only servers, **93–94**, *93*, **591–592**, *592*
  delegated administration, **959**
  description, *5*
  devolution, **84**, **582**
  dynamic
    database population, **67**, *68*, **565–566**, *565*
    overview, **65–66**, *67*, **563–565**, *564*
  exam essentials, **159–160**, **614–615**, **973**
  forwarding, **101–102**, **599**
  installing, **91–93**, *92–93*, **588–591**, *589–590*
  introduction, **556–557**
  IP addresses, **59–64**, *60*, *63*, **557–562**, *558*, *561*
  load balancing with round robin, **93**, **591**
  logging, **956–959**, *957–958*
  monitoring, **104–107**, *105–107*, **601–603**, *601–603*
  netmask ordering, **960–961**
  non-dynamic, **65–66**, **563–565**
  queries, **68–70**, *69*, **566–568**, *566*
  record types, **86–91**, **583–588**
  recursion, **959**, *960*
  registration, **952–953**, *952*
  resource records, **102–103**, **599–600**
  review questions, **161–163**, **616–618**, **974–976**
  security. *See* security
  servers, clients, and resolvers, **64–65**, 192, **562–563**
  socket pools, **82**, **580**, **955**
  summary, **158**, **614**, **973**
  TCP/IP for, **556–557**
  troubleshooting
    DNSCmd, **113–114**, **610**
    DNSLint, **111–112**, **608–609**
    ipconfig, **112–113**, **609**
    log files, **114–115**, **611**
    non-Microsoft DNS servers, **115–116**, *115*, **611–612**, *611*
    nslookup, **108–111**, **604–607**
    overview, **107–108**, **603–604**
    root zones, **115**, **611**
  zones, 64, **71–72**, **569**
    Active Directory, **74–75**, *74*, **572–573**, *572*
    delegating, **100–101**, **571–572**, **597–598**
    DNS Notify, **78**, *79*, **576**, *577*
    dynamic updates, **98–100**, *99–100*, **595–597**, *596–597*
    GlobalName, **77**, **575**, **961**

Domain Name System (DNS) (*continued*)
primary, **72–73**, **569–570**
properties, **95–98**, *96–97*, **592–595**, *593–594*
secondary, **73–74**, **571**
signing, *953–954*
statistics, **84–85**, **962**
stub, **75–77**, *76*, **573–575**, *574*
transfers and replication, **77–80**, *80*, **575–578**, *577*
Domain Name System Security Extensions (DNSSEC), **83–84**, **581–582**, **953–955**, *954–955*
Domain Naming Masters, 724, 1027
Domain Profile tab in Windows Firewall, 377, *378*
domain users and groups, **360**, **702**
Domain Users group, 366, 709
domains
controllers. *See* domain controllers
functional levels, **174–176**
GPOs, 303, 758
joining, **194–195**
multiple. *See* multiple domains
names, 64, 560–561
namespaces, 61–62, *559*
operations masters, **725–726**, **1027–1028**
promotion process, **1017**
renaming, 177
structure, **178**
trees. *See* trees in Active Directory
DORA process, **116–117**
dotted decimal notation, *59*, *557*
down-level servers, configuring, **238–239**
DPM (Data Protection Manager) application, **919–921**
drivers
printers, 231
provisioning in WDS, 479
DRPs (disaster recovery plans), 1024
DRS (Device Registration Service), 1090
DS behavior command in ntdsutil, 743
Dsacls command, 291
Dsadd command, 291
Dsamain command
description, 291
recovery process, **744**, **916**
Dsdbutil command, 291
Dsget command, 291
DsGetSiteName API, 1068
Dsmgmt command, 291
Dsmod command, 291
Dsmove command, 291
Dsquery command, 291
DsQuerySitesByCost API, 1068
DSRM (Directory Services Restore Mode), 735, 908
Dsrm command, 291
dual stack in IPv6 addresses, **431**, *431*
DUIDs (device unique identifiers), 943
DUN (Dial-Up Networking)
infrastructure, **621–623**
overview, **621**
Point-to-Point Protocol, **623–624**
duplicate content in BranchCache, 868
DVD drives in virtual machines, 464
Dynamic Access Control (DAC), **875**
Access-Denied Assistance remediation, **887–889**, *888–889*
access rules and policies, **881–884**, *882–883*
enabling, **876–877**, *876–877*
file classification, **884–885**, *884–885*
policy changes and staging, **885–887**, *886–887*
resource properties and lists, **879–881**, *880–881*
user and device claim types, **875–879**, *876–879*
uses, **371–372**, **719**
Dynamic Bandwidth Control Using BAP Or BACP option, 631
dynamic disks, configuring, **32–34**, *33*
Dynamic DNS (DDNS) standard, **65–66**, *67*, **563–565**, *564*
database population, **67**, *68*, *565–566*, *565*
DHCP integration with, **153–155**, *155*, **612–614**

Dynamic Host Configuration Protocol (DHCP), 66, 564
advantages, **118**
allow and deny filtering, **950**
authorizing, **126–128**, *127–128*
description, 5
DHCP snap-in, **125–126**, *126*
disadvantages, **118–119**
DNS registration, **952–953**, *952*
DORA process, **116–117**
enforcement in network access, **690**
exam essentials, **159–160**, **973**
failover, **946–949**, *947–949*
high availability, **946–950**, *947–950*
hot standby, **156**
installing, **122–125**, *123–125*
leases
duration, 131, *131*, 138
options, **119–120**
releases, **118**
renewals, **117–118**
load sharing, **156**
name protection, **950–951**, *951*
overview, **116**
relay agent, **122**
review questions, **161–163**, **974–976**
scope
activating and deactivating, **149**
database files, **156–158**
details, **120–122**
DHCPv6, **943–945**, *944–945*
dynamic DNS with, **153–155**, *155*, **612–614**
exclusions. *See* exclusions in DHCP
IPv4 addresses, **129–136**, *129–135*, **146–149**, *148*
IPv6 addresses, **136–138**, *136–139*
multicast, **151–152**, *153*, **940–943**, *942–943*
multiple servers, **155–156**
properties, **138**, **140**
reservations, **145–146**, *145*
server properties, **140–143**, *141–143*
split scopes, **949**
superscopes, **149–151**, **939–940**
summary, **158**, **973**
dynamic least queue depth, 41
Dynamic Memory feature in Hyper-V, 443
dynamic quorum management, **834**
Dynamic Updates field, 96, 593
dynamic updates in DNS zones, **98–100**, *99–100*, **595–597**, *596–597*
dynamic volumes in NTFS file system, **169**
dynamic witness in failover clustering, **852**
dynamically expanding virtual hard disks, 456
Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates option, 154, 613
Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients option, 154–155, 613, 950

E

E-mail Notifications option, 492
EAP (Extensible Authentication Protocol)
networks, **665**
VPNs, 626
EAP-RADIUS authentication, **665**
EAP-Transport Level Security (EAP-TLS), **665**
EAP types in networks, 665
Easy Print Driver, **233**
Edit Claim Rules For Claimapp window, 1088–1089
Edit Disk tool, 459
Edit right, 1099
Edit Rights right, 1099
Edit Virtual Hard Disk Wizard, 459–460, *459*
edu domain, 62, 560
Effective Permissions tab, 771
EFI (Extensible Firmware Interface), 31
EFS (Encrypting File System)
features, **537–539**
NTFS file system, 218–219, *219*

802.1X standard, 666, 690
elevation-of-privileges attacks, 1030
Enable-AdfsDeviceRegistration cmdlet, 1090
Enable-BCDistributed cmdlet, 867
Enable-BCHostedClient cmdlet, 867
Enable-BCHostedServer cmdlet, 867
Enable-BCLocal cmdlet, 867
Enable Bidirectional Support option, 230
Enable Broadcast Name Resolution option, 632
Enable Certificate Templates dialog box, 1066–1067
Enable Default Route Advertisement option, 633
Enable DNS Dynamic Updates According To The Settings Below option, 154, 613, 950
Enable IPv4 Forwarding option, 632
Enable IPv6 Forwarding option, 632
Enable Low-Resolution Video option, 928
Enable-WdsBootImage cmdlet, 482
Enable-WdsDriverPackage cmdlet, 482
Enable-WdsInstallImage cmdlet, 482
Enabled option in Group Policy, 299, 754
encapsulation
  PPP, 624
  VPNs, **627–628**, *627*
Encrypt Contents To Secure Data option, 219
Encrypting File System (EFS)
  features, **537–539**
  NTFS file system, 218–219, *219*
encryption, **532**
  AD CS, **1049–1051**, *1050*
  BitLocker Drive Encryption, **532–537**, *536–537*
  BranchCache, 868
  Encrypting File System, 218–219, *219*, **537–539**
  NTFS file system, **168–169**
  remote access profiles, **683–684**, *683*
  VPN clients, 649
  VPN tunnels, 625
  wireless access, 663
Encryption pane, 683–684, *683*
End IP Address field, 140, 144
End IPv6 Address field, *137*
endpoints in AD FS, **1072–1073**
Enforce Password History option, 372, 720
Enforced option in GPOs, **304**, **759**
Enhanced Session Mode in Hyper-V, 442
Enroll Certificates Automatically option, 1062
Enterprise Administrators group, 1093
Enterprise Admins group, 366, 709
enterprise certificate authorities, **1051–1052**, *1052*
enumerate command in WinRM, 234
error messages in nslookup, **110–111**, **605–606**
Event Logging tab, 105, *105*, 601, *601*
event logs
  DNS, 105, *105*, 601, *601*
  replication, **1008**
  RRAS, **641–642**
Event Properties dialog box, 516–517, *517*
Event Viewer
  for Active Directory installation, **190–192**
  audit events, 546, 873
  DNS logs, 957, *958*
  working with, **515–519**, *516–519*
evicting cluster nodes, 840
exclusions in DHCP
  adding, 130, *131*, 138, *138*
  DHCPv6 scopes, 944
  multicast scopes, 152, 942
  overview, **120–121**
  ranges, **144–145**, *145–146*
Expand action for virtual hard disks, 460
expiration dates of certificate authorities, 1054
Expires After field in DNS zones, 97, 594
Export-AdfsDeploymentSQLScript cmdlet, 1081
Export-BCSecretKey cmdlet, 867
Export-DfsrClone cmdlet, 542
Export right, 1099
Export Trusted Publishing Domain dialog box, **1103**
Export-WdsBootImage cmdlet, 482

Export-WdsInstallImage cmdlet, 482
exporting
NPS policies, **678–679**
trusted publishing domains, **1103**
Windows Firewall policies for, **383–384**
expression-based audit policies, 377, 548, 874–875
Extended User Interface 64-bit (EUI-64) format, **429**
Extensible Authentication Protocol (EAP)
networks, **665**
VPNs, 626
Extensible Firmware Interface (EFI), 31
extensions, mapping, **340**, **800–801**
external forwarding in DNS, 101–102, *599*
external networks in Hyper-V, 454
external trusts, **1030**
Extract right, 1099

F

failback in MPIO, 41
failover clustering, **830**
clusters
application settings, **844–848**, *845–848*
creating, **839–840**, *840*
nodes, **840**
validating configuration, **834–839**, *835–838*
description, 5, *9*
DHCP, **946–949**, *947–949*
features, **850–853**
quorums, **833–834**, *833*
requirements, **831–833**
resource properties, **847–850**, *848–849*
roles, **840–844**, *841–843*
failover in MPIO, 41
FAST (Flexible Authentication Secure Tunneling), 1088
FAT (File Allocation Table), 218
FAT partitions, 170
fault tolerance. *See* high availability
FDE (Full Disk Encryption), 534
Features On Demand, **30–31**, **895–896**
Features screen
DHCP, 122
IPAM, 964
federated identity management, **177**
federated trusts, 1101
Federation Metadata endpoint, 1072
Federation Service Proxy, 1074
FederationServiceName option, 1081
FederationServiceTrustCredentials option, 1081
Fibre Channel feature
Hyper-V, 442
vs. iSCSI, 890
overview, 49–50
File Access Settings or Exit Virtual Machine Connection option, 466
File Allocation Table (FAT), 218
File and Storage Services, 9
File Server Resource Manager (FSRM), **868–870**
Access-Denied Assistance, 889, *889*
description, 5
features, **530–531**
installing, **531–532**, 869
file servers, **552–554**
Access-Based Enumeration, **212**
Active Directory object availability, **210–212**, *210–211*, **548–551**
audit policies, **543–548**
DFS, **539–543**, *541*
encryption
BitLocker, **532–537**, *536–537*
Encrypting File System, **537–539**
exam essentials, **551**
FSRM, **530–532**
offline files, **212–215**, *213–215*
overview, **208–209**
permissions, **218–224**, *218–223*
review questions, **552–554**
sharing folders, **209**
summary, **551**
VSS, **215–217**

File Sharing dialog box, 287, *549*
file systems
DFS. *See* Distributed File System (DFS)
encryption, **168–169**
NTFS, **168–171**, *170–171*, **218–224**, *218–223*
verifying, **166–171**, *167*, *170–171*
filename extensions, mapping, **340**, **800–801**
files
classification in DAC, **884–885**, *884–885*
conflicts in Microsoft Windows Installer, **328**, **789**
screening in FSRM, 869
files command in ntdsutil, 743
Filter Options dialog box, 280, *281*
filtering
AD objects, **280–282**, *281*
DHCP, **950**, *950*
GPOs
inheritance, **315**, *315–316*, **771–772**, *772*
security groups, **311–313**, *311*, **768–769**, *768*
Find Users, Contacts, And Groups dialog box, 287–288, *288*
fine-grained password policies, **723–725**, *724*
firewalls
verifying configuration, **1008**
Windows. *See* Windows Firewall
fixed size virtual hard disks, 457
flat addressing, **394**
flexibility in multiple domains, 1012
Flexible Authentication Secure Tunneling (FAST), 1088
flexible host isolation, 690
floppy disks for virtual machines, 464
folders
offline
configuring, **212–215**, *213–215*, **549–551**
vs. folder redirection, **323**, **780**
redirecting, **322–323**, *323*, 778–780, *779*
shared, **286–287**, **549**
sharing, **209**
footprint in Server Core version, 19
Force Policy Inheritance option, **304**, **759**
forcing GPO updates, **764–766**
foreign security principals, 268, **367**, **710**
forests
authentication, 1031
domain functional levels, **176–178**
joining trees to, **1023–1024**
operations masters, **724**, **1026–1027**
planning, **1013**
working with, **1015–1017**, *1016*
Format-table cmdlet, 237
Format Volume page, 35
Forward right, 1099
forwarding in DNS, **101–102**, **599**
ForwardProxy option, 1081
FQDNs. *See* fully qualified domain names (FQDNs)
Framed Protocol attribute, 672
`FsConfigWizard.exe` file, 1079
FSMO roles
assigning, **727–728**, **1028–1029**
managing, **725–726**, **1026**
seizing, **728–729**
FSRM. *See* File Server Resource Manager (FSRM)
full backups, 733, 906
Full control right, 1099
Full Disk Encryption (FDE), 534
Full Volume Encryption (FVE), 534
full zone transfers (AXFR), 78, 575
fully qualified domain names (FQDNs)
AD RMS, 1092
certificate authorities, 1061
description, 1012
host contacts, 63, 560
FVE (Full Volume Encryption), 534

G

gateways, default, 132–133, *133*
GC (global catalog)
replication enhancements, 177
trees and forests, 1013, **1016–1017**

GC (global catalog) servers
managing, **1034–1035**
placing, **1004**
General tab
certificate templates, 1065
DNS zones, **95–96**, **592–593**
IPv4 server, 141, *141*
IPv6 server, 143, *143*
iSNS, 48, 894
multicast scopes, 152, *153*, 942, *942*
OUs, 261, *262*
Performance Monitor, **506–507**, *506*
printers, 228, *228*
user templates, 273–274
VPN clients, **645–646**, *645*
Generic Routing Encapsulation (GRE) headers, 628
geoclustering, **839**
Get-ADDomain cmdlet, 729
Get-ADForest cmdlet, 729
Get-BCClientConfiguration cmdlet, 867
Get-BCContentServerConfiguration cmdlet, 867
Get-BCDataCache cmdlet, 867
Get-BCStatus cmdlet, 867
get command in WinRM, 234
Get-Date cmdlet, 237
Get-DnsServerStatistics cmdlet, 84
Get-event cmdlet, 237
Get-Fsrm cmdlets, 531, 869–870
Get Help And Support option, 485
Get-Help cmdlet, 237
Get-NetIPAddress cmdlet, 237, 239
Get-NetIPConfiguration cmdlet, 239
Get-NetIPInterface cmdlet, 239
Get-WdsBootImage cmdlet, 482
Get-WdsClient cmdlet, 482
Get-WdsDriverPackage cmdlet, 482
Get-WdsInstallImage cmdlet, 482
Get-WdsInstallImageGroup cmdlet, 482
Get-WdsMulticastClient cmdlet, 482
Get-WindowsFeature cmdlet
AD CS, 1058
AD FS, 1078
description, 237
global catalog (GC)
replication enhancements, 177
trees and forests, 1013, **1016–1017**
global catalog (GC) servers
managing, **1034–1035**
placing, **1004**
global groups
description, 280
predefined, **365–367**, **709–710**
security, **361**, **704**
global object access auditing, 376–377, **547**, 874
global unicast addresses, **428**
Global Update Manager (GUM)
failover clustering, **852**
settings, **931**
GlobalName zones, **77**, **575**, **961**
gov domain, 62, 560
GPMC. *See* Group Policy Management Console (GPMC)
GPPs (Group Policy preferences), 300, 755
`gpresult.exe` utility, **349–350**, **809–810**
GPTs (GUID Partition Tables), **31–32**
`GPUpdate.exe` command, **765–766**
GPUs (graphical processing units) in Hyper-V, 452
Graph tab
logs and alerts, **509–510**
Performance Monitor, 507–508, *508*
Graph view in Performance Monitor, **504**, *504*
graphical deployment for AD FS, **1079–1080**, *1080*
graphical processing units (GPUs) in Hyper-V, 452
Graphical User Interface (GUI)
installation with, 17, **22–24**, *23–24*
MBSA, **520–521**
GRE (Generic Routing Encapsulation) headers, 628
Group Membership Evaluation command in ntdsutil, 743
group objects, 269

Group Policy and Group Policy Objects (GPOs), 298
automatic updates, **337**, **798**
backing up, **782–783**
certificates, **319–321**, *321*, **776–778**, *778*, **1062**
creating, **305–309**, *307–308*, **760–763**, *762–763*
delegating control of, **313–314**, **770–771**, *770*
description, 9
exam essentials, **351–352**, **812–813**
folder redirection, **322–323**, *323*, 778–780, *779*
importing and copying, **783**
inheritance, **303–304**, **315**, *315–316*, **758–759**, **771–772**, *772*
item-level targeting, **781–782**
levels, **302–303**, **757–758**
linking, **309**, **764**
Loopback Policy, **318**, **774–775**
managing, **309–310**, **766–767**, *767*
migration tables, **784**
network configuration, **318–319**, *319*, **775–776**, *775*
offline folders, 212, 549
OUs, **255**
overview, **298–299**, **753–754**
PowerShell, **324**, **780–781**
restoring, **736**, **783**, **909**
review questions, **353–355**, **814–816**
script policies, ***316–318***, *317*, **773–774**, *773–774*
security
filters, **311–313**, *311*, **768–769**, *768*
settings, **301–302**, **372–373**, **719–722**, *722*, **756–757**
settings, **299–301**, *301*, **754–756**, *755*
slow link detection, **333–334**, **794**
software deployment. *See* software deployment
strategy, **304–305**, **759–760**
summary, **350–351**, **811**
troubleshooting, **344–350**, *345–348*
updates, forcing, **764–766**
Windows Firewall, **383**
WMI, **310–311**, **767**
WSUS clients, 496, **498**
Group Policy Creator Owners group, 366, 709
Group Policy Management Console (GPMC)
backups, 736, **909**
BranchCache, 863–864
certificates, 321, 711, 1062
DAC, 876
GPOs, **305–306**, 309, 736, **760**, 764–765
item-level targeting, 782
migration tables, 784
offline folders, **213–214**, 550
publishing applications, 334, 795
restoring GPOs, 783, 909
security policies, 721
software policies, 333, 794
software updates, 336, 796
Group Policy Management Editor
BranchCache, 863–864
DAC, 876, *876*
GPOs, 307, 721, *722*, 762
Group Policy Management Tool, 888
Group Policy preferences (GPPs), 300, *755*
Group Policy Results Wizard, 345–346, *345–346*, 805–806, *806–807*
groups. *See also* Group Policy and Group Policy Objects (GPOs)
AD RMS, 1093
creating, **280**
delegating control of, **370–371**, **717–719**
properties, **279–280**
purpose, **279**
security
built-in domain local groups, **363–365**, *363*, *365*, **705–707**, *706*, *708*
creating, **714–716**, *715*
foreign security principals, **367**, *367*, **710**, *710*
predefined global groups, **365–367**, **709–710**
scope, **360–361**, *362*, **703–704**, *705*
types, **359–360**, **702–703**

Guest accounts, 365, 707
Guests group, 364, 707
GUI (Graphical User Interface)
installation with, 17, **22–24**, *23–24*
MBSA, **520–521**
GUID Partition Tables (GPTs), **31–32**
GUM (Global Update Manager)
failover clustering, **852**
settings, **931**

H

hardware
Hyper-V, **446–447**, *447*
virtual machines, 463–464
hardware failures, backups for, 903
hash algorithms, 1050
HBAs (host bus adapters), 44, 890–891
HCAP (Host Credential Authorization Protocol) User Groups attribute, 673
headers in IPv6 addresses, 423–424
Help And Support dialog box, 926
Help command in ntdsutil, 743
helpmsg command in WinRM, 235
hierarchies
certificate authorities, **1049–1051**
IP addresses, **393–394**
multiple domains, **1011**
OUs, 252
high availability, **821**
Active Directory, 982
Active Directory Integrated zones, 75, 573
components, **821–822**
DHCP, **946–950**, *947–950*
domain controllers, **1024**
exam essentials, **854**
failover clustering. *See* failover clustering
foundation, **822–823**
local databases, 73, 570
NLB, **824–830**, *825–829*
patches, **823–824**
review questions, **855–856**
summary, **853–854**
Histogram view in Performance Monitor, **505**, *505*
historical information, backups for, 730, 904
history in performance monitoring, **501**
Hold Mismatched Documents option, 231
home folders in file servers, 209
host (A) records
addressing space, 60
format, **88**, **585**
IPv6 addresses, 425
stub zones, 76, 574
host addresses in IP addresses, 395
host bus adapters (HBAs), 44, 890–891
Host Credential Authorization Protocol (HCAP) User Groups attribute, 673
host records, **88**, **585**
hosted mode in BranchCache, 862, **865–866**, *866*
hostnames, resolving. *See* Domain Name System (DNS)
HOSTS files, 60, *60*, *557–559*, *558*
hot standby in DHCP, **156**
HTTP.SYS feature, **1074–1075**
Hyper-V Recovery Broker, 853
Hyper-V role, 9, 440
architecture, **445–446**, *445*
description, 5–6, 700
exam essentials, **469–470**
fault tolerance, **930–931**, *930*
features, **441–443**
Hyper-V Manager, **450–451**, *451*
installing, **447–450**, *448–449*
Integration Components, **468**
operating system support, **443–445**
requirements, **446–447**, *447*
review questions, **471–472**
Server Manager, **450**, *450*
settings, *452*
summary, **469**
virtual hard disks, **455–461**, *458–459*
virtual machines, **461–468**, *463*, *465–467*
virtual switches, **453–456**, *454–455*
virtualization overview, **440–441**
hypervisors, 445

I

IaaS, 189–190
IANA (Internet Assigned Numbers Authority), 391
ICANN (Internet Corporation for Assigned Names and Numbers), 63, 560–561
IDE controllers in virtual machines, 464
Identifiers field in relying-party trusts, 1083
identity command in WinRM, 234
Idle Time Before Hanging Up menu, 647
IDNs (Internationalized Domain Names), 1048
If All The Restart Attempts Fail, Begin Restarting Again After The Specified Period option, 849
If Resource Fails, Attempt Restart On Current Node option, 849
If Resource Fails, Do Not Restart option, 849
If Restart Is Unsuccessful, Fail Over All Resources In This Service Or Application option, 849
IGMP multicast clusters, 828
image types in WDS, 479
Immediately Uninstall The Software From Users And Computers option, 341, 802
Import-BCCachePackage cmdlet, 867
Import-BCSecretKey cmdlet, 867
Import-DfsrClone cmdlet, 542
Import-Module cmdlet, 189, 237
Import-WdsBootImage cmdlet, 482
Import-WdsDriverPackage cmdlet, 482
Import-WdsInstallImage cmdlet, 482
importing
  GPOs, **783**
  NPS policies, **679–680**
  objects, **274**
  Windows Firewall policies for, **383–384**
inbound rules in Windows Firewall, **381–383**, *381–382*
Include Windows Logon Domain option, 647
inconsistency in multiple domains, **1011**
incremental backups, **733**, **906**
incremental zone transfers (IXFR), 78, *575*
InetOrgPerson object, 269
information commands for IPv6 addresses, **433**
Infrastructure Masters, **727**, **1027–1028**
infrastructure mode in wireless access, 663–664
inheritance
  GPOs
    controlling, **315**, *315–316*, **771–772**, *772*
    overview, **303–304**, **758–759**
  OUs, **252–254**, 267
Initialize-ADDeviceRegistration cmdlet, 1090
initializing disks, **31–32**
Inspect Disk tool, 459
Install-ADDSForest cmdlet, 189
Install-AdfsFarm cmdlet, 1081
Install-AdfsStand-alone cmdlet, 1081
Install The Printer Driver page, 227, 285
Install Windows dialog box, 932
Install-WindowsFeature cmdlet
  AD CS, 1058
  features, 30
  FSRM, 531, 869
  Server Core, 21
  Windows Server Migration Tools, 11
installation of Windows Server
  exam essentials, **53**
  Features On Demand, **30–31**
  with GUI, **22–24**, *23–24*
  planning, **7**
    migrating roles and features, **10–11**
    NIC Teaming, **22**
    reduced roles and features, **12–15**
    server roles, **7–10**, *8*
    type, **17–21**
    versions, **16–17**
  review questions, **54–56**
  Server Core, **24–26**
  storage. *See* storage
Installation Options page, 462
Installation Progress screen, 182
Installation Results page, 41
Installation User Interface Options settings, 339, 800

installing
Active Directory, **179–190**, *181–189*
AD CS, **1055–1058**, *1056*
AD FS, **1076–1078**
AD RMS, **1094–1097**, *1094–1096*
Backup utility, **736–739**, *737–739*, **910–912**, *910–912*
DHCP, **122–125**, *123–125*
DNS, **91–93**, *92–93*, **588–591**, *589–590*
FSRM, **531–532**, **869**
Hyper-V, **447–450**, *448–449*
IPAM, **964–966**, *965–966*
NLB nodes, **825–829**, *825–829*
patches, **823–824**
Remote Access role, 633–634, *633*
WDS, **481–483**
Windows Server. *See* installation of Windows Server
Installing Printer page, 227, 285
Installing Windows screen, 25
instances in Performance Monitor, **503**
int domain, 62, 560
Integrated Services Digital Network (ISDN), **622**
Integrated Windows authentication, 1076
Integration Components in Hyper-V, **468**
integration in IPv6 addresses, **430–433**, *431*, *433*
Interactive Logon: Do Not Display Last User Name option, 373, 721
internal networks in Hyper-V, 454
Internationalized Domain Names (IDNs), 1048
Internet
connectivity tests, 172
overview, **980**
Internet Assigned Numbers Authority (IANA), 391
Internet Corporation for Assigned Names and Numbers (ICANN), 63, 560–561
Internet layer in TCP/IP model, 390–391
Internet Protocol (IP), 390, 980. *See also* IP addresses
Internet Protocol Security (IPsec), **424**
encryption in failover clustering, **852–853**
enforcement in network access, 690
policies in Windows Firewall, **384**
tunneling, **629**
Internet service providers (ISPs)
subnets, **417**
wide area networks, 980
Internet Small Computer System Interface (iSCSI), **43–44**
configuring, **44–46**, *45–46*
target and initiator, **890–892**, *891–892*
Internet Storage Name Service (iSNS), **46–49**, *47–49*, **892–895**, *893–895*
intersite replication, **995–996**, *996*
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), **432**
intrasite replication, **995**
inverse queries in DNS, **70**, **567**
Invoke-command cmdlet, 237
invoke command in WinRM, 234
Invoke-GPUpdate cmdlet, 765
IP (Internet Protocol), 390, 980. *See also* IP addresses
IP Address Management (IPAM), 6
collections, **972**
databases, **972**
delegating control of, **971**, *972*
description, 701
exam essentials, **973**
installing, **964–966**, *965–966*
IP address space utilization, **970**, *971*
IP blocks and ranges, **968–969**, *969*
migrating to, **971**
review questions, **974–976**
server discovery, **967**, *967*
summary, **973**
IP Address Range page, 130, *130*, 135, 152, 942
IP addresses, **393**
form, **59–64**, *60*, *63*, **557–562**, *558*, *561*
hierarchical, **393–394**
IPAM, **968–969**, *969*
IPv4. *See* IPv4 addresses
IPv6. *See* IPv6 addresses
network classes, **395–398**
space utilization, **970**

IP addresses (*continued*)
structure, **394–395**
subnets. *See* subnets
IP-based connections in remote access services, **631–634**, *631–633*
IP Control Protocol (IPCP), 623–624
IP datagrams in virtual private networks, 628
IP Settings pane, 682, *683*
IPAM. *See* IP Address Management (IPAM)
ipconfig utility
connectivity tests, 172, *173*
IPv6 addresses, 427, *428*, 432–433, *433*
lease options, **119–120**
options, **112–113**, **609**
IPsec Defaults option, 384
IPsec Exemptions option, 384
IPsec Setting tab, 379, *380*
IPsec Tunnel Authorization option, 384
IPv4 addresses
DHCP integration with dynamic DNS, **153–155**, *155*, **612–614**
IPv6 address interoperability, **424–425**
scope
DHCP, **129–136**, *129–135*
multicast, **151–152**, *153*
options, **146–149**, *148*
superscopes, **149–151**
server properties, **141–142**, *141–142*
IPv4 tab, 631–632, *631*
IPv6 addresses, **422**
assigning, **427**, *427–428*
concepts, **423–425**
DHCP scope, **136–138**, *136–139*
DNS, **81–82**, **579–580**
dual stack, **431**, *431*
format, **425–426**, *426*
history and need, **422**
information commands, **433**
integration/migration, **430–433**, *431*, *433*
server properties, **143**, *143*
subnets, **433–434**
tunneling, **431–433**, *433*
types, **428–430**
IPv6 tab, 632–633, *632*
iscsicli command, 893
ISDN (Integrated Services Digital Network), **622**
item-level targeting in GPOs, **781–782**
Items To Back Up screen, 1069
iterative queries, **68**, **566**
IXFR (incremental zone transfers), 78, *575*

J

J50.chk file, 157
J50.log file, 157
JET (Joint Engine Technology) databases, 157
Join Microsoft Update Improvement Program screen, 494
joining
domains, **194–195**
trees to forests, **1023–1024**
Joint Engine Technology (JET) databases, 157
jp domain, 62, 560

K

KCC (Knowledge Consistency Checker), 198, 988, 997
Kerberos authentication
AD FS, 1076, 1088
description, 6, 701
networks, 666
Key Distribution Center Service accounts, 365, 707
key masters in DNSSEC, 954
Key Recovery Agent template, 1069–1070
Key Signing Key (KSK) key, 954
key storage providers (KSPs), 1049
keyboard in Hyper-V, 453
keys
AD CS, **1051**
archive and recovery, **1069–1070**
certificate renewal, **1063–1064**
length, 1050

Knowledge Consistency Checker (KCC), 198, 988, *997*
krbtgt accounts, 365, 707
KSK (Key Signing Key) key, 954
KSPs (key storage providers), 1049

L

L2TP (Layer 2 Tunneling Protocol), 626
L2TP/IPsec tunneling, **629**
LANs (local area networks)
  connectivity tests, 172
  overview, **980**
large-scale clusters, **850–851**
Last Known Good Configuration option, 928
Launch NPS option, 670, *671*
Layer 2 Tunneling Protocol (L2TP), 626
LBFO (load balancing and failover)
  overview, **21**
  virtual machines, **466–467**, *467*
LCP (Link Control Protocol), 623, 631
LDAP (Lightweight Directory Access Protocol)
  configuring, 197
  description, 8
LDAP policies command in ntdsutil, 743
ldifde utility
  Active Directory, 291
  importing objects, 274
LDP tool, **197**, *197*
Lease Duration page, 131, *131*, 135, 152
leases in DHCP
  duration, 131, *131*, 138
  options, **119–120**
  releases, **118**
  renewals, **117–118**
legacy applications, 370
license terms screen, 23, 25
licenses for software, **325**, **786**
Lifetime tab for multicast scopes, 152, *153*, 943, *943*
Lightweight Directory Access Protocol (LDAP)
  configuring, 197
  description, 8
limitations of organizational units, 252
linear logging in Performance Monitor, 510
Link Control Protocol (LCP), 623, 631
Link Control Protocol (LCP) Extensions option, 631
Link layer in TCP/IP model, 390, *391*
link-local addresses, **428–429**
Linked Group Policy Objects tab, 310, 766
linked value replication, 177, 984
links
  creating, 987, *987*
  GPOs, **309**, **764**
  replication, **997–999**, *997*
list command in ntdsutil, 199
List Contents permission, 369, 712
List In The Directory option, 229
List Object permission, 369, 712
List Providers command in `vssadmin.exe`, 217, 924
List Shadows command in `vssadmin.exe`, 217, 924
List ShadowStorage command in `vssadmin.exe`, 217, 924
List Volumes command in `vssadmin.exe`, 217, 924
List Writers command in `vssadmin.exe`, 217, 924
live migration, 453, 830
load balancing. *See also* Network Load Balancing (NLB)
  with round robin, **94**, **591**
  secondary zones, 73, 571
load balancing and failover (LBFO)
  overview, **21**
  virtual machines, **466–467**, *467*
load sharing in DHCP, **156**
local area networks (LANs)
  connectivity tests, 172
  overview, **980**
Local Computer Policy tool, **305**, **760**

local databases in DNS zones, **72–73**, **570–571**
Local File Logging dialog box, 642
local group objects, 303, 757
Local Log File Properties dialog box, 641
Local Security Policy tool, 375, 545, 872
local users and groups, 360, 702
Locate Network File System page, 861, *861*
Location field for printers, 228
Location Groups attribute, 673
Lockout Duration screen, 725
Lockout Threshold screen, 725
Log All Events option, 640
Log Errors And Warnings option, 640
Log Errors Only option, 640
Log File tab, 641–642, *641*
Log Properties page, 957, *958*
logging database in AD RMS, 1100
logging mode in RSoP, **345–347**, *345–347*, **805–808**, *806–809*
Logging tab for RRAS, 640
Logman tool, **691**
logon events, auditing, 375, 544–545, 872
Logon/Logoff Scripts settings, 316, 773
logs
  audit events, **873**
  boot, **926–928**, *927*
  DNS
    configuring, **956–959**, *957–958*
    creating, **114–115**, **611**
    event, 105, *105*, 601, *601*
  Event Viewer, 192, **518**, *518*
  Graph tab, **509–510**
  replication, **1008**
  RRAS, **639–643**, *641–642*
Loopback Policy for GPOs, **318**, 773
loopback test addresses, 396

M

MADCAP (Multicast Address Dynamic Client Allocation Protocol), **151**, **941**
mail exchanger (MX) records, **90**, **587**
maintenance in Server Core version, 19
Managed By tab, 262, *262*
Managed Service Accounts (MSAs)
  container, 268
  description, 6, 701
  working with, **708–709**
management
  auditing, 375, 872
  FSRM, 530
  multiple domains, **1011**
  PowerShell, 236
mandatory software updates, 336, 797
mapping filename extensions, **340**, **800–801**
masks in subnets, **402–405**, *403–404*
Master Boot Records (MBRs), **31–32**
Maximum Password Age screen, 725
Maximum Strength Encryption option, 649
maximum transmission units (MTUs), 623–624
MBRs (Master Boot Records), **31–32**
MBSA (Microsoft Baseline Security Analyzer), **519–521**
`mbsacli.exe` utility, **521**
mbsasetup.msi file, 519
mean time between failures (MTBF), 730, 822, 903
mean time to recovery (MTTR), 822
Members Of tab for user templates, 273–274
memory
  Hyper-V, 447
  virtual machines, 462, 464
Merge action for virtual hard disks, 460
Merge mode Loopback Policy, 318, 774
Message security mode in AD FS, 1073
metadata cleanup command in ntdsutil, 743
Microsoft Baseline Security Analyzer (MBSA), **519–521**
Microsoft CHAPv2 (MS-CHAPv2) authentication, 665
Microsoft-developed accounting for networks, 688
Microsoft Device Specific Module (Microsoft DSM), 41

Microsoft Federation Gateway, 1101
Microsoft Management Console (MMC)
  Active Directory, **193**
  Active Directory Administrative Center, 193
  Group Policy, 299, 305
  GUI version, 17
  Hyper-V Manager, 450
  OUs, 255
  Performance Monitor, 502
  Windows Firewall with Advanced Security, 379
Microsoft Point-to-Point Encryption (MPPE) algorithm, 628
Microsoft Transformation (MST) files, 329, 790
Microsoft Update Improvement Program option, 492
Microsoft Windows Installer (MSI)
  application installation issues, **327**, **787–788**
  benefits, **327–329**, **788–790**
  description, **326–327**, **787**
  file types, **329–330**, *330*, **790**, *791*
  packages, 327, 329, 787, 790
  settings, **342–343**, *343*, **803–804**, *803*
migration
  DFS, 539
  Hyper-V, 453
  IPAM, **971**
  IPv6 addresses, **430–433**, *431*, *433*
  objects, **274–275**
  print servers, **232–233**
  roles and features, **10–11**
Migration Table Editor (MTE), 784
migration tables in GPOs, **784**
.migtable extensions, 784
mil domain, 62, 560
Minimal Server Interface, 1047
Minimum (Default) TTL field, 97, 594
Minimum Password Age screen, 724
Minimum Password Length option, 372, 720
Minimum Password Length screen, 721–723, *722*
MinShell version, 17
mirrored volumes, 34
Mixed security mode in AD FS, 1073
MMC. *See* Microsoft Management Console (MMC)
mobility in IPv6 addresses, **424**
modems, 622
monitoring
  DNS, **104–107**, *105–107*, **601–603**, *601–603*
  NAP, **691**
  replication, **744–745**, **917**, **1007**
  RRAS, **639**
  Windows Firewall, **384**
Monitoring tab, 105, *106*, 602, *602*
mount points, **40–41**
mounted drives in NTFS file system, **169**
mouse release key in Hyper-V, 453
Move-ADDirectoryServerOperationMaster Role cmdlet, 729
Move Server dialog box, 1000–1001, *1000*
moving
  database files, **158**
  objects, **282–283**, **1000–1001**, *1000*
  OUs, **260–261**, *260–261*
MPIO (Multipath I/O), **41–43**, *42–43*
MPIO Properties dialog box, 41, *41*
MPPE (Microsoft Point-to-Point Encryption) algorithm, 628
MS-CHAPv2 (Microsoft CHAPv2) authentication, 665
MS RAS Vendor attribute, 673
MSAs (Managed Service Accounts)
  container, 268
  description, 6, 701
  working with, **708–709**
MSI. *See* Microsoft Windows Installer (MSI)
MSIMaging-PSPs container, 269
MSMQ Queue Alias object, 269
MST (Microsoft Transformation) files, 329, 790
MTBF (mean time between failures), 730, 822, 903

MTE (Migration Table Editor), 784
MTTR (mean time to recovery), 822
MTUs (maximum transmission units), 623–624
Multi-valued Distinguished Name dialog box, 725
Multicast Address Dynamic Client Allocation Protocol (MADCAP), **151**, **941**
multicast addresses, 429
multicast clusters, **828**
Multicast Scope Name page, 152, 942
Multicast Scope Properties dialog box, 152, *153*
multicast scopes, **151**
  building, **152**, **941–942**
  creating, **940–941**
  MADCAP, **941**
  properties, **152**, *153*, **942–943**, *942–943*
multicasting in WDS, 479
multifactor authentication, **1088–1089**
multihomed routers, 402
Multilink And Bandwidth Allocation Protocol (BAP) pane, 682–683
Multilink Connections option, 630
multilink extensions in PPP, **624**
multimaster replication, 984
Multipath I/O (MPIO), **41–43**, *42–43*
multiple domains, **1010**
  benefits, **1010–1012**
  drawbacks, **1012–1013**
  Global Catalog servers, **1034–1035**
  Name Suffix Routing, **1034**
  operations masters
    domains, **725–727**, **1027–1028**
    forests, **725–727**, **1026–1027**
  role seizing, **728–729**
  single-master operations, **725–728**, **1026**, **1028–1029**
  trusts, **1029–1033**, *1029*, *1031*
  UGMC, **1035–1036**
  UPN suffixes, **1033**
multiple PKIs, 1053, *1053*
multiserver management, 236, 970
multisite clusters, **839**
MX (mail exchanger) records, **90**, **587**

N

N-Port Identification Virtualization (NPIV), 50
name protection in DHCP, **950–951**, *951*
name server (NS) records
  format, **87–88**, **584–585**
  stub zones, 76, 574
Name Servers page, **97**, *97*, 101, **594–595**, *594*, 598
Name Suffix Routing, **1034**
Name The Server Licensor Certificate screen, 1097
names
  certificate authorities, **1061–1062**, *1061*
  domains, 64, 177, 560–561
  objects, **282–283**
  OUs, 252
namespaces in DFS, 540
NAP (Network Access Protection)
  monitoring, **691**
  networks, **688–689**
  tasks, 141, *142*
NAS (network attached storage), **50**
NAS Identifier attribute, 673
NAS IP Address attribute, 673
NAS Port Type attribute, 673
NAT (Network Address Translation), 422, **643–644**
nbtstat command, 146
NDDNS (non-dynamic DNS), **65–66**, **564–565**
NDES (Network Device Enrollment Service), 1049
NDP (Neighbor Discovery Protocol), 429
negative cache TTL, 70, 568
neighbor discovery, 425, 429
Neighbor Discovery Protocol (NDP), 429
net domain, 62, 560
netmask ordering in DNS, **85**, **582**, **960–961**
netsh command
  IPv6 addresses, 433
  Windows Firewall, 241
Network Access layer in TCP/IP model, 390, *391*

Network Access Permission settings, 668
network access policies, **670**
attributes, **670–673**, *671–672*
creating, **673–676**, *673–675*
Network Access Protection (NAP)
monitoring, **691**
networks, **688–689**
tasks, 141, *142*
network adapters
connectivity tests, 172
virtual machines, 464
Network Address Translation (NAT), 422, **643–644**
network attached storage (NAS), **50**
network classes in IP addresses, **395–398**
network configuration for GPOs, **318–319**, *319*, **775–776**, *775*
Network Device Enrollment Service (NDES), 1049
Network File System (NFS) data store, **858–862**, *859–861*
network folders, publishing, **549**
Network Isolation in Hyper-V, 443
network layer protection in networks, **689**
Network Load Balancing (NLB)
description, 9
Hyper-V, 441
nodes, installing, **825–829**, *825–829*
purpose, **824**
upgrading, 830
Network Monitor, **511**
Network Monitor Agent, **511**
Network Policy and Access Services server role, 9
Network Policy Server (NPS)
certificates, 666
configuring, **677**
exporting, **678–679**
importing, **679–680**
network access policies, 674
policies, **678–680**
RADIUS clients, **677**
RADIUS proxy servers, **676–677**
remote access, 640, *640*, 684
templates, **678**
VPN access, 686
network printers, 226
network services
DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
DNS. *See* Domain Name System (DNS)
exam essentials, **159–160**
review questions, **161–163**
summary, **158**
WDS, **27**, **479**
network traffic
Active Directory Integrated DNS, 75, *573*
local databases, 73, *570*
subnets for, 398
Network Unlock feature, **534**
Networking tab for VPN clients, **650**, *650*
networks and networking, **662**
bandwidth, **980–981**
connectivity, **171–174**, **1007–1008**
costs, **981**
description, 6, *9*
exam essentials, **692**
remote access, **664–668**
review questions, **693–695**
security, **687–691**, *687*
summary, **691**
types, **980**
user access. *See* user access
VPNs. *See* virtual private networks (VPNs)
wireless access, **662–664**
New Class dialog box, 148
New Delegation Wizard, 101, 598
New-event cmdlet, 237
new features, **4–6**
New-Fsrm cmdlets, 531–532, 870
New GPO dialog box, 307, 762–763
New Inbound Rule Wizard
BranchCache, 863, *863–864*
Windows Firewall, 381
New Mirrored Volume Wizard, 38, *38–39*
New Multicast Scope Wizard, 152, 941
New-NetIPAddress cmdlet, 239

New Network Policy Wizard
network access policies, 671, 674
VPN access policies, 686
New Object - Group dialog box, 361
New Object - Shared Folder dialog box, 211, *211*, 287, *549*
New Object - Site dialog box, 989
New Object - Site Link dialog box, 998
New Object - Site Link Bridge dialog box, 999
New Object - Subnet dialog box, 991, *992*
New Outbound Rule Wizard
BranchCache, 864–865
Windows Firewall, 381
New Packages settings, 339, 799
New Reservation dialog box, 145, *145*
New Scope Wizard
DHCPv6 scopes, 944–945, *944*
IPv4 addresses, 129–135, *129–135*
IPv6 addresses, 136–138, *136–139*
New Spanned Volume Wizard, 35
New Superscope Wizard, 150, 940
New Trust Wizard, 1032
New Virtual Hard Disk Wizard, 457, 461
New Virtual Switch page, 455
New-WdsClient cmdlet, 482
New-WdsInstallImageGroup cmdlet, 483
New Zone Wizard, 596, *596*, 961
next-generation (CNG) providers, 1050
Next Secure (NSEC/NSEC3) records, 953
NFS Advanced Sharing page, 859, *860*
NFS (Network File System) data store, **858–862**, *859–861*
NFS Share Permissions page, 859, *859*
NIC Teaming
overview, **21**
virtual machines, **466–467**, *467*
NLB. *See* Network Load Balancing (NLB)
No Callback option, 669
No Encryption option, 684
No Encryption Allowed option, 649
No Override option, **304**, **759**
nodes
cluster, **840**
NLB, **825–829**, *825–829*
non-domain-joined computers
automatic certificate renewal, 1048
key-based certificate renewal, **1063**
non-domain servers in PowerShell, 236
non-dynamic DNS (NDDNS), **65–66**, **564–565**
non-Microsoft DNS servers, troubleshooting, **115–116**, *115*, **611–612**, *611*
nonauthoritative restores, **741**, **914**
nonmandatory software updates, 336, 797
Nonsecure setting in DDNS, 66, *565*
normal backups, 733, 906
Not Configured option, 299, 754
NPIV (N-Port Identification Virtualization), 50
NPS. *See* Network Policy Server (NPS)
NS (name server) records
format, **87–88**, **584–585**
stub zones, 76, 574
NSEC/NSEC3 (Next Secure) records, 953
nslookup command, **108–111**, **604–607**
NT Directory Services (NTDS), 988
ntbtlog.txt file, 927, *927*
NTDS Settings Properties dialog box, 1004, *1004*, 1035
NTDS Site Settings Properties dialog box, 996, *996*, 1036
ntdsutil utility
Active Directory, 291
application data partitions, **197–200**, *200*
offline maintenance, **742–743**, **915–917**
NTFS file system
overview, **168–169**
partitions, **170–171**, *170–171*
permissions, **218–224**, *218–223*
NTLMv2 (Windows NT LAN Manager), 666
NUMA spanning, 453

O

objects in Active Directory. *See also* Group Policy and Group Policy Objects (GPOs)
audit policies for, 545

auditing, 375, 872
availability, **210–212**, *210–211*, **284**, **548–551**
computer accounts, **283–284**
creating, **270–272**, *271*
exam essentials, **292–293**
filtering, **280–282**, *281*
groups, **279–280**
importing, **274**
managing, **289–290**, *289*
migrating, **274–275**
moving, renaming, and deleting, **282–283**
offline domain joins, **275**
organization, **268–269**
properties, **275–278**, *277*
publishing
printers, **284–286**, *285–286*
shared folders, **286–287**
querying, **287–289**, *288*
review questions, **294–296**
summary, **292**
types, **269–270**
user principal names, **272**
user templates, **272–274**
Observation Window screen, 725
OCSP (Online Responder), 1049, **1055**
octets in IP addresses, 59, 393, 425
offer step in DORA process, 116–117
offline domain joins for objects, **275**
offline folders
configuring, **212–215**, *213–215*, **549–551**
vs. folder redirection, **323**, **780**
offline maintenance, **742–744**, **915–917**
Offline Settings dialog box, 551
offline stand-alone certificate authorities, 1052–1053
on-demand installations, **328–329**, **789**
one-way trusts, 1030
Online Certificate Status Protocol (OCSP), 1055
Online Responder (OCSP), 1049, **1055**
operating modes in wireless access, 663
operating system support
Hyper-V, 441, **443–445**
WDS, 479
operations masters
domains, **725–726**, **1027–1028**
forests, **724**, **1026–1027**
Operations Masters dialog box, 728, 1028
Optional Encryption option, 649
Options tab for VPN clients, **646–647**, *646*
org domain, 62, 560
organizational units (OUs)
benefits, **250**
creating, **255–259**, *256–257*, *259*
delegating control of, **253–254**, **263–267**, *264–266*
GPOs, 303, 758
group policies, **255**
inheritance, **252–254**
moving, deleting, and renaming, **260–261**, *260–261*
overview, **248–249**
properties, **261–262**, *262*
purpose, **249–250**, *249*
resource grouping, **250–252**, *251*
troubleshooting, **267**
Out-file cmdlet, 237
outbound rules in Windows Firewall, **381–383**
OverwriteConfiguration option, 1081

P

packages
assigning, 331
defaults, **338–340**, *338–339*, **799–800**, *799–800*
overview, 329
properties, 330, *330*
removing, 341, *342*
restriction policies, 333
PAP (Password Authentication Protocol), **664–665**
parent-child relationships in OUs, **254**
parent domains, 1014, *1014*

partial attribute set (PAS), 1034
Partition And Configure The Disk screen, 29, **478–479**
partitions
  application data
    creating, **196–198**, *197*
    ntdsutil for, **197–200**, *200*
    overview, **195–196**
    replicas, **198**
  NTFS file system, **170–171**, *170–171*
PAS (partial attribute set), 1034
pass-through authentication, **652**
pass-through claim rules, **1084–1087**, *1085–1087*
Pass Through or Filter an Incoming Claim template, 1084
Password Authentication Protocol (PAP), **664–665**
Password Complexity screen, 724
Password History Length screen, 724
Password Replication Policy (PRP), 1003
Password Reversible Encryption Status For Users Accounts screen, 723
Password Settings objects (PSOs), 723
Password Settings Precedence screen, 723
passwords
  Active Directory, 188
  AD FS, 1076
  AD RMS, 1092, 1096, 1100
  BitLocker, **534**
  fine-grained policies, **723–725**, *724*
  key-based renewal, 1063
  objects, 271
  RODCs, 1003
  VPN clients, 648–649
PAT (Port Address Translation), 422
patch files (MSP)
  description, 329, 790
  for high availability, **823–824**
Paths screen
  Active Directory, 185
  trees, 1022
Pause option for virtual machines, 463
payload files in Features on Demand, 896
PDC Emulator Masters, **725**, **1027**
Pending Timeout option, 849
per-user access in VPNs, **684**
Performance Monitor
  monitoring decisions, **502–505**, *503–505*
  properties, **505–509**, *506–509*
  uses, **501–502**
  views, **504–505**, *504–505*
performance monitoring
  Event Viewer, **515–519**, *516–519*
  exam essentials, **524**
  guidelines, **499–501**
  MBSA, **519–521**
  Network Monitor, **511**
  Performance Monitor, **501–510**, *503–509*
  review questions, **525–527**
  SNMP, **521–523**, *523*
  summary, **523–524**
  Task Manager, **511–514**, *512–515*
performance objects, **503**
performance of domain controllers, **1024**
Performance tab in Task Manager, 512
permissions
  DAC, 879, 886–887, *886–887*
  NTFS file system, **218–224**, *218–223*
  OUs, 264–265
  printers, 232
  security, **367–369**, *367–368*, **711–712**, *711*
  shared, **220–224**, *221–223*
Permissions dialog box, 224
Permissions page, 265
Personalization option in WSUS servers, 493
Personalize Windows Update option, 485
physical GPUs in Hyper-V, 452
Pick Updates To Install option, 485
ping command, **173**, 433
PINs in BitLocker, **534**
PKI (public key infrastructure) certificates, 4
  AD CS, 700
  components, **320**, **776–777**
  hierarchy, 1051–1053, *1052*

PKI-savvy applications, 320, *776–777*
Plain Old Telephone Service (POTS), 622
planning mode in RSoP, **347**, *348*, **809**
Point-to-Point Protocol (PPP)
  connecting with, **623–624**
  encapsulation, **627–628**, *627*
  options, **630–631**, *630*
Point-to-Point Tunneling Protocol (PPTP), 626, **628–629**
pointer (PTR) records
  inverse queries, 70, *567*
  overview, **89**, **586–587**
policies
  AD RMS, **1101–1104**
  auditing. *See* audit policies and auditing
  DAC, **881–884**, *882–883*
  DAS, **885–887**, *886–887*
  network access, **670–676**, *671–675*
  NPS, **678–680**
  resources, 848, *848*
pools
  printer, 230, **233**
  socket, **82**, **580**, **955**
Port Address Translation (PAT), 422
Port Status dialog box, 643, *643*
ports
  printers, 229–230, *230*
  RRAS, **643**, *643*
  TCP/IP, **391–393**
  VPNs, **636–637**, *636*
Possible Owners option, 850
POTS (Plain Old Telephone Service), 622
PowerShell
  Active Directory, 193
  AD CS, **1057–1058**
  AD FS, **1081–1082**
  BranchCache, **866–867**
  DFS replication, **541–542**
  DNS, **85–86**
  failover clustering, 850
  FSRM, **869–870**
  GPOs, **324**, **780–781**
  remote management, **235–238**
  WDS installation, **481–483**
PPP (Point-to-Point Protocol)
  connecting with, **623–624**
  encapsulation, **627–628**, *627*
  options, **630–631**, *630*
PPP frames in VPNs, 628
PPP tab, 630–631, *630*
PPTP (Point-to-Point Tunneling Protocol), 626, **628–629**
Preboot Execution Environment (PXE) network devices, **28**, 481
precreate command in ntdsutil utility, 199
predefined global groups, **365–367**, **709–710**
predefined options in DHCP scope, 146
Predefined Rules screen, 864–865
prefixes in IPv6 addresses, 426, 429–430
Prerequisites Check screen
  Active Directory, 185
  trees, 1022, *1023*
presentation virtualization, 440
Prevent Failback option, 845
Prevent Removable Media Source For Any Install option, 343, 804
Primary Server field, *96*, *594*
primary zones, **72–73**, **569–570**
PrimaryComputerName option, 1082
PrimaryComputerPort option, 1082
principal objects in AD FS, **1075–1076**
Print and Document Services role, 9–10
Print Operators group, 364, 707
Print right, 1099
print servers, 226
print services, **226**
  failover clustering, **842–843**, *842–843*
  migrating print servers, **232–233**
  printers
    configuring, **228–232**, *228–232*
    creating and publishing, **226–228**, *227*
    Easy Print Driver, **233**
    pooling, 230, **233**
Print Spooled Documents First option, 231
`Printbrm.exe` tool, 233
Printer Migration Wizard, 233
Printer objects, 269
printer pools, 230, **233**

Printer Sharing page, 285
private keys in AD CS, **1051**, 1059
private networks
failover clustering, 832
virtual. *See* virtual private networks (VPNs)
Private Profile tab, 378, *378*
privileges
audit policies, 545
auditing use of, 375, 872
Microsoft Windows Installer, **328**, **788–789**
Processes tab in Task Manager, 512, *512*
processors in virtual machines, 464
Products And Classifications option, 492
Profile field in relying-party trusts, 1083
Profile tab for user templates, 273–274
profiles, user, **668–670**, *669*
programs, removing, **325**, **341**, *342*, **787**, **802–803**, *802*
Prohibit Rollback option, 343, 804
Promote This Server To A Domain Controller link, 183
promotion process for domains, **1017**
Prompt For Name And Password, Certificate, Etc. option, 647
Prompt For Phone Number option, 647
Protect Container From Accidental Deletion option, 257
Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2), **665–666**
provisioning
BitLocker, **533**
drivers, 479
IPAM, **964–966**, *965–966*
thin, **895–896**
PRP (Password Replication Policy), 1003
PSOs (Password Settings objects), 723
PTR (pointer) records
inverse queries, 70, 567
overview, **89**, **586–587**
public key infrastructure (PKI) certificates, 4
AD CS, 700
components, **320**, **776–777**
hierarchy, 1051–1053, *1052*
public networks, failover clustering in, 832
Public Profile tab in Windows Firewall, 379, *379*
publishing
Active Directory objects, 210
applications, **331**, **334–335**, **651–652**, **792**, **794–796**
certificate templates, **1066–1067**
printers, **226–228**, *227*, **284–286**, *285–286*
shared folders, **286–287**, **549**
PXE (Preboot Execution Environment) network devices, **28**, 481

Q

quads in IP addresses, 393
Quality of Service (QoS) for storage, **467–468**
queries
DNS, 65, **68–70**, *69*, 563, **566–568**, *566*
objects, **287–289**, *288*
zone statistics, **962**
Query Reverts command in `vssadmin.exe` utility, 924
quick migration feature in Hyper-V, 441
quickconfig command in WinRM, 235
quorums, cluster, **833–834**, *833*
quotas
disk, 168–169, 224–225
FSRM, 530, 869
NTFS file system, 218

R

RADIUS. *See* Remote Authentication Dial-In User Service (RADIUS)
RAID (Redundant Array of Independent Disks), **36–39**, *38–39*
RAID-5 volumes, 34

ranges of IP addresses, **968–969**, *969*
RDC (Remote Differential Compression) feature, **543**
read-only domain controllers (RODCs), 20
  DNS, **82**, **580**
  local groups, 366, 710
  replication, **1002–1003**
Read permission, 369, 712
realm trusts, 1030
"Reason For Access" reporting, 377, **547–548**, 874
Receive-job cmdlet, 237
Reconnect action for virtual hard disks, 460
record types
  alias, **89**, **586**
  creating, **102–103**, **599–600**
  DNS, **86**, **583**
  host, **88**, **585**
  mail exchanger, **90**, **587**
  name server, **87–88**, **584–585**
  pointer, **89**, **586–587**
  service, **90–91**, **587–588**
  start of authority, **86–87**, **583–584**
record weighting in DNS, 85, 582
recovering databases in DFS, **542–543**
recovery point objectives (RPOs), **821–822**
recovery time objectives (RTOs), **821–822**
recursive queries in DNS, **68**, **566–567**, **959**, *960*
recycle bin
  forests, **178**
  limitations, 282
  working with, **741–742**, **914–915**
Redial Attempts field, 647
Redial If Line Is Dropped option, 647
Redialing Options settings, **647**
redirecting folders, **322–323**, *323*, 778–780, *779*
Redundant Array of Independent Disks (RAID), **36–39**, *38–39*
Refresh Interval field, 96, 594
ReFS (Resilient File System), **167–168**
registry
  backing up, 734, 907
  WSUS clients, **496–497**
Relative ID (RID) Masters, **724–725**, **1027**
relay agents in DHCP, **122**
/release switch in ipconfig, 119
reliability in domain controllers, 1024
relying parties in AD FS
  certificate decryption, 1082
  claims rules, 1087
  description, **1072**
  trusts, **1083**
Remote Access class, 149
Remote Access Connections (Inbound Only) option, 637
Remote Access role, 633–634, *633*
Remote Authentication Dial-In User Service (RADIUS), **639**
  clients for NPS, **677**
  network accounting, 688
  network authentication, 688
  proxy servers, NPS as, **676–677**
Remote Desktop Services, 6, 10
Remote Differential Compression (RDC) feature, **543**
remote management, **233–234**
  down-level servers, **238–239**
  PowerShell, **235–238**
  Windows Firewall, **240**, *241*
  WinRM, **234–235**
Remote Procedure Call (RPC) protocol, 995
Remote Server Administration Tools (RSAT), 324, 781
remote storage in NTFS file system, **169**
RemoteFX in Hyper-V, 442
removable storage device auditing, 377, 548, 875
remove command in ntdsutil utility, 200
Remove-FsrmClassificationRule cmdlet, 532, 870
Remove-FsrmFileScreen cmdlet, 532, 870
Remove-FsrmQuota cmdlet, 532, 870
Remove-job cmdlet, 237
Remove-WdsBootImage cmdlet, 483
Remove-WdsClient cmdlet, 483
Remove-WdsDriverPackage cmdlet, 483
Remove-WdsInstallImage cmdlet, 483

Remove-WdsInstallImageGroup cmdlet, 483
removing
  database files, **157**
  programs, **325**, **341**, *342*, **787**, **802–803**, *802*
  replicas, **198**
renaming
  domains, 177
  objects, **282–283**
  OUs, **260–261**, *260–261*
Render Print Jobs On Client Computers option, 229
/renew switch in ipconfig, 119
Repadmin utility
  commands, **1009**
  description, 291
  purpose, **745**, **917**
repairing corrupted applications in Microsoft Windows Installer, **328**, **789**
Replace mode Loopback Policy, 318, 775
replicas and replication
  Active Directory
    application data partitions, **198**
    bridgehead servers, **1001–1002**, *1001–1002*
    changing environments, **1005**
    configuring, **994**
    connection objects, **999–1000**, *999*
    DFS, **540–542**, **986**
    intersite, **995–996**, *996*
    intrasite, **995**
    monitoring, **744–745**, **917**, **1007**
    moving objects between sites, **1000–1001**, *1000*
    overview, **981–982**
    RODCs, **1002–1003**
    server topology, **1003–1004**
    site links, **997–999**, *997*
    sites, **983–984**
    troubleshooting, **1007–1009**
    UGMC, **1006**
  DFS, **540–542**
  DNS zones, **77–80**, *80*, **575–578**, *577*
  Hyper-V, 453
Replication indicator in DNS zones, 95, 593
Replicator group, 364, 707
Reply right, 1099
Reply All right, 1099
Report view in Performance Monitor, **505**, *506*
Reporting Rollup option, 492
reports
  cluster configuration, **838–839**, *838*
  FSRM, 531, 869
Reports page in WSUS servers, 495
request messages, 117
Require BAP For Dynamic Multilink Requests option, 683
Require Encryption option, 649
reservations, IP address, **120–121**, **145–146**, *145*
Reset Account Lockout Counter After option, 373, 720
reset check boxes in Hyper-V, 453
Reset option for virtual machines, 463
Resilient File System (ReFS), **167–168**
Resize ShadowStorage command in `vssadmin.exe`, 217, 924
resolvers in DNS, 65, **563–564**
resolving hostnames. *See* Domain Name System (DNS)
resource grouping in OUs, **250–252**, *251*
resource metering in Hyper-V, 441
resource properties and lists
  DAC, **879–881**, *880–881*
  failover clustering, **847–850**, *848–849*
Resource Record Signature (RRSIG) records, 953
Responsible Person field, 96, 594
Restart The Destination Server Automatically If Required option, 536
Restartable Active Directory Services, 742, **915**
restoresubtree command, 740, 914
restoring
  Active Directory, **739–741**, **913–915**
  bare-metal, **734–735**, **907–908**
  Group Policy objects, **735–736**, **783**, **909**
  system state data, **735**, **908–909**
Restricted Groups settings, **302**, **757**

restriction policies for software, **333**, **793–794**
Resultant Set of Policy (RSoP), **344–345**, **804–805**
logging mode, **345–347**, *345–347*, **805–808**, *806–809*
planning mode, **347**, *348*, **809**
Results dialog box, 1060
Resume option for virtual machines, 463
Retry Interval field, 96, 594
Revert Shadow command in `vssadmin.exe`, 217, 924
Review And Install Updates option, 485
Review Options screen
Active Directory, 185
trees, 1022
revoking certificates, 1054–1055, **1067**
RID (Relative ID) Masters, **724–725**, **1027**
rights in AD RMS, 1099
robustness of Microsoft Windows Installer, 328, 788
RODCs (read-only domain controllers), 20
DNS, **82**, **580**
local groups, 366, 710
replication, **1002–1003**
roles and features
failover clustering, **840–844**, *841–843*
migrating, **10–11**
reduced, **12–15**
seizing, **728–729**
Roles screen, 964
root certificate authorities, 1051
root domains, 1014, *1014*, 1016
Root Hints tab, 93, *93*, 592, *593*
root servers, 64, 561–562
root zones, troubleshooting, **115**, **611**
round robin
load balancing with, **93**, **591**
MPIO, 41
round robin with subset paths, 41
route command, 433
route print command, 433
Router (Default Gateway) page, 132, *133*, 136
routers
configuring, 132, *133*
description, 981
verifying configuration, **1008**
Routing and Remote Access Services (RRAS), **620**
Dial-Up Networking, **621–624**
DirectAccess technology, **653–656**
exam essentials, **656**
IP-based connections, **631–634**, *631–633*
logging, **639–643**, *641–642*
managing, **638–639**
monitoring, **639**
NAT, **643–644**
ports, **643**, *643*
PPP options, **630–631**, *630*
RADIUS, **639**
review questions, **657–660**
summary, **656**
VPNs. *See* virtual private networks (VPNs)
Web Application Proxy, **651–652**
RPC (Remote Procedure Call) protocol, 995
RPC over IP protocol, 996
RPOs (recovery point objectives), **821–822**
RRAS. *See* Routing and Remote Access Services (RRAS)
RSAT (Remote Server Administration Tools), 324, 781
RTOs (recovery time objectives), **821–822**
Rule Type screen, 863–865, *863*
rules
AD FS, **1073**, **1083–1089**, *1085–1087*
BranchCache, 863–864, *863–864*
DAC, **881–884**, *882–883*
Windows Firewall, **381–383**, *381–382*
Run This Resource In A Separate Resource Monitor option, 850

S

Safe Mode, **925–926**
Safe Mode With Command Prompt option, 928

Safe Mode With Networking option, 928
SAML Artifact Resolution endpoint, 1072
SAML authentication for AD FS, **1076**
SAML Token (Asymmetric) endpoint, 1072
Save option for virtual machines, 463
Save A Certificate Request To File On The Target Machine option, 1060
Save right, 1099
scalability
  multiple domains, **1010**
  Resilient File System, 168
scale-out file servers, 851
scavenging in DNS, **103–104**, **600–601**
Schannel, 6, **666**, 701
scheduling
  backups, **735**, **908**
  replication, 996, *996*, 998
  shadow copies, 216, 922–923
Schema Admins group, 366, 709–710
Schema Masters, **724**, **1026–1027**
schemas for forests, **1016**
scope in DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
Scope Lease page
  DHCPv6 scopes, 944
  IPv6, 138, *139*
Scope Name page
  DHCPv6 scopes, 944
  IPv4, 130
  IPv6, 136, *136*
Scope Options dialog box, 147, *148*
Scope Prefix page
  DHCPv6 scopes, 944, *944*
  IPv6, 137
script policies for GPOs, **316–318**, *317*, **773–774**, *773–774*
scripting
  Hyper-V, 442
  WDS, 479
SCSI controllers, 464
secondary zones, **73–74**, **571**
Secure setting in DDNS, 66, *565*
Secure Only setting in DDNS, 66, *565*
Secure Sockets Tunneling Protocol (SSTS), **629**
security
  accounts, **708–709**
  ACLs and ACEs, **369**, *369*, **712**, *712*
  Active Directory features, **700–701**
  Active Directory Integrated DNS, 75, *573*
  audit policies, 6, **373–377**
  DAC, **371–372**, **719**
  delegating control, **370–371**, **717–719**
  DFS, 540
  DNS, **83**, **581**
    cache locking, **956**
    DNSSEC, **953–955**, *954–955*
    logging, **956–959**, *957–958*
    socket pools, **955**
  Event Viewer, 192
  exam essentials, **385**
  fine-grained password policies, **723–725**, *724*
  GPOs
    filters, **311–313**, *311*, **768–769**, *768*
    settings, **301–302**, **372–373**, **719–722**, *722*, **756–757**
  groups, **359**, **702–703**
    built-in domain local groups, **363–365**, *363*, *365*, **705–707**, *706*, *708*
    foreign security principals, **367**, *367*, **710**, *710*
    predefined global groups, **365–367**, **709–710**
    scope, **360–361**, *362*, **703–704**, *705*
    types, **360**, 703
  local databases, 73, 571
  networks, **664–668**, **687–691**, *687*
  new features, 10
  NTFS file system, **169**, 219–220, *220*
  overview, **358**, **699–700**
  permissions, **367–369**, *367–368*, **711–712**, *711*
  principles, **358–359**, **701–702**
  review questions, **386–387**
  Server Core version, 19
  summary, **385**
  User Account Control, **370**

user templates, **716–717**
users and groups, **714–716**, *715*
Windows Firewall, **377–384**, *378–382*
security account management command in ntdsutil, 743
security groups, **279**
security identifiers (SIDs)
deleted objects, 741, 914
description, 358
external trusts, **1030**
objects, 278, 282
security modes in AD FS, **1072–1073**
Security Policy Settings dialog box, 721
Security Support Provider Interface (SSPI), 6
security support providers (SSPs), 6
Security tab
DAC, 885
DNS, *202*
networks, 687–688, *687*
printers, **232**, *232*
VPN clients, **647–649**, *648*
security templates for Group Policy, 300, 756
seizing roles, **728–729**
Select A Password screen, 1069
Select Backup Configuration screen, 738, 912
select command in ntdsutil utility, 200
Select Condition dialog box, 671, 673, 675, *675*, 686
Select Configuration Database screen, 1095
Select Destination screen, 1018
Select Destination Server screen
Active Directory, 181
AD CS, 1056
AD FS, 1077
Backup utility, 736, 910
failover clusters, 835
Hyper-V, 448
Select Disks page, 35, 38, *39*
Select Features screen
Active Directory, 181
AD CS, 1057
AD FS, 1077
Backup utility, 736, 910
BitLocker, 536
BranchCache, 866
DFS, 540
failover clusters, 835
Hyper-V, 448
iSNS, 47, 893
MPIO, 42, *42*
SNMP, 522
WSUS servers, 489
Select GPO dialog box, 309, 764
Select Installation Type screen
Active Directory, 181
AD CS, 1056
AD FS, 1077, *1077*
Backup utility, 736, 910
failover clusters, 835
Hyper-V, 448
Select Role screen, 842
Select Role Services screen
AD CS, 1057
AD RMS, 1095
Remote Access role, 634
WSUS servers, 489
Select Rule Template screen, 1088
Select Scopes page, 150, 940
Select Server Roles screen
Active Directory, 181
AD CS, 1056–1057, *1056*
AD FS, 1077
Backup utility, 736, 910
BitLocker, 536
BranchCache, 865
DFS, 540
failover clusters, 835
Hyper-V, 448, *448*
Remote Access role, 633, *633*
SNMP, 522
trees, 1019, *1019*
Select Storage page, 843
Select Storage Type page, 861
Select The Operating System That You Want To Install screen, 22, *23*, 25
Select User page
disk quotas, 225
shared folders, 223–224

Select Website screen, 1096
Selection type page
DNS, 92, 589
Remote Access role, 633
selective authentication, 1031, 1033
self-healing NTFS, **169**
Send Claims Using a Custom Rule template, 1084
Send Group Membership as Claim template, 1084
Send LDAP Attributes as Claims template, 1084
Serial Number field in DNS zones, 96, 594
server backups for certificate authorities, **1068–1069**
server-class hardware, 823
Server Cleanup Wizard option, 492
Server Core version
Active Directory installation on, 186–187
AD CS, 1047
Hyper-V installation in, **449–450**
installing, **24–26**
overview, **17–19**
server discovery in IPAM, **967**, *967*
Server Manager
Access-Denied Assistance, 888
AD CS, 1056–1057, 1059
AD FS, 1076–1079, *1077*, *1079*
AD RMS, 1094–1095
Backup utility, 736, 910
BitLocker, 536
BranchCache, 865
DAC, 876, 882
DFS, 540
DHCP, 122–124, *124*
DNS, 92, *92*, 589, *589*
failover clusters, 835
Hyper-V, 448, **450**, *450*
IPAM, 964, *966*, 967–970, *969–970*
iSNS, 893
NFS data store, 859
NPS policies, 678–679
Remote Access role, 633
SNMP, 522
trees, 1018–1021, *1018*, *1020–1021*
WSUS servers, 491, *491*
Server Operators group, 364, 707
Server Properties dialog box
DHCP-DNS integration, 155, 613
name protection, 951
server virtualization, 440
servers, **476**
caching-only, **93–94**, *93*, **591–592**, *592*
DHCP
multiple, **155–156**
properties, **140–143**, *141–143*
scope, 146–147
DNS, 64–65, 563
down-level, **238–239**
overview, **7–10**, *8*
PPTP, 623
print, **232–233**
WDS. *See* Windows Deployment Services (WDS)
WSUS. *See* Windows Server Update Services (WSUS)
service connection points (SCPs), **1097**
service level agreements (SLAs), **821–822**
service principal names (SPNs), 6
service profiles for VPNs, 687
service (SRV) records, **90–91**, **587–588**
service requests for sites, **983**
service set identifiers (SSIDs), 664
Service Type attribute, 673
ServiceAccountCredential option, 1081
Services tab in Task Manager, 513, *514*
Set-AD cmdlet, 1076
Set-ADUser cmdlet, 1088
Set-BCAuthentication cmdlet, 867
Set-BCCache cmdlet, 867
Set-BCSecretKey cmdlet, 867
Set By Caller option, 669
set commands
nslookup, 109, 605
ntdsutil, 200
WinRM, 234

Set-Date cmdlet, 237
Set-DNSClientServerAddress cmdlet, 240
Set DSRM Password command in ntdsutil, 743
Set-FsrmFileScreen cmdlet, 532, 870
Set-FsrmQuota cmdlet, 532, 870
Set-NetIPAddress cmdlet, 237
Set-NetIPv4Protocol cmdlet, 237
Set Sync Schedule screen, 495
Set-WdsBootImage cmdlet, 483
Set-WdsClient cmdlet, 483
Set-WdsInstallImage cmdlet, 483
Set-WdsInstallImageGroup cmdlet, 483
/setclassid switch in ipconfig, 119
Settings tab
  folder redirection, 323, 780
  remote access profiles, **682–684**, *683–684*
  RRAS logs, 640–642
Setup Type screen, 1059
shadow copies
  configuring, **922–923**, *922–923*
  overview, **215–217**, **921–922**
Shadow Copies dialog box, 216
Share This Printer option, 229
Shared Folder objects, 269–270
shared folders, **286–287**, **549**
shared permissions, **220–224**, *221–223*
Shared Virtual Hard Disk feature in Hyper-V, 442
shared virtual hard disks in failover clustering, **851**
sharing folders, **209**
Sharing tab
  printers, 227–229, *228–229*, 286
  VPN clients, **650**, *651*
shortcuts
  IPv6 addresses, 426
  trusts, 1031
Shut Down option, 463
Shutdown: Allow System To Be Shut Down Without Having To Log On option, 373, 721
SHV (system health validator), 690
SIDs. *See* security identifiers (SIDs)
Signing Options page, 954–955
Simple Mail Transfer Protocol (SMTP), **996**
Simple Network Management Protocol (SNMP), **521–523**, *523*
simple volumes, 34
single-master operations
  assigning, **727–728**, **1028–1029**
  managing, **725–726**, **1026**
single sign-on (SSO), 652, 1071
site link bridges, **997–999**, *997*
site links
  creating, 987, *987*
  replication, **997–999**, *997*
sites
  certificate authorities, **1067–1068**
  certificates, 1047–1048
  concepts, **982–983**, *983*
  configuring, **993**
  creating, **988–990**, *989–990*
  description, **987–988**, *987*
  fault tolerance, **929–931**, *930*
  GPO levels, 303, 758
  moving objects between, **1000–1001**
  planning, **984–985**, *985*
  replication, **983–984**
  service requests, **983**
6to4 mechanism in IPv6 addresses, 425, **432**
size of shadow copies, 216, 922
slash notation in IPv6 addresses, 426
slow link detection, **333–334**, **794**
smart cards, 6
Smart Paging files, 464–465
SMTP (Simple Mail Transfer Protocol), **996**
snapshots
  Hyper-V, 441
  virtual machines, 464
sneakernet, 298
SNMP (Simple Network Management Protocol), **521–523**, *523*
SOA (start of authority) records
  structure, **86–87**, **583–584**
  stub zones, 76, 574
socket pools in DNS, **82**, **580**, **955**

Software Compression option, 631
software deployment, **324–325**, **785**
AppLocker, **333**, **794**
group policy slow link detection, **333–334**, **794**
MSI. *See* Microsoft Windows Installer (MSI)
preparing for, **332–333**, **792–793**
process, 330–331, 334–335, 791–792, *794–796*
publishing, **324–325**, **781**
restriction policies, **333**, **793–794**
settings, **338–343**, *338–339*, *341–342*, **798–802**, *799–801*
software management life cycle, **325–326**, **785–786**
updates, **335–337**, **796–797**
verifying installation, **336–337**, **797–798**
Software Installation Properties dialog box, **338–339**, *338*, **799–802**, *799*, *801*
software management life cycle, **325–326**, **785–786**
software providers for VDS, 50
software restriction policies, **302**, **757**
Software Settings options, 300, 754–755
solid-state drives (SSDs), 896
Source tab in Performance Monitor, 507, *507*
spanned volumes, 34
Specify Access Permission page, 673, 675, 686
Specify Backup Time window, 735, 908
Specify Cluster Address screen, 1096
Specify Conditions page, 675, 686
Specify Intranet Microsoft Update Service Location Properties option, 498
Specify Name And Location page, 458, 461
Specify Proxy Server screen, 494
Specify Service Account screen, 1096
Specify The Order In Which Windows Installer Searches option, 343, 804
Specify The Partner Server To Use For Failover page, 946
split scopes, **949**
SQL Server Management Studio, 1100
SQLConnectionString option, 1081
SSO (single sign-on), 652, 1071
SSPI (Security Support Provider Interface), 6
SSPs (security support providers), 6
SSTS (Secure Sockets Tunneling Protocol), **629**
stale records, scavenging, **104**, 601
stand-alone certificate authorities, 1052
Start IP Address field, 140, 144
Start IPv6 Address field, *137*
Start-job cmdlet, 237
start of authority (SOA) records
structure, **86–87**, **583–584**
stub zones, 76, 574
Start Of Authority (SOA) tab, **96–97**, *96*, **593–594**, *593*
Start option for virtual machines, 462
Start Windows Normally option, 929
Starter Group Policy objects, **301**, **757**
Startup Properties dialog box, 317, *317*, 774, *774*
Startup Repair tool, **932**
Startup/Shutdown Scripts settings, 316, *317*, 773, *773*
stateless autoconfiguration, **423**
static IP addresses, **190**
statistics for zones, **962**
Status indicator in DNS zones, 95, 592
Stop-job cmdlet, 237
storage, **30**, **858**
audit policies and auditing, **870–875**
BranchCache technology, **862–868**, *863–864*, *866*
configuring basic and dynamic disks, **32–34**, *33*
DAC. *See* Dynamic Access Control (DAC)
exam essentials, **897**
Features on Demand, **895–896**
Fibre Channel, 49–50
FSRM, **868–870**
initializing disks, **31–32**
iSCSI, **43–46**, *45–46*, **890–892**, *891–892*
iSNS, **46–49**, *47–49*, **892–895**, *893–895*
mount points, **40–41**
MPIO, **41–43**
NAS, **50**
NFS data store, **858–862**, *859–861*

RAID, **36–39**, *38–39*
review questions, **898–900**
shadow copies, 216, 922
Storage Spaces, **35–36**
summary, **897**
thin provisioning and trim, **895–896**
tiered storage, **896**
VDS, **50–51**, *51*
volume management, **34–35**
storage pools, 35
Storage Quality of Service (QoS) for virtual machines, **467–468**
Storage Spaces
failover clustering, 851
overview, **35–36**
Store Migration feature, 453
stretched clusters, **839**
striped volumes, 34
Strong Encryption (MPPE 56-Bit) option, 684
Strongest Encryption (MPPE 128-Bit) option, 684
stub zones, **75–77**, *76*, **573–575**, *574*
subdomains, 63, 561
subnets
Active Directory
creating, **991–993**, *992*
description, **987–988**, *987*
applying
Class A, **417–418**, **420**
Class B, **415–416**, **420**
Class C, **410–415**, **419–420**
easy method, **406–410**, *407*
benefits, 399
calculating number of, **405**, *406*, **421**
CIDR notation, **419–420**
implementing, **400–402**, *401–402*
IPv6 addresses, **433–434**
masks, **402–405**, *403–404*
overview, **398–400**
requirements, **400**
sites, 984
supernets, **421**
subordinate certificate authorities, 1051–1052, *1052*
subscriptions in Event Viewer, 519, *519*
suffixes for user principal names, 272, **1033**
Summary Of Selections page, 346, *346*, 807, *807*
Superscope Name page, 150, 940
superscopes
creating and configuring, **939–940**
DHCP, **120**
IPv4 addresses, **149–151**
symmetric multiprocessor support, 441
synchronization, verifying, **1008**
synchronization logs in WSUS servers, 495
Synchronization Schedule option, 492
Synchronize All Offline Files Before Logging Off option, 213–214, 550
Synchronize All Offline Files When Logging On option, 213–214, 550
Synchronize Offline Files Before Suspend option, 213–214, 550
`sysprep.exe` utility, 1006
system, Event Viewer for, 192
system backups, 733, 906
System folder for objects, 281, *281*
system health validator (SHV), 690
System Monitor for replication, **1007**
System Recovery Options dialog box, 932
System Stability Index, **502**
system state data, backing up, **733–734**, **906–907**
Sysvol directory, backing up, 734, 907

T

Task Manager, **511–514**, *512–515*
task scheduling in PowerShell, 236
Tasks To Delegate page, 263
TCP (Transmission Control Protocol), 390
TCP/IP. *See* Transmission Control Protocol/Internet Protocol (TCP/IP)
Telemetry service, 10
templates
AD RMS, **1098–1099**, **1104**
administrative, 299–300, 754–755

templates (*continued*)
certificates
compatibility, **1064–1065**
creating, **1065**, *1066*
description, 777
overview, **1064**
Group Policy, 299–300, 754–755
NPS, **678**
objects, **272–274**
quotas, 225
transform claims rules, **1083–1084**
users, **272–274**, **716–717**
Templates Administrators group, 1093
Temporal Key Integrity Protocol (TKIP), 663
Teredo mechanism, 425, **432**
Test-ComputerSecureChannel cmdlet, 284
test environments for performance monitoring, **500**
TGS-REP (ticket-granting service replies), 1088
TGS-REQ (ticket-granting service requests), 1088
TGSs (ticket-granting services), 1088
TGTs (ticket-granting tickets), 1088
thin provisioning, **895–896**
third parties
application data partitions, 196
backups, 731–732, 905–906
CAs, 1049
EAP, 665
third-tier CA hierarchy model, 1053
Thorough Resource Health Check Interval option, 850
ticket-granting service replies (TGS-REP), 1088
ticket-granting service requests (TGS-REQ), 1088
ticket-granting services (TGSs), 1088
ticket-granting tickets (TGTs), 1088
Tie Breaker For 50% Node Split option, 852
tiered storage, 36, **896**
Time Between Redial Attempts menu, 647
Time Of Day Constraints dialog box, 671, 675, *675*
time to live (TTL)
choosing, **70–71**, **568–569**
DNS, **70**, **567–568**
multicast scopes, 152
TKIP (Temporal Key Integrity Protocol), 663
TLDs (top-level domains), **62**, **559–561**, *560*
TLS (Transport Layer Security)
AD FS, 1076
description, 6
TLS/SSL (Schannel)
description, 6, 701
networks, **666**
security, 699
top-level domains (TLDs), **62**, **559–561**, *560*
TPDs (trusted publishing domains), 1101, **1103–1104**
Trace-command cmdlet, 237
tracert command
connectivity tests, 173
IPv6 addresses, 433
tracert6 command, 433
traffic reduction
Active Directory Integrated DNS, 75, 573
local databases, 73, 570
multiple domains for, **1010**
subnets for, 398
transfer statistics for zones, **962**
transfers in DNS zones, **77–80**, *80*, **575–578**, *577*
Transform an Incoming Claim template, 1084
transform claims rules, **1083–1084**
transformation rules, **1084–1087**, *1085–1087*
transitive trusts, 1030
Transitivity Of Trust page, 1032
Transmission Control Protocol (TCP), 390
Transmission Control Protocol/Internet Protocol (TCP/IP), 58–59, **390**
connectivity tests, **172**
for DNS, **556–557**
exam essentials, **435**
IP addresses. *See* IP addresses
model, **390–393**, *391–392*
port numbers, **391–393**
review questions, **436–438**
summary, **435**

Transport layer in TCP/IP model, 390–391
Transport Layer Security (TLS)
  AD FS, 1076
  description, 6
Transport security mode in AD FS, 1073
transports in bridgehead servers, 1002
trees in Active Directory
  creating, **1017–1023**, *1018–1023*
  forests. *See* forests
  joining to forests, **1023–1024**
  planning, **1013**
  single, **1014–1015**, *1015*
trim feature, **895–896**
troubleshooting
  DNS. *See* Domain Name System (DNS)
  GPOs, **344–350**, ***345–348***, **804–810**, *806–808*
  OUs, **267**
  replication, **1007–1009**
  VPNs, **637–638**
Trust Anchor key, 954
trust anchors in DNS, **83–84**, **581–582**, 954
Trust Name page, 1032
Trust Password page, 1033
Trust Type page, 1032
Trustbridge. *See* Active Directory Federation Services (AD FS)
Trusted Publishing Domain File dialog box, 1104
trusted publishing domains (TPDs), 1101, **1103–1104**
Trusted User Domain File dialog box, 1102
trusted user domains (TUDs), **1101–1103**
trusts
  AD FS, **1083**
  AD RMS, **1101–1104**
  forests, 177
  managing, **1029–1033**, *1029*, *1031*
TTL (time to live)
  choosing, **70–71**, **568–569**
  DNS, **70**, **567–568**
  multicast scopes, 152
TTL For This Record field, 97, 594
TUDs (trusted user domains), **1101–1103**
Tunnel Type attribute, 673
tunneling
  IPv6 addresses, **431–433**, *433*
  L2TP/IPsec, **629**
  PPTP, **628–629**
  SSTP, **629**
Turn Off option, 462
two-tier CA hierarchy model, 1053
two-way trusts, 1030
Type A Printer Name page, 227, 285
Type indicator in DNS zones, 95, 592–593

U

UAC (User Account Control), **370**
UEFI (Unified Extensible Firmware Interface) support, 460–461
UGMC (Universal Group Membership Caching)
  description, 361, 704
  managing, **1035–1036**
  overview, **1006**
uk domain, 62, 560
unicast addresses
  clusters, **828**
  DHCP, 137, 151
  IPv6 addresses, **428–429**
unidirectional replication, 1002
Unified Extensible Firmware Interface (UEFI) support, 460–461
Uninstall Applications When They Fall Out Of The Scope of Management option, 339–340, 800
Uninstall-WindowsFeature cmdlet, 30, 237
unique local addresses, 429
unique name suffixes, 1034
Universal Group Membership Caching (UGMC)
  description, 361, 704
  managing, **1035–1036**
  overview, **1006**
universal groups
  description, 280
  security, **361**, **704**

Unlinked Test GPO Security Settings dialog box, 311, 768
Update Files And Languages option, 492
update sequence number (USN) journals, 986
Update Source And Proxy Server option, 492
updates
  Automatic Updates, **485–486**, *486–487*
  GPOs, forcing, **764–766**
  overview, **484**
  Resilient File System, 168
  software deployment, **335–337**, **796–797**
  Windows Update, **484–485**
  WSUS. *See* Windows Server Update Services (WSUS)
  zone statistics, **962**
upgrading
  AD FS, **1078**
  NLB clusters, 830
UPNs (user principal names)
  configuring, **272**
  suffixes, **1033**
URLs in AD RMS, 1092
us domain, 62, *560*
Use A Migration Table option, 784
Use A Migration Table Exclusively option, 784
Use Extensible Authentication Protocol (EAP) option, 649
Used Disk Space Only option, **533–534**
user access, **668**
  network policies, **670–676**
  NPS, **676–680**
  profiles, **668–670**, *669*
  remote profiles, **680–684**, *681–683*
  VPN policies, **684–687**
User Account Control (UAC), **370**
user accounts in security, 359, 703
user certificates, **319–321**, *321*, **776–778**, *778*
user claim types, **875–879**, *876–879*
User Network Options settings, 318, 775
User objects, 270, **300**, 754
user principal names (UPNs)
  configuring, **272**
  suffixes, **1033**
User Selection page, 345, *346–347*, 806, *806–807*
usernames
  AD FS, 1076
  key-based renewal, 1063
users
  access. *See* user access
  authentication, **664–666**
  delegating control of, **370–371**, **717–719**
  disk quota setting by, 224
  properties, **277–278**
  security, **714–716**, *715*
  templates, **272–274**, **716–717**
Users built-in domain local group, 364, 707
Users container, 268
Users Or Groups page, 263
Users tab in Task Manager, 513, *513*
USN (update sequence number) journals, 986

V

Validate A Configuration Wizard, 832, **834–838**
Validate My Identity As Follows menu, 648
validating
  certificates, **1054–1055**
  cluster configuration, **834–839**, *835–838*
validity periods in AD CS, **1054**
Variable Length Subnet Masking (VLSM), 70, 417, *567*
VDS (Virtual Disk Service), **50–51**, *51*
Verify Caller-ID option, *668–669*
verifying
  file system, **166–171**, *167*, *170–171*
  multifactor authentication, **1089**
  replication, **1007–1009**
  software installation, **336–337**, **797–798**
versions, choosing, **16–17**
VHDs. *See* virtual hard disks (VHDs)
View Current Activity option, 509
View Installation History option, 485
View Log File Data option, 509
View right, 1099
View Rights right, 1099
views
  Event Viewer, 518–519, *518*
  Performance Monitor, **504–505**, *504–505*

virtual accounts, **708–709**
Virtual Disk Service (VDS), **50–51**, *51*
Virtual Fibre Channel, 442
virtual hard disks (VHDs)
  booting from, **52**
  creating, **457–459**, *458*
  failover clustering, **851**
  generation 1 vs. generation 2, **460–461**
  Hyper-V, 452
  managing, **459–460**, *460*
  types, **456–457**
Virtual Machine Migration screen, 449
Virtual Machine Monitoring feature, 853
virtual machines and devices
  architecture, 446
  connections, **465–466**, *466*
  creating, **461–463**, *463*
  deleting, **465**, *465*
  Hyper-V, 452
  NIC Teaming, **466–467**, *467*
  settings, **463–465**, *465*
  Storage Quality of Service, **467–468**
  switches, **453–456**, *454–455*
  VHDs. *See* virtual hard disks (VHDs)
  Windows Azure, **190**
virtual private networks (VPNs), 980
  access policies, **684–687**
  clients, **644–650**, *645–646*, *648*, *650–651*
  description, 620, **625**
  vs. DirectAccess, **653**
  encapsulation, **627–628**, *627*
  L2TP/IPsec tunneling, **629**
  operation, **626–627**, **634–635**, *635*
  ports, **636–637**, *636*
  PPTP tunneling, **628–629**
  RRAS enabled as, **635–636**
  SSTP tunneling, **629**
  troubleshooting, **637–638**
  working with, **625–626**, *625*
Virtual Switch Manager, 453–454, *454*
virtualization. *See* Hyper-V role
VLSM (Variable Length Subnet Masking), 70, 417, *567*
Volume Activation feature, 10
Volume Shadow Copy Service (VSS), **215–217**, *919*, **921–923**, *922*
volumes
  disk quota setting by, 224
  managing, **34–35**
VOM ports, 464
VPN enforcement in network access, 690
VPNs. *See* virtual private networks (VPNs)
VSS (Volume Shadow Copy Service), **215–217**, *919*, **921–923**, *922*
`vssadmin.exe` utility, **217**, **923–924**

W

WANs (wide area networks)
  connectivity tests, 172
  multiple domains, **1010–1011**
  overview, **980**
warnings in Event Viewer, 516
wbadmin command, **745–746**, **918**
WCF (Windows Communication Foundation) components, 1082
WDS. *See* Windows Deployment Services (WDS)
WDSUTIL utility, **27–28**, **480–481**
Web Application Proxy, **651–652**
web enrollment role in AD CS, 1048
Web Proxy Service for AD FS, **1075**
Web Server (IIS) role, 10
Web Server Role (IIS) page, 634
weighted paths in MPIO, 41
WEP (Wired Equivalent Privacy), **663**
Which Type Of Installation Do You Want? screen, 23, *23*, 25
Wi-Fi Protected Access (WPA), **663**
Wi-Fi Protected Access 2 (WPA2), **664**
WID (Windows Internal Database), **972**
wide area networks (WANs)
  connectivity tests, 172
  multiple domains, **1010–1011**
  overview, **980**
WIM images, 30–31
Windows authentication, **688–689**

Windows Azure
  Active Directory deployment in, **189–190**
  backups, **919–921**
Windows Azure Management Portal, 920
Windows Communication Foundation (WCF) components, 1082
Windows Deployment Services (WDS)
  client preparation, **29**, **483–484**
  description, 6, 10, 701
  functionality, **478**
  installing, **481–483**
  network services, **27**, **479**
  preparing for, **478**
  requirements, **478**
  server components, **27–29**, **480–481**
  server preparation, **26–27**
  server requirements, **27**
  working with, **26**, **477–478**
Windows Deployment Services Configuration Wizard, 27
Windows Firewall
  configuring, **240**, *241*
  GPOs, **383**
  import/export policies, **383–384**
  inbound and outbound rules, **381–383**, *381–382*
  IPsec policies, **384**
  monitoring, **384**
  options, **377–381**, *378–380*
Windows Firewall with Advanced Security snap-in, 379
Windows Groups attribute, 673
Windows Identity Foundation (WIF), **1075**
Windows installer. *See* Microsoft Windows Installer (MSI)
Windows Integrated authentication, 1063
Windows Internal Database (WID), **972**
Windows Internet Name Service (WINS)
  name resolution, 65, 563
  settings, **133–134**, *134*
Windows Live ID, 1101
Windows Management Instrumentation (WMI), **310–311**, 765, **767**
Windows PowerShell. *See* PowerShell
Windows Recovery Environment (Windows RE), **928**
Windows Remote Management (WinRM) utility, **234–235**, **542**
Windows Script Host (WSH), 316, 773
Windows Server 2012 R2 Datacenter version, 16
Windows Server 2012 R2 Essentials version, 16
Windows Server 2012 R2 Foundation version, 16
Windows Server 2012 R2 Standard version, 16
Windows Server Backup feature, 10
Windows Server Migration Tools, **11**
Windows Server Update Services (WSUS), **487**
  advantages, **487–488**
  clients, **496–499**
  description, 10
  server configuration, *483–485*, **492–496**
  server installation, **489–491**, *489–491*
  server requirements, **488**
Windows Settings options, 300, 755
Windows token-based agents, 1074
Windows Update service, **325**, **484–485**, **786**
WINS (Windows Internet Name Service)
  name resolution, 65, 563
  settings, **133–134**, *134*
WINS page, **97**, **595**
WINS Servers page, 133–134, *134*, 136
Wired Equivalent Privacy (WEP), **663**
wireless access, **662–664**
witnesses
  configuration, **834**
  dynamic, 852
WMI (Windows Management Instrumentation), **310–311**, 765, **767**
workflows, 235
Workplace Join feature, **1089–1091**
World Wide Names (WWNs), 49–50
WPA (Wi-Fi Protected Access), **663**
WPA-Enterprise mode, 663
WPA-Personal mode, 663
WPA2 (Wi-Fi Protected Access 2), **664**
WPA2-Enterprise mode, **664**
WPA2-Personal mode, **664**

Write permission, 369, 712
WS-Federation Passive/SAML Web SSO endpoint, 1072
WS-Trust 1.3 endpoint, 1072
WS-Trust 2005 endpoint, 1072
WS-Trust WSDL endpoint, 1072
WSH (Windows Script Host), 316, 773
WSUS. *See* Windows Server Update Services (WSUS)
WSUS Server Configuration Wizard, 493–494
WWNs (World Wide Names), 49–50

X

X.509 certificates, 1076

Z

zone signing, 83, 581, 953–954
Zone Signing Key (ZSK) key, 954
Zone Signing Wizard, 954, *954*
Zone Type screen, 99, 596, 961
zones. *See* Domain Name System (DNS)

Free Interactive Online Study Environment

Register on Sybex.com to gain access to our interactive learning environment and study tools to help you study for your MCSA Windows Server 2012 R2 certification.

Our Superior Study Tools include:

- Assessment Test to help you focus your study to specific objectives
- Chapter Tests to reinforce what you learned
- Three Practice Exams to test your knowledge of the material
- Electronic Flashcards to reinforce your learning and give you that last-minute test prep before the exam
- Searchable Glossary gives you instant access to the key terms you'll need to know for the exam

Visit `www.sybex.com/go/mcsawin2012r2`, type in your PIN and instantly gain access to our interactive learning environment.

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.

The Community Book of PowerShell Practices

>

PowerShell.org

The Community Book of PowerShell Practices

PowerShell.org

This project can be followed at:

https://www.penflip.com/powershellorg/the-community-book-of-powershell-practices

©2015 PowerShell.org

Contents

1 The Community Book of PowerShell Practices **5**

Foreword 5

2 DOC-01 Write comment-based help **7**

3 DOC-02 Describe each parameter **8**

4 DOC-03 Provide usage examples **9**

5 DOC-04 Use the Notes section for detail on how the tool works **10**

6 DOC-05 Keep your language simple **11**

7 DOC-06 Comment your code **12**

8 DOC-07 Don't over-comment **13**

9 **14**

10 PREPARE VARIABLES **15**

11 **16**

12 VER-01 Write for the lowest version of PowerShell that you can **17**

13 VER-02 Document the version of PowerShell the script was written for **18**

14 PERF-01 If performance matters, test it **19**

15 PERF-02 Consider trade-offs between performance and readability **20**

16 READ-01 Indent your code **22**

17 READ-02 Avoid backticks **23**

18 OUT-01 Don't use write-host unless writing to the host is all you want to do **24**

19 OUT-02 Use write-verbose to give information to someone running your script **25**

20 OUT-03 Use write-debug to give information to someone maintaining your script 26

21 OUT-04 Use [CmdletBinding()] if you are using write-debug or write-verbose 27

22 TOOL-01 Decide whether you're coding a 'tool' or a 'controller' script 28

23 TOOL-02 Make your code modular 29

24 TOOL-03 Make tools as re-usable as possible 30

25 TOOL-04 Use PowerShell standard cmdlet naming 31

26 TOOL-05 Use PowerShell standard parameter naming 32

27 TOOL-06 Tools should output raw data 33

28 TOOL-07 Controllers should typically output formatted data 34

29 PURE-01 Use native PowerShell where possible 35

30 PURE-02 If you can't use just PowerShell, use .net, external commands or COM objects, in that order of preference 36

31 PURE-03 Document why you haven't used PowerShell 37

32 PURE-04 Wrap other tools in an advanced function or cmdlet 38

33 PIPE-01 Avoid using pipelines in scripts 39

One-Liners 39

"The PowerShell Way" 40

34 ERR-01 Use -ErrorAction Stop when calling cmdlets 41

35 ERR-02 Use $ErrorActionPreference='Stop' or 'Continue' when calling non-cmdlets 42

36 ERR-03 Avoid using flags to handle errors 43

37 ERR-04 Avoid using $? 44

38 ERR-05 Avoid testing for a null variable as an error condition 45

39 ERR-06 Copy $Error[0] to your own variable 46

40 WAST-01 Don't re-invent the wheel 47

41 WAST-02 Report bugs to Microsoft 48

1 The Community Book of PowerShell Practices

By Don Jones, Matt Penny and the Windows PowerShell Community
Cover design by Nathan Vonnahme

Visit Penflip.com/powershellorg to check for newer editions of this ebook.

This guide is released under the Creative Commons ShareAlike License. The authors encourage you to redistribute this file as widely as possible, but ask that you do not modify the document.

PowerShell.org ebooks are works-in-progress, and many are curated by members of the community. We encourage you to check back for new editions at least twice a year, by visiting Penflip.com/powershellorg.

You can download this book in a number of different formats (including Epub, Pdf, Microsoft Word and Plain Text) by clicking on the 'Download' link on the right.

PDF Users: Penflip's PDF export often doesn't include the entire ebook content. We've reported this problem to them; in the meantime, please consider using a different format, such as EPUB, when you're downloading the book.

You may register to make corrections, contributions, and other changes to the text - we welcome your contributions! check out our contributor tips and notes before jumping in.

You may also subscribe to our monthly e-mail TechLetter for notifications of updated ebook editions. Visit PowerShell.org for more information on the newsletter.

Foreword

During the 2013 Scripting Games, it became apparent that a great many folks in the PowerShell community have vastly different ideas about what's "right and wrong" in the world of PowerShell scripting. Some folks down-scored techniques that others praised, and vice-versa.

After the Games, PowerShell.org ran a series of "Great Debate" blog posts, outlining some of the more controversial issues and asking for community input. The catch is the input had to not only state what the person thought was best, but very specifically why they thought that.

This book, which will likely be an ongoing effort, is a compilation of those Debates' comments, formed as a "best practices" guide that is based on community input.

It's important to realize that practices are not hard-and-fast rules. Best practices are the things you usually do as a starting point, and deviate from when it's appropriate. You should understand that these practices were formed primarily by people who are writing scripts to manage their own environment, and who are often pressed for time. They are not developing commercial software, they rarely have the luxury of extended test-and-develop cycles, and for the most part are not professional software developers. Their perspective definitely drives what they consider "best" and "worst," but if you are working from a different perspective then you'll have to take all of this with a grain of salt.

The format of the headings was inspired by reading Steven Feuerstein's excellent book 'Oracle PL/SQL Best Practices'.

If you've got any comments or contributions please contact Matt Penny through either:

- @salisbury_matt on twitter or
- mattypenny@gmail.com

2 DOC-01 Write comment-based help

You should always write comment-based help in your scripts and functions.

Comment-based help is formatted as follows:

```
function your-function {
<#
.SYNOPSIS
A brief description of the function or script.

.DESCRIPTION
A longer description.

.PARAMETER FirstParameter
Description of each of the parameters

.PARAMETER SecondParameter
Description of each of the parameters

.INPUTS
Description of objects that can be piped to the script

.OUTPUTS
Description of objects that are output by the script

.EXAMPLE
Example of how to run the script

.LINK
Links to further documentation

.NOTES
Detail on what the script does, if this is needed

#>
```

‘

Comment-based help is displayed when the user types ‘help ’

Your help should be helpful. That is, if you've written a tool called “Get-LOBAppUser”, don't write help that merely says, “Gets LOB App Users.” Duh.

Further information: You can get more on the use of comment-based help by typing ‘help about_Comment_Based_Help’ within Powershell.

3 DOC-02 Describe each parameter

Your help should describe the proper use of each parameter in the comment-based help.

4 DOC-03 Provide usage examples

Your help should provide examples for each major use case.

A ‘usage example’ is just an example of what you would type in to Powershell to run the script - this can be cut and pasted from the command line.

5 DOC-04 Use the Notes section for detail on how the tool works

If you need to explain some of the detail about how the tool works, do so in the Notes section.

6 DOC-05 Keep your language simple

Comment-based help should be written in simple language.

You're not writing a thesis for your college Technical Writing class - you're writing something that describes how a function works. Avoid grandiloquent, multisyllabic verbiage and phrasing. In other words, put the thesaurus down. You're not impressing anyone.

If you're writing in what is, for you, a foreign language, simpler words and simpler sentence structures are better, and more likely to make sense to a native reader.

Be complete, but be concise.

7 DOC-06 Comment your code

Inline comments are also useful.

Keep in mind that these should explain the working of the code, but not how to use the tool itself, since an ordinary user won't see inline comments. Try to put a small block of inline comment before each functional hunk of your code.

8 DOC-07 Don't over-comment

Don't precede each line of code with a comment - doing so breaks up the code and makes it harder to follow. Don't restate the obvious:

```
\# Get the WMI BIOS object from the computer
Get-WmiObject -Class Win32\_BIOS -ComputerName $computer
```

Duh. A well-written PowerShell command, with full command and parameter names, can be pretty self-explanatory. Don't comment-explain it unless it isn't self-explanatory. Comments should describe the logic of your code, not attempt to document what each command is going to do.

Another example:
""

9

10 PREPARE VARIABLES

11

$computers = @()
“”
Really? Five lines of comment to one line of functional code? That is not okay. It actually makes the code harder to read. It doesn't add value - anyone looking at the code can tell that a variable is being set up for something. It's just noise.

12 VER-01 Write for the lowest version of PowerShell that you can

As a rule, write for the lowest PowerShell version that you can, especially with scripts that you plan to share with others. Doing so provides the broadest compatibility for other folks.

That said, don't sacrifice functionality or performance just to stick with an older version. If you can safely write for a higher version (meaning you've deployed it everywhere the script will need to run), then take advantage of that version. Keep in mind that some newer features that seem like window dressing might actually have underlying performance benefits. For example, in PowerShell v3:

```
Get-Service | Where-Object -FilterScript { $\_.Status -eq 'Running' }
```

Will run significantly slower than:

```
Get-Service | Where Status -eq Running
```

because of the way the two different syntaxes have to be processed under the hood.

Further information: You can get some detail on the differences between versions of Powershell by typing 'help about_Windows_PowerShell_2.0' (or _3.0 or 4.0) in Powershell

| | In the context of the Scripting Games, don't ever down-score someone for writing to a particular version, so long as they've documented it, unless the scenario explicitly states that a particular version must be used. |
| — | — |

13 VER-02 Document the version of PowerShell the script was written for

All that said, make sure you specify the version of PowerShell you wrote for by using an appropriate'#requires'statement:

```
#requires -version 3.0
```

The #requires statement will prevent the script from running on the wrong version of PowerShell.

14 PERF-01 If performance matters, test it

PowerShell comes equipped with 3.2 million performance quirks. Approximately.

For example, the first line below executes a lot faster than the second:

```
[void]Do-Something Do-Something | Out-Null
```

If you're aware of multiple techniques to accomplish something, and you're writing a production script that will be dealing with large data sets (meaning performance will become a cumulative factor), then test the performance using Measure-Command or some other tool.

| | In the context of the Scripting Games, if performance is a stated goal, then it's fine to down-score someone for using a technique that's demonstrably slower than an alternative, but never down-grade for personal, subjective, or aesthetic reasons. |
| — | — |

15 PERF-02 Consider trade-offs between performance and readability

Performance is not the only reason you write a script. If a script is expected to deal with ten pieces of data, a 30% performance improvement will not add up to a lot of actual time. It's okay to use a slower-performing technique that is easier to read, understand, and maintain - although "easier" is a very subjective term. Of the two commands above, any given person might select either of them as being "easier" to understand or read.

This is an important area for people in the PowerShell community. While everyone agrees that aesthetics are important - they help make scripts more readable, more maintainable, and so on - performance can also be important. However, the advantages of a really tiny performance gain do not always outweigh the "soft" advantages of nice aesthetics.

For example:
"“

$content = Get-Content file.txt

ForEach ($line in $content) {
Do-Something -input $line
}
"“

Most folks will agree that the basic aesthetics of that example are good. This snippet uses a native PowerShell approach, is easy to follow, and because it uses a structural programming approach, is easy to expand (say, if you needed to execute several commands again each line of content). However, this approach could offer extremely poor performance. If file.txt was a few hundred kilobytes, no problem; if it was several hundred megabytes, potential problem. Get-Content is forced to read the entire file into memory at once, storing it in memory (in the $content variable).

Now consider this alternate approach:

```
Get-Content file.txt | ForEach-Object -Process { Do-Something -input $\_ }
```

As described elsewhere in this guide, many folks in the community would dislike this approach for aesthetic reasons. However, this approach has the advantage of utilizing PowerShell's pipeline to "stream" the content in file.txt. Provided that the fictional "Do-Something" command isn't blocking the pipeline (a la Sort-Object), the shell can send lines of content (String objects, technically) through the pipeline in a continuous stream, rather than having to buffer them all into memory.

Some would argue that this second approach is always a poor one, and that if performance is an issue then you should devolve from a PowerShell-native approach into a lower-level .NET Framework approach:

```
$sr = New-Object -Type System.IO.StreamReader -Arg file.txt

while ($sr.Peek() -ge 0) {
$line = $sr.ReadLine()
Do-Something -input $line
}
```

There are myriad variations to this approach, of course, but it solves the performance problem by reading one line at a time, instead of buffering the entire file into memory. It maintains the structured programming approach of the first example, at the expense of using a potentially harder-to-follow .NET Framework model instead of native PowerShell commands. Many regard this third example as an intermediate step, and suggest that a truly beneficial approach would be to write PowerShell commands as "wrappers" around the .NET code. For example (noting that this fourth example uses fictional commands by way of illustration):

```
$handle = Open-TextFile file.txt

while (-not Test-TextFile -handle $handle) {
Do-Something -input (Read-TextFile -handle $handle)
}
```

This example reverts back to a native PowerShell approach, using commands and parameters. The proposed commands (Open-TextFile, Test-TextFile, and Read-TextFile) are just wrappers around .NET Framework classes, such as the StreamReader class shown in the third example.

You will generally find that it is possible to conform with the community's general aesthetic preferences while still maintaining a good level of performance. Doing so may require more work - such as writing PowerShell wrapper commands around underlying .NET Framework classes. Most would argue that, for a tool that is intended for long-term use, the additional work is a worthwhile investment.

The moral here is that both aesthetic and performance are important considerations, and without some work context, neither is inherently more important than the other. It is often possible, with the right technique, to satisfy both. As a general practice, you should avoid giving up on aesthetics solely because of performance concesrns - when possible, make the effort to satisfy both performance and aesthetics.

| | In the context of the Scripting Games, do not penalize entries for using a particular aesthetic approach on the grounds of poor performance, unless the Games assignment explicitly makes performance a goal and sets up a scenario where performance would be a problem. In other words, don't penalize someone because "if such-and-such were true, performance would be bad," unless it's made clear that such-and-such is in fact true. |
| — | — |

16 READ-01 Indent your code

Consider this code example:

```
if ($this -gt $that){ Do-Something -with $that }
```

And now consider this one:

```
if ($this -gt $that){ Do-Something -with $that }
```

Neither of these is better than the other. Ask 100 coders which they prefer and you'll get roughly half liking either one. Now, when you start dealing with commands that accept script blocks as parameters, things can get trickier because of the way PowerShell parses syntax. "Wrong" is wrong. With scripting constructs, like the two examples above, there's no functional difference.

Continuing in that vein, understand that the following are basically guidelines from mass consensus; they're not hard-and-fast rules. That said, there are arguments in favor of these, and you should consider the arguments before dismissing these ideas.

First, format your code properly. The convention is to indent within constructs, to make it clearer what "belongs to" the construct.

```
ForEach ($computer in $computers){ Do-This Get-Those }
```

You will probably be reviled if you don't format carefully.

| | In the context of the Scripting Games, don't down-score someone for using an approach that you personally don't like to use for aesthetic reasons. If performance is a stated goal, then it's fine to down-score someone for using a technique that's demonstrably slower than an alternative, but never down-grade for personal, subjective, or aesthetic reasons. |
| — | — |

17 READ-02 Avoid backticks

Consider this:

```
Get-WmiObject -Class Win32\_LogicalDisk ` -Filter "DriveType=3" `    -ComputerName SERVER2
```

In general, the community feels you should avoid using those backticks as "line continuation characters" when possible. They're hard to read, easy to miss, and easy to mis-type. Also, if you add an extra whitespace after the backtick in the above example, then the command won't work. The resulting error is hard to correlate to the actual problem, making debugging the issue harder.

Here's an alternative:
""
$params = @{Class=Win32_LogicalDisk;
Filter='DriveType=3';
ComputerName=SERVER2}

Get-WmiObject @params
""

The technique is called *splatting*. It lets you get the same nice, broken-out formatting without using the backtick. You can also line break after almost any comma, pipe character, or semicolon without using a backtick.

The backtick is not universally hated - but it can be inconvenient. If you have to use it for line breaks, well then, use it. Just try not to have to.

18 OUT-01 Don't use write-host unless writing to the host is all you want to do

It is generally accepted that you should never use Write-Host to create any script output whatsoever, unless your script (or function, or whatever) uses the Show verb (as in, Show-Performance). That verb explicitly means "show on the screen, with no other possibilities." Like Show-Command.

19 OUT-02 Use write-verbose to give information to someone running your script

Verbose output is generally held to be output that is useful or anyone running the script, providing status information ("now attempting to connect to SERVER1") or progress information ("10% complete").

20 OUT-03 Use write-debug to give information to someone maintaining your script

Debug output is generally held to be output that is useful for script debugging ("Now entering main loop," "Result was null, skipping to end of loop"), since it also creates a breakpoint prompt.

21 OUT-04 Use [CmdletBinding()] if you are using write-debug or write-verbose

Both Verbose and Debug output are off by default, and when you use Write-Verbose or Write-Debug, it should be in a script or function that uses the [CmdletBinding()] declaration, which automatically enables the switch.

The CmdletBinding attribute is specified on the first line of the script or function. After the name and inline help, but before the parameter definition:

```
function your-function { <# <Comment-based help> #> [CmdletBinding()] Param( [String] $Parameter1)
```

22 TOOL-01 Decide whether you're coding a 'tool' or a 'controller' script

For this discussion, it's important to have some agreed-upon terminology. While the terminology here isn't used universally, the community generally agrees that several types of "script" exist:

1. Some scripts contain tools, when are meant to be reusable. These are typically functions or advanced functions, and they are typically contained in a script module or in a function library of some kind. These tools are designed for a high level of re-use.
2. Some scripts are controllers, meaning they are intended to utilize one or more tools (functions, commands, etc) to automate a specific business process. A script is not intended to be reusable; it is intended to make use of reuse by leveraging functions and other commands

For example, you might write a "New-CorpUser" script, which provisions new users. In it, you might call numerous commands and functions to create a user account, mailbox-enable them, provision a home folder, and so on. Those discrete tasks might also be used in other processes, so you build them as functions. The script is only intended to automate that one process, and so it doesn't need to exhibit reusability concepts. It's a standalone thing.

Controllers, on the other hand, often produce output directly to the screen (when designed for interactive use), or may log to a file (when designed to run unattended).

23 TOOL-02 Make your code modular

Generally, people tend to feel that most working code - that is, your code which does things - should be modularized into functions and ideally stored in script modules.

That makes those functions more easily re-used. Those functions should exhibit a high level of reusability, such as accepting input only via parameters and producing output only as objects to the pipeline

24 TOOL-03 Make tools as re-usable as possible

Tools should accept input from parameters and should (in most cases) produce any output to the pipeline; this approach helps maximize reusability.

25 TOOL-04 Use PowerShell standard cmdlet naming

Use the verb-noun convention, and use the PowerShell standard verbs.

You can get a list of the verbs by typing 'get-verb' at the command line.

26 TOOL-05 Use PowerShell standard parameter naming

Tools should be consistent with PowerShell native cmdlets in regards parameter naming.

For example, use $ComputerName and $ServerInstance rather than something like $Param_Computer and $InstanceName

27 TOOL-06 Tools should output raw data

The community generally agrees that tools should output raw data. That is, their output should be manipulated as little as possible. If a tool retrieves information represented in bytes, it should output bytes, rather than converting that value to another unit of measure. Having a tool output less-manipulated data helps the tool remain reusable in a larger number of situations.

28 TOOL-07 Controllers should typically output formatted data

Controllers, on the other hand, may reformat or manipulate data because controllers do not aim to be reusable; they instead aim to do as good a job as possible at a particular task.

For example, a function named Get-DiskInfo would return disk sizing information in bytes, because that's the most-granular unit of measurement the operating system offers. A controller that was creating an inventory of free disk space might translate that into gigabytes, because that unit of measurement is the most convenient for the people who will view the inventory report.

An intermediate step is useful for tools that are packaged in script modules: views. By building a manifest for the module, you can have the module also include a custom .format.ps1xml view definition file. The view can specify manipulated data values, such as the default view used by PowerShell to display the output of Get-Process. The view does not manipulate the underlying data, leaving the raw data available for any purpose.

29 PURE-01 Use native PowerShell where possible

This means not using COM, .NET Framework classes, and so on when there is a native Windows PowerShell command or technique that gets the job done.

30 PURE-02 If you can't use just PowerShell, use .net, external commands or COM objects, in that order of preference

First, at the end of the day, get the job done the best way you can. Utilize whatever means you have at your disposal, and focus on the techniques you already know, because you'll spend less time coding that way.

That said, there are advantages to sticking with "PowerShell native." In general, folks tend to prefer that you accomplish tasks using the following, in order of preference:

1. PowerShell cmdlets, functions, and other "native" elements. These are (or can be) very well documented right within the shell itself, can (and should) use consistent naming and operation, and are generally more discoverable and easier to understand by someone else.
2. NET Framework classes, methods, properties, and so on. While not documented in-shell, they at least stay "inside the boundaries" of .NET, and .NET Framework classes are typically well-documented online.
3. External commands, like Cacls.exe or PathPing.exe. While not documented in-shell, most tools do offer help displays, and most (especially ones that ship with the OS or server product) have numerous online examples.
4. COM objects. These are rarely well-documented, making them harder for someone else to research and understand. They do not always work flawlessly in PowerShell, as they must be used through .NET's Interop layer, which isn't 100% perfect.

31 PURE-03 Document why you haven't used PowerShell

So when is it okay to move from one item on this list to another? Obviously, if a task can't be accomplished with a more-preferred way, you move on to a less-preferred way.

If a less-preferred approach offers far superior performance, and performance is a potential issue, then go for the better-performing approach. For example, Robocopy is superior in nearly every way to Copy-Item, and there are probably numerous circumstances where Robocopy would do a much better job.

Document the reason for using tools other than PowerShell in your comments.

32 PURE-04 Wrap other tools in an advanced function or cmdlet

That said, you truly become a better PowerShell person if you take the time to wrap a less-preferred way in an advanced function or cmdlet. Then you get the best of both worlds: the ability to reach outside the shell itself for functionality, while keeping the advantages of native commands.

Ignorance, however, is no excuse. If you've written some big wrapper function around Ping.exe simply because you were unaware of Test-Connection, then you've wasted a lot of time, and that is not commendable. Before you move on to a less-preferred approach, make sure the shell doesn't already have a way to do what you're after.

33 PIPE-01 Avoid using pipelines in scripts

Consider this:

```
Get-Content computer-names.txt | ForEach-Object -Process { Get-WmiObject -Class Win32\_BIOS
-ComputerName $\_ }
```

And now this alternative:

“‘

$computers = Get-Content computer-names.txt

foreach ($computer in $computers) {
Get-WmiObject -Class Win32_BIOS -ComputerName $computer
}
“‘

The world definitely prefers the latter approach in a script or function.

Constructs offer far more flexibility, especially when you’re looping through multiple commands. Error handling becomes far easier and more structured with the latter approach, as does debugging.

Constructs often exhibit higher performance than pipeline-only approaches, but not always - it’s worth testing if you are dealing with large data-sets and if you’re in a context where performance matters. See PERF-02 for more detail on this.

On the command-line, by yourself, do whichever you prefer. It’s as you move into a script - an inherently more structured environment - that you want to start shifting to a more programming-style approach.

One-Liners

| | In the context of the Scripting Games, if you are asked to do something as a “one-liner,” that means a single, continuous pipeline. Using semicolons to jam multiple “lines” into a single “line” does not count.If someone is asking for a one-liner, they’re doing it to test a certain type of PowerShell mettle. Mashing multiple lines together by means of semicolons does not fulfill the intent of the question. |
| — | — |

“The PowerShell Way”

There is no one, true way to do anything in PowerShell. To resurrect a previous pair of examples:
“‘

[void]Do-Something

Do-Something | Out-Null
“‘

Same end effect, but some folks will argue that the first command is more “programmer-y” and less “PowerShell-y.” The first example runs faster, however, so there’s more than an aesthetic difference here.

It’s important to note that although PowerShell isn’t a programming language, it - like most good shells - does contain a programming language. It’s okay to use it. It’s fine to use more programming-style approaches. Don’t dismiss a technique or approach because ‘it looks like programming’ to you, and because you aren’t a programmer and don’t want to be one. You might actually be missing out on something.

34 ERR-01 Use -ErrorAction Stop when calling cmdlets

When trapping an error, try to use -ErrorAction Stop on cmdlets to generate terminating, trappable exceptions.

35 ERR-02 Use $ErrorActionPreference='Stop' or 'Continue' when calling non-cmdlets

When executing something other than a cmdlet, set $ErrorActionPreference='Stop' before executing, and re-set to Continue afterwards. If you're concerned about using -ErrorAction because it will bail on the entire pipeline, then you've probably over-constructed the pipeline. Consider using a more scripting-construct-style approach, because those approaches are inherently better for automated error handling.

Ideally, whatever command or code you think might bomb should be dealing with one thing: querying one computer, deleting one file, updating one user. That way, if an error occurs, you can handle it and then get on with the next thing.

36 ERR-03 Avoid using flags to handle errors

Try to avoid setting flags:
“‘
Try {
$continue = $true
Do-Something -ErrorAction Stop
} Catch {
$continue = $false
}

if ($continue) {
Do-This
Set-That
Get-Those
}
`Instead, put the entire "transaction" into the Try block:`
Try {
Do-Something -ErrorAction Stop
Do-This
Set-That
Get-Those
} Catch {
Handle-Error
}
“‘
It’s a lot easier to follow the logic.

37 ERR-04 Avoid using $?

When you need to examine the error that occurred, try to avoid using $?. It actually doesn't mean an error did or did not occur; it's reporting whether or not the last-run command considered itself to have completed successfully. You get no details on what happened.

38 ERR-05 Avoid testing for a null variable as an error condition

Also try to avoid testing for a null variable as an error condition:
“‘
$user = Get-ADUser -Identity DonJ

if ($user) {
$user | Do-Something
} else [
Write-Warning “Could not get user $user”
}
“‘

There are times and technologies where that’s the only approach that will work, especially if the command you’re running won’t produce a terminating, trappable exception. But it’s a logically contorted approach, and it can make debugging trickier.

39 ERR-06 Copy $Error[0] to your own variable

Within a Catch block, $_ will contain the last error that occurred, as will $Error[0]. Use either - but immediately copy them into your own variable, as executing additional commands can cause $_ to get "hijacked" or $Error[0] to contain a different error.

It isn't necessary to clear $Error in most cases. $Error[0] will be the last error, and PowerShell will maintain the rest of the $Error collection automatically.

40 WAST-01 Don't re-invent the wheel

There are a number of approaches in PowerShell that will "get the job done." In some cases, other community members may have already written the code to achieve your objectives. If that code meets your needs, then you might save yourself some time by leveraging it, instead of writing it yourself.

For example:

```
Function Ping-Computer ($computername){ $ping = Get-WmiObject Win32\_PingStatus -filter "Address='$computername'"
if ($ping.StatusCode -eq 0){ return $true } else { return $false } }
```

This function has a few opportunities for enhancement. First of all, the parameter block is declared as a basic function; using advanced functions is generally preferred. Secondly, the command verb ("Ping") isn't an approved PowerShell command verb. This will cause warnings if the function is exported as part of a PowerShell module, unless they are otherwise suppressed on import.

Thirdly, there's little reason to write this function in PowerShell v2 or later. PowerShell v2 has a built-in command that will allow you to perform a similar function. Simply use:

```
Test-Connection $computername -Quiet
```

This built-in command accomplishes the exact same task with less work on your part - e.g., you don't have to write your own function.

It has been argued by some that, "I didn't know such-and-such existed, so I wrote my own." That argument typically fails with the community, which tends to feel that ignorance is no excuse. Before making the effort to write some function or other unit of code, find out if the shell can already do that. Ask around. And, if you end up writing your own, be open to someone pointing out a built-in way to accomplish it.

On the flip side, it's important to note that writing your own code from the ground up can be useful if you are trying to learn a particular concept, or if you have specific needs that are not offered by another existing solution.

41 WAST-02 Report bugs to Microsoft

An exception: if you know that a built-in technique doesn't work properly (e.g., it is buggy or doesn't accomplish the exact task), then obviously it's fine to re-invent the wheel. However, in cases where you're doing so to avoid a bug or design flaw, then you should - as an upstanding member of the community - report the bug on Connect.Microsoft.com also.