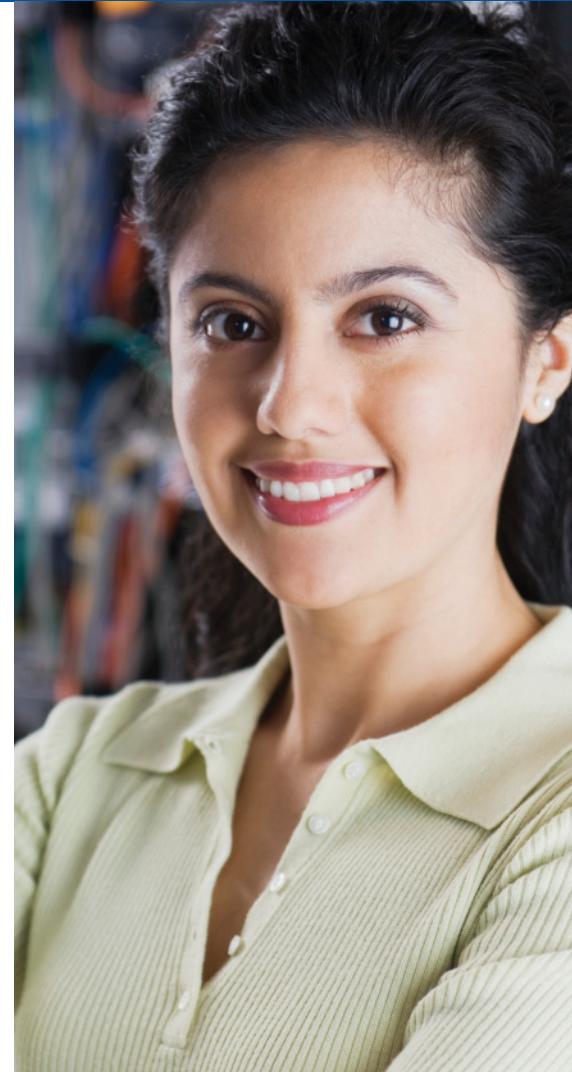


Microsoft Official Academic Course

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
	Debbie Martin
ASSISTANT MARKETING MANAGER	Joyce Poh
ASSOCIATE PRODUCTION MANAGER	Wendy Ashenberg
CONTENT EDITOR	Harry Nolan
CREATIVE DIRECTOR	Tom Nery
COVER DESIGNER	Thomas Kulesa
SENIOR PRODUCT DESIGNER	

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

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	<i>Warning</i> 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

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

- 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

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

Deploying and Managing Server Images

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.



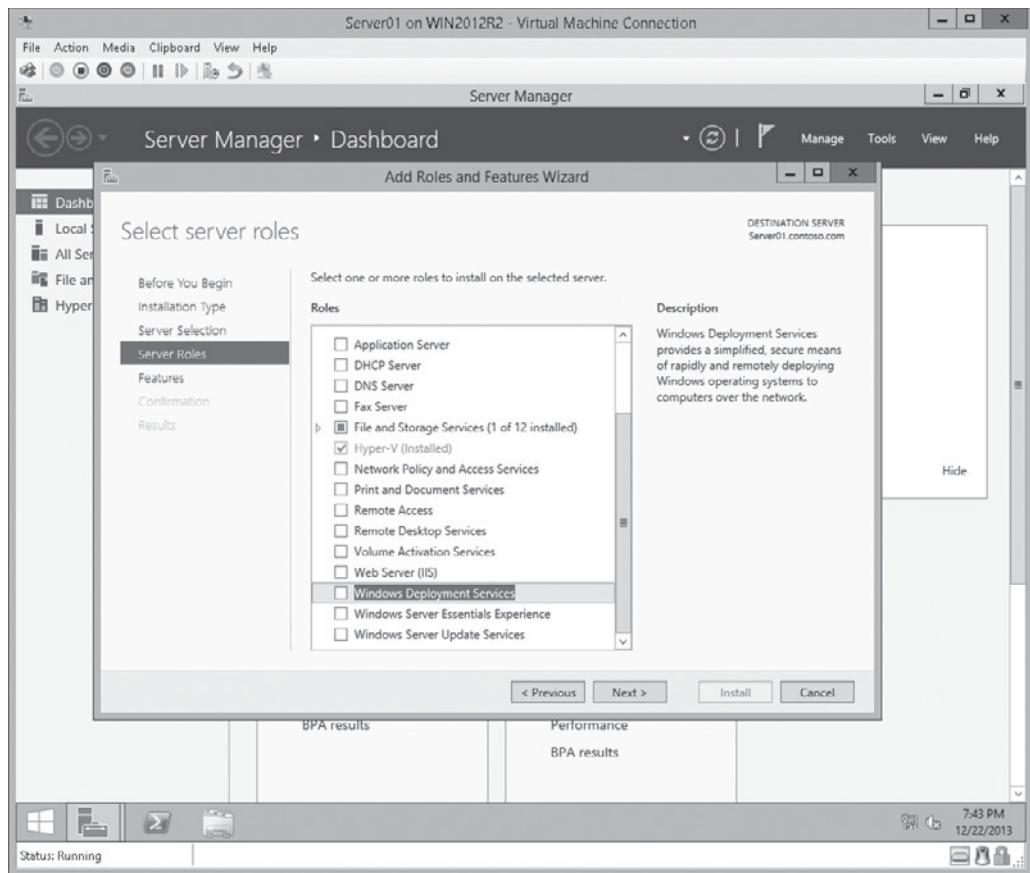
DEPLOY WDS

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.



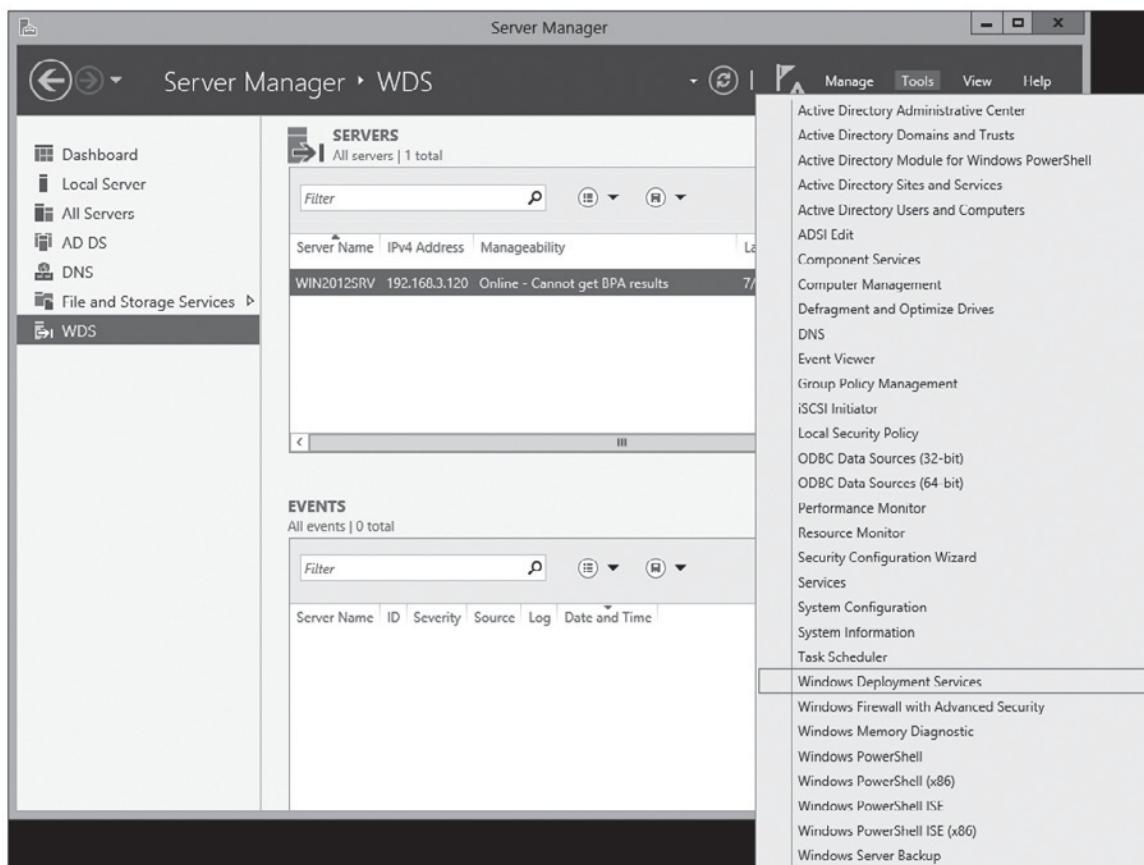
PERFORM THE INITIAL CONFIGURATION OF WDS

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



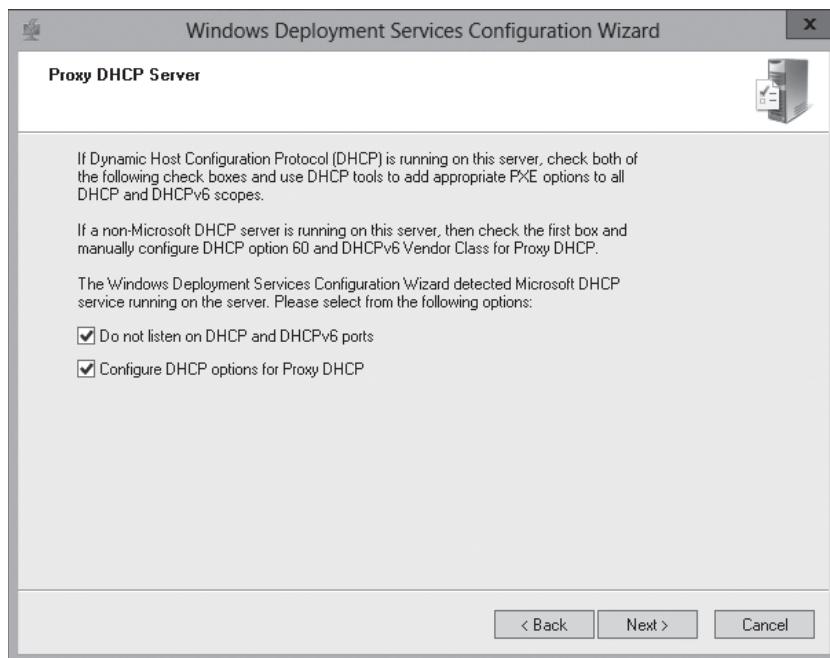
3. Expand [Servers](#), right-click the WDS server, and then select [Configure Server](#).
4. When the [Before You Begin](#) page appears, click [Next](#).
5. On the [Install Options](#) page, select the [Integrated with Active Directory](#) option, and then click [Next](#).



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.

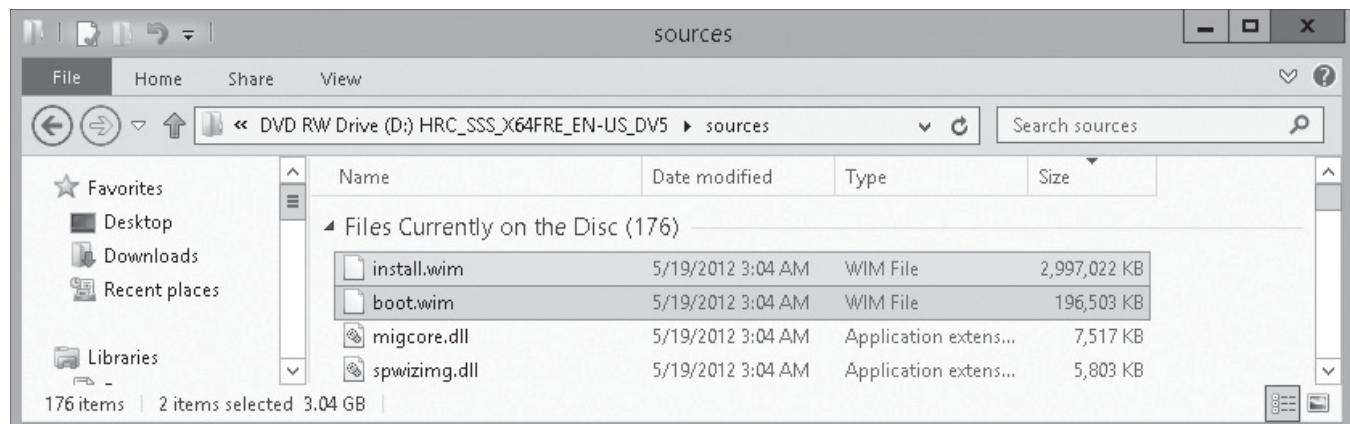
The boot images and the install images use the **Windows Imaging Format (WIM)**, a file format that allows a file structure (folders and files) to be stored inside a single WIM database. By using a database, the system does not have to open and close several individual files during the data transfer.

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





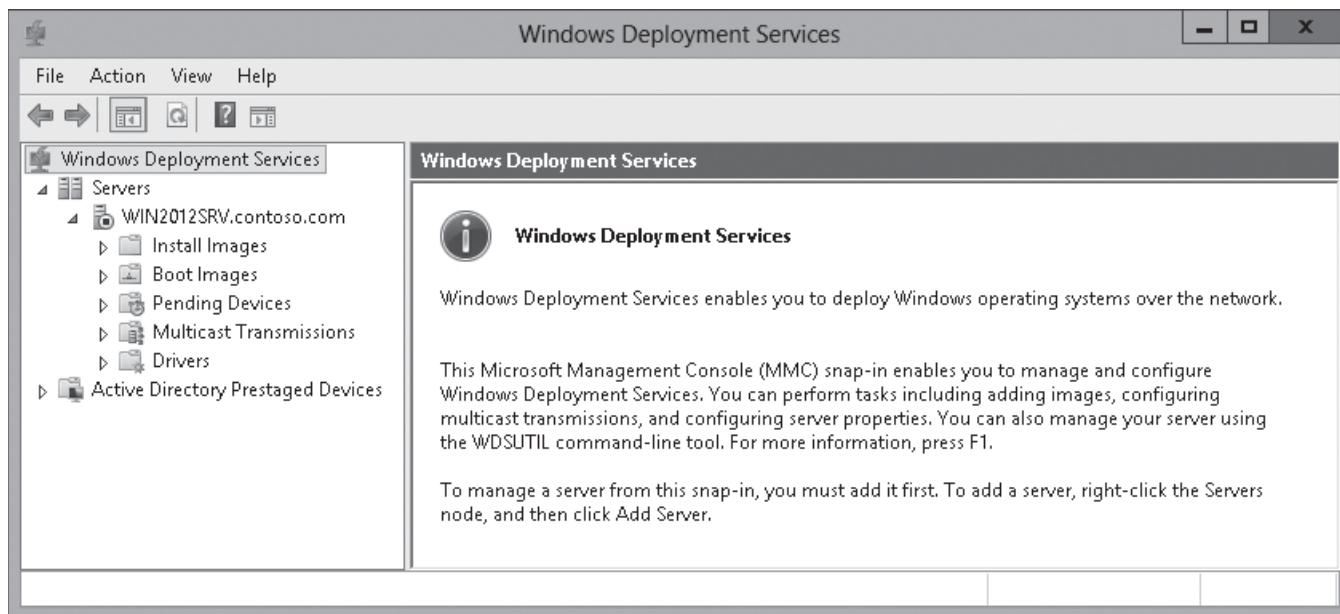
ADD A BOOT IMAGE

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.



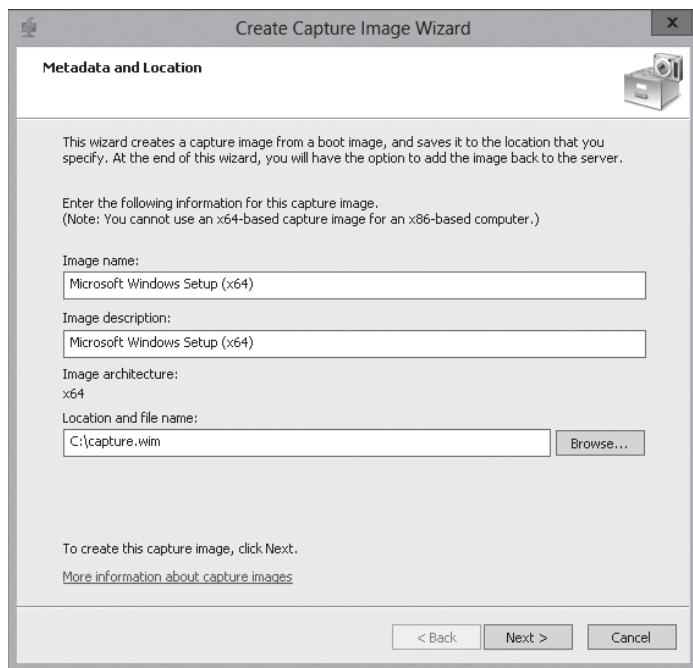
CREATE AN IMAGE FILE

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.



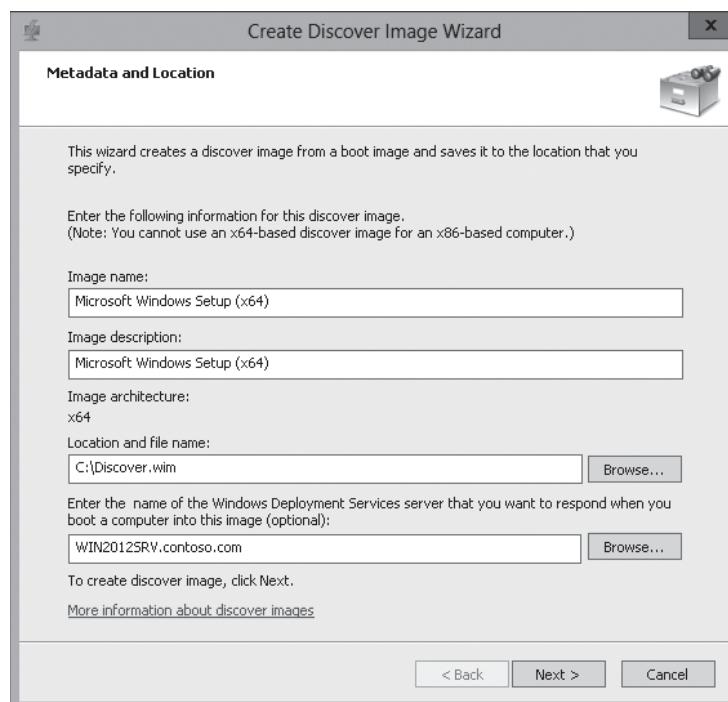
CREATE A DISCOVER IMAGE

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 multi-cast 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.



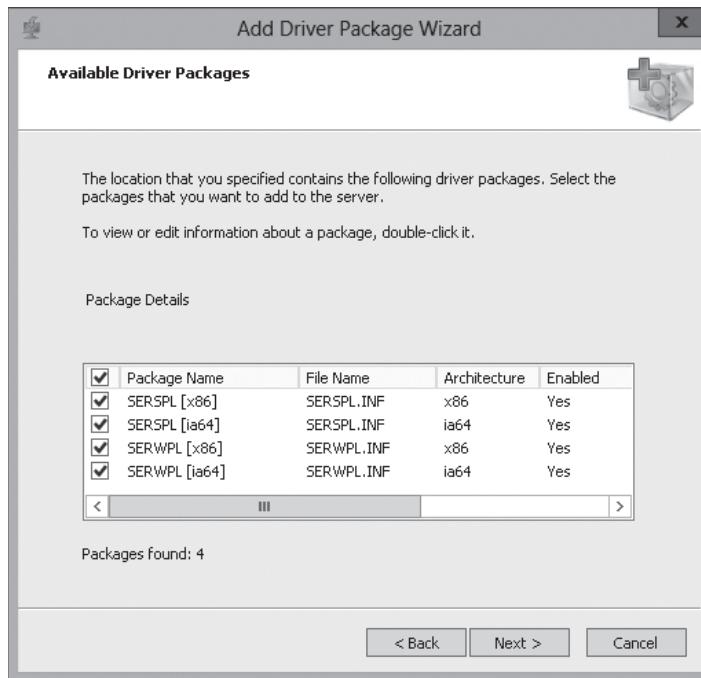
ADD DRIVERS TO AN IMAGE

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

■ Deploying Windows Server Update Services (WSUS)



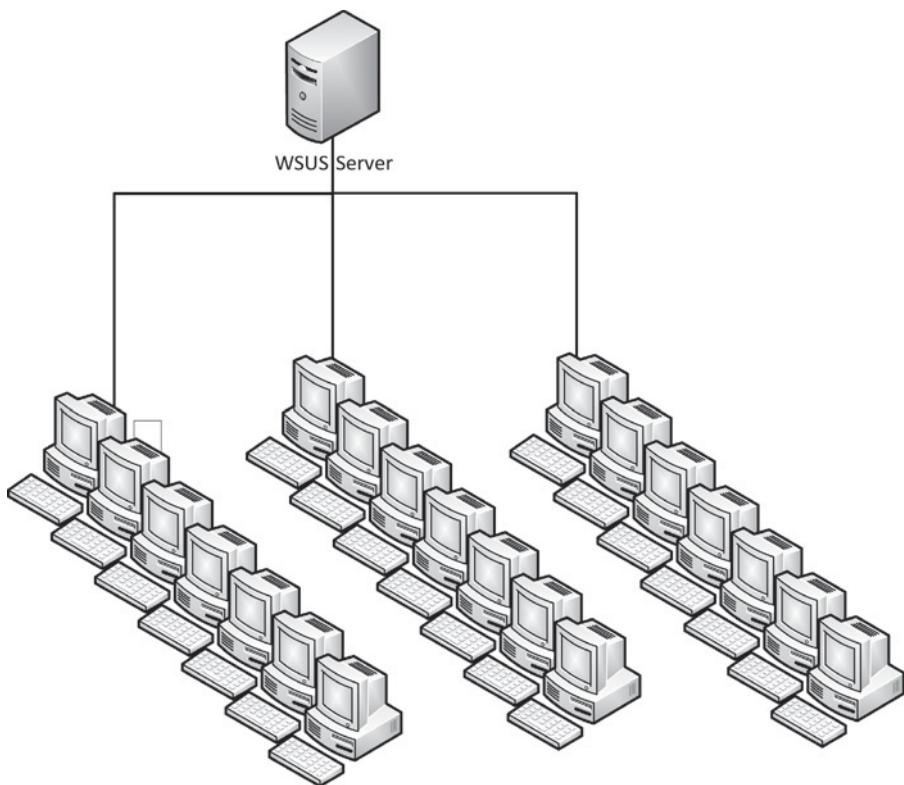
An organization that needs to update hundreds of computers can present a daunting challenge for administrators. First, hundreds of computers downloading updates can affect network performance. Second, because an update can cause unforeseen problems, it is better to have the patch or update tested before 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.

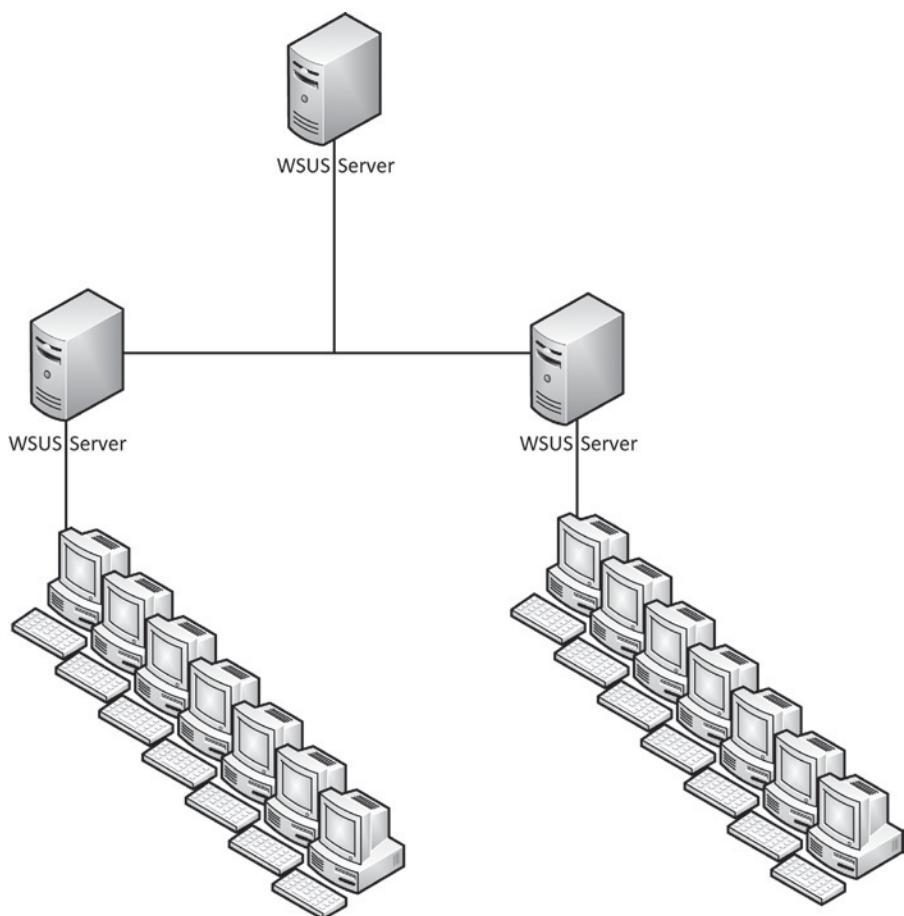
If you administer more than a few hundred computers or you administer multiple sites, you can create a hierarchy of WSUS servers (see Figure 2-2). The number of WSUS servers will be determined by the number of sites, the speed and load of the links between sites, and the number of clients that you must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



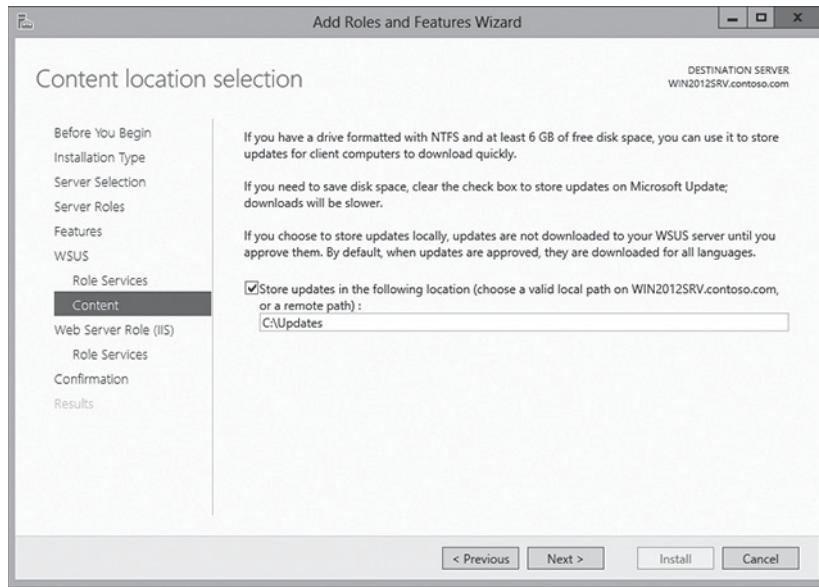
MORE INFORMATION

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.



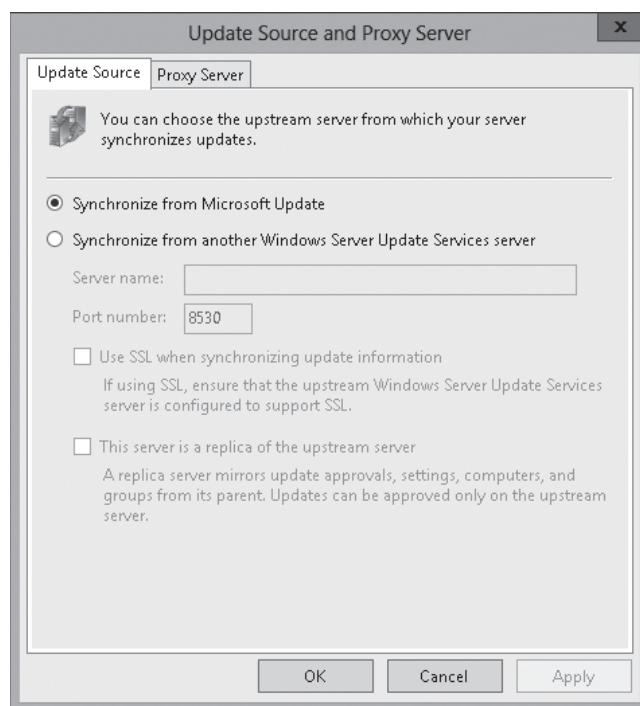
CONFIGURE THE UPDATE SOURCE AND PROXY SERVER

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

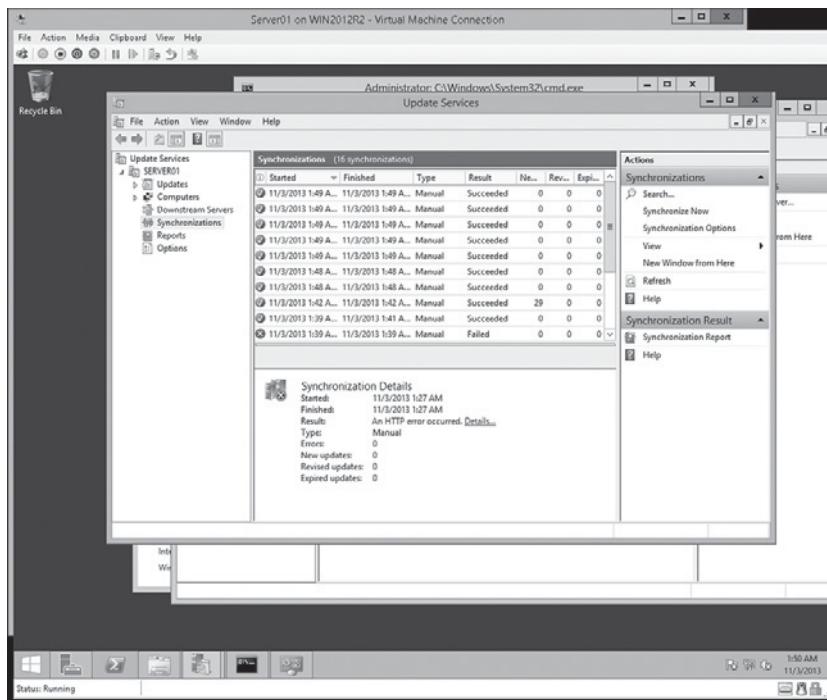
GET READY. To specify what WSUS will synchronize, perform the following steps:

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.



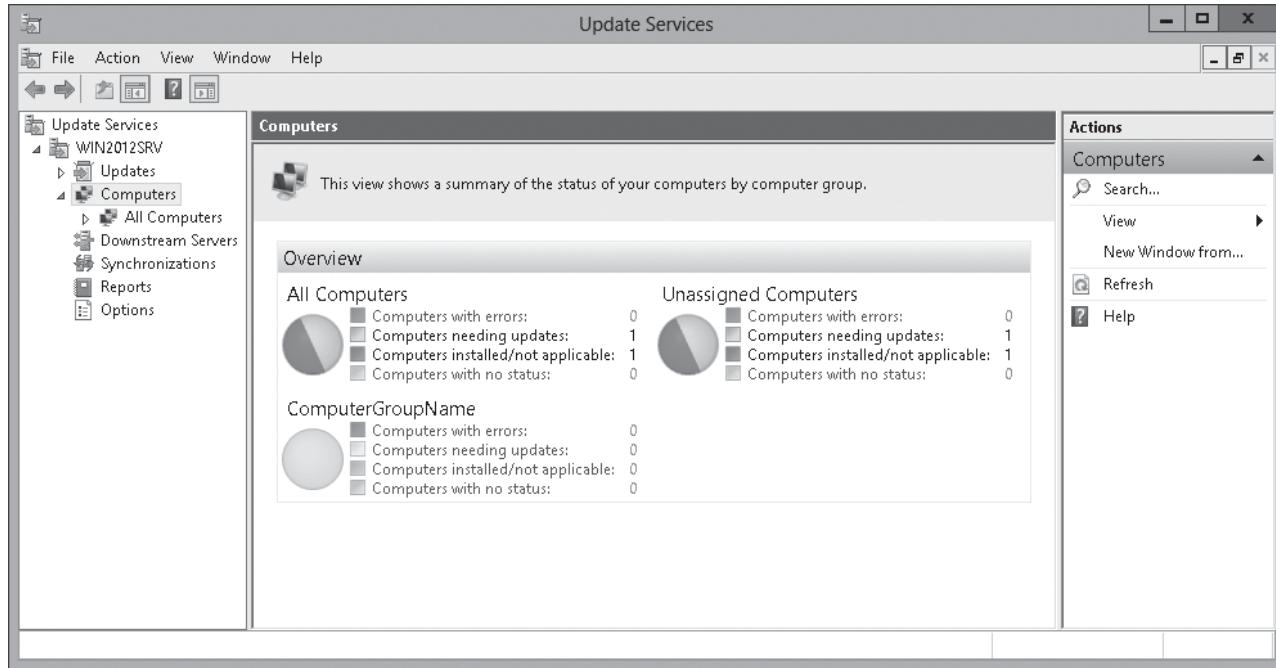
CREATE A COMPUTER GROUP

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.



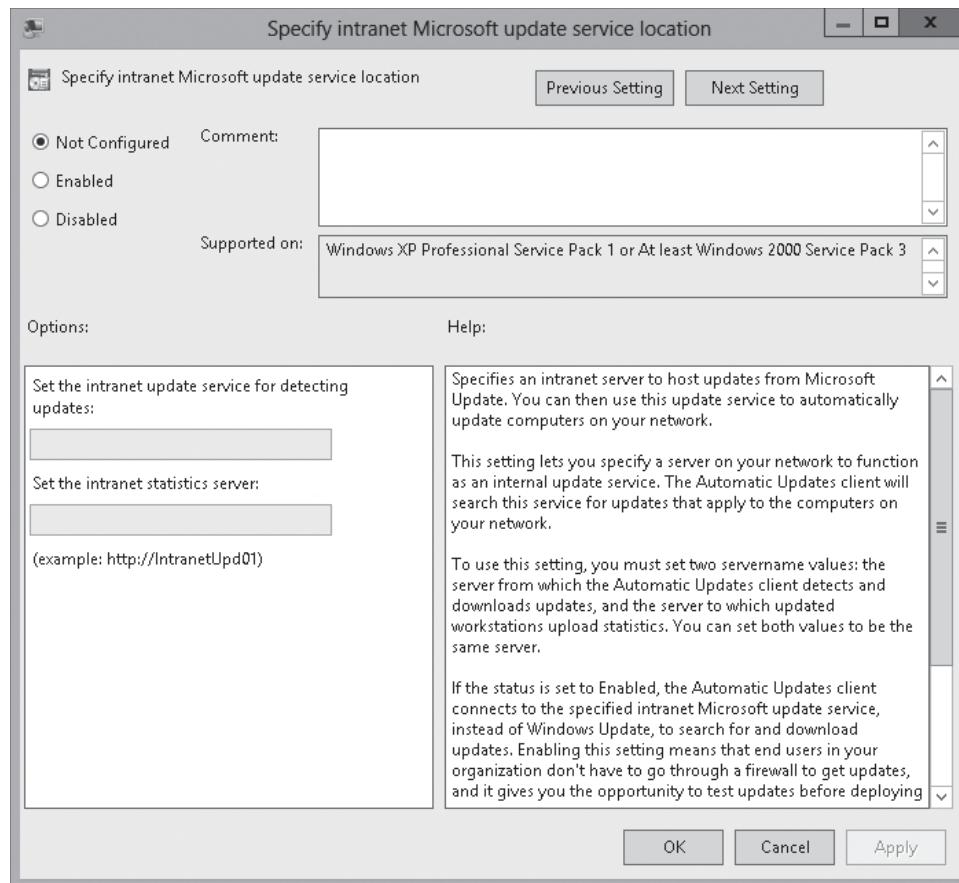
CONFIGURE A COMPUTER TO USE WSUS FOR UPDATES USING GROUP POLICY

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

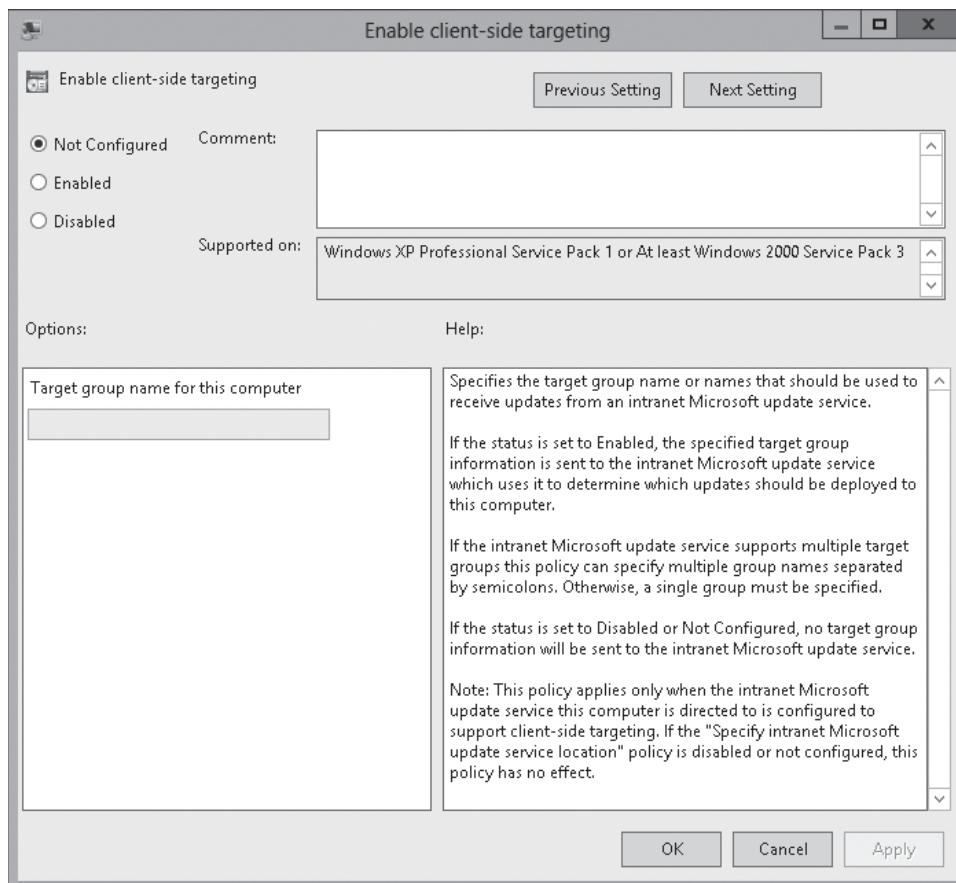
GET READY. To enable client-side targeting using Group Policy, perform the following steps on a domain controller or any computer that has Group Policy Management console:

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

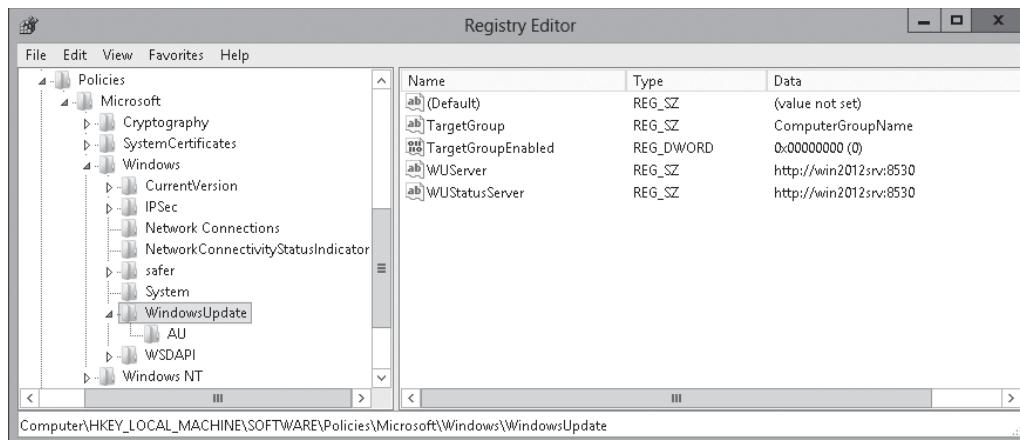
To enable client-side targeting, change the TargetGroupEnabled (Reg_DWord) value to a 1 and use the TargetGroup (Reg_SZ) value to specify the group that you want the computer to be a member of (see Figure 2-9). You also need the following subkey:

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.



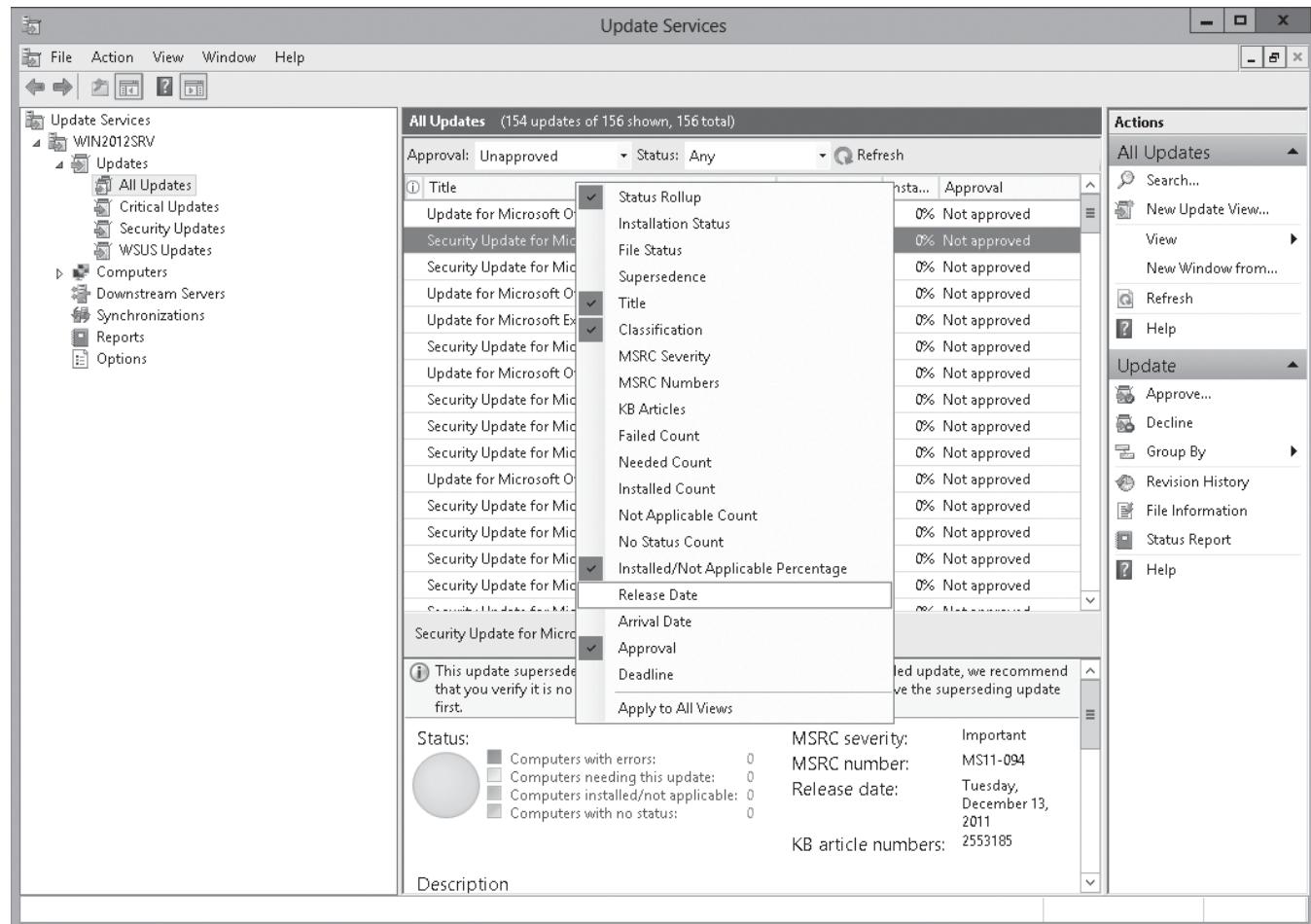
APPROVE UPDATES

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

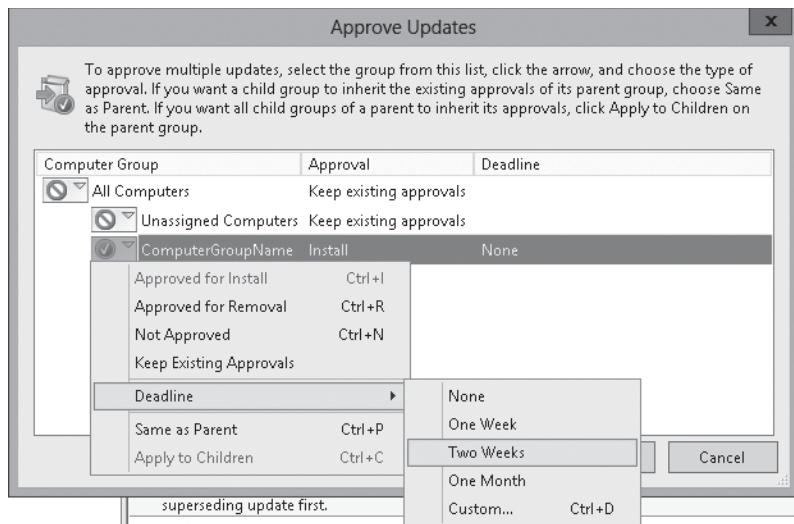
Choosing the Release Date option



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 versions 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?

Monitoring Servers

■ Introducing the Microsoft Management Console (MMC)



THE BOTTOM LINE

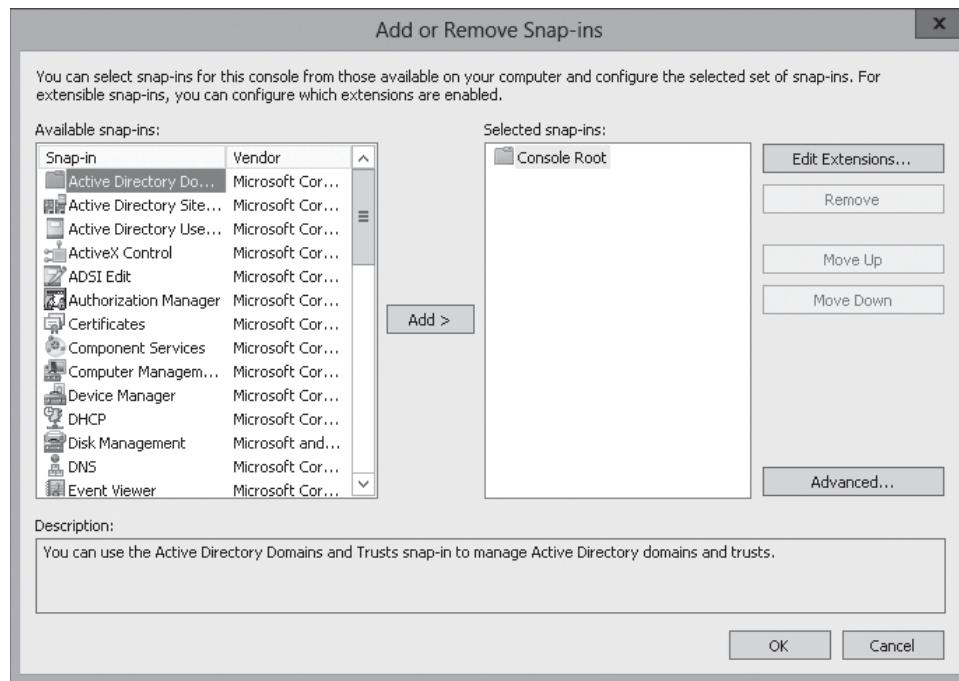
The **Microsoft Management Console (MMC)** is one of the primary administrative tools used to manage Windows and many of the network services provided by Windows. It provides a standard method to create, save, and open the various administrative tools provided by Windows. When you open Administrative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

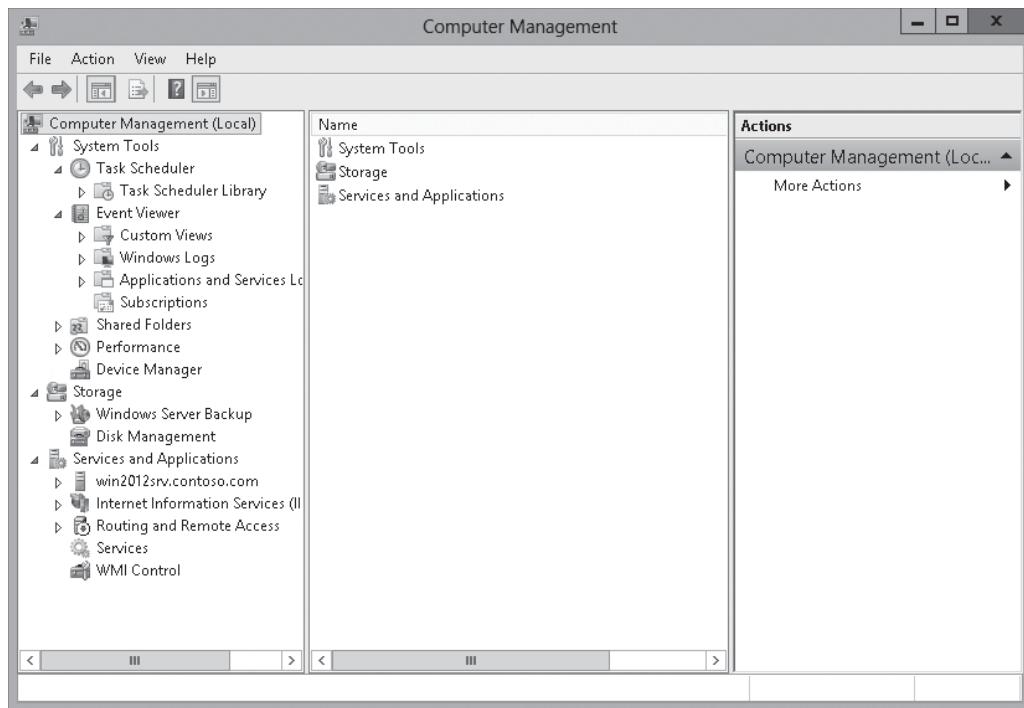
Using Computer Management

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.

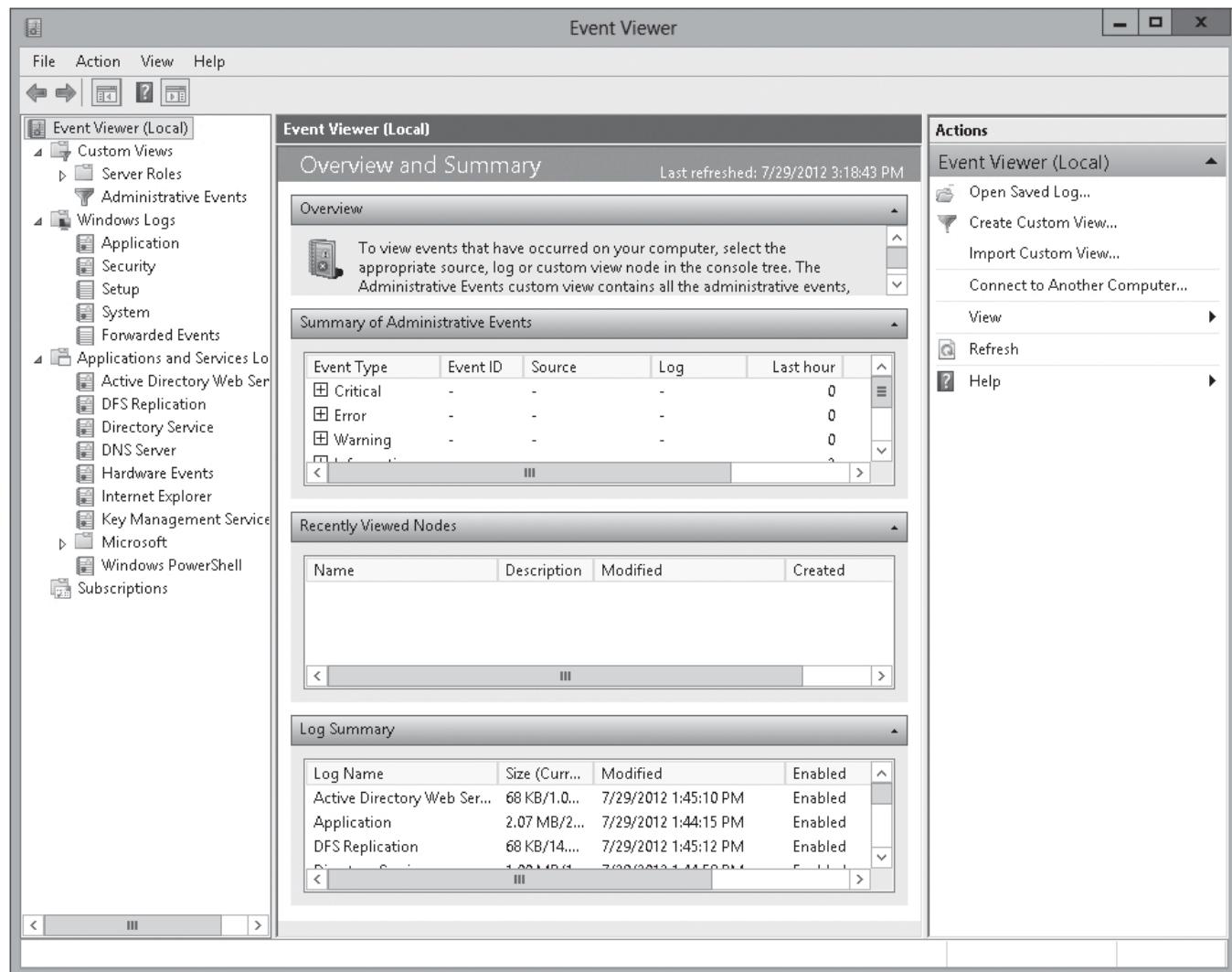
The **Event Viewer** is an MMC snap-in that enables you to browse and manage event logs. It is included in the Computer Management and is included in Administrative Tools as a stand-alone console. You can also execute the `eventvwr.msc` command.

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:

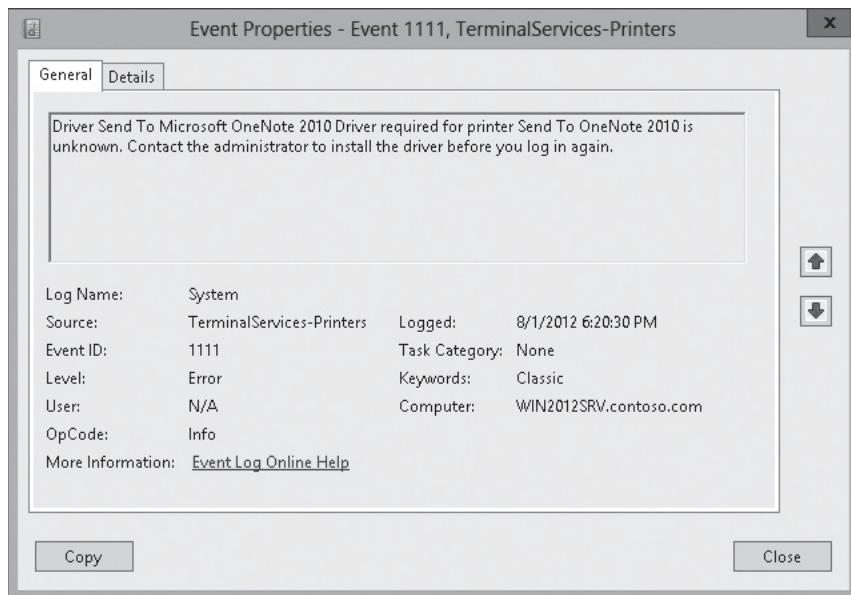
- **Custom Views:** Allows you to create custom views of events. By default, it includes Administrative Events, which collects Critical, Error, and Warnings from all logs on the server. However, you can create your own customer view by right-clicking Custom Views and selecting Create Custom View.
- **Windows 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.

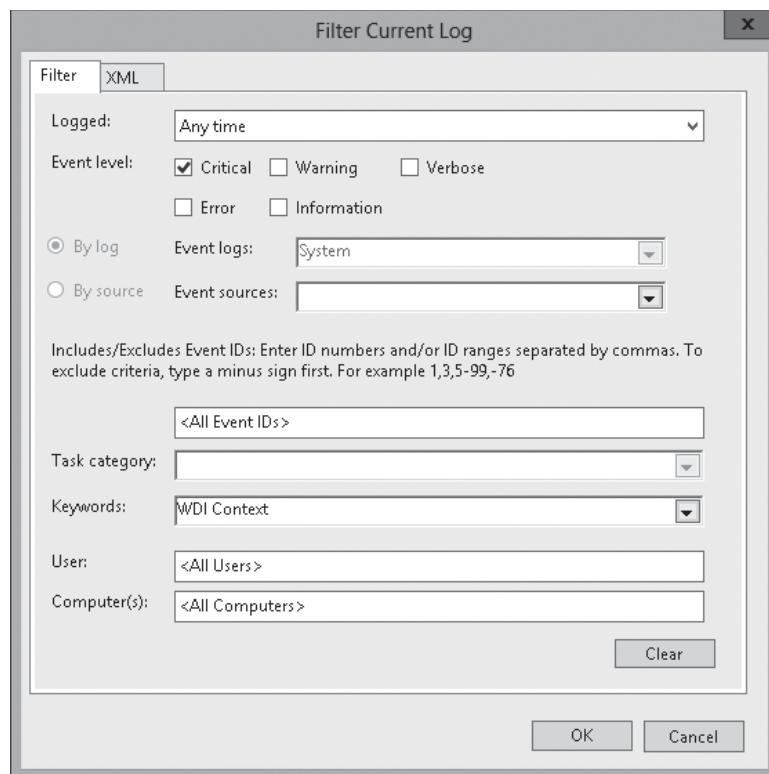
When you open any of these logs, particularly the Application, Security, or System logs, they might display thousands of entries. Unfortunately, this means that it might take some time to find what you are looking for.

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.



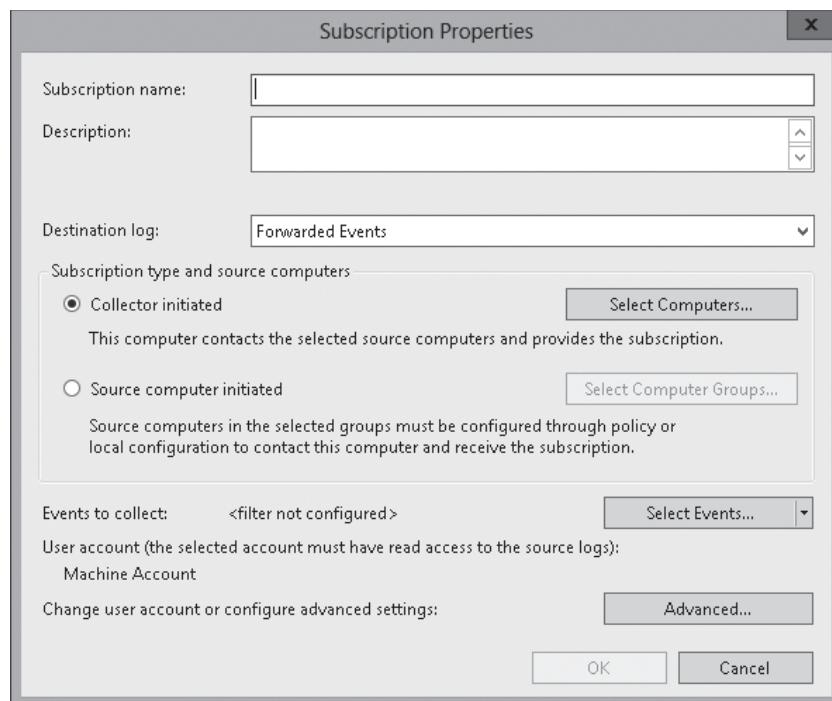
CREATE AN EVENT SUBSCRIPTION

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

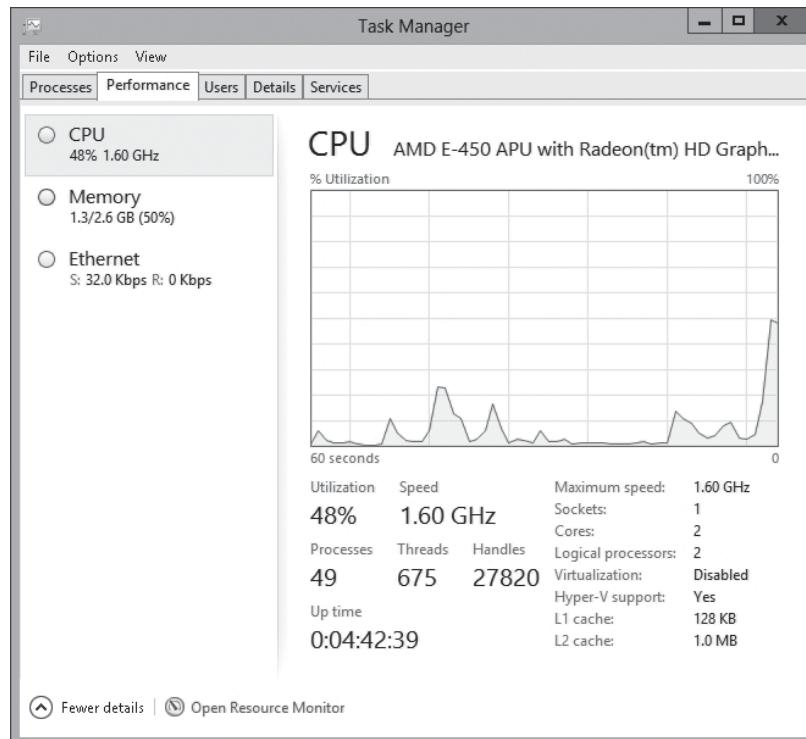
The Processes tab shows all processes running in memory and how much processing and memory each process uses. The processes will display applications (as designated by apps), background processes, and Windows Processes. On the Processes tab, you can perform the following tasks:

- 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

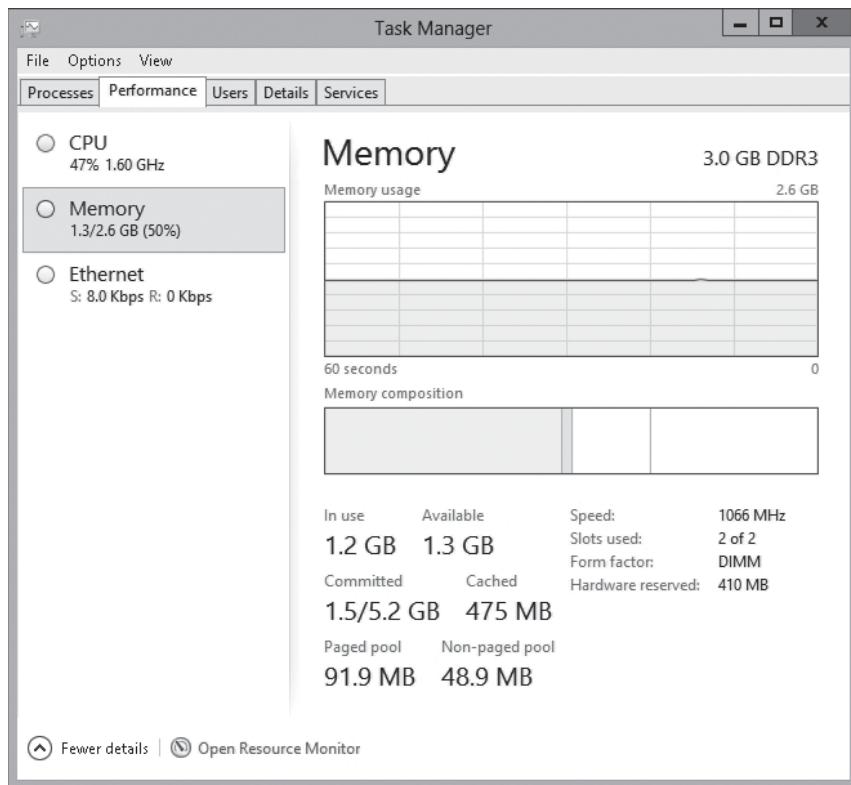
Viewing CPU usage



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

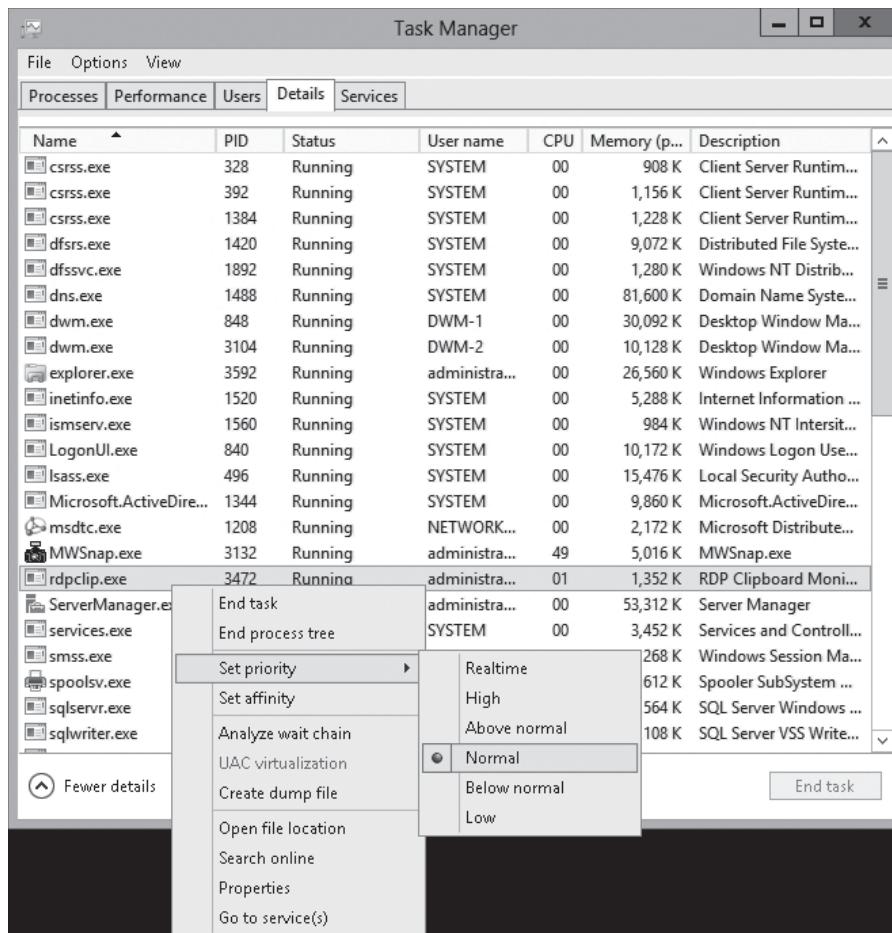


The *Users* tab displays the users who are currently logged in, the amount of CPU and memory usage that each user is using, and the processes the user is running. It also gives you the ability to disconnect them.

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.

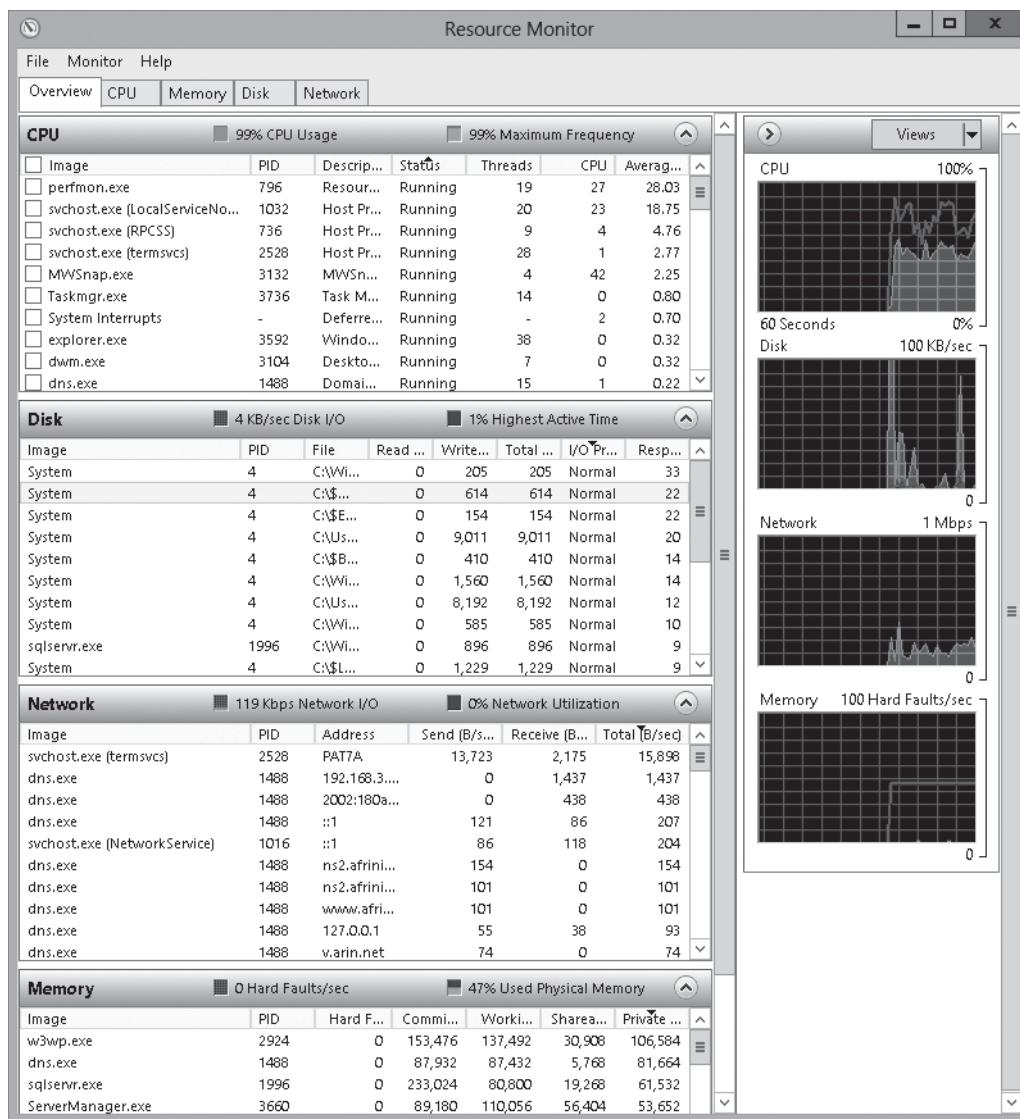
Using Resource Monitor

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.

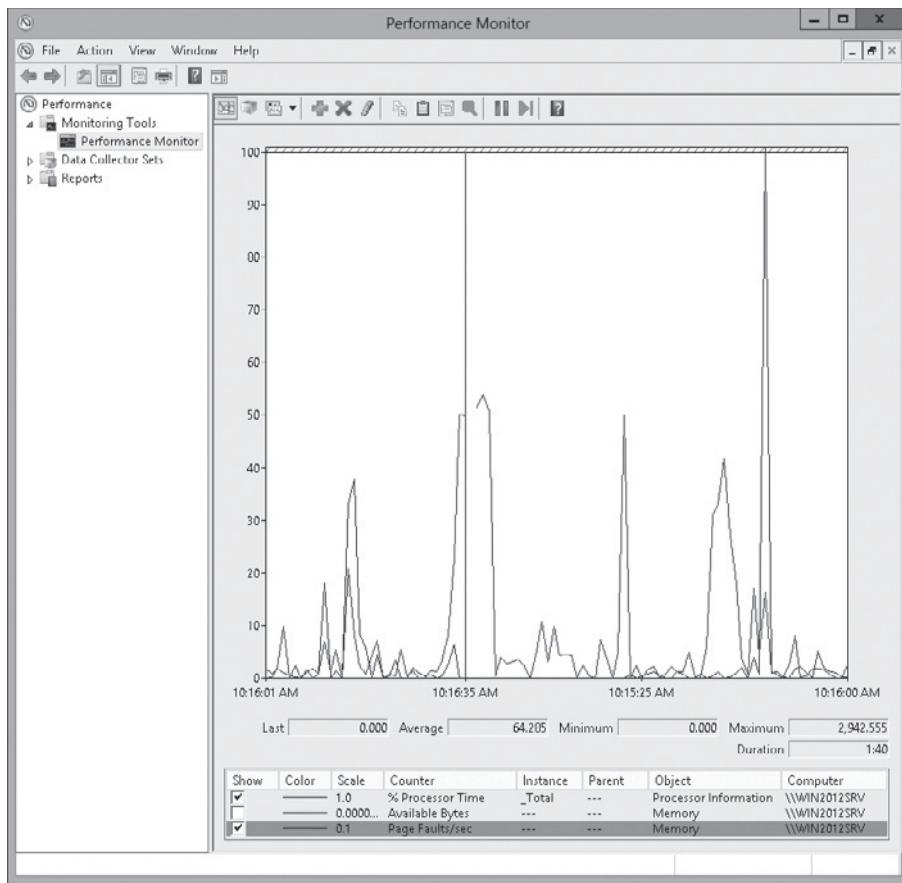
Using Performance Monitor

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

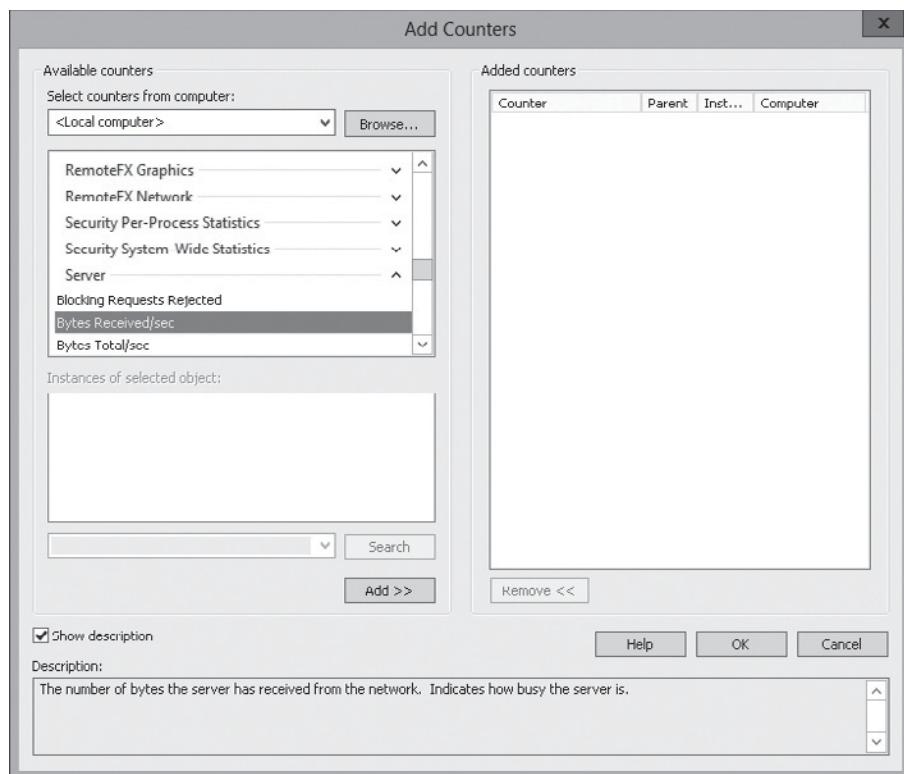
Viewing Performance Monitor



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 collector 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.

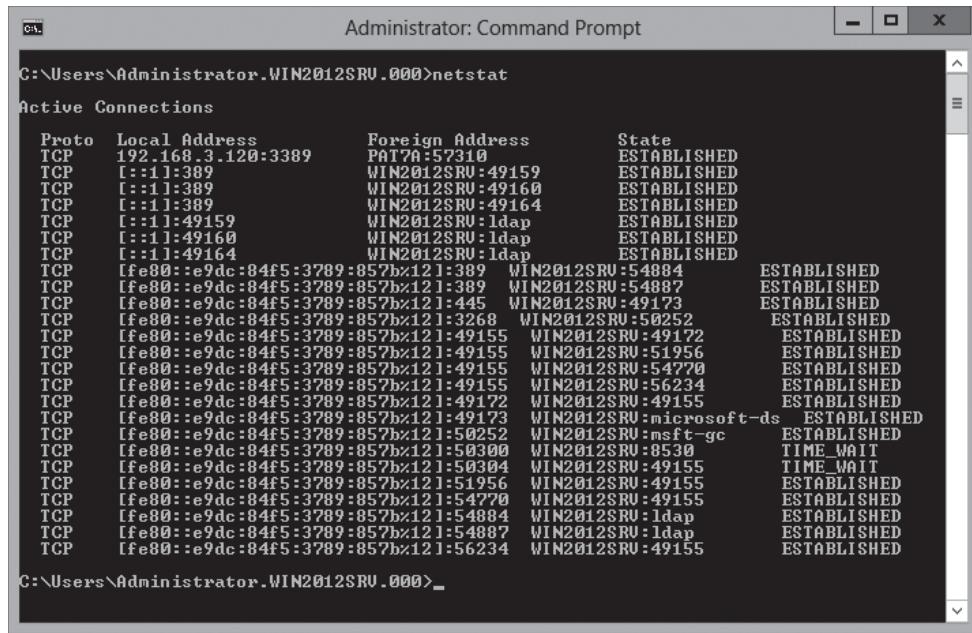
Using the `netstat` Command

The `netstat` command is used to view the TCP/IP connections, both inbound and outbound, on your computer. You can also use it 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%121:389  WIN2012SRU:54884   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:389  WIN2012SRU:54887   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:445  WIN2012SRU:49173   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:3268  WIN2012SRU:50252   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:49155  WIN2012SRU:49172   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:49155  WIN2012SRU:51956   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:49155  WIN2012SRU:54770   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:49155  WIN2012SRU:56234   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:49172  WIN2012SRU:49155   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:49173  WIN2012SRU:microsoft-ds  ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:50252  WIN2012SRU:msft-gc  ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:50300  WIN2012SRU:8530  TIME_WAIT
TCP    [fe80:::e9dc:84f5:3789:857b%121:50304  WIN2012SRU:49155  TIME_WAIT
TCP    [fe80:::e9dc:84f5:3789:857b%121:51956  WIN2012SRU:49155   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:54770  WIN2012SRU:49155   ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:54884  WIN2012SRU:ldap      ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:54887  WIN2012SRU:ldap      ESTABLISHED
TCP    [fe80:::e9dc:84f5:3789:857b%121:56234  WIN2012SRU: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.



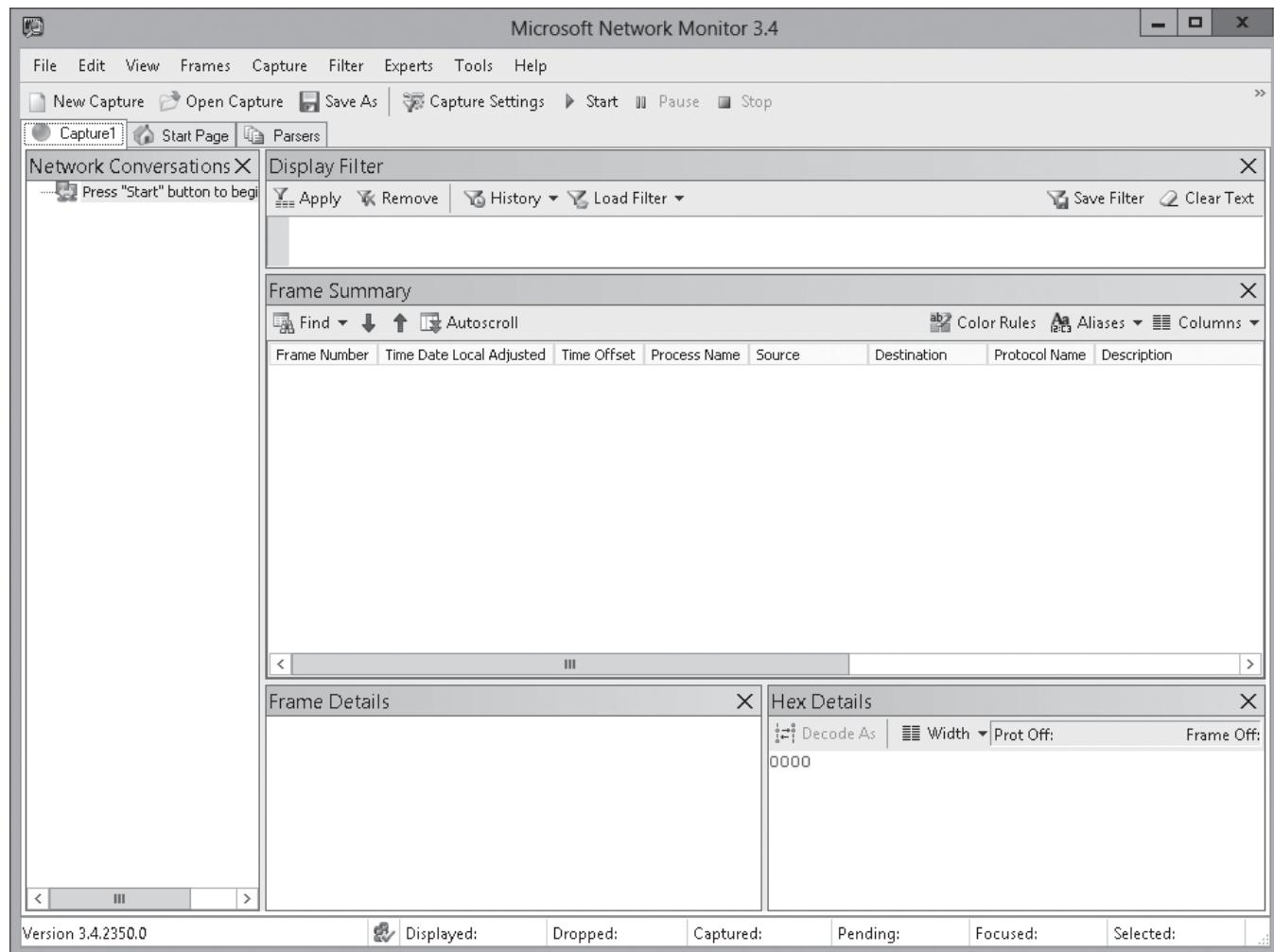
CAPTURE PACKETS

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).

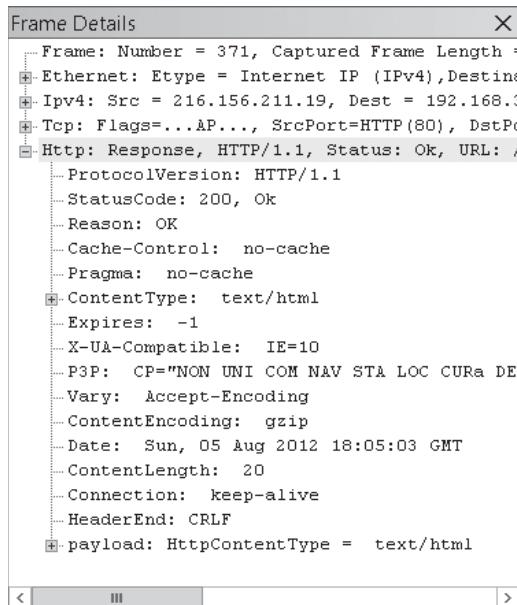
Most packets will be using the TCP/IP mode, which is a simplified OSI model that will have up to four parts:

- 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 10.0.0.1, execute the following command:

```
nmcap /network * /capture Ipv4.address ==  
10.0.0.1 /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

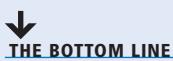
You have several file servers. Several times during the day, the file server performance degrades significantly. What steps should you perform to determine the cause of the problem?

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)

■ Using Distributed File System



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

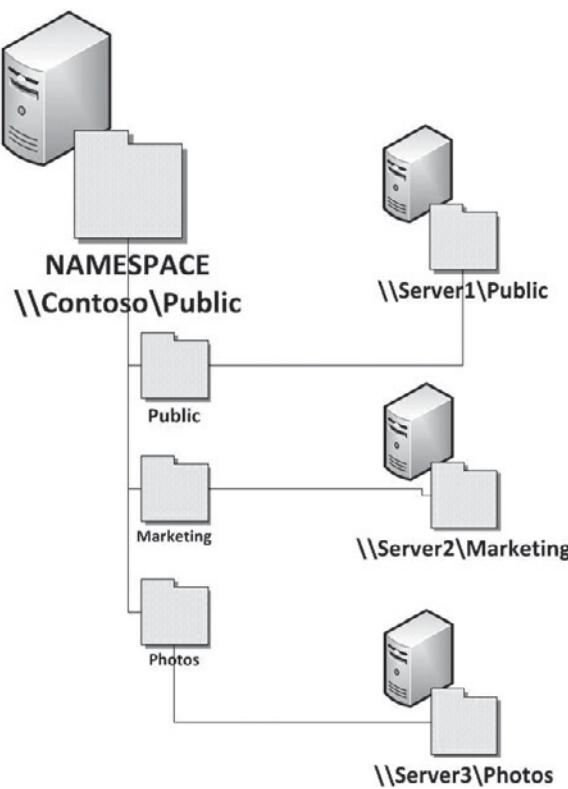
Installing and Configuring DFS Namespace

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.



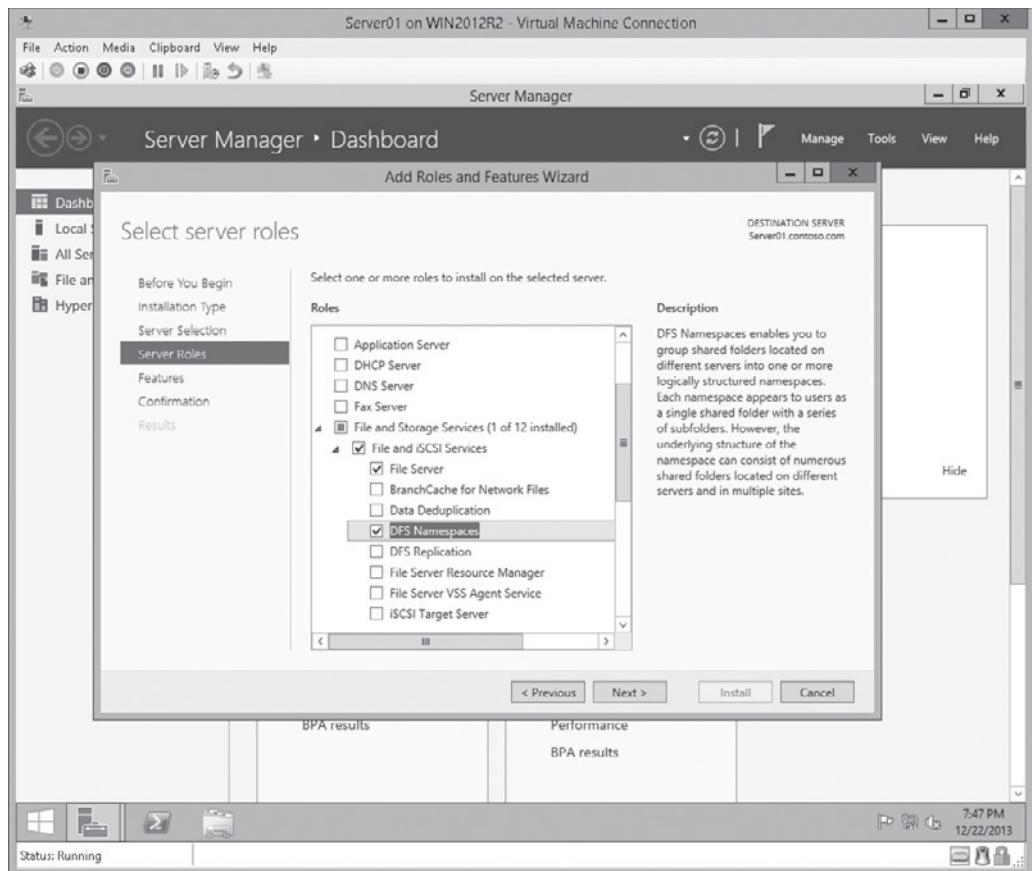
INSTALL DFS NAMESPACE

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.



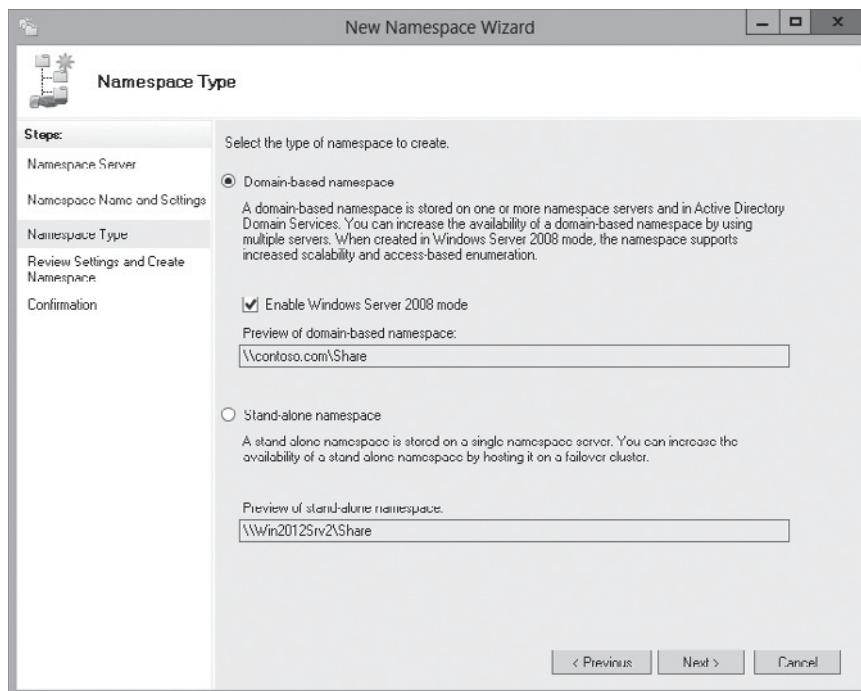
CREATE A DFS NAMESPACE

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 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 site* 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, particularly 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**, where 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:

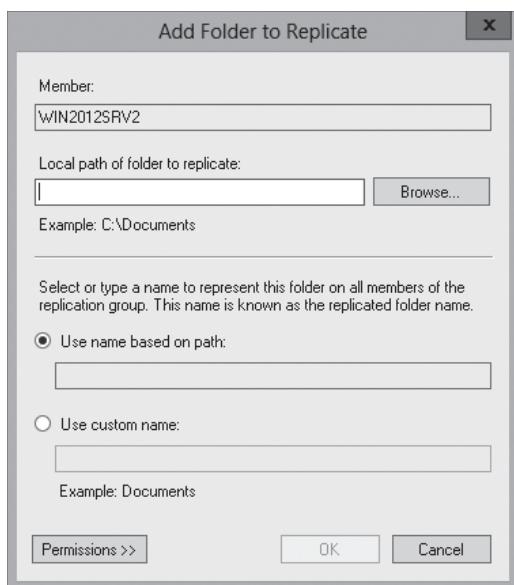
1. Open **Server Manager**.
2. Click **Tools > DFS Management**. The *DFS Management console* opens.



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

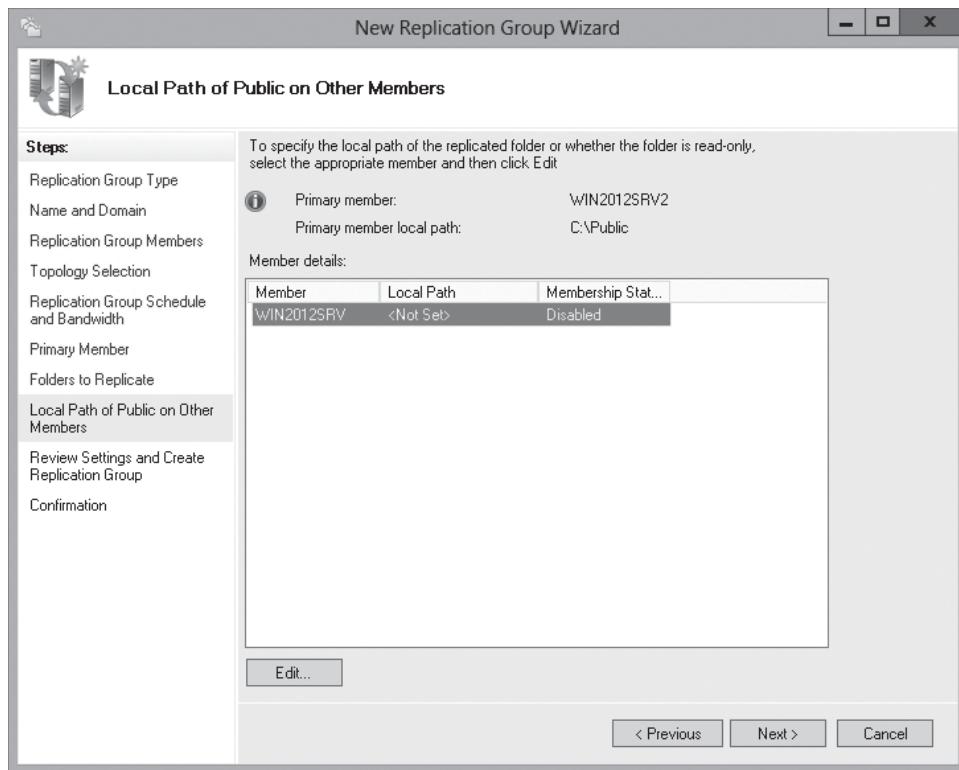
Specifying the local folders to replicate



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



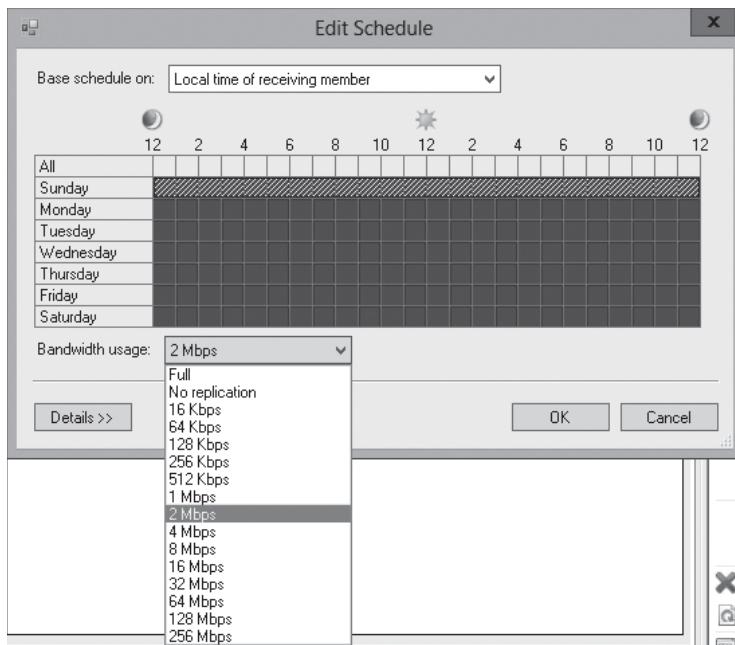
18. When the *Edit* dialog box opens, select **Enabled** and type the local path on the member server. Click **OK** to close the *Edit* dialog box.
19. Back on the *Local Path of Public on Other Members* page, click **Next**.
20. On the *Review Settings and Create Replication Group* page, click **Create**.
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.



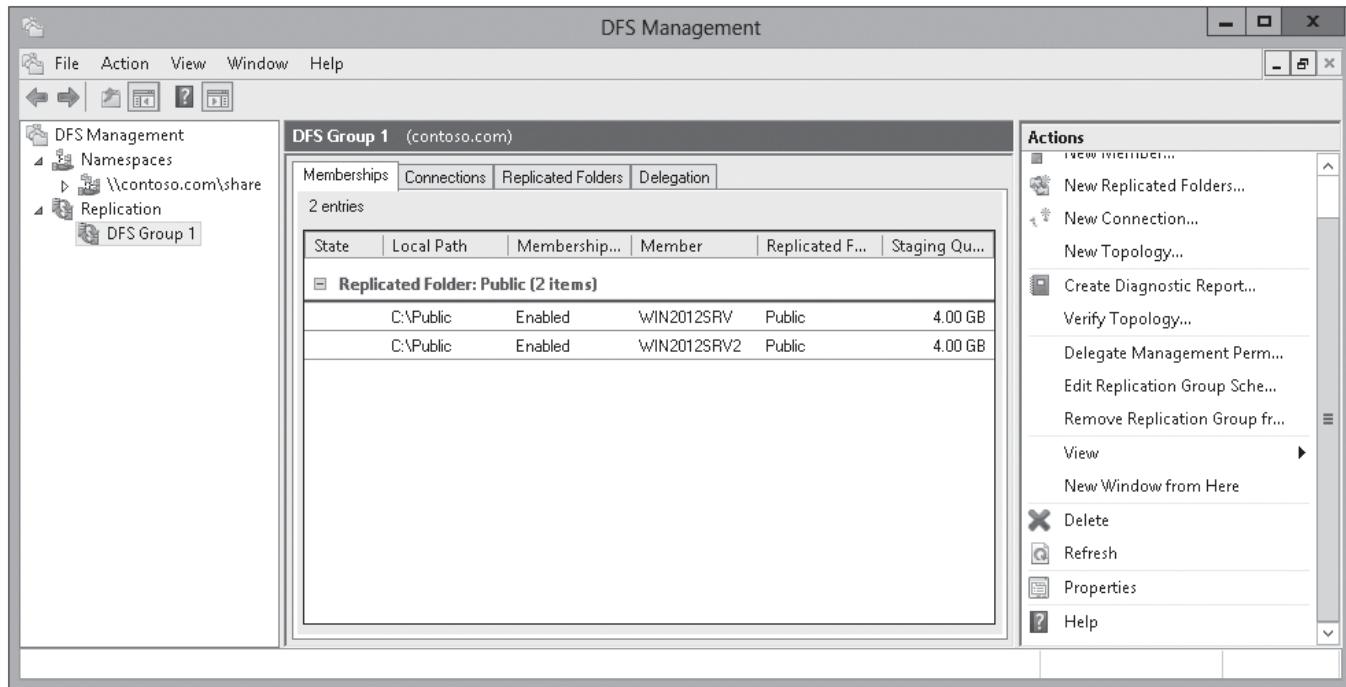
DISABLE REMOTE DIFFERENTIAL COMPRESSION

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

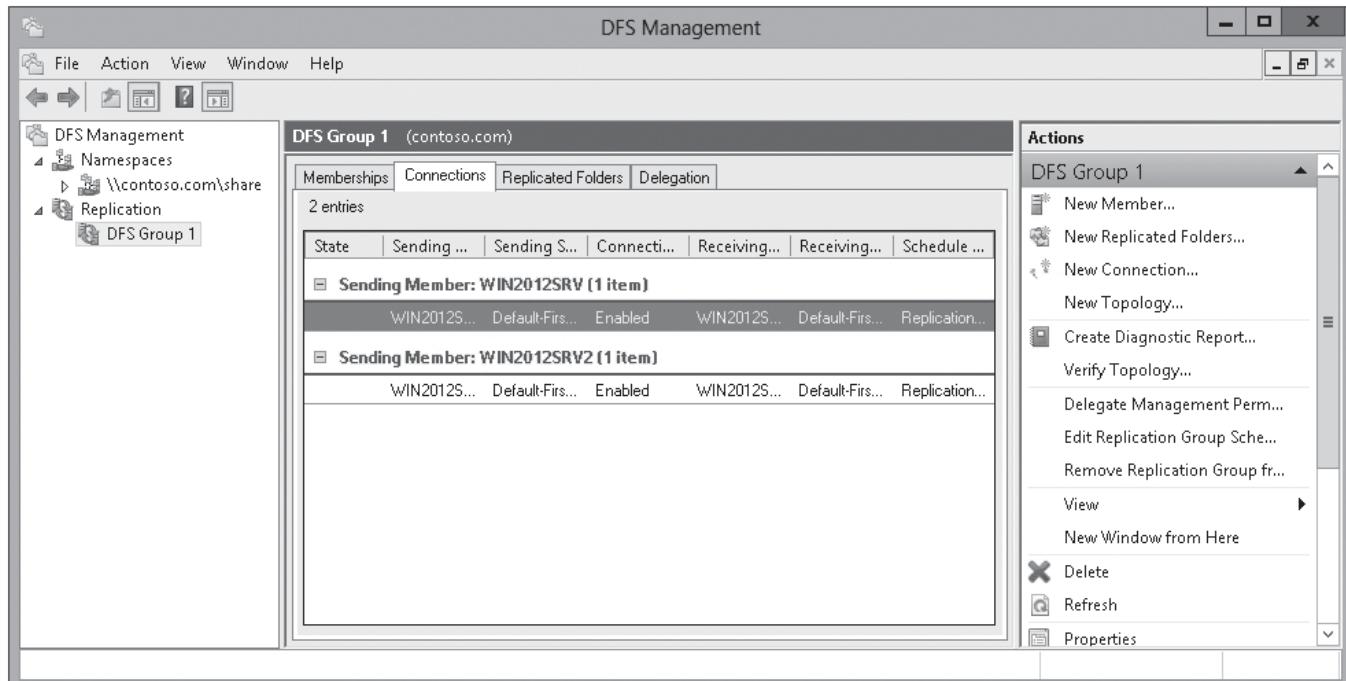
Showing a created DFS Replication Group



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:\dfsrlclone
```

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?

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.



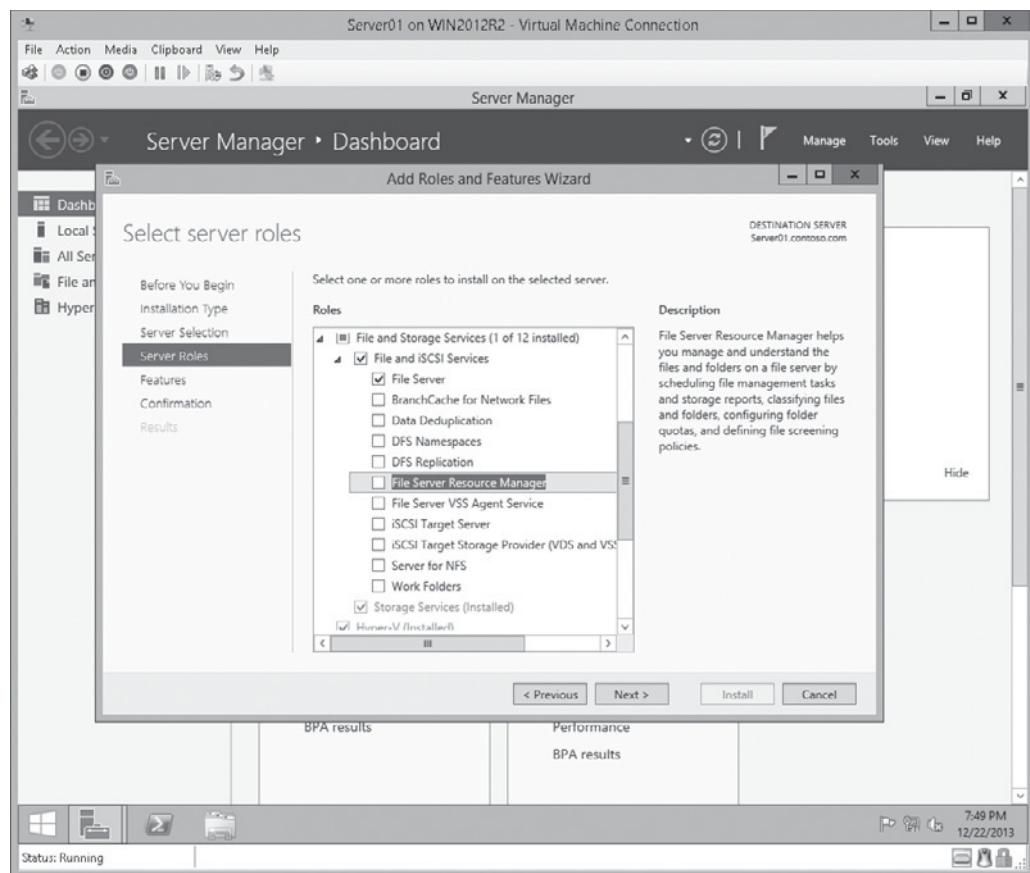
INSTALL FILE SERVER RESOURCE MANAGER

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.



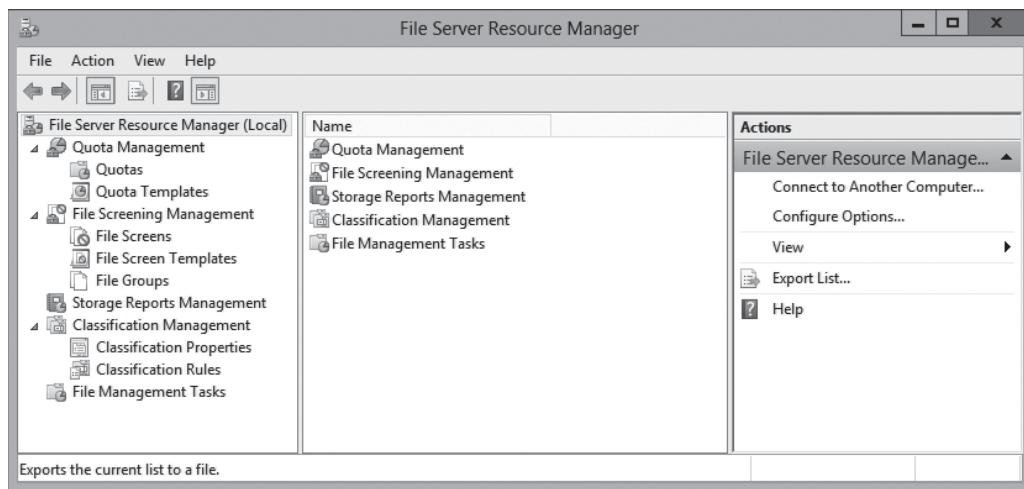
CREATE A QUOTA TEMPLATE

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

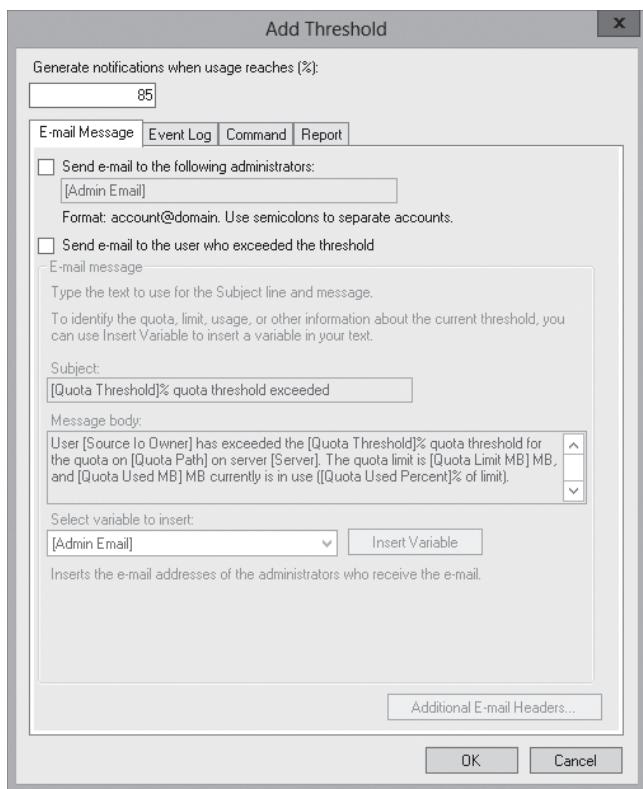
Viewing the File Server Resource Manager console



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.



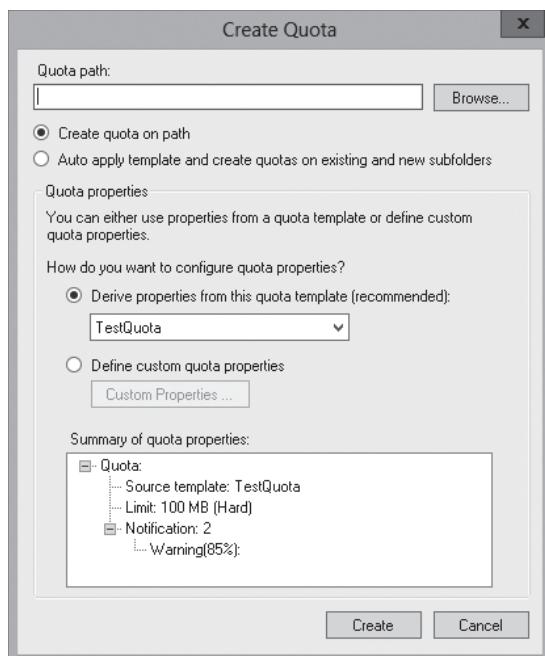
CREATE A QUOTA FROM A QUOTA TEMPLATE

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.



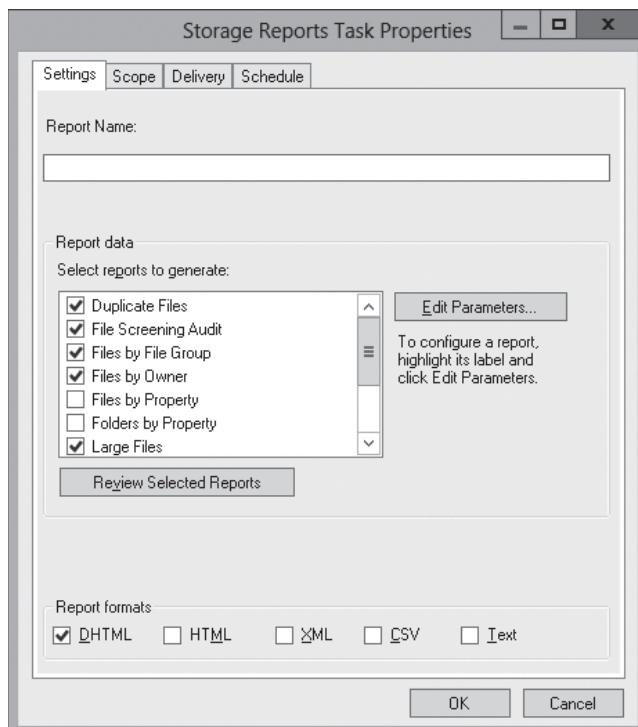
SCHEDULE A STORAGE REPORT

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.



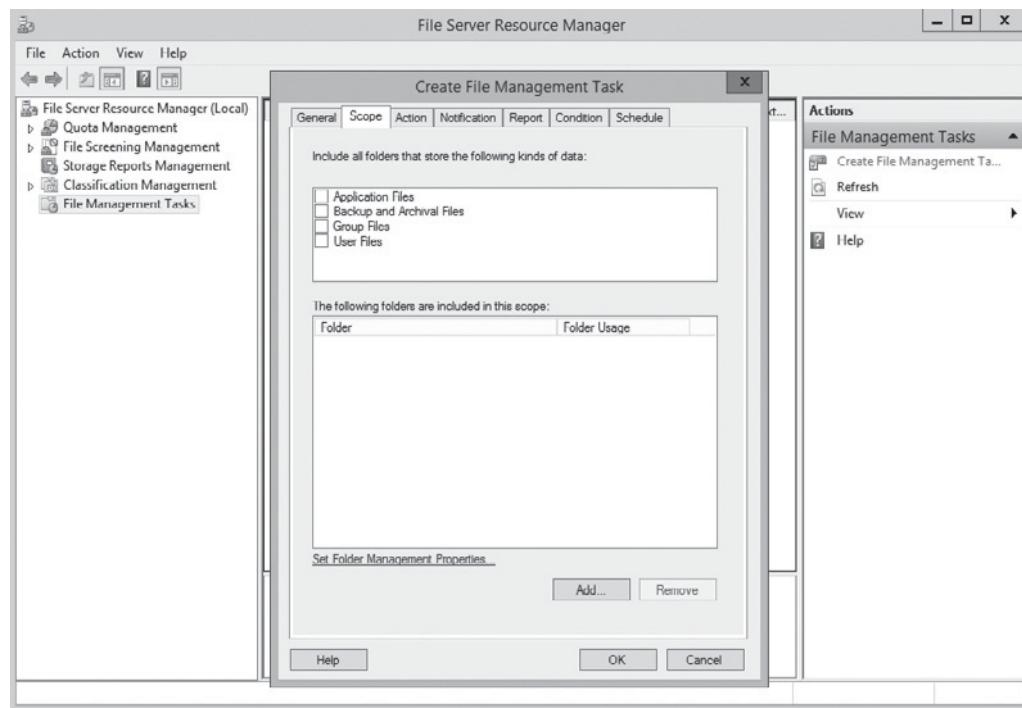
CREATE A FILE MANAGEMENT TASK

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

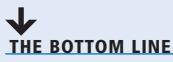
You were just hired as an administrator for Contoso Corporate. You looked for a file server and discovered that several users have been using the file server as a personal repository for audio and video files that have been downloaded using the corporate network. How should you stop users from saving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

■ Securing Files



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

The screenshot shows the 'Group Policy Management Editor' window. The left pane displays a navigation tree under 'Security Settings'. The 'Public Key Policies' node is expanded, showing sub-options like 'Encrypting File System', 'Data Protection', etc. The right pane is a table titled 'Certificates' with the following data:

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
Administrator	contoso-WIN2012SRV-CA	8/18/2014	File Recovery	<None>
Administrator	contoso-WIN2012SRV-CA	8/17/2014	File Recovery	<None>
Administrator	contoso-WIN2012SRV-CA-1	10/8/2014	File Recovery	<None>
administrator	administrator	6/26/2112	File Recovery	<None>
Ted Wilson	contoso-WIN2012SRV-CA	8/18/2014	File Recovery	<None>

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.



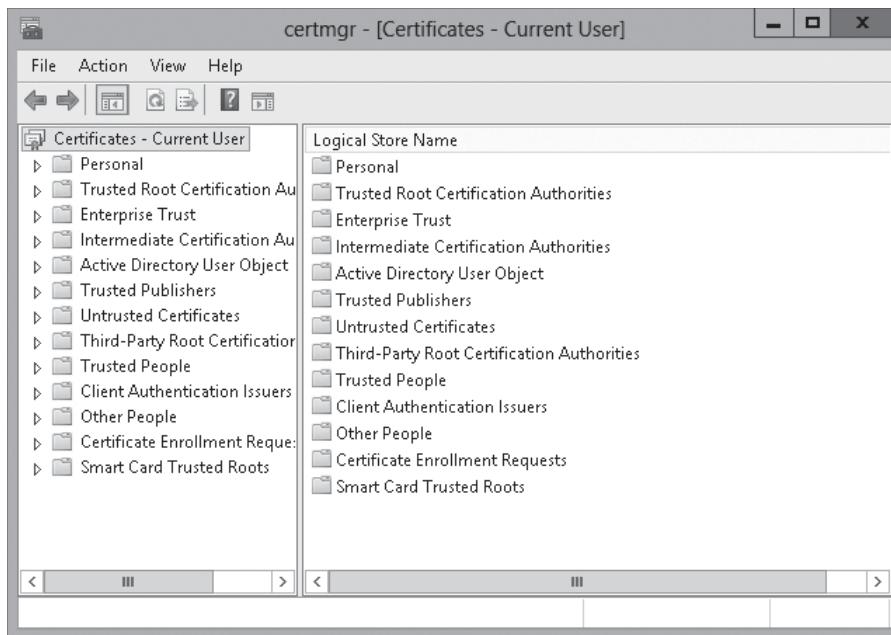
BACK UP AN EFS CERTIFICATE

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.



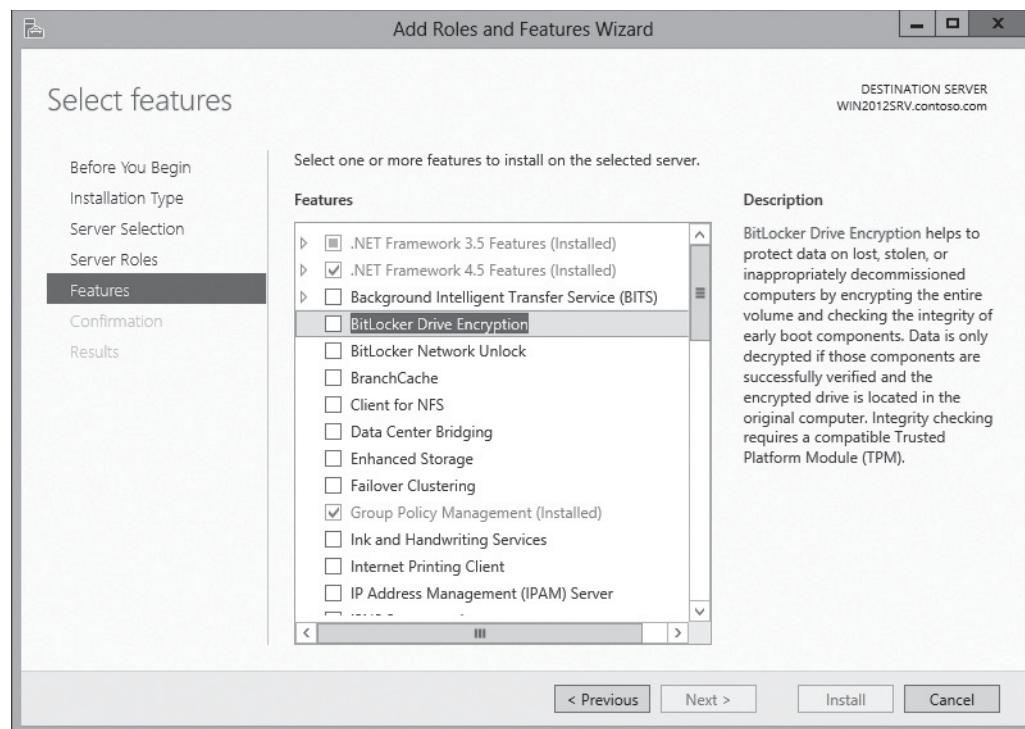
INSTALL BITLOCKER

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

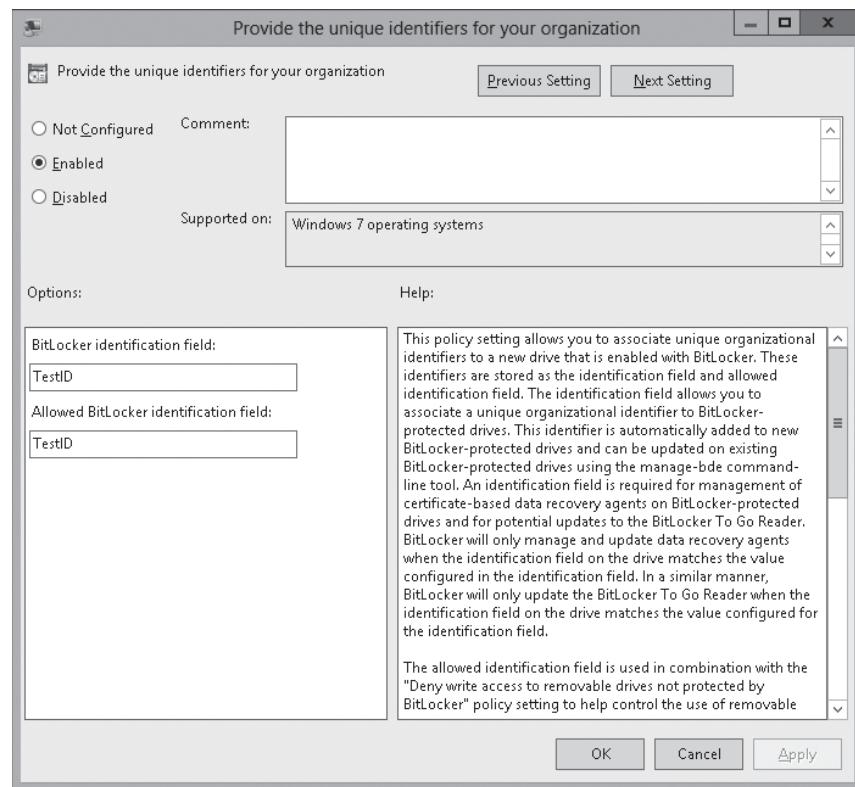
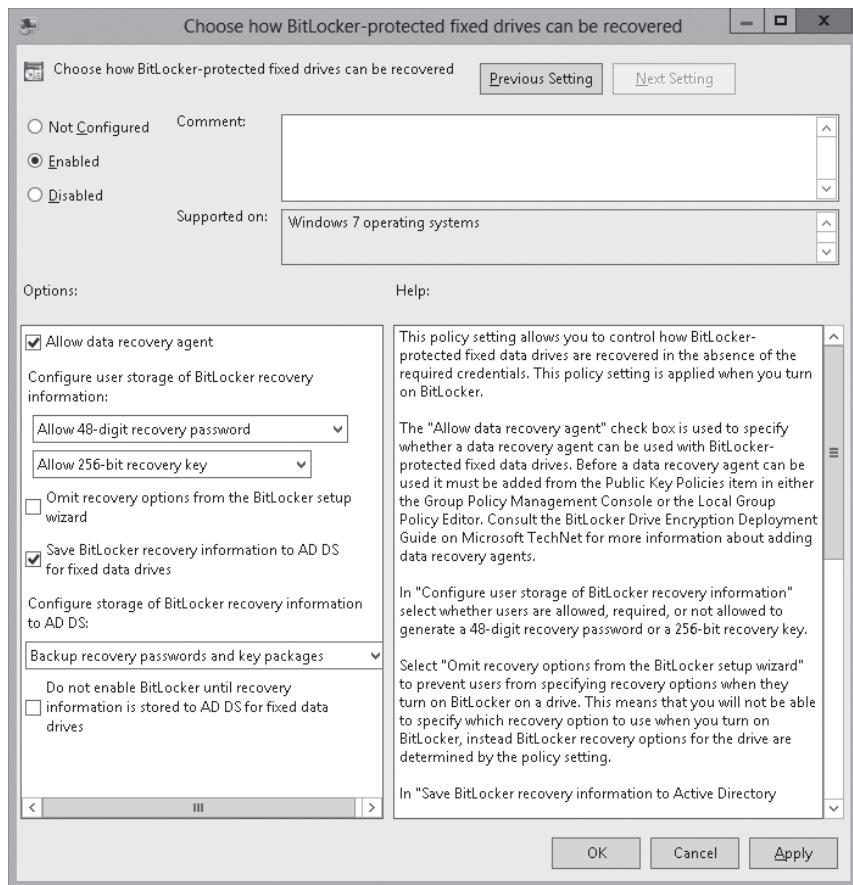


Figure 6-5

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

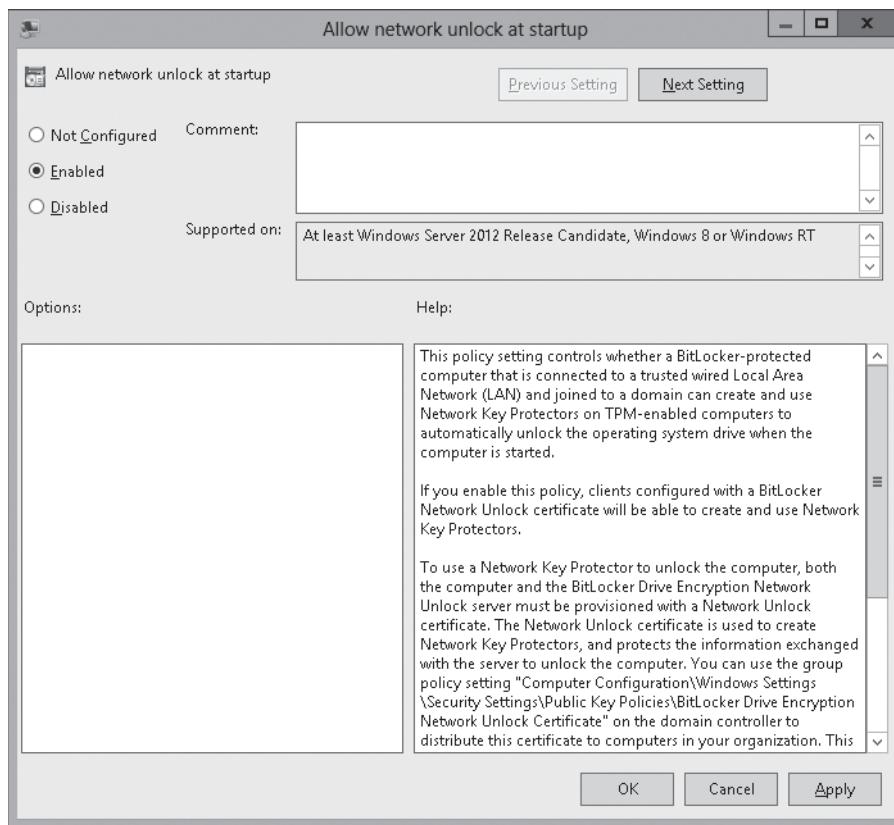
Network Unlock provides an automatic unlock of operating system volumes at system reboot when connected to a trusted wired corporate network.

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?

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

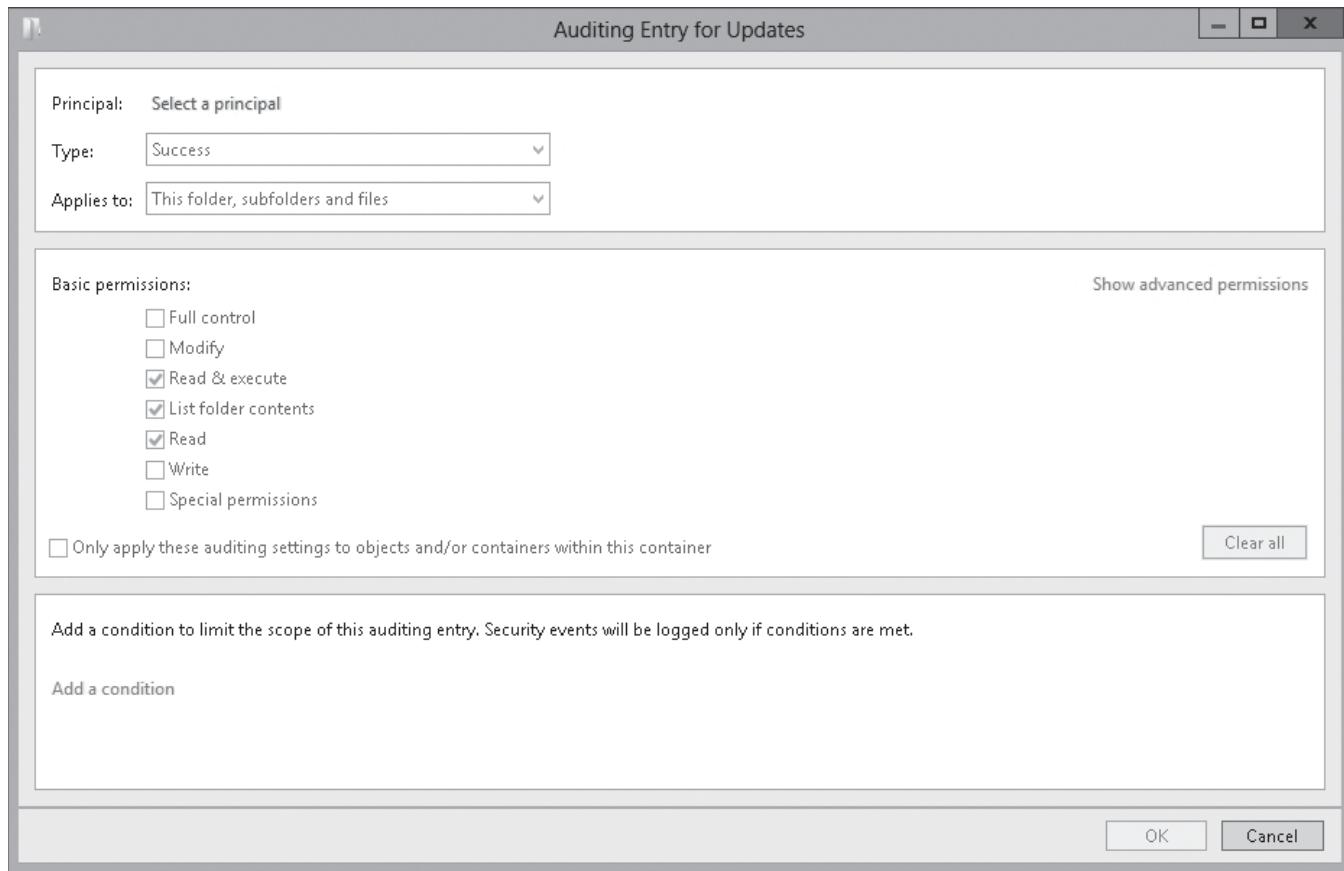
GET READY. To audit files and folders, perform the following steps:

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 object access 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	<p>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.</p> <p>Note: Directory Service Changes auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed.</p>	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none"> • 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:
	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 /
```

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.



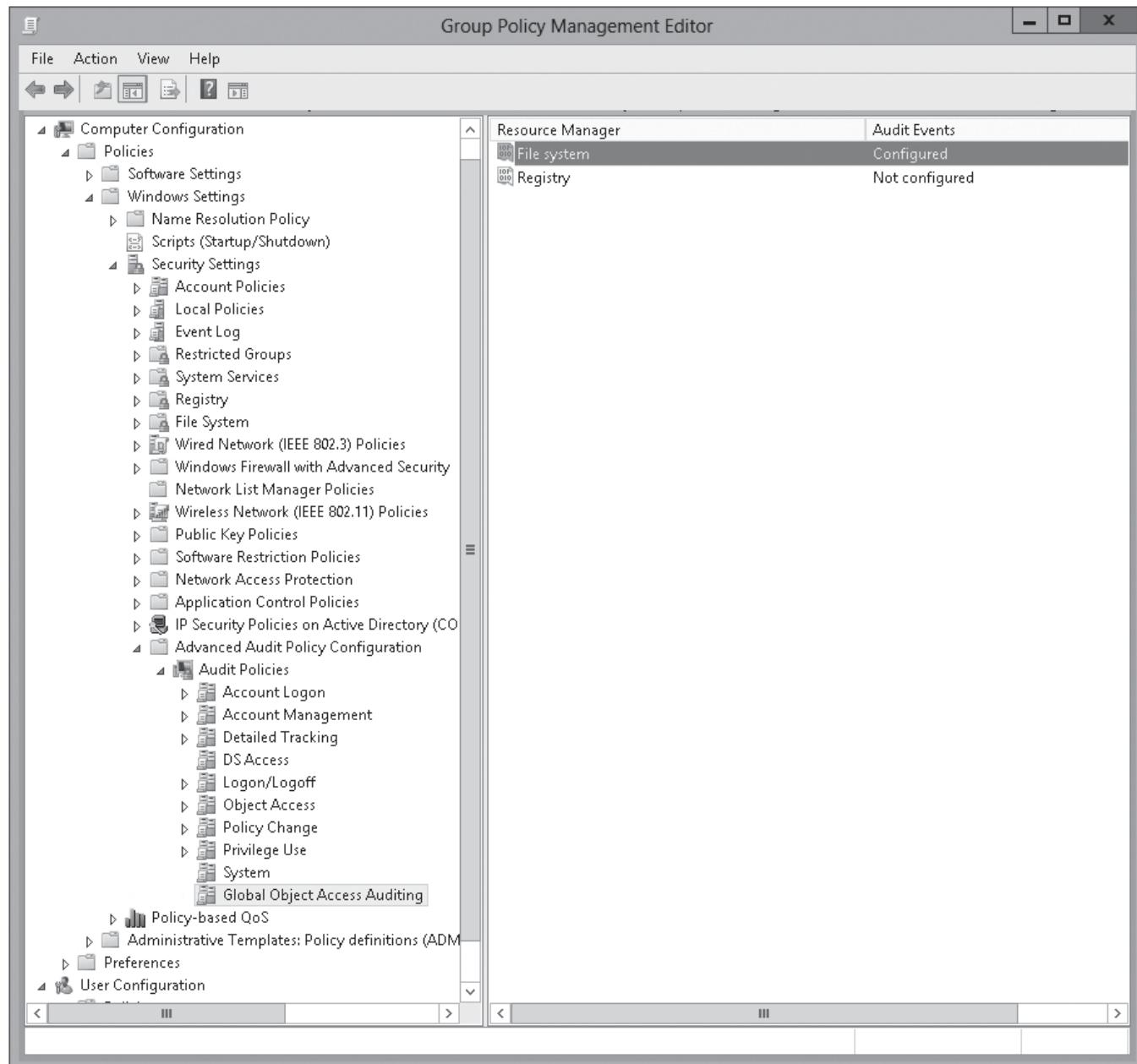
DEFINE GLOBAL OBJECT ACCESS AUDITING

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

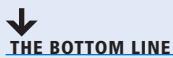
You just established an audit policy that enables account logon, logon, object access, and account management. However, when you look at the logs, you see a large number of Audit Filtering Platform Connection and Audit Filtering Platform Packet Drop events that consume most of the security logs. What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

■ Understanding DNS



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.



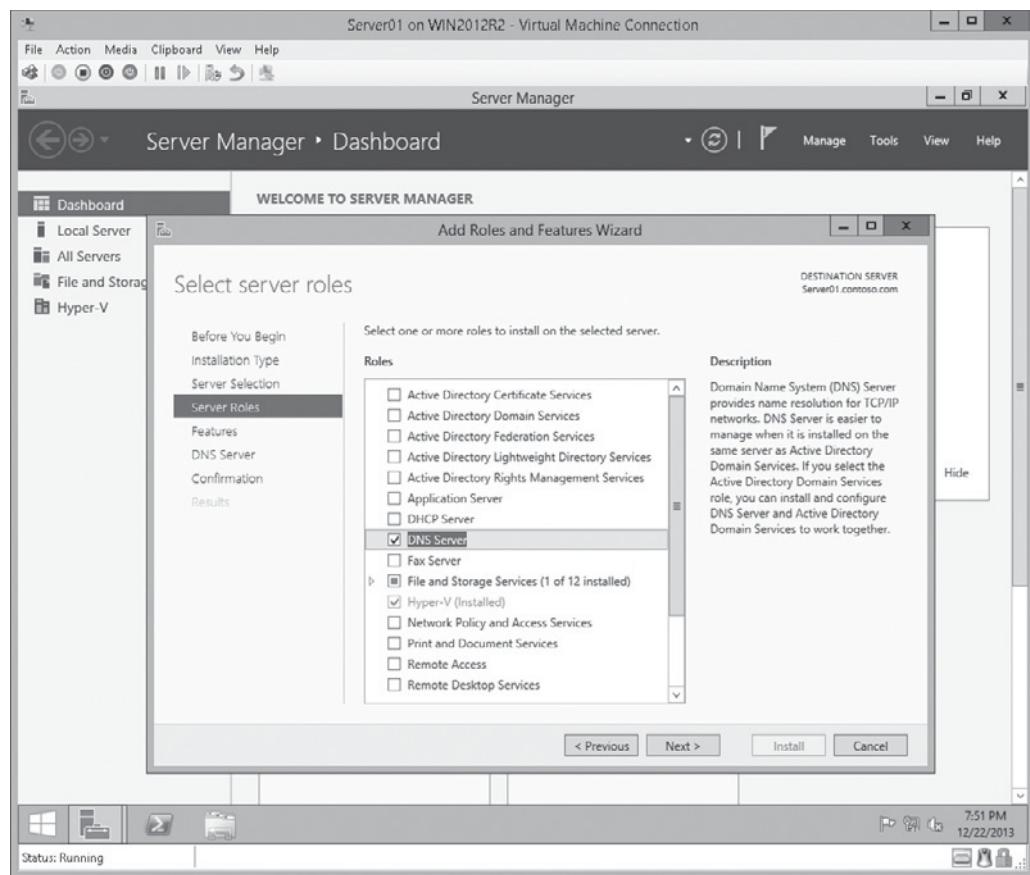
INSTALL DNS

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



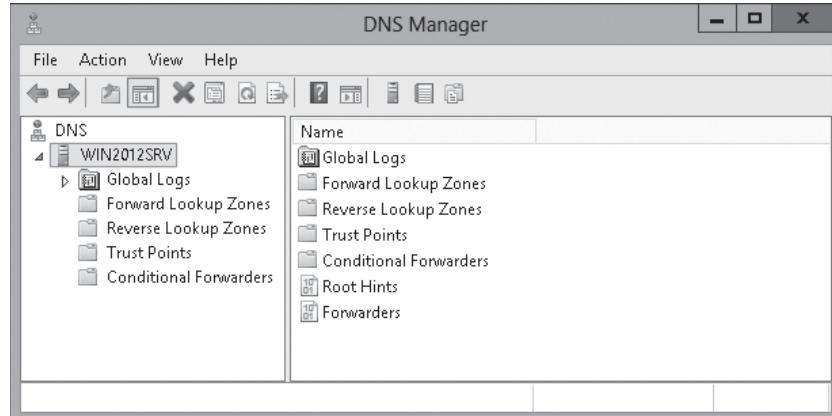
7. When the *Add Roles and Features Wizard* dialog box appears, select **Add Features**, and then click **Next**.
8. When the *Select features* page opens, click **Next**.
9. On the *DNS Server* page, click **Next**.
10. On the *Confirm installation selections* page, click the **Install** button.
11.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



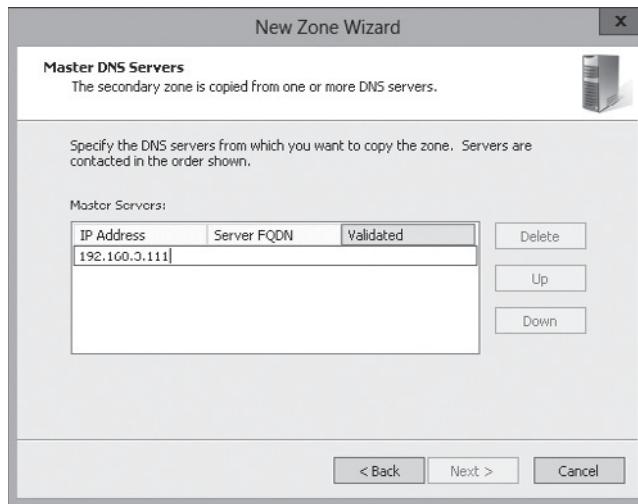
CREATE A STANDARD FORWARD LOOKUP SECONDARY ZONE

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.



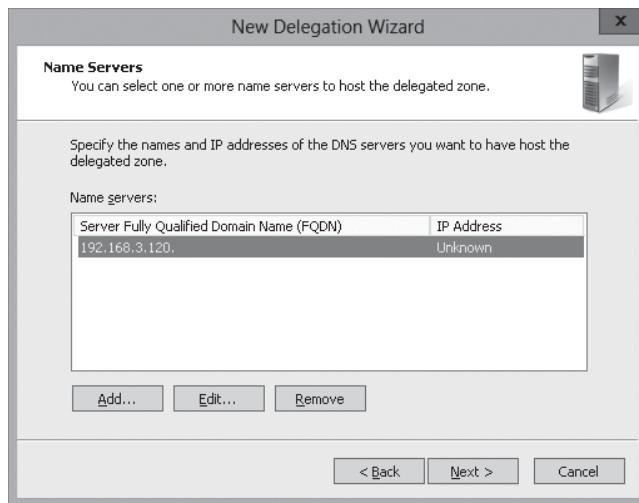
DELEGATE A DNS DOMAIN

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.



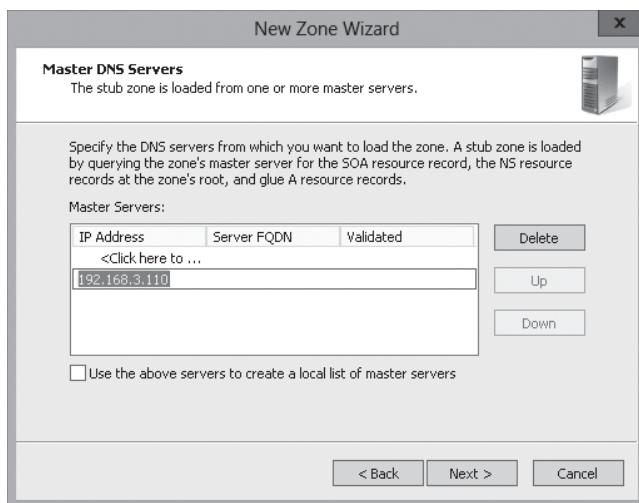
CREATE A STUB ZONE

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

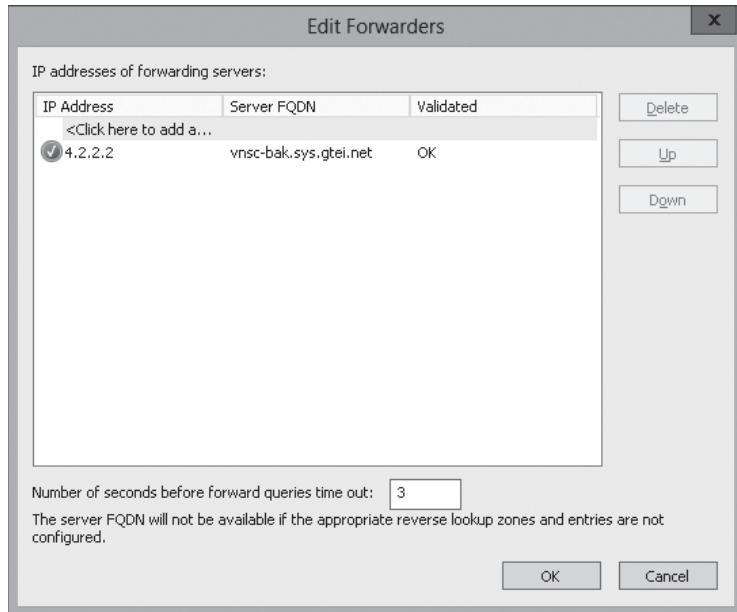
GET READY. To configure a DNS server to forward DNS queries to another DNS server, perform the following steps:

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 requests 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

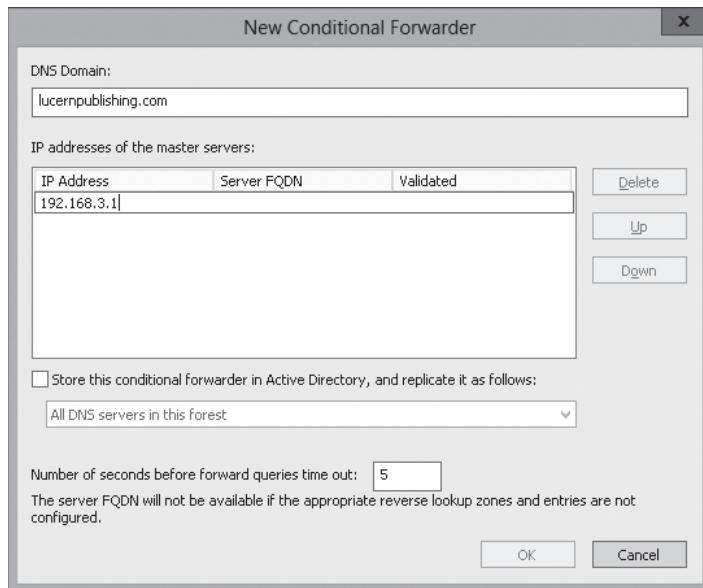
GET READY. To configure a DNS server to forward DNS queries to another DNS server, perform the following steps:

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?

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:

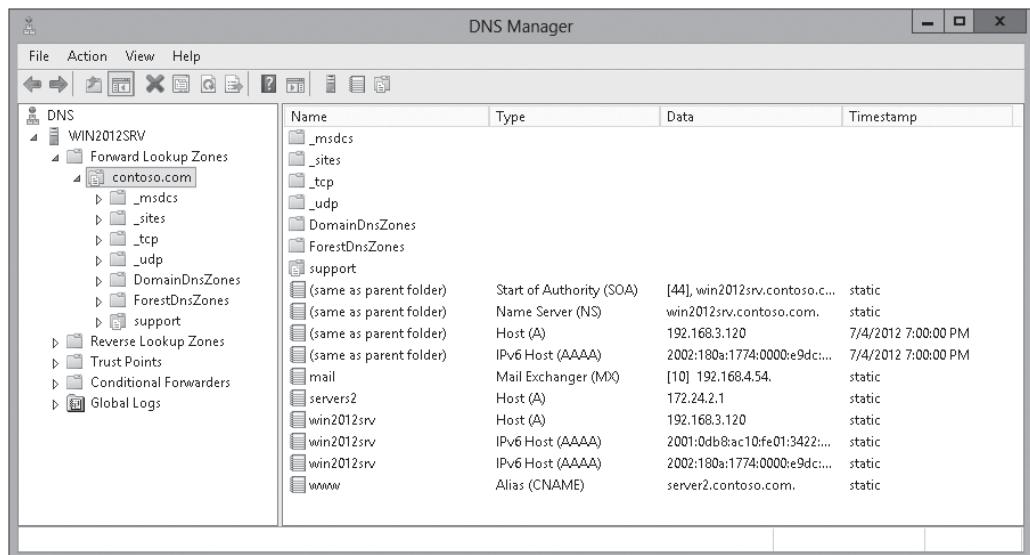
- **Start of Authority (SOA) record:** Specifies authoritative information about a DNS zone, including the primary name server, the e-mail of the domain administrator, the domain serial number, and the expiration and reload timers of the zone.
- **Name Server (NS) record:** Specifies an authoritative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

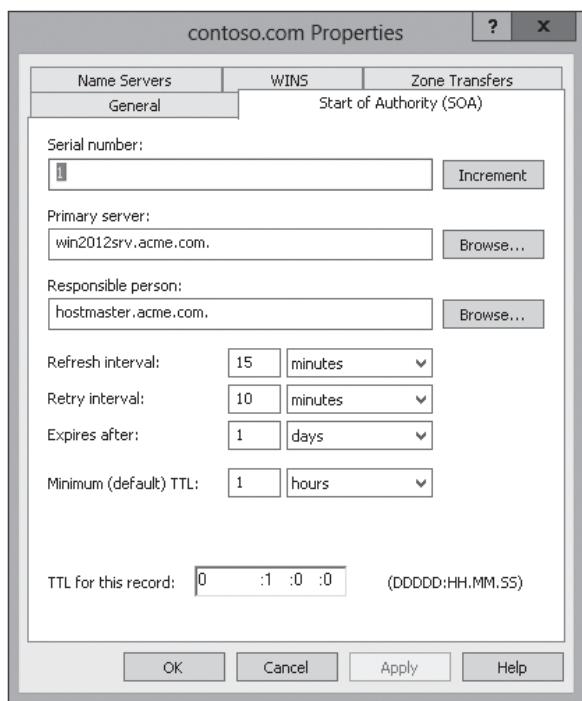
The SOA record specifies authoritative information about the zone. Therefore, there is only one SOA record for a zone. It includes the following fields:

- **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

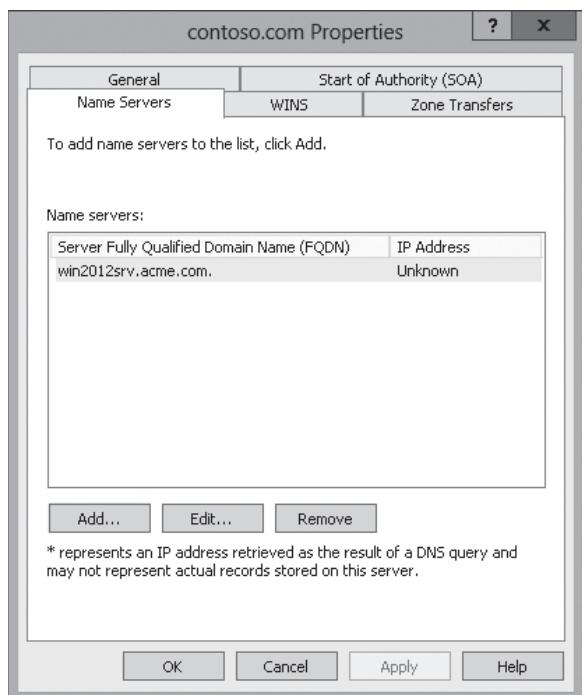


NAME SERVER (NS) RECORDS

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.

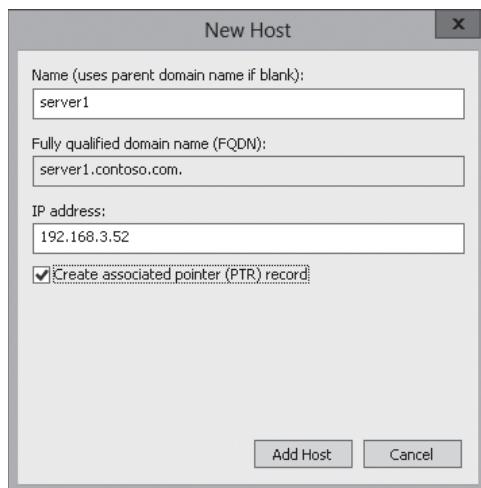
For example, the following A resource record is located in the zone `server1.sales.contoso.com` and maps the Fully Qualified Domain Name (FQDN) of a server to an IP address of 192.168.3.41:

```
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



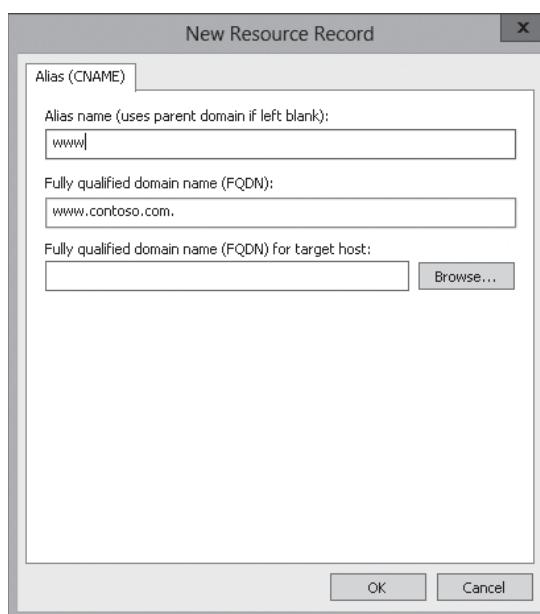
CANONICAL NAME (CNAME) RECORDS

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

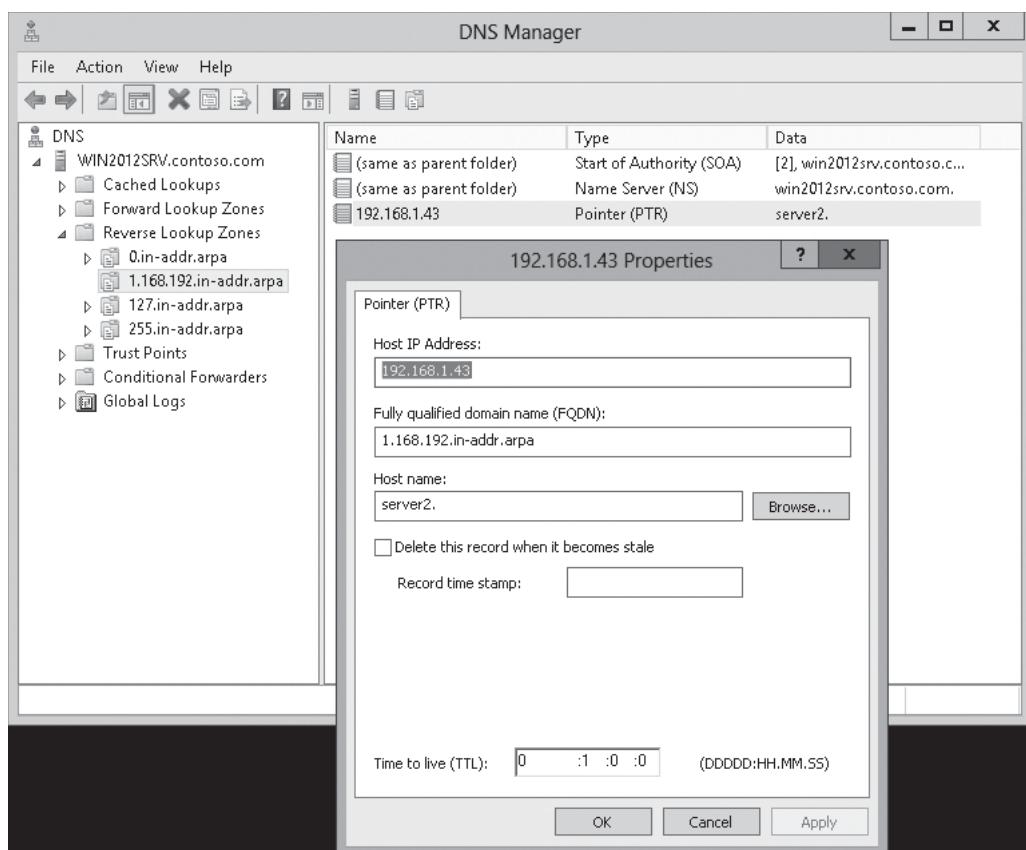
The Pointer records (PTR) are used for the opposite reason of the Host records. They resolve host names from an IP address. Different from the Host record, the IP address is written in reverse. For example, the IP address 192.168.3.41 that points to `server1.sales.contoso` is:

```
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.

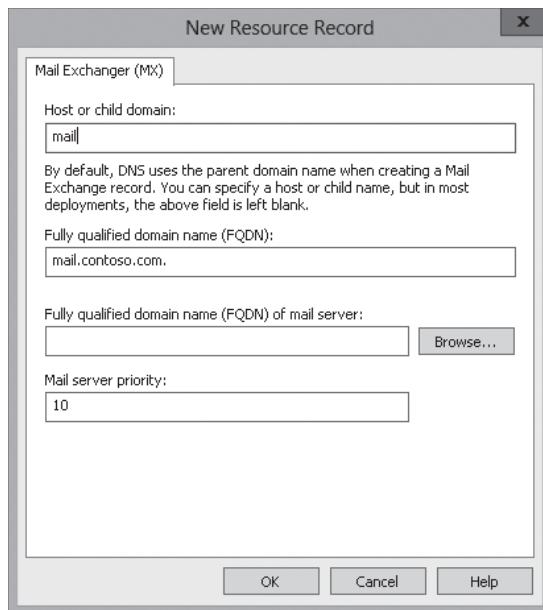
For example, if you have three mail servers that can receive e-mail over the Internet, you would have three MX records for the `contoso.com` domain:

```
@ 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

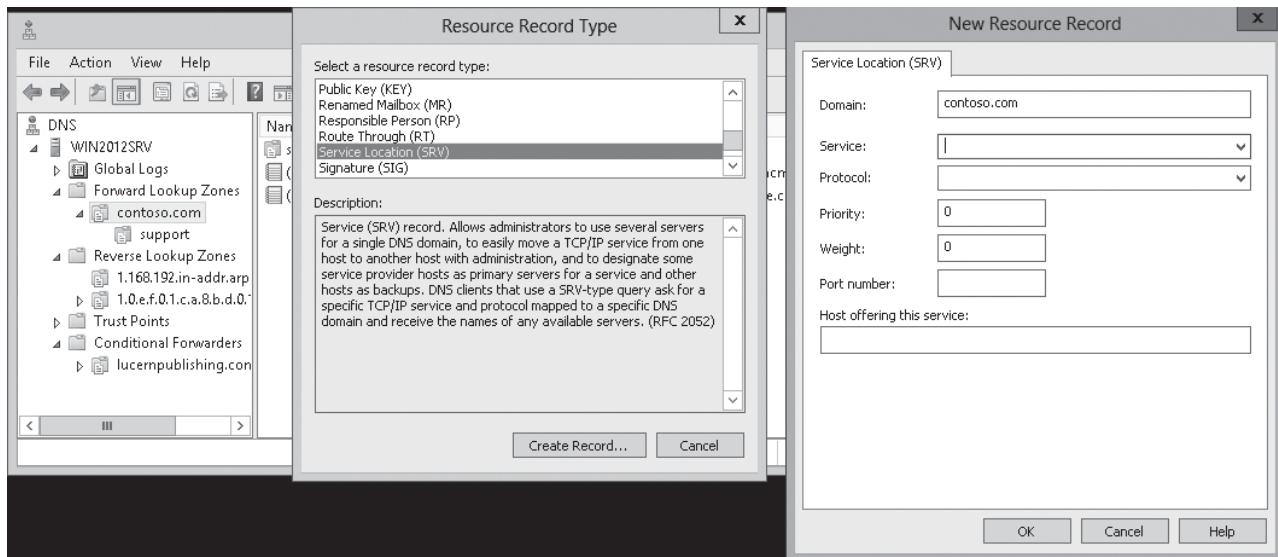
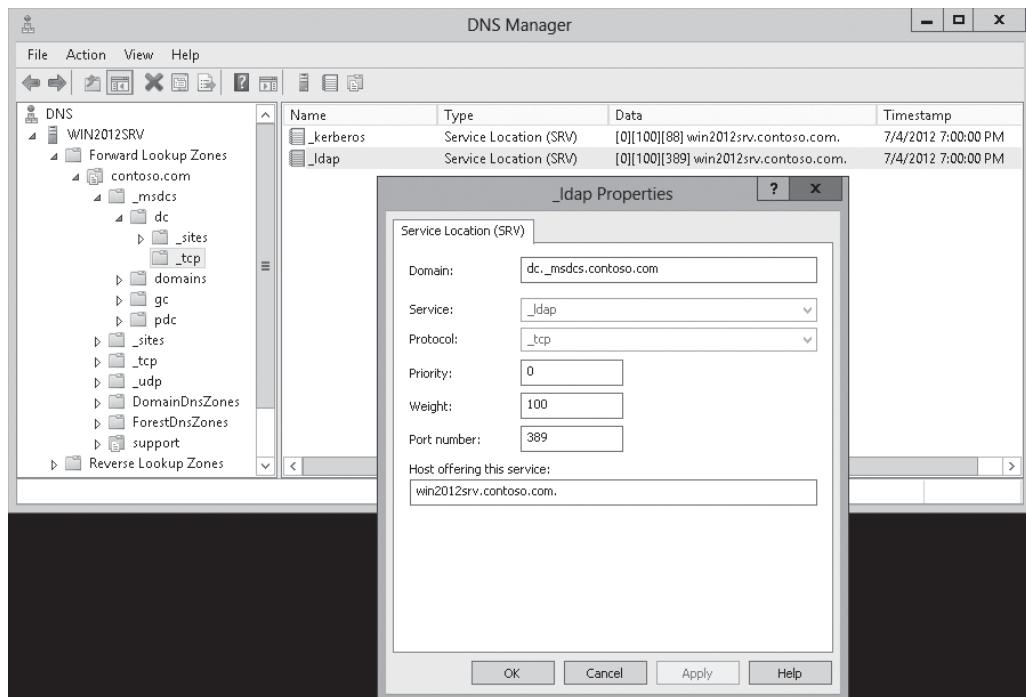


Figure 9-9

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:

TAKE NOTE *

Scavenging and aging must be enabled at the DNS server and on the zone.



WARNING Be careful when enabling scavenging because it can accidentally remove records that you want to keep. As a result, users cannot resolve certain DNS queries, making some network services unavailable.

- 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.

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.

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.



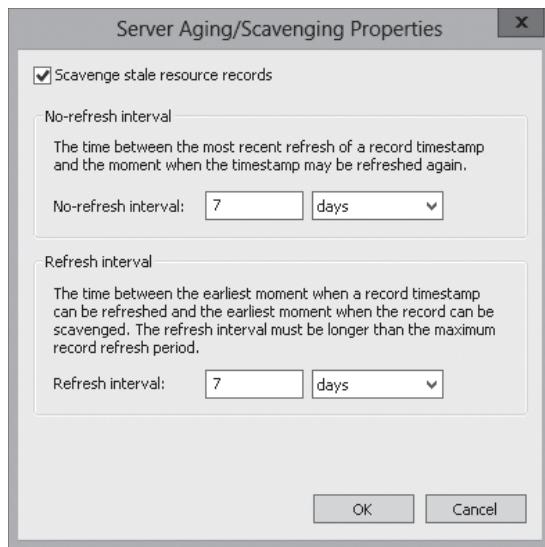
ENABLE AGING/SCAVENGING AT THE SERVER

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?

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.



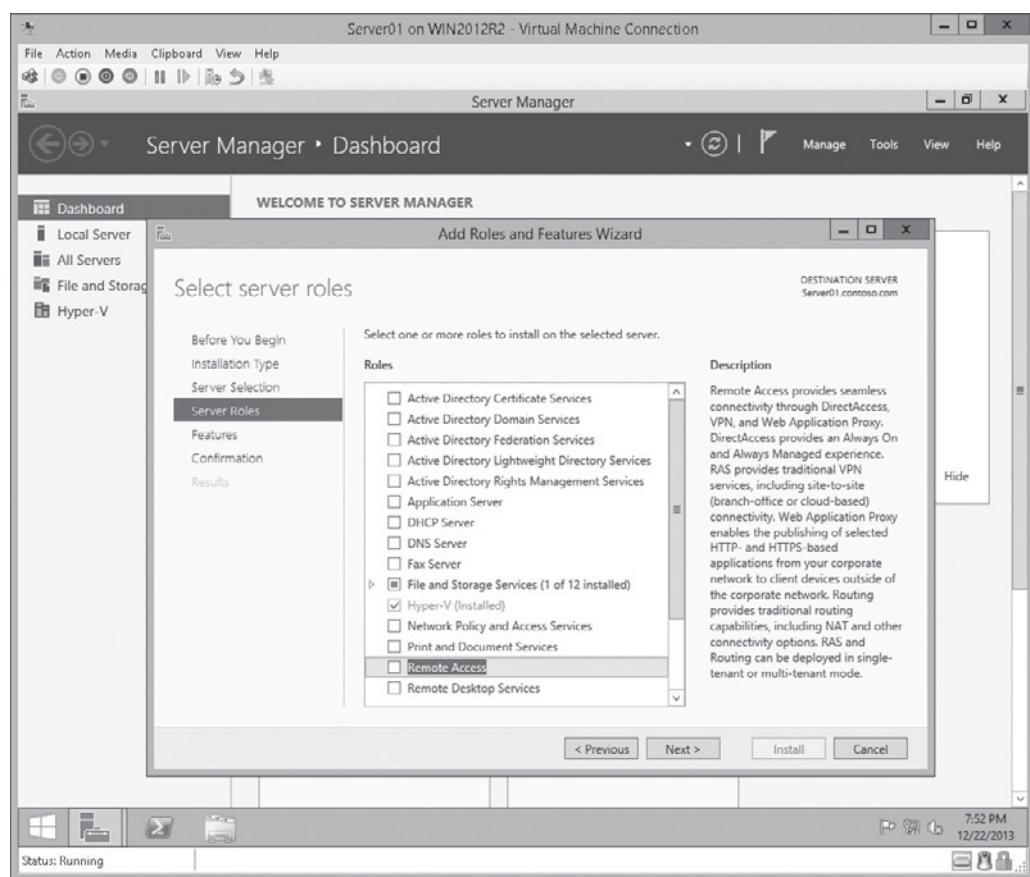
INSTALL THE REMOTE ACCESS ROLE

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*

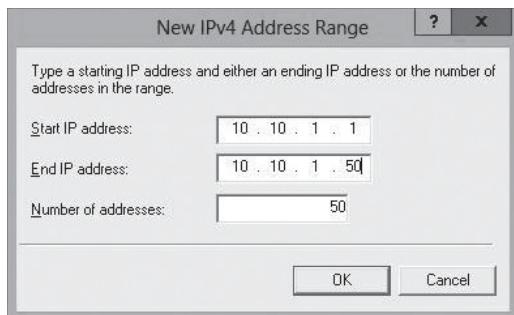
If you intend to protect your RRAS server by using a firewall instead, do not enable the *Enable security on the selected interface by setting up static packet filters* option. In addition, if you enable this option, by default, you will not be able to ping the IP address of the public network adapter 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

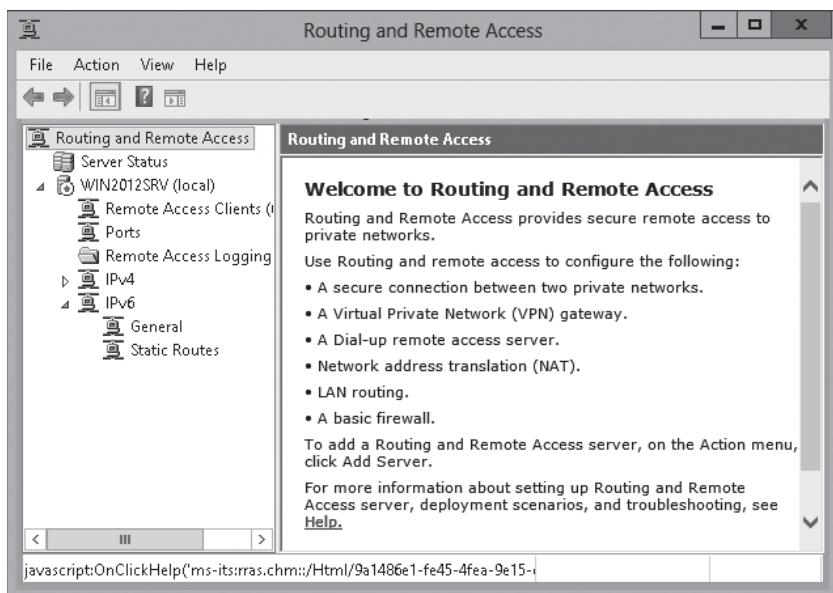
Using the New IPv4 Address Range dialog box



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 connect.
- **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 offer 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 connect 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:

TAKE NOTE*

If you wish to use smart cards for remote connections, you need to use Extensible Authentication Protocol (EAP)

- **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.

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.

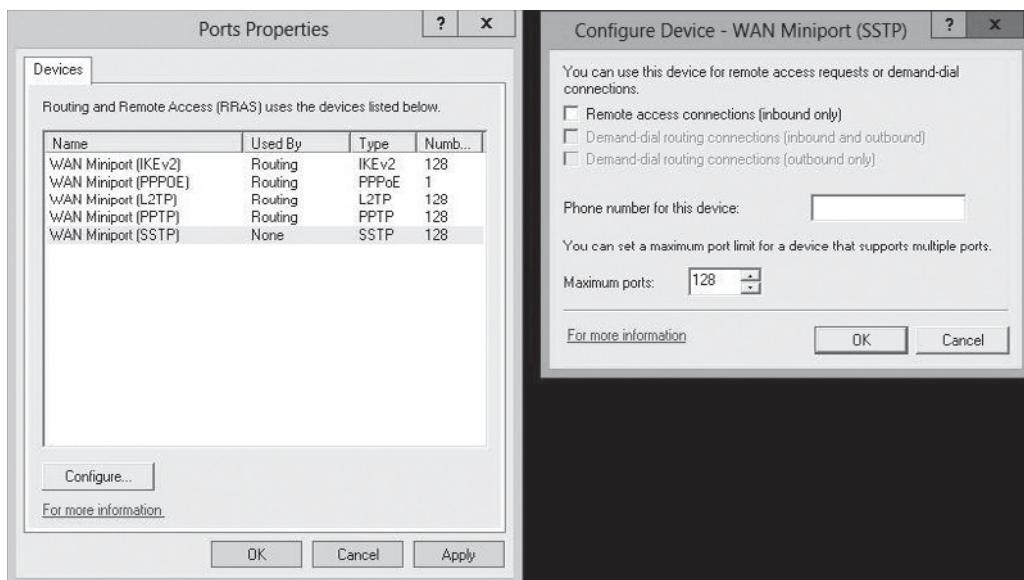
From the *Security* tab, you can configure authentication methods, specify the Preshared key for IPsec and L2TP/IKEv2 connections, and specify the SSL certificate that is used by SSTP.

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.

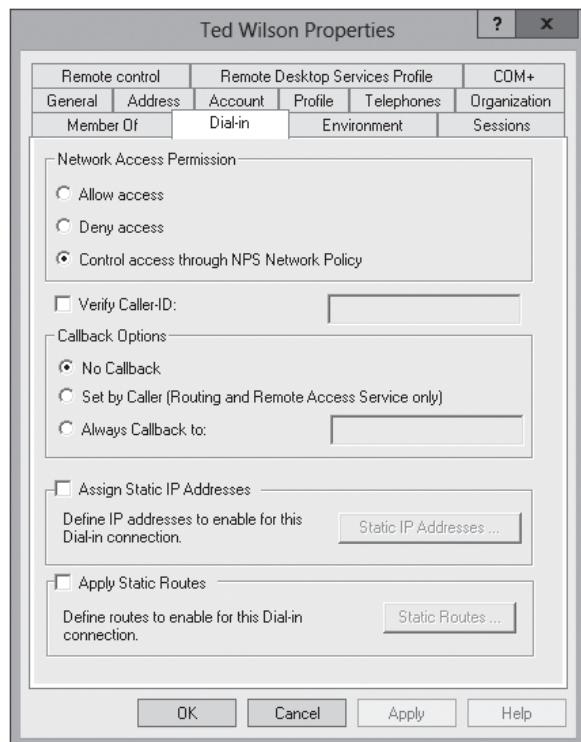
Configuring Remote Dial-In Settings for Users

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:

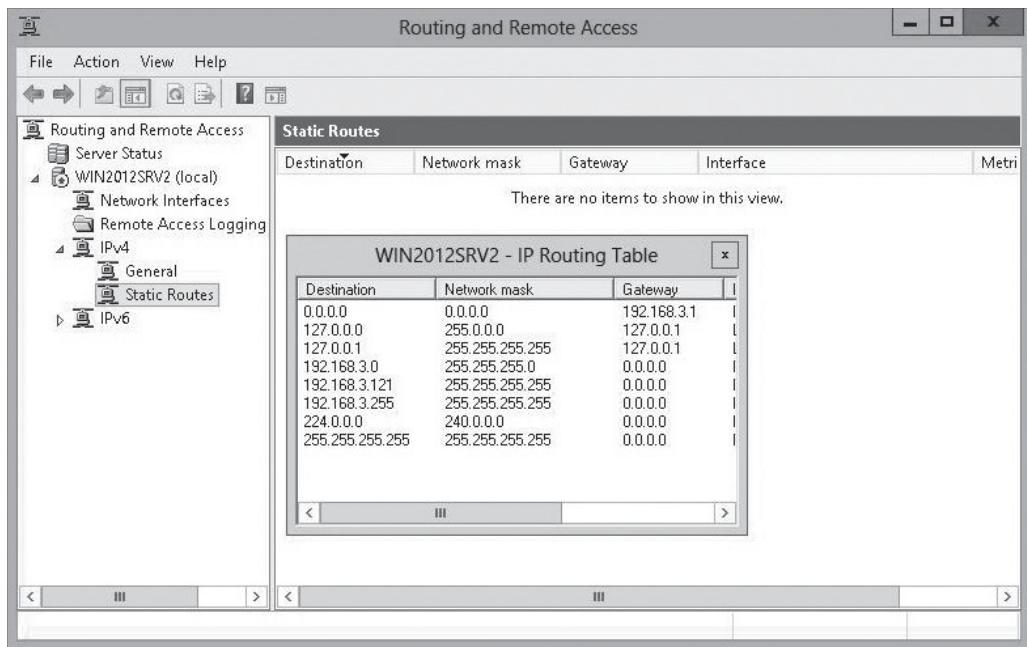
1. Open **Server Manager**.
2. Click **Tools > Routing and Remote Access**.
3. Right-click the server and select **Configure and Enable Routing and Remote Access**.
4. When the **Routing and Remote Access Server Setup Wizard** opens, click **Next**.
5. On the **Configuration** page, select **Custom configuration** 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

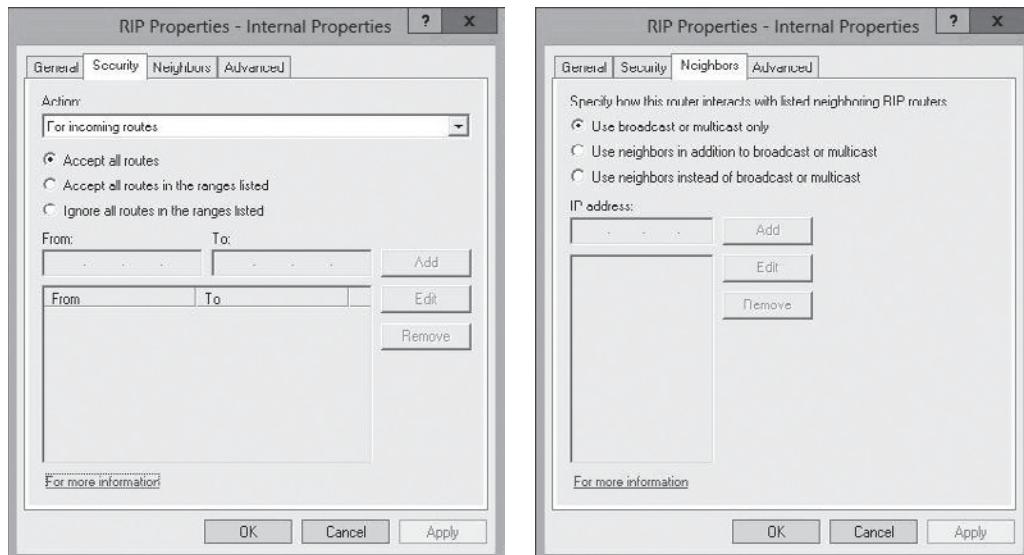
GET READY. To configure RIP on Windows Server 2012 or Windows Server 2012 R2, perform the following steps:

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.

Preatentication 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

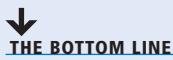
Your manager comes up to you and says that you need to install a VPN server so that users can work while they are doing sales calls with customers. Your manager wants you to make it as secure as possible with the VPN technologies that appear in this lesson. How would you configure the server?

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

■ Understanding DirectAccess



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 than 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 field 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

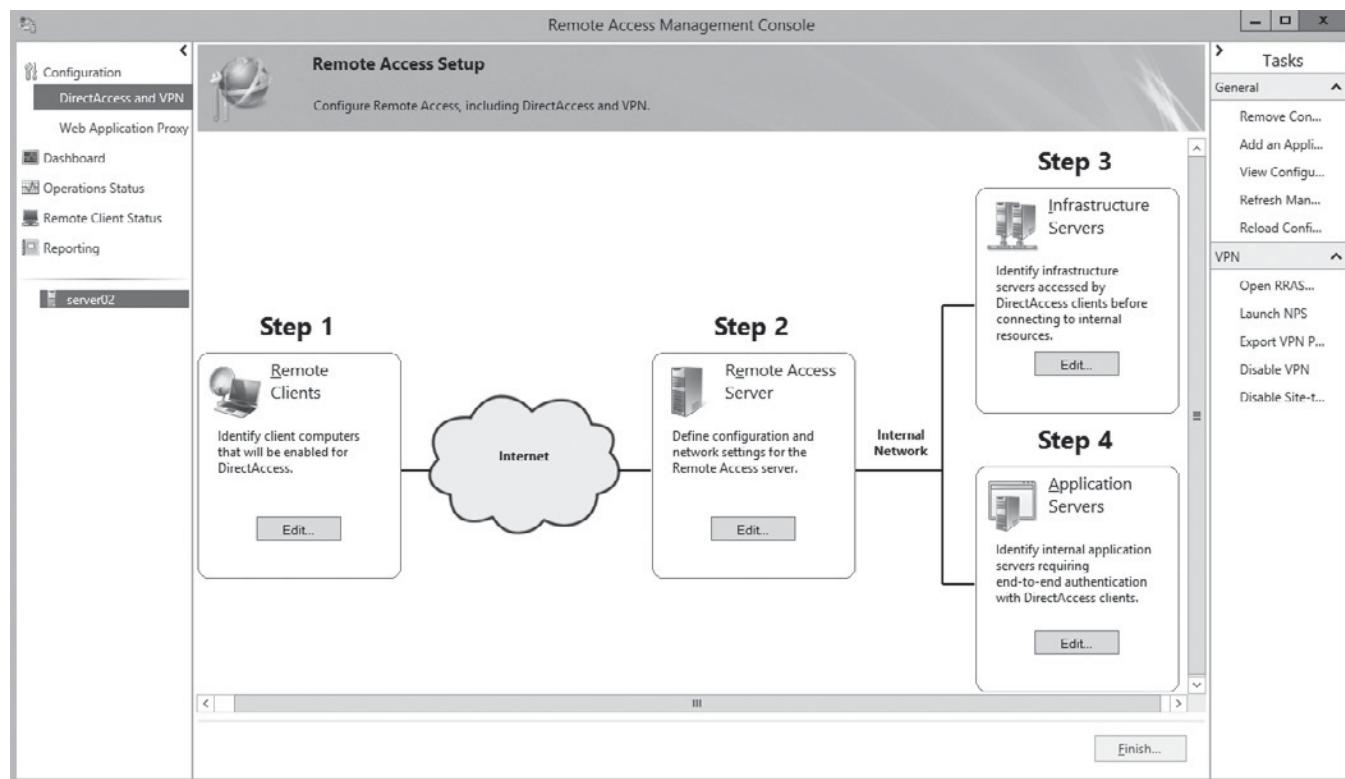
To configure DirectAccess itself, you use the newly created Remote Access Management console. By using the Remote Access Management console, you can configure DirectAccess using the Remote Access Setup Wizard.

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.



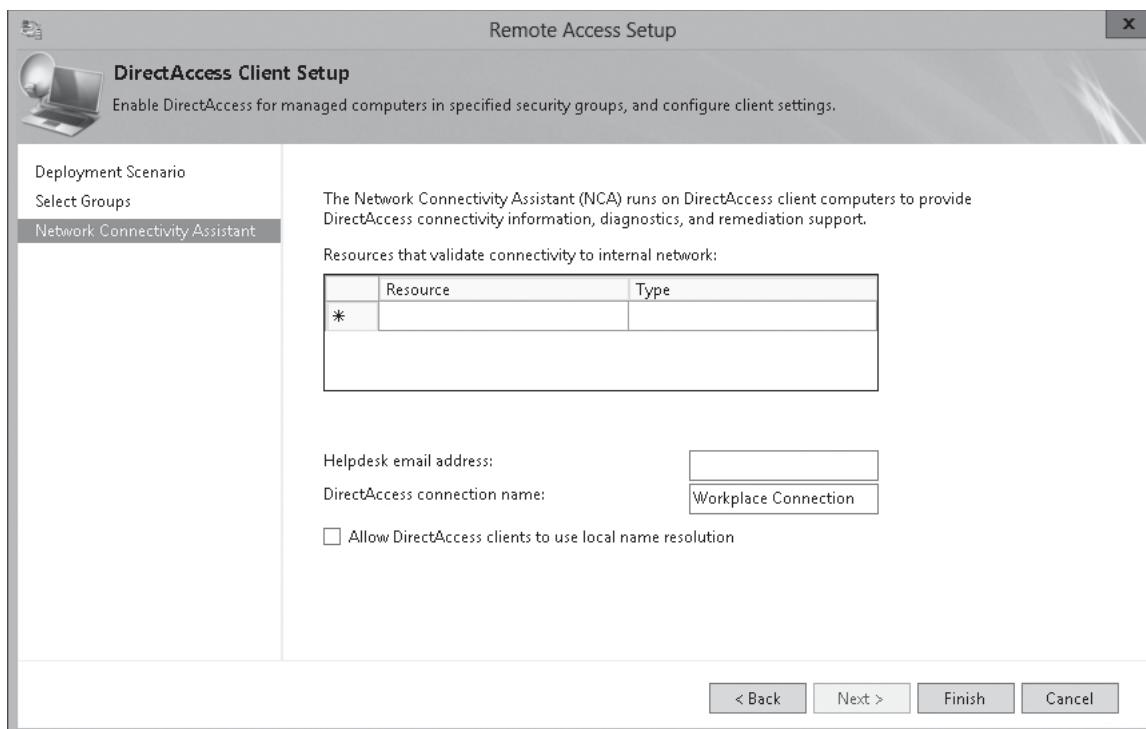
CONFIGURE REMOTE CLIENTS

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.



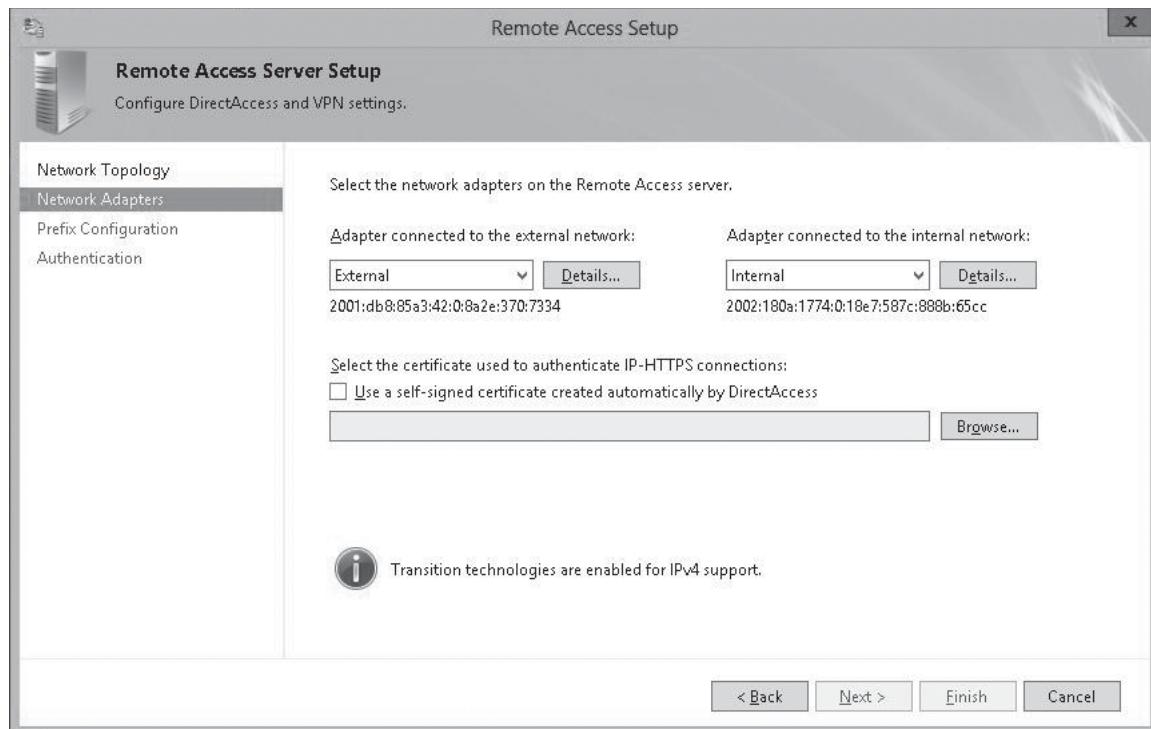
CONFIGURE THE DIRECTACCESS REMOTE ACCESS SERVER

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.



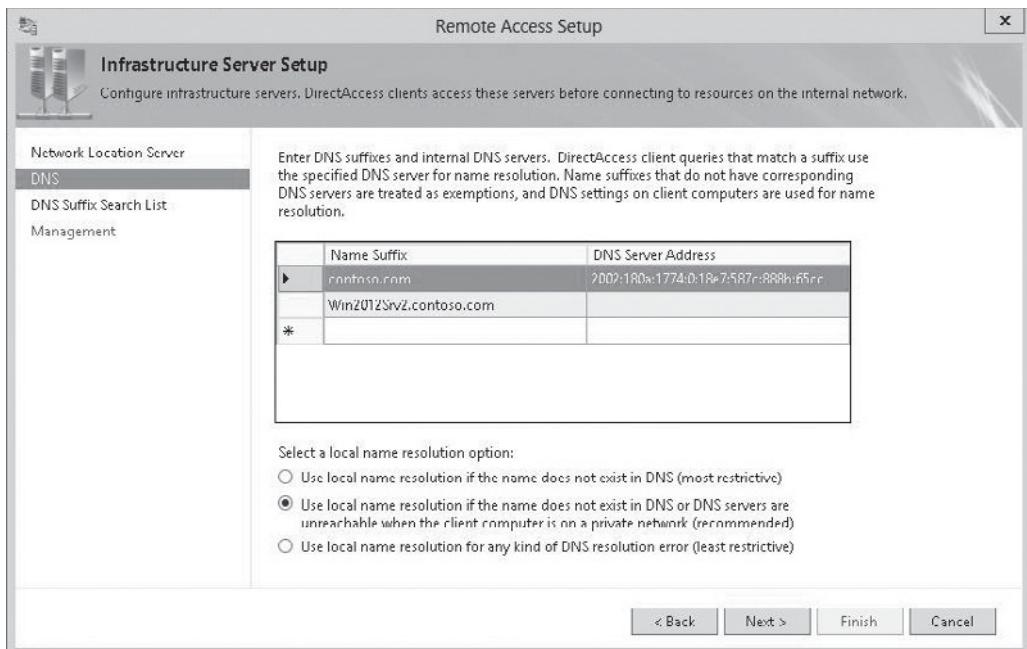
CONFIGURE THE DIRECTACCESS INFRASTRUCTURE SERVERS

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.



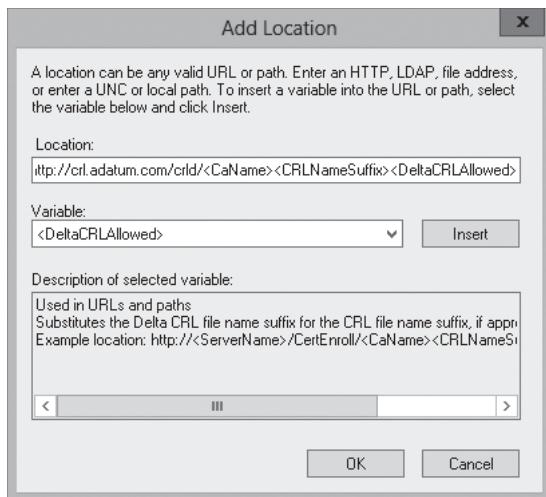
CONFIGURE CERTIFICATE REQUIREMENTS

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/crl/> in the *Location* text box.
7. Select the [CName](#) 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

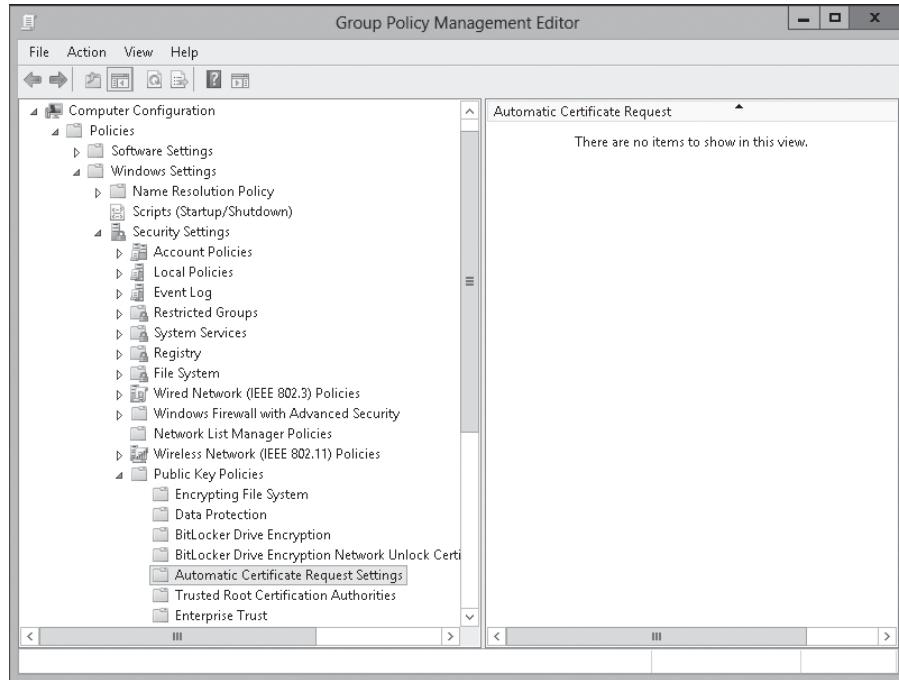


11. Click **OK** to close the *Add Location* dialog box.
12. Select **Include in CRLs. Clients use this to find Delta CRL locations.** option and the **Include in the CDP extensions of issued certificates** option.
13. On the *Add Location* dialog box, type `\win2012srv\crldist$` in the *Location* text 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

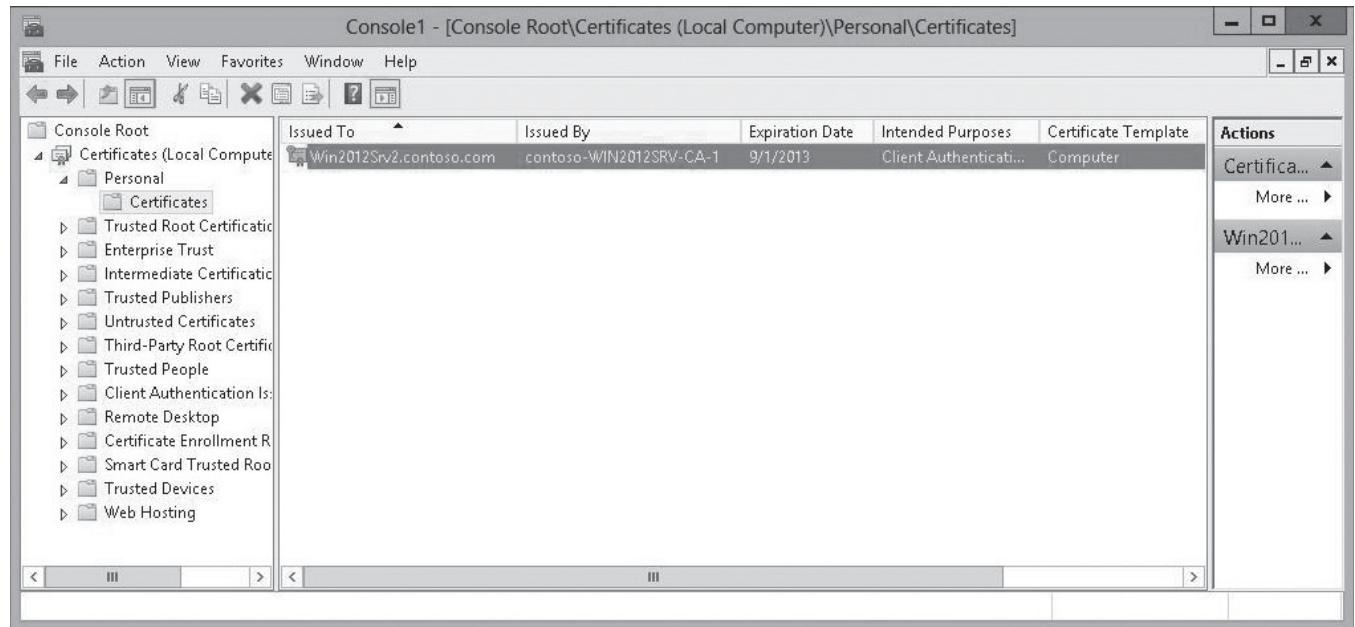
GET READY. To install a digital certificate on the Network Locator Server, perform the following steps:

1. To acquire the Computer certificate, open a command prompt and execute the following command:
`gpupdate /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

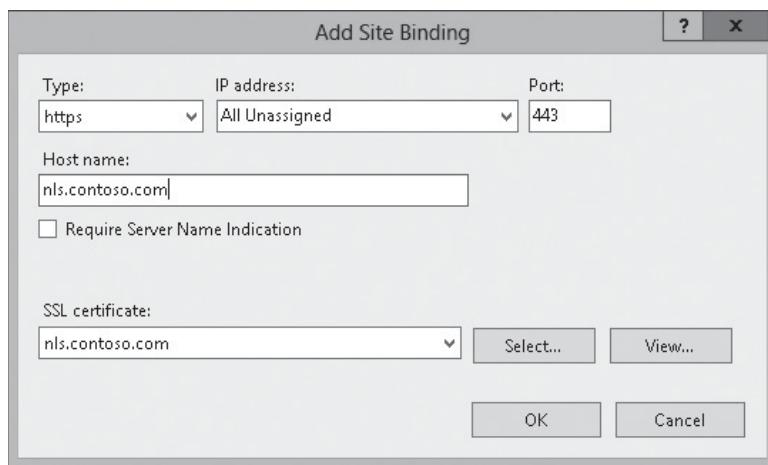


9. Right-click **Certificates**, select **All Tasks**, and then select **Request New Certificate**.
10. When the *Certificate Enrollment Wizard* opens, click **Next**.
11. On the *Select Certificate Enrollment Policy* page, click **Next**.
12. On the *Request Certificates* page, select **Contoso Web 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

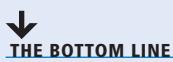
You are an administrator with the Contoso Corporation. The Contoso Corporation has about 1,100 users. Among those 1,100 users, there are 200 users who use VPN to connect to the organization network when they are not in the office. However, you realize that you are having trouble keeping the clients updated 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

■ Configuring a Network Policy Server Infrastructure



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.

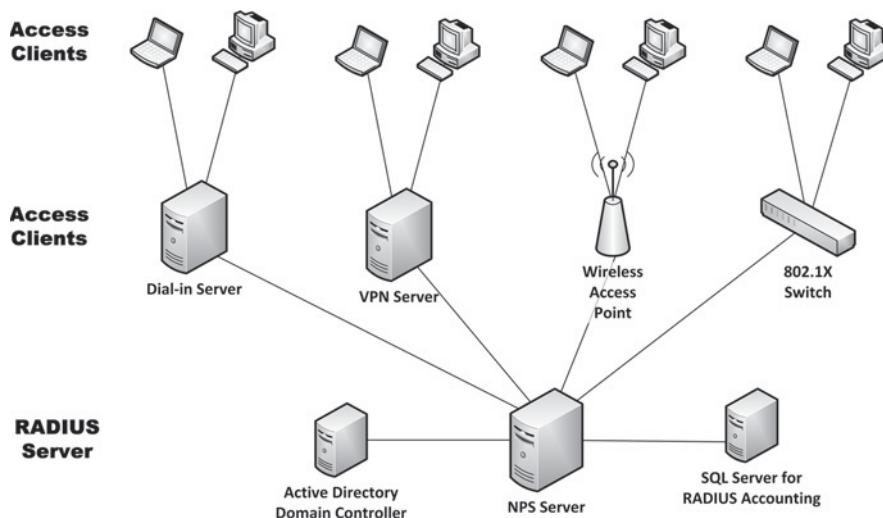
RADIUS is defined in the Internet Engineering Task Force (IETF) RFCs 2865 and 2866. Microsoft's RADIUS server is **Network Policy Server (NPS)**. By installing and configuring RADIUS, you can create and enforce wide network access policies for client health, connection request authentication, and connection 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 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 and 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.



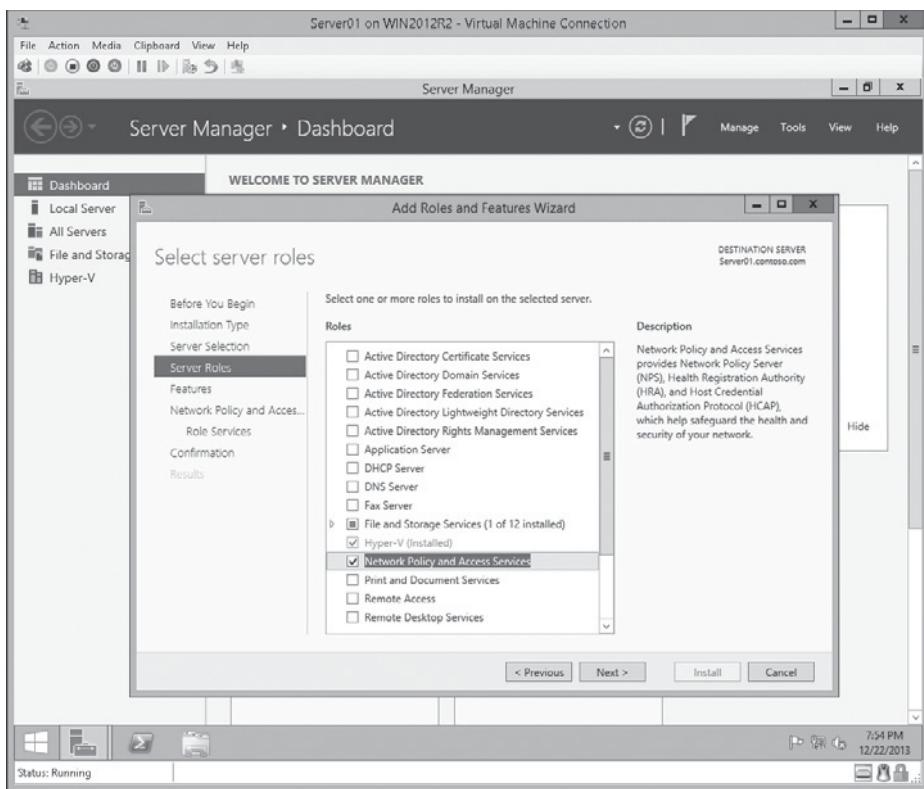
INSTALL NETWORK POLICY SERVER (NPS)

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

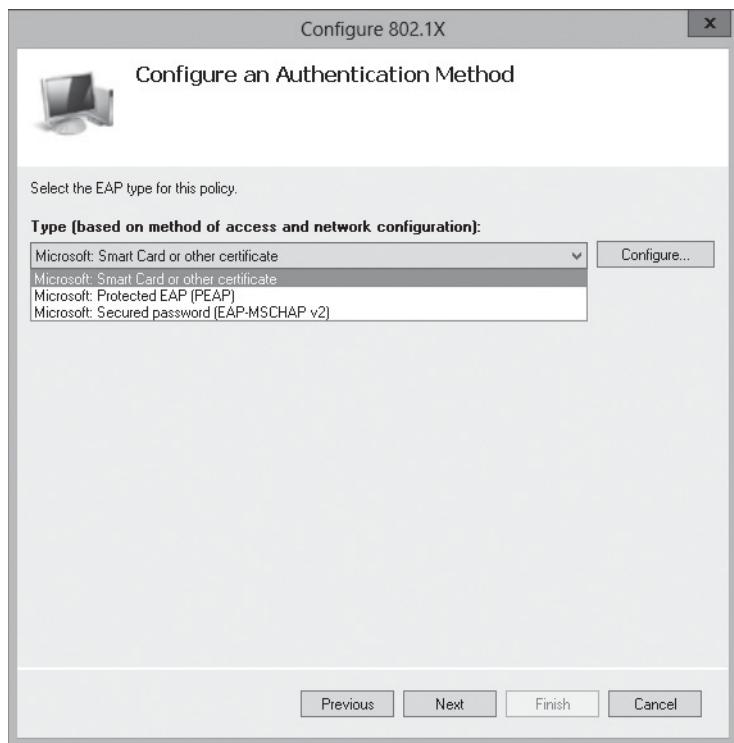
GET READY. To configure NPS for 802.1X wireless or wired connections, perform the following steps:

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

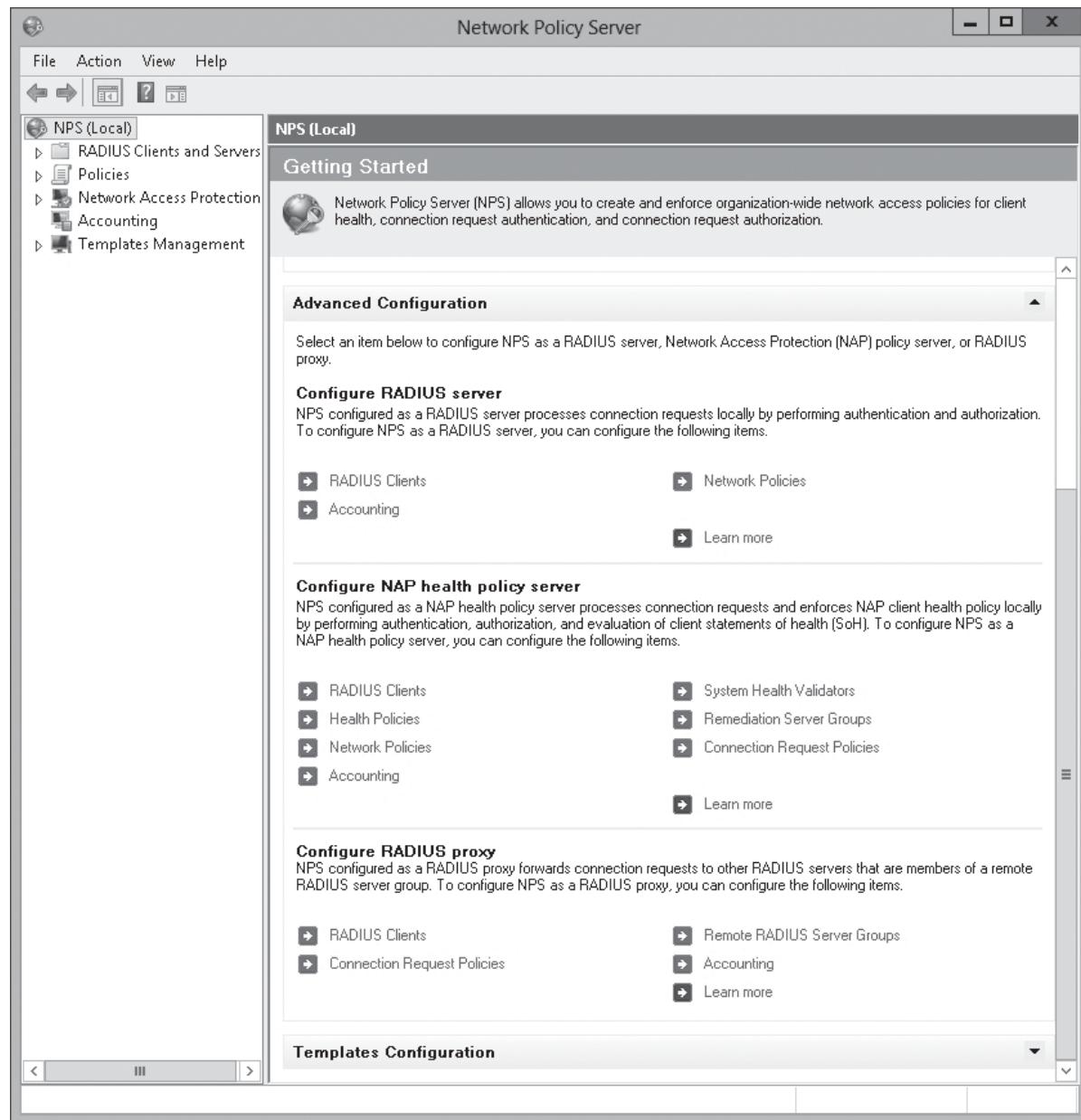


13. On the *Specify User Groups* page, click **Add**.
14. When the *Select Group* dialog box opens, type a name of the group in the *Enter the object name to select* text box and click **OK**.
15. Back at the *Specify User Groups* page, click **Next**.
16. On the *Configure Traffic Controls* page, you 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*.

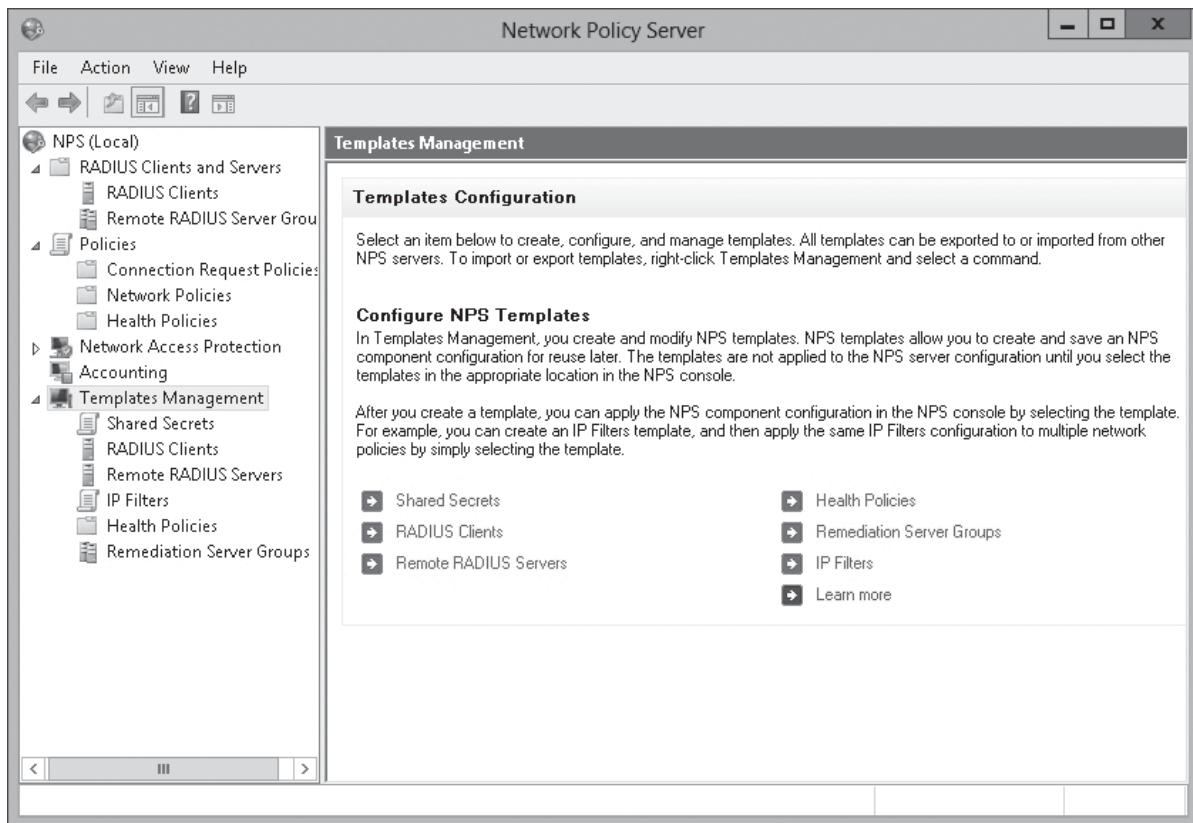
Configuring NPS Templates

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

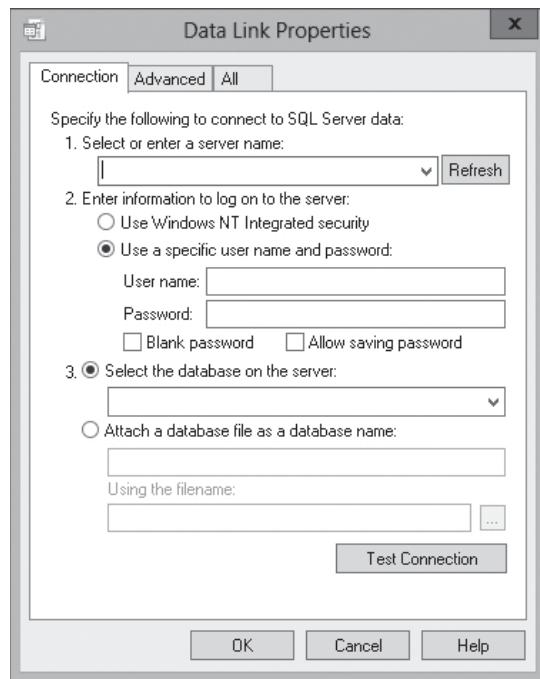
Configuring SQL Server logging



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.



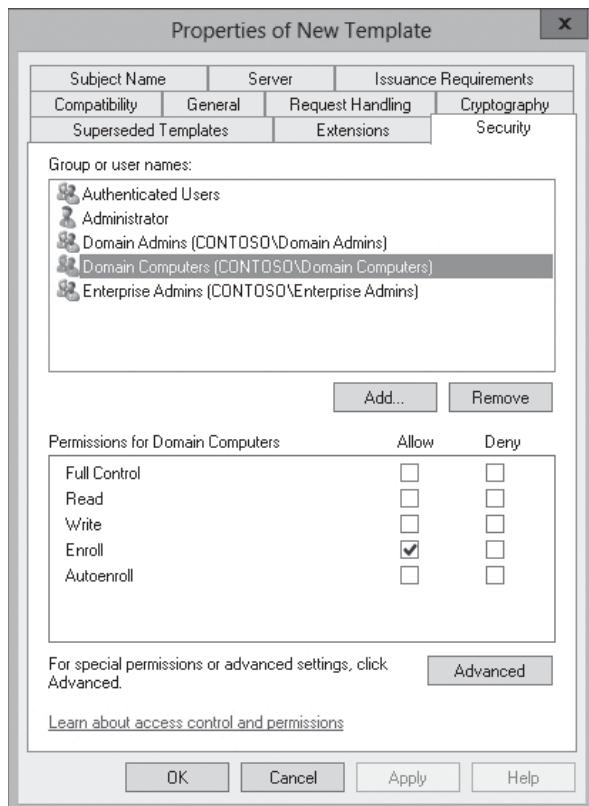
AUTOMATICALLY ADD WORKSTATION AUTHENTICATION CERTIFICATES TO ALL WORKSTATIONS

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?

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.

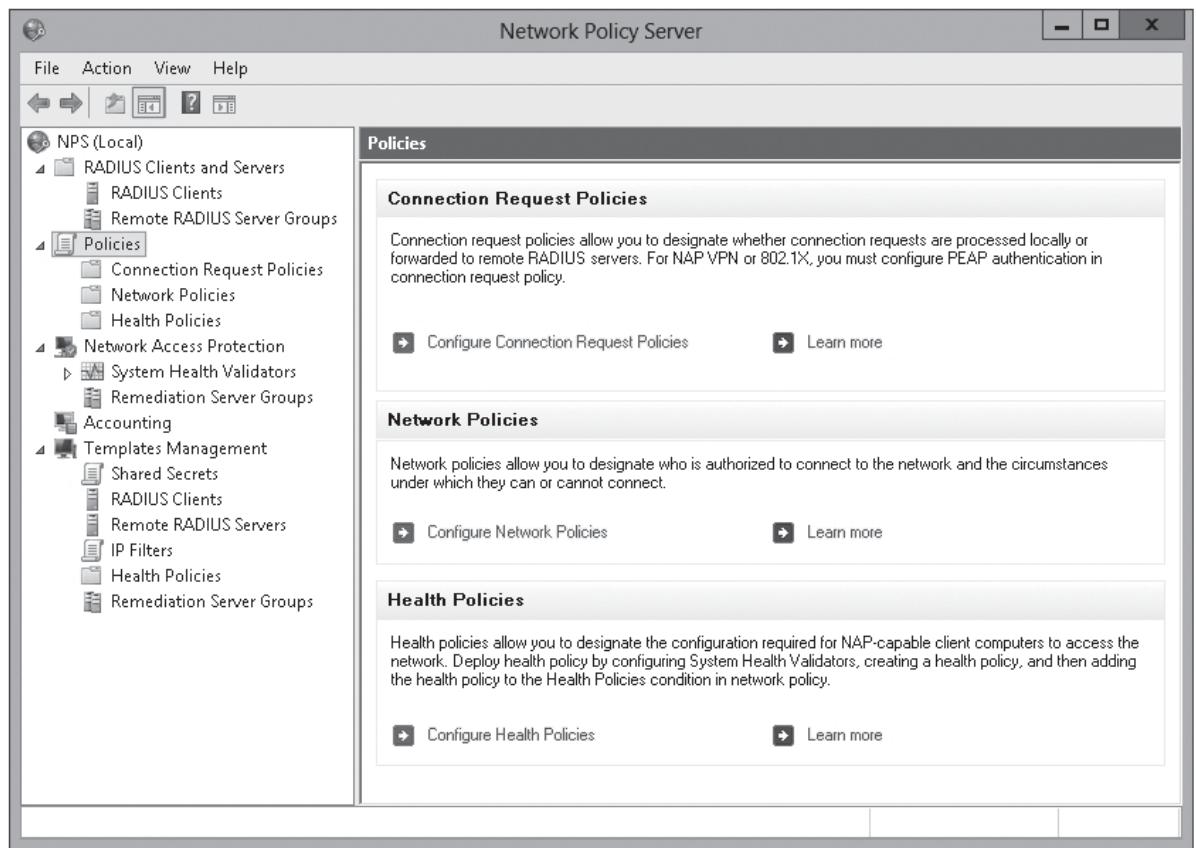
Network Policy Server (NPS) provides three types of policies:

- **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 policies 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 specifies 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
Gateway	Client Vendor	Specifies the name of the vendor of the RADIUS client that sends reconnection requests to NPS.
	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.



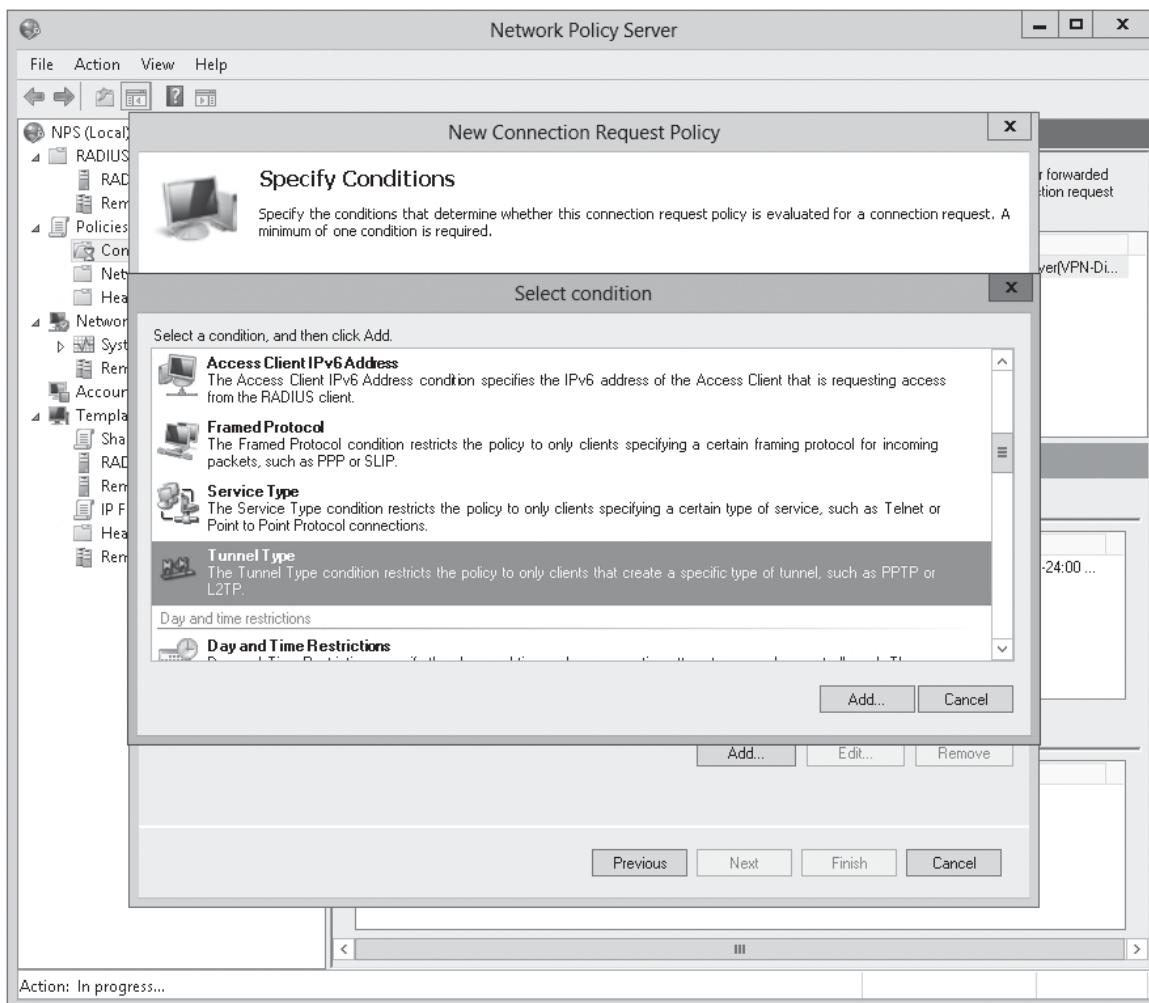
CREATE A CONNECTION REQUEST POLICY

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.

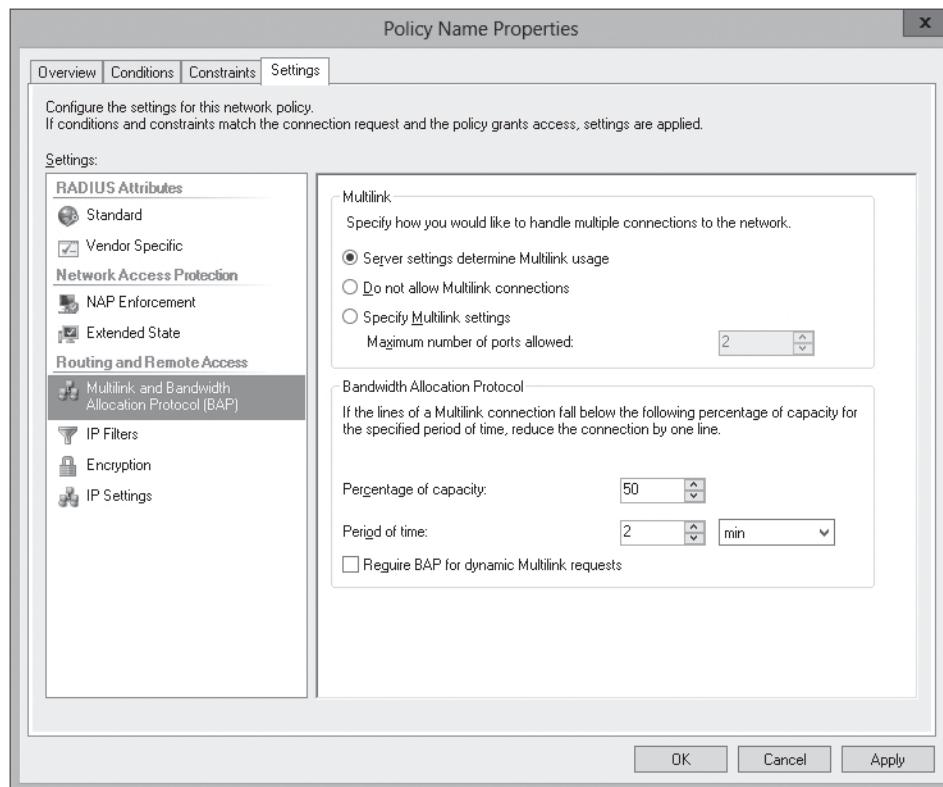
After the network policy has been created, you can modify the network policy by right-clicking the network policy and selecting *Properties*. When the Properties dialog box opens, you can then select the *Overview* tab, *Condition* tab, *Constraints* tab, and *Settings* tab.

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

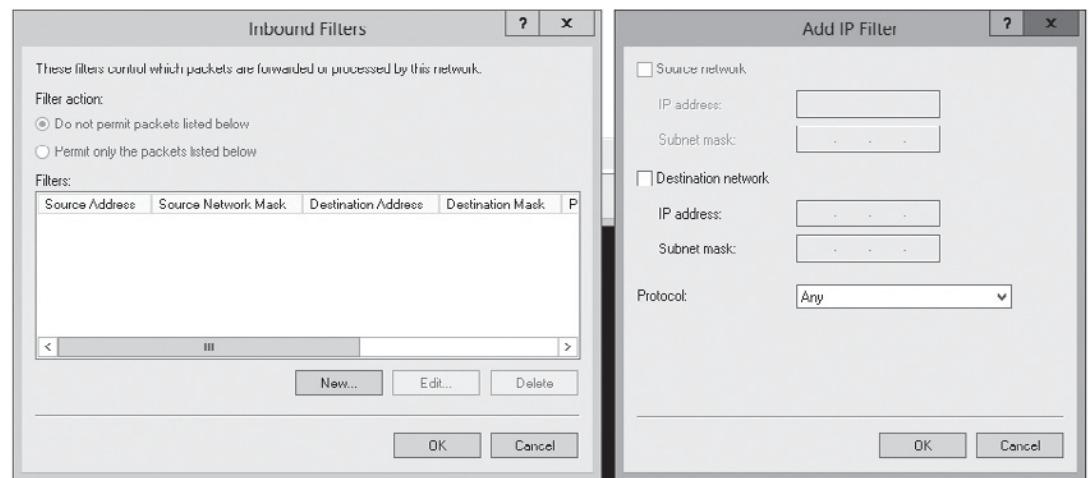


IP FILTERS

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



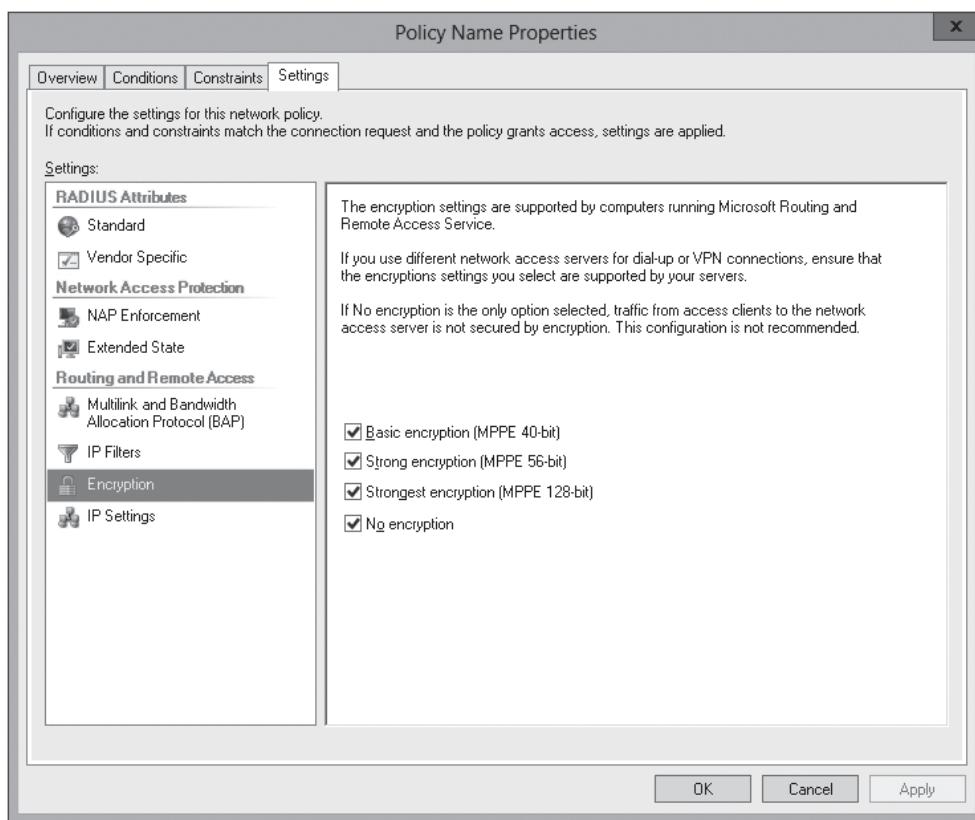
ENCRYPTION

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.

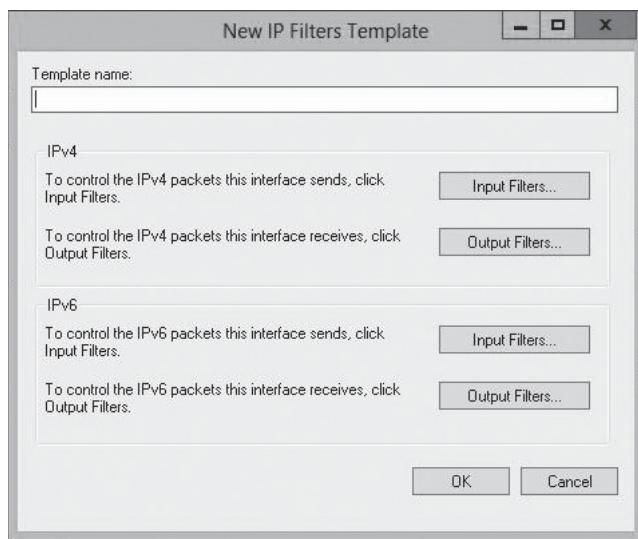
The following NPS template types are available for configuration in Templates Management:

- 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)

■ 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](#).
-



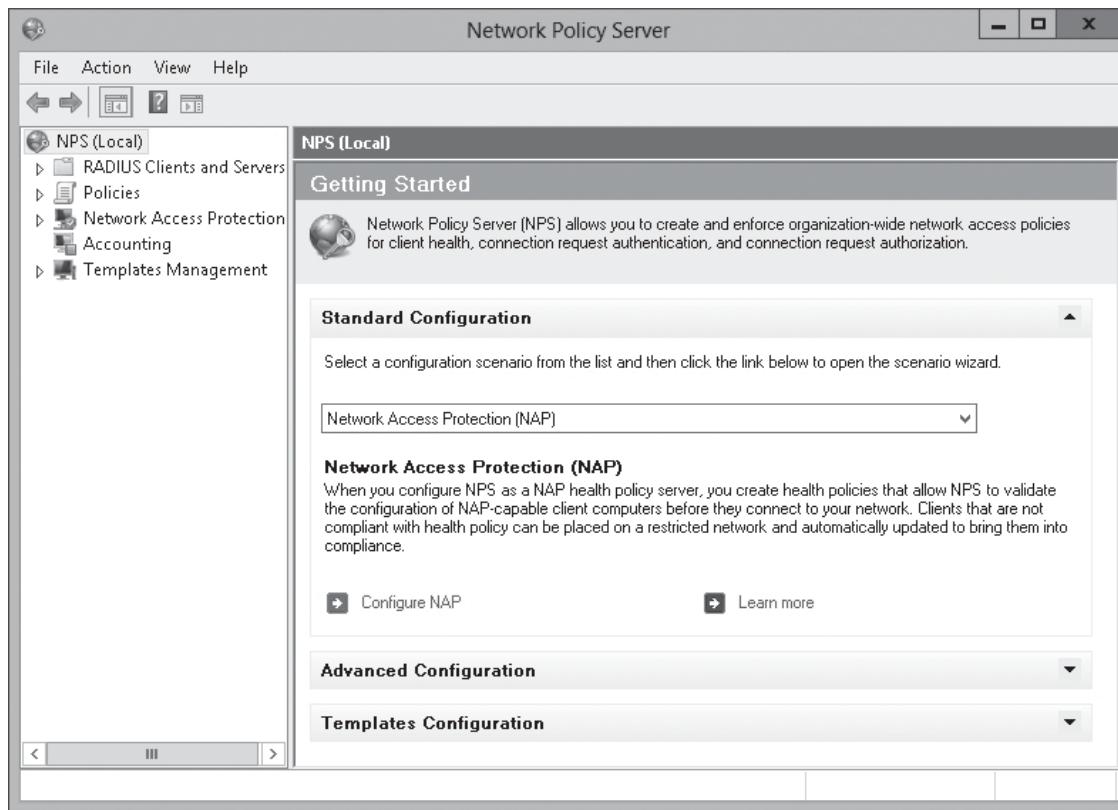
CONFIGURE NAP FOR DHCP SERVER

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 servers, 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.



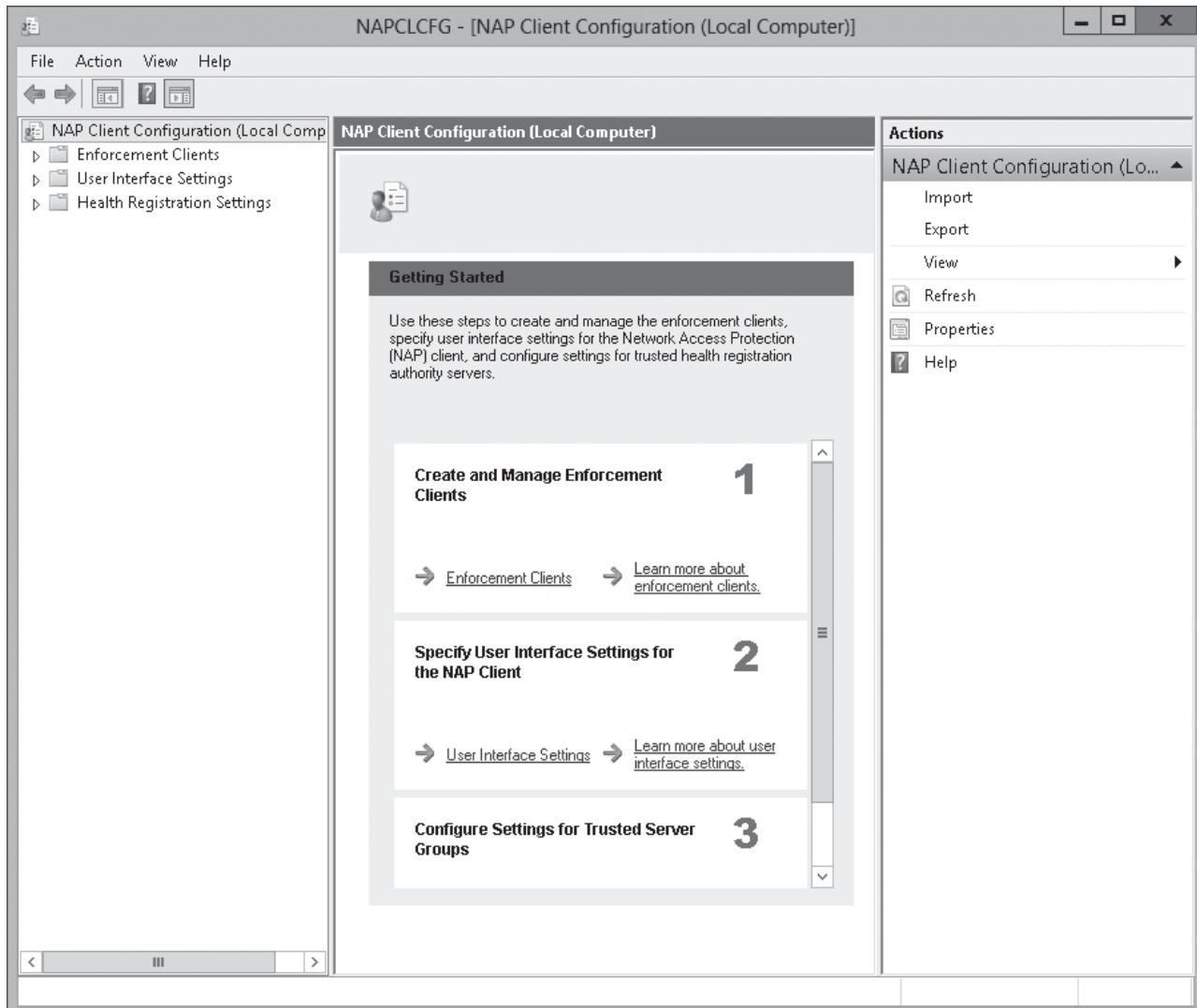
ENABLE THE NAP DHCP QUARANTINE ENFORCEMENT CLIENT AND START NAP SERVICE ON A DHCP SERVER

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 servers, 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 servers, 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**.

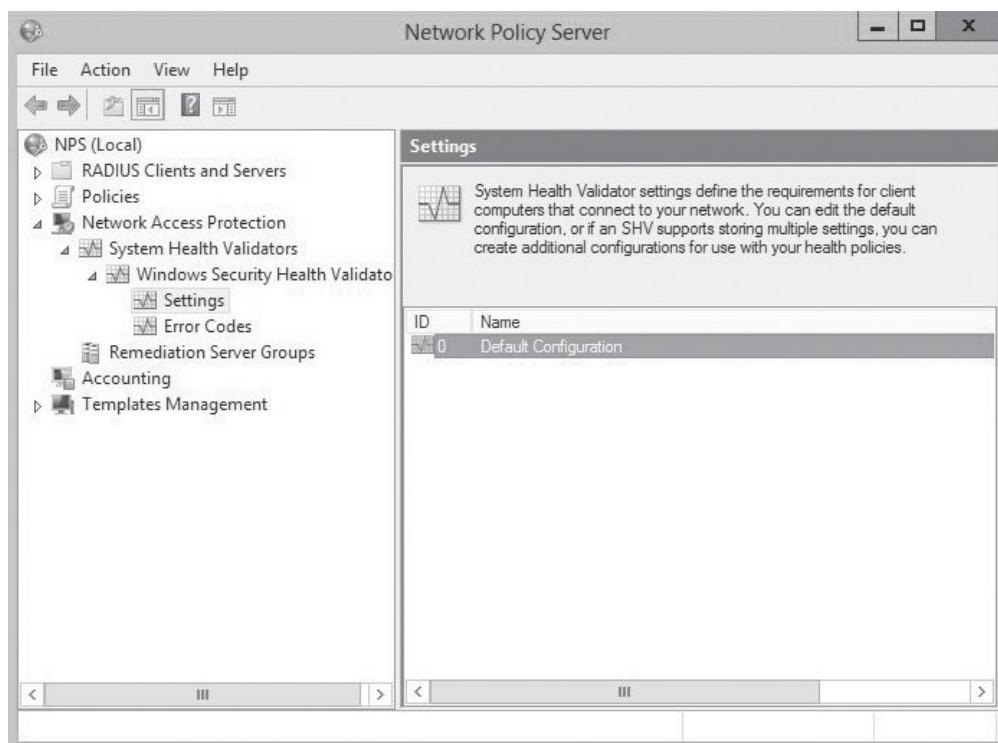
Configuring System Health Validators

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).

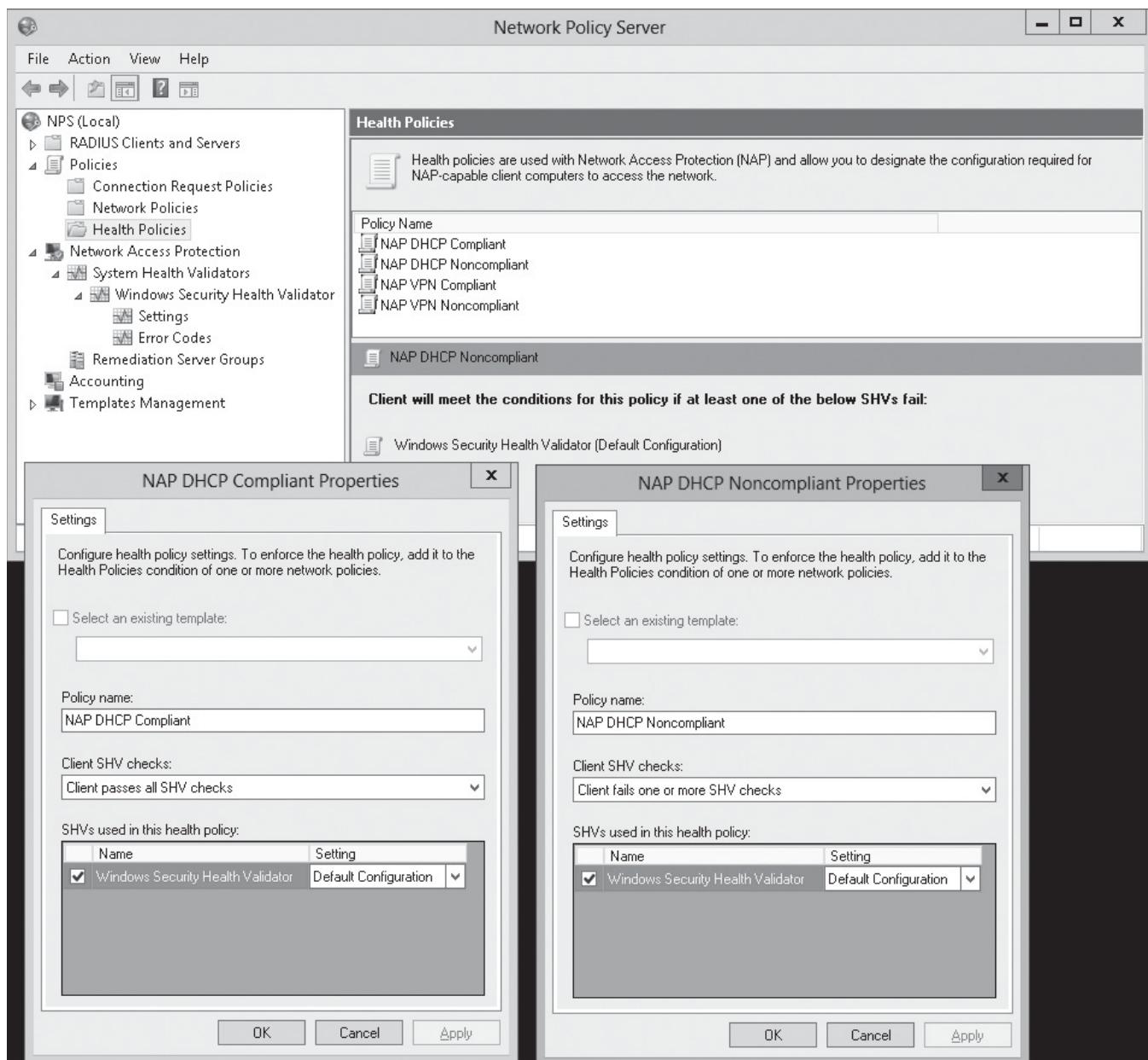
Configuring Health Policies

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



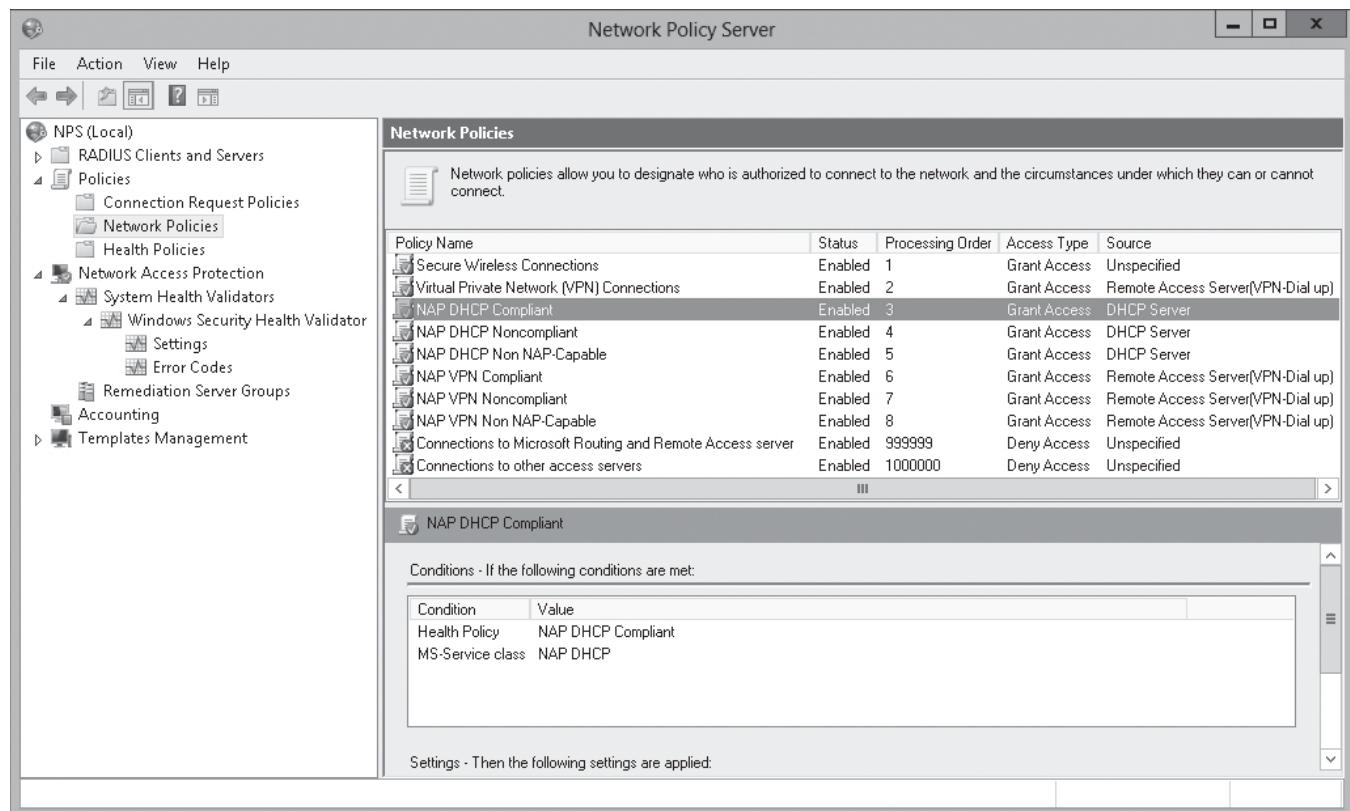
The health policies are connected directly to the network policies and connection Request Policies. As you open the network policies, the Condition tab specifies the health policy that it is connected to.

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?

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.



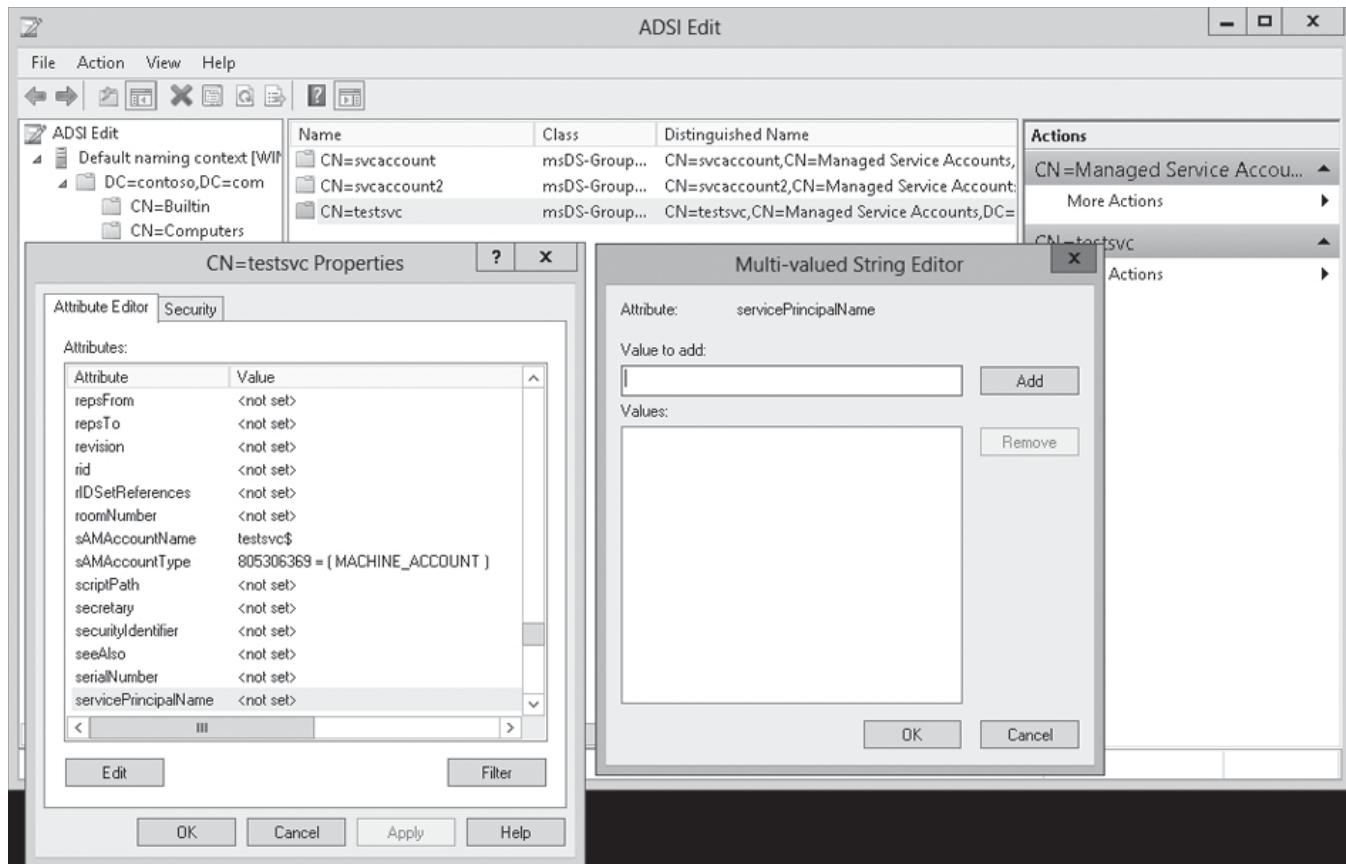
CONFIGURE AN SPN FOR A SERVICE OR APPLICATION POOL ACCOUNT

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.

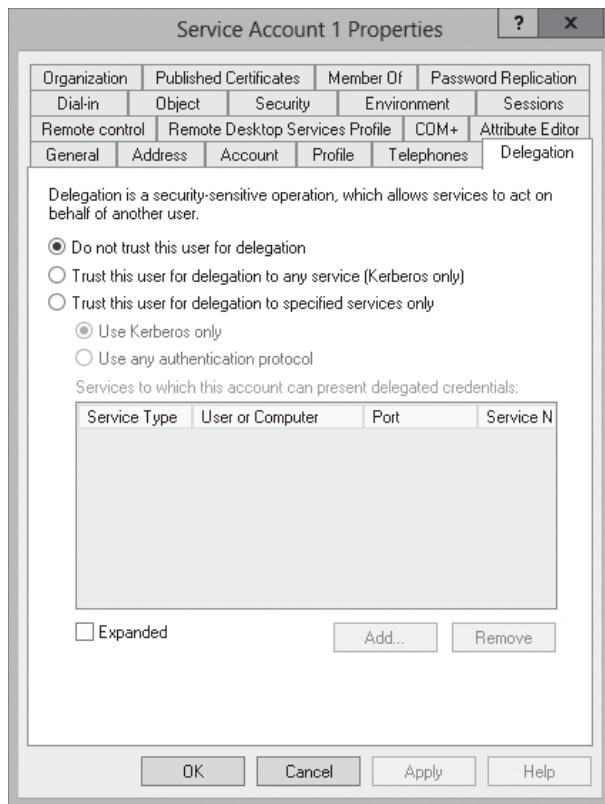
Configuring Kerberos Delegation

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



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.

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 seize 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.

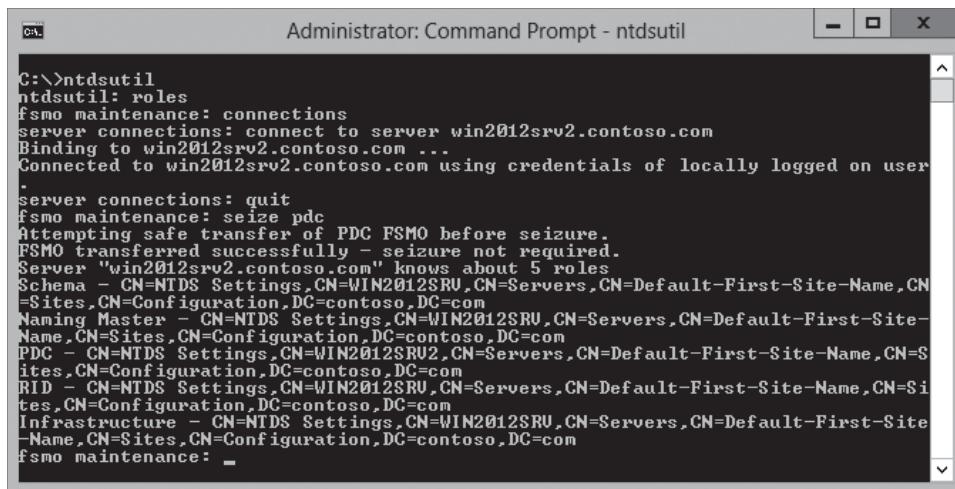


3. At the ntdsutil prompt, execute the `roles` command.
4. At the fsmo maintenance prompt, execute the `connections` command.
5. At the server connections prompt, execute the following command:
`connect to server <FQDN_of_desired_role_holder>`
An example of this would be:
`connect to server server1.contoso.com`
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

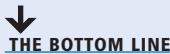


The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - ntdsutil". The command entered is:

```
C:\>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server win2012srv2.contoso.com
Binding to win2012srv2.contoso.com ...
Connected to win2012srv2.contoso.com using credentials of locally logged on user
.
server connections: quit
fsmo maintenance: seize pdc
Attempting safe transfer of PDC FSMO before seizure.
FSMO transferred successfully - seizure not required.
Server "win2012srv2.contoso.com" knows about 5 roles
Schema - CN=NTDS Settings,CN=WIN2012SRV,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
Naming Master - CN=NTDS Settings,CN=WIN2012SRV,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
PDC - CN=NTDS Settings,CN=WIN2012SRV2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
RID - CN=NTDS Settings,CN=WIN2012SRV,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
Infrastructure - CN=NTDS Settings,CN=WIN2012SRV,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
fsmo maintenance: _
```

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.



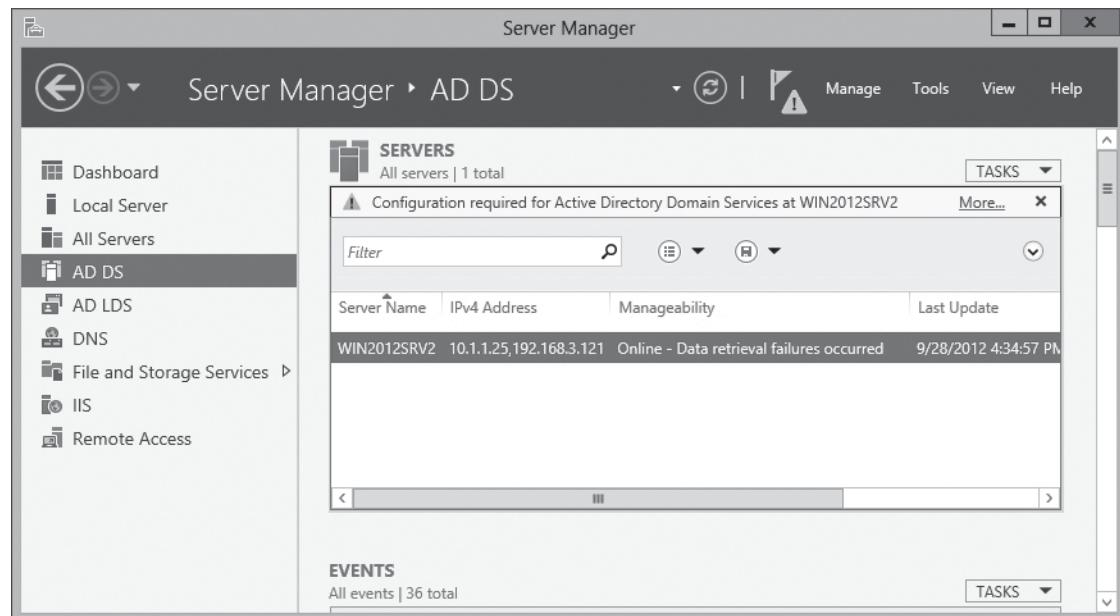
INSTALL A READ-ONLY DOMAIN CONTROLLER

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

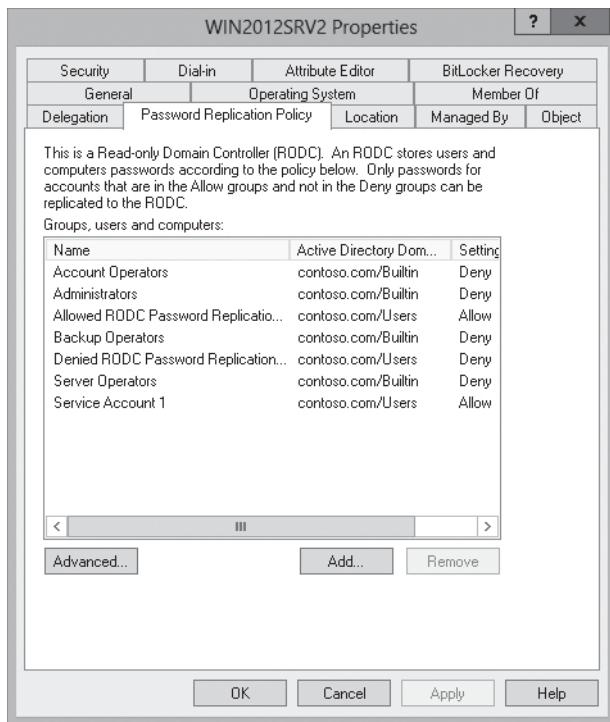


3. When the *All Servers Task Details* window opens, click [Promote this server to a domain controller](#). The *Active Directory Domain Services Configuration Wizard* starts.
4. On the *Deployment Configuration* page, with the [Add a domain controller to an existing domain](#) already selected, click [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.



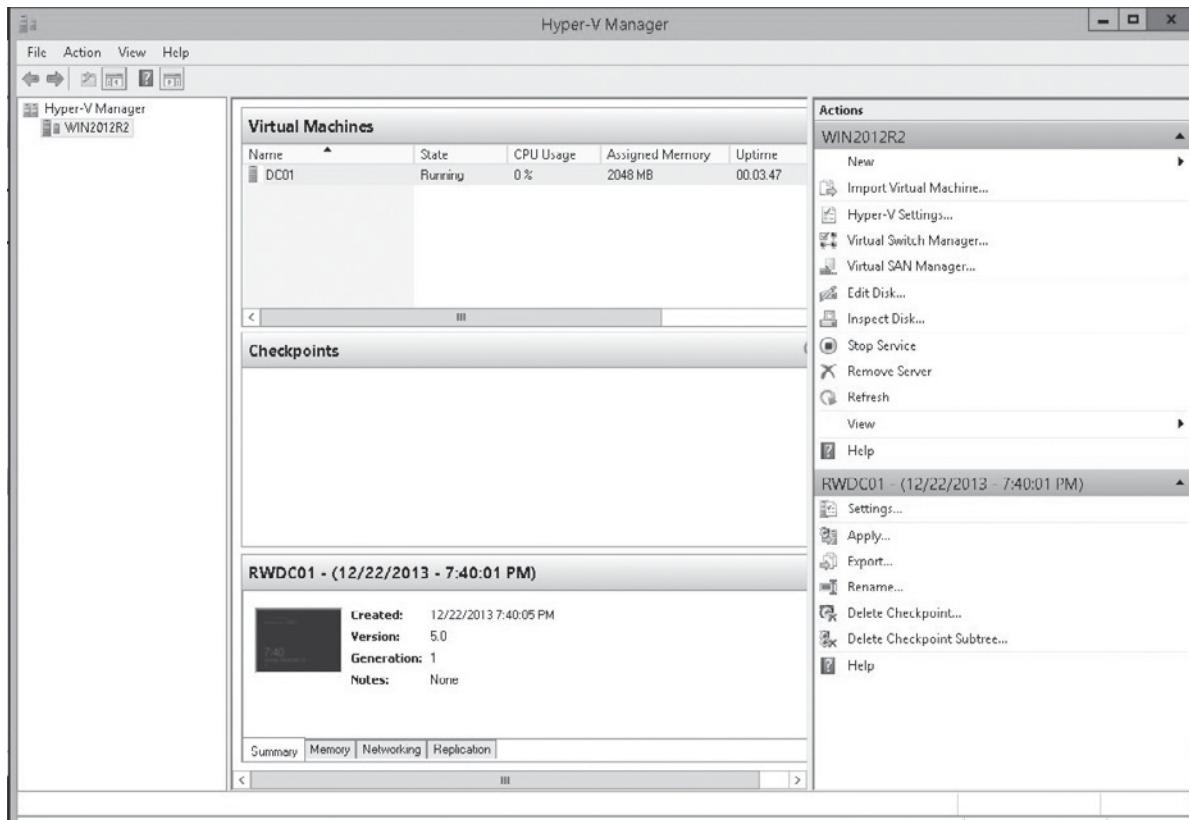
DEPLOY A CLONED VIRTUALIZED DOMAIN CONTROLLER

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?

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](#).



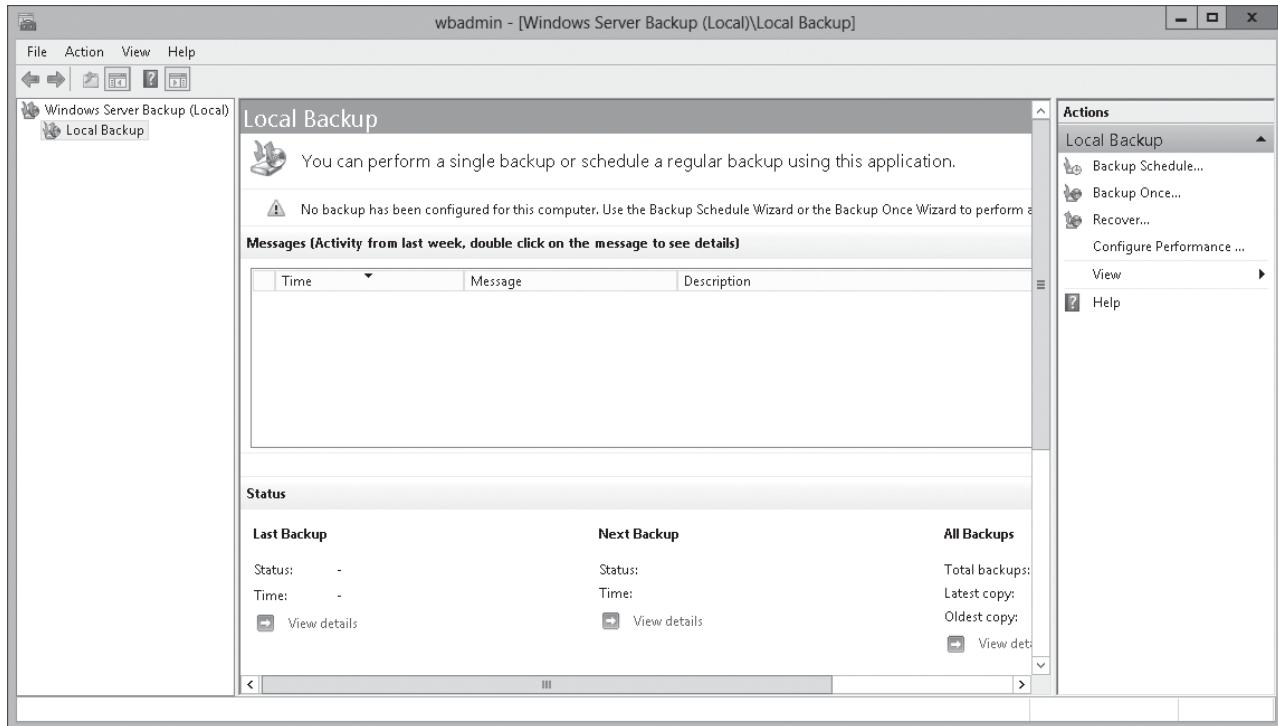
PERFORM A BACKUP OF THE SYSTEM STATE INCLUDING ACTIVE DIRECTORY

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.



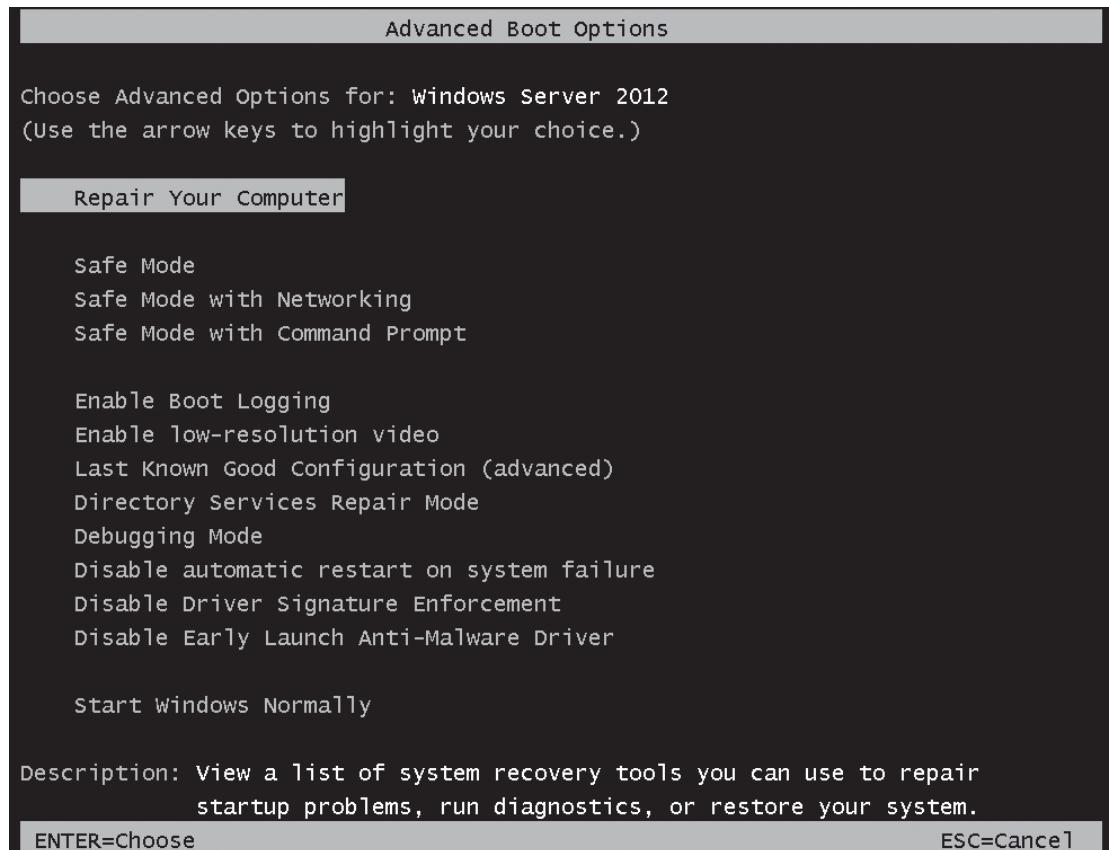
PERFORM A RESTORE OF THE SYSTEM STATE

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



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 LDP.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.



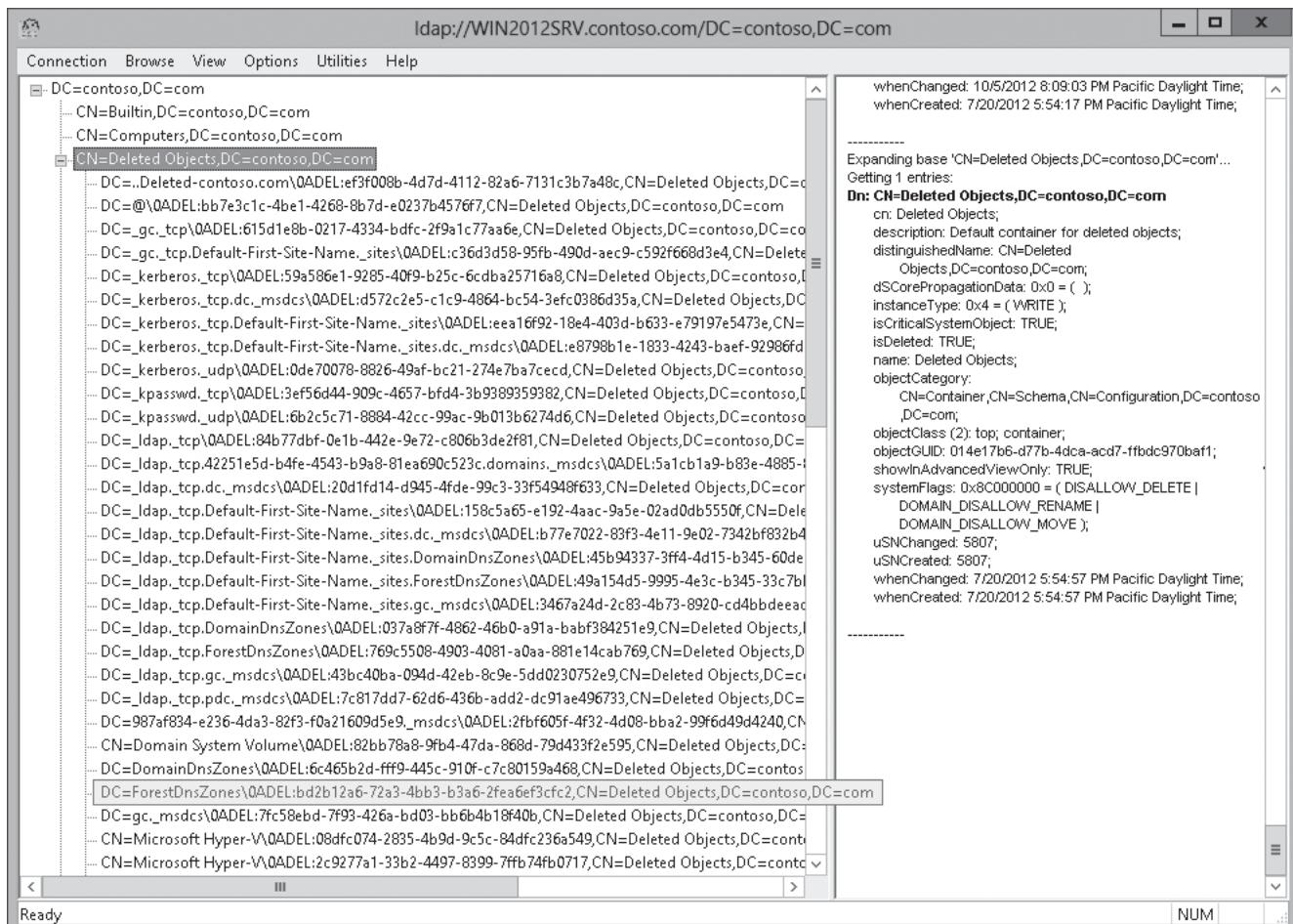
RESTORE A DELETED OBJECT WITHOUT USING THE RECYCLE BIN

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



Ready

NUM



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.



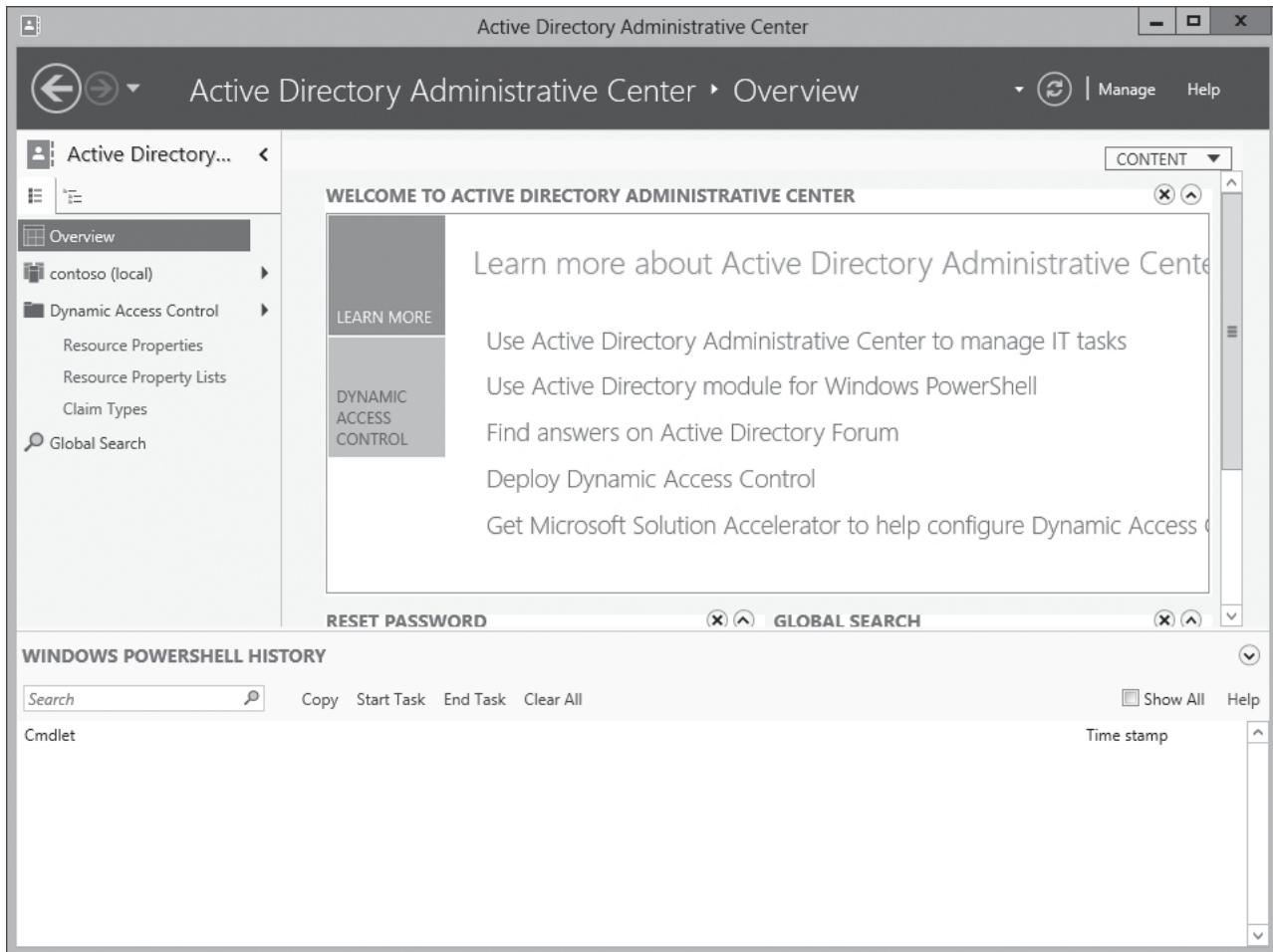
ENABLE THE ACTIVE DIRECTORY RECYCLE BIN

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

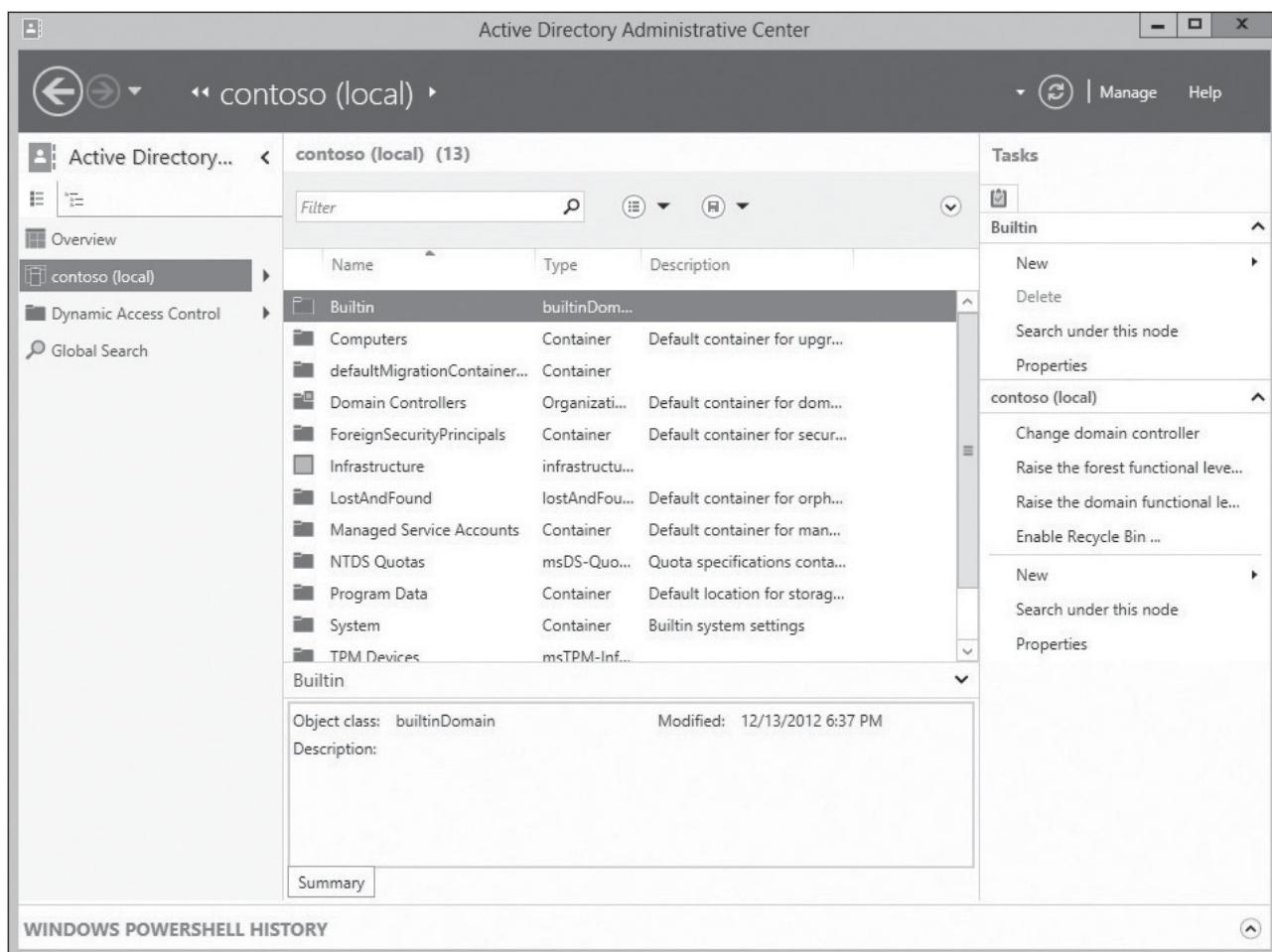
Opening Active Directory
Administrative Center



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

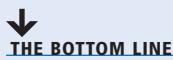
You are an administrator at the Contoso Corporation. Just before you got hired, the company had an incident where a lot of information was removed from Active Directory and it could not be recovered. What would you do to make sure that you have the best chance to recover deleted accounts with minimal 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

■ Working with Account Policies



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:

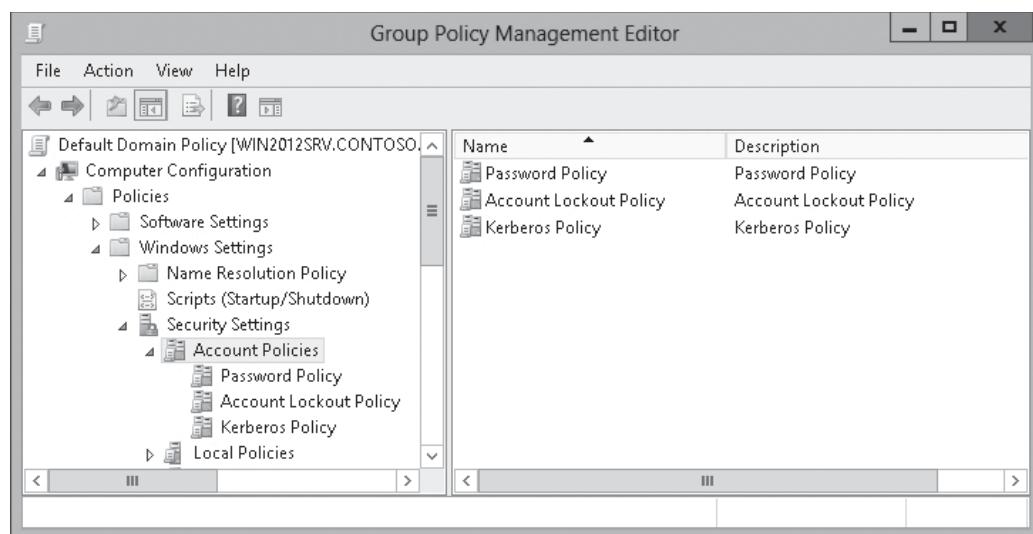
- **System settings:** Application settings, desktop appearance, and behavior of system services.
- **Security settings:** Local computer, domain, and network security settings.
- **Software installation settings:** Management of software installation, updates, and removal.
- **Scripts settings:** Scripts 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 screenshot shows the Windows Server 2012 R2 Group Policy Management Editor. The left pane displays a tree structure under 'Computer Configuration / Policies / Security Settings / Account Policies / Password Policy'. The right pane is titled 'Group Policy Management Editor' and contains a table of password policy settings:

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

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.

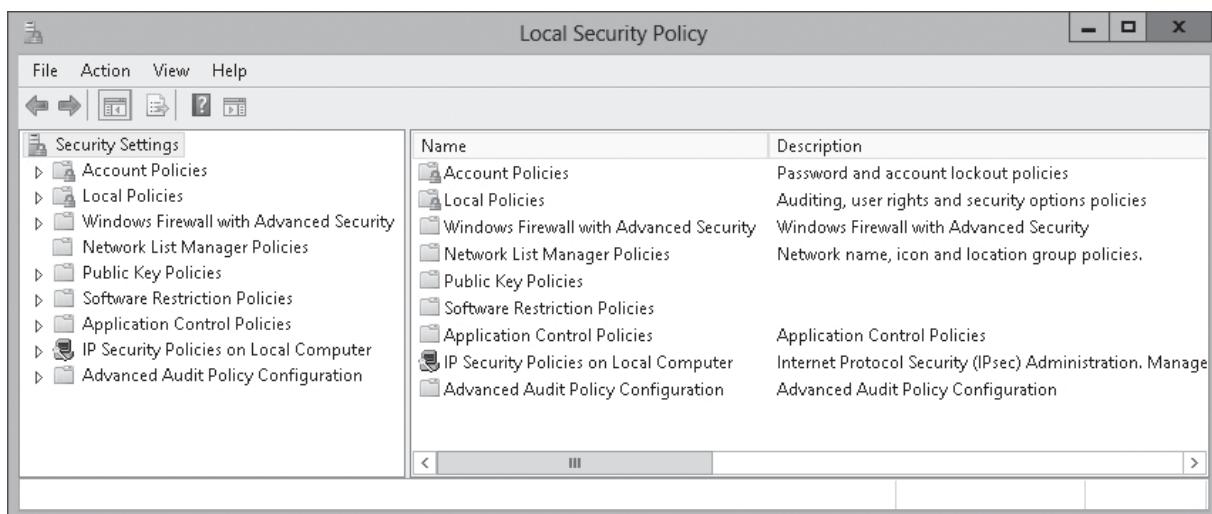
Configuring Local User Password Policy

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

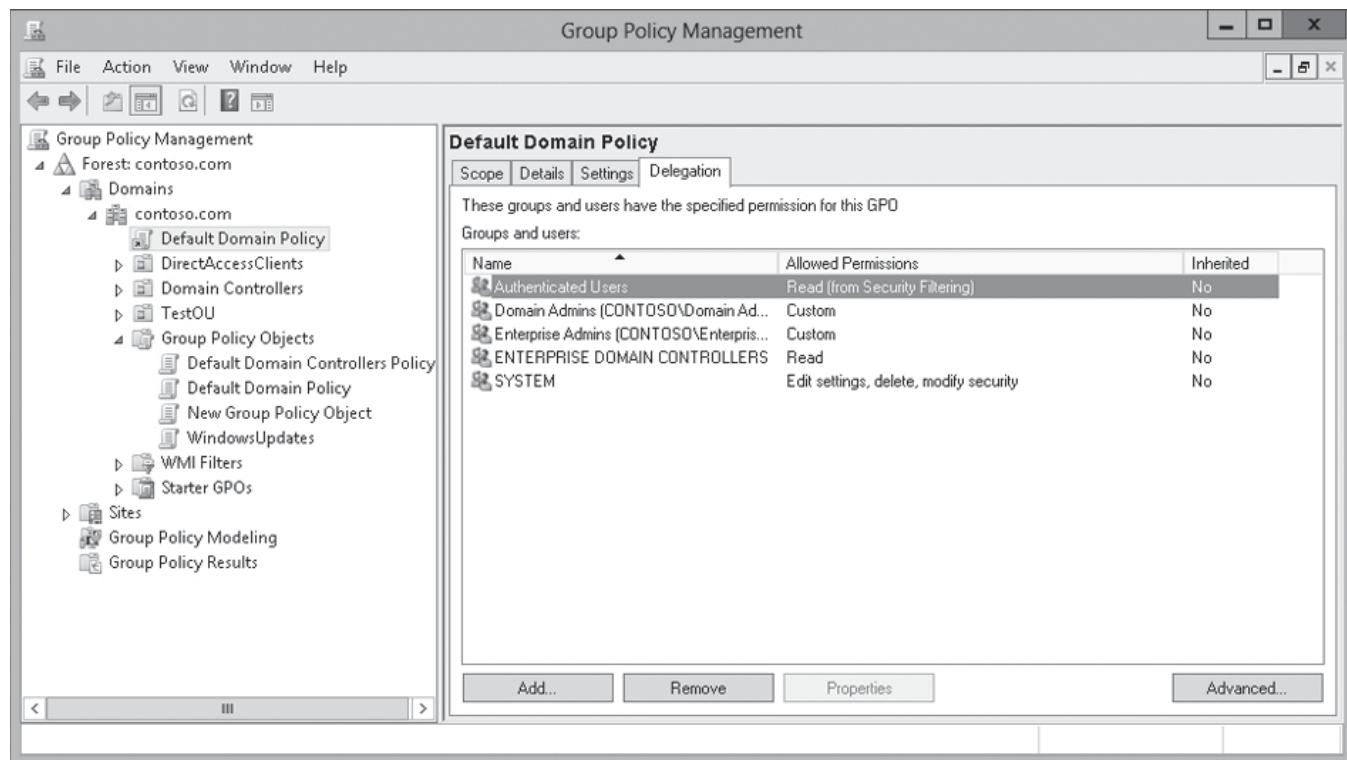
GET READY. To manage GPO permissions, perform the following steps:

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**.

- 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



- 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**.
- When the *Add Group or Users* dialog box appears, select the appropriate permissions in the *Permissions* list and click **OK**.
- Click **OK** to submit the creation of the PSO.
- 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:

- Open **Server Manager**.
- Open **Tools > Active Directory Administrative Center**. The *ADAC* opens.
- Navigate to the **System\Password Settings Container**.
- Right-click the **Password Settings Container** and click **Properties**. The *Password Settings Object Settings* window opens.
- 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**.
- 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

■ Understanding Group Policy Processing



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).

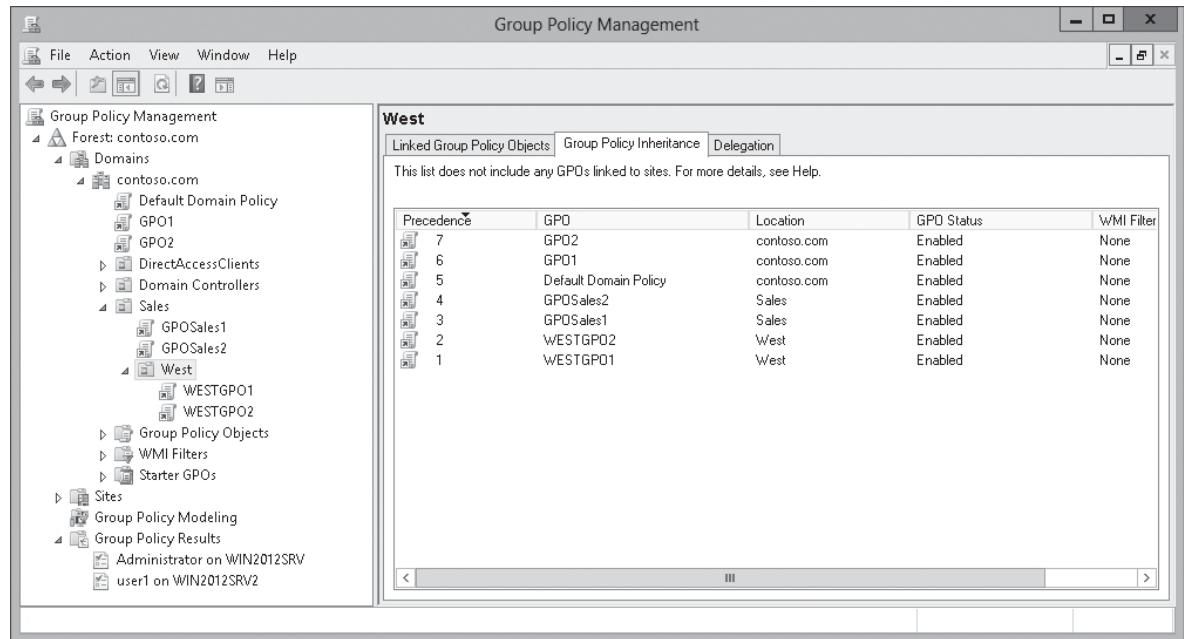
When Active Directory is installed, two domain GPOs are created by default:

- **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.



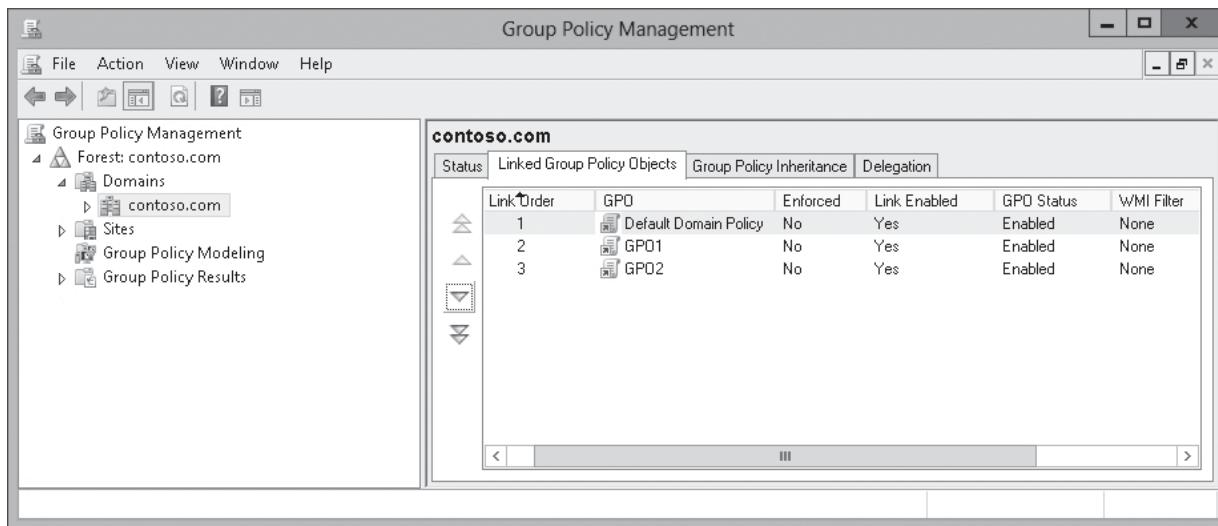
CHANGE THE PRECEDENCE OF A GPO

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.



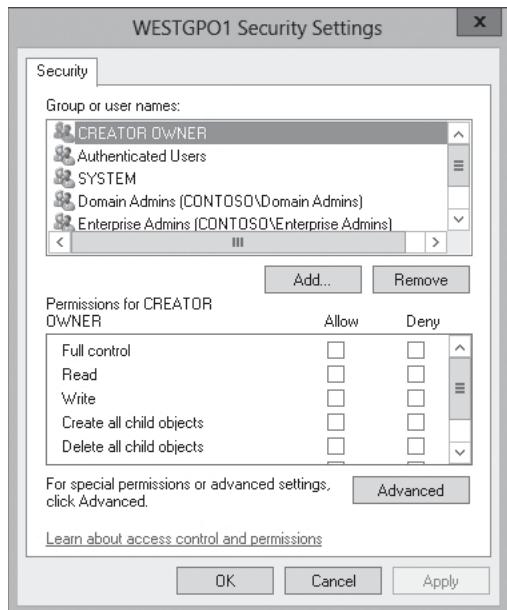
CONFIGURE A SECURITY GROUP FILTERING

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

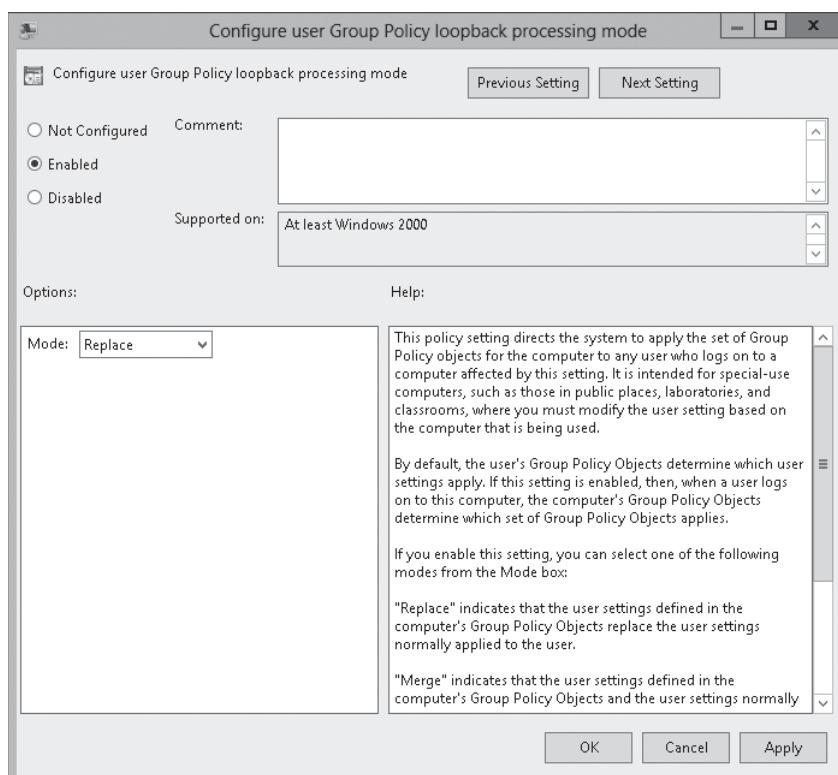
As you recall, GPO computer configuration settings are applied when a computer starts up, and GPO user configuration settings are applied when a user logs on. Group Policy **loopback processing** is used to assign user policies to computer objects. Therefore, no matter who logs on to a computer, the 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.

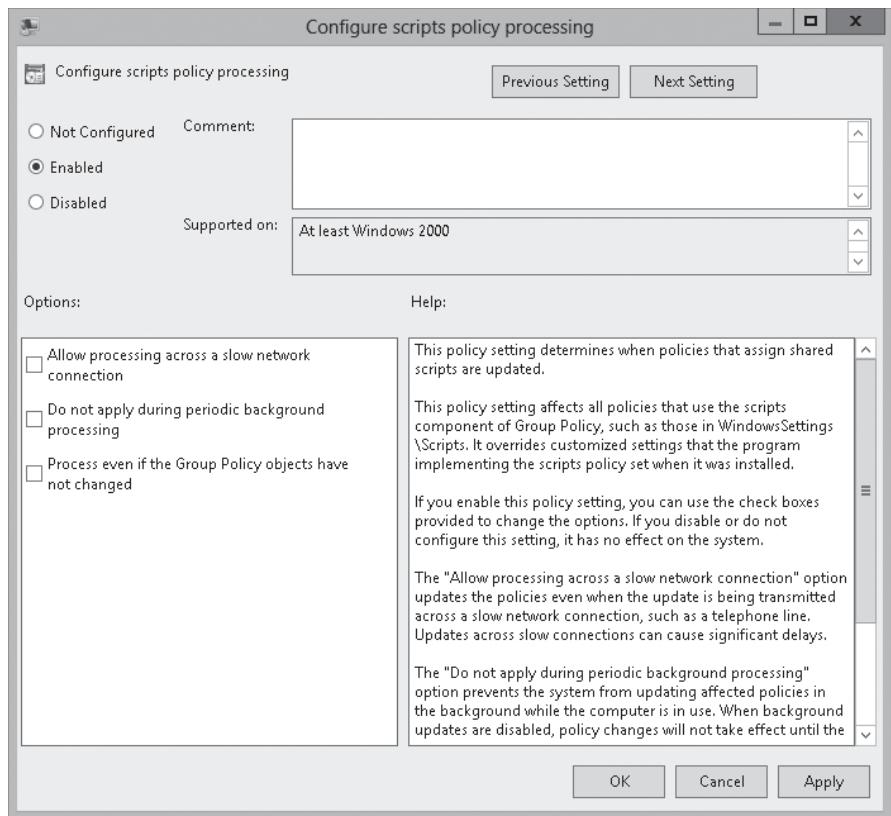
Each major category of policy setting has CSEs. For example, the Security CSE applies security changes, while the script CSE applies startup and logon scripts. Each version of Windows has added CSEs to extend the functional reach of Group Policy.

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 GPOs 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 be 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

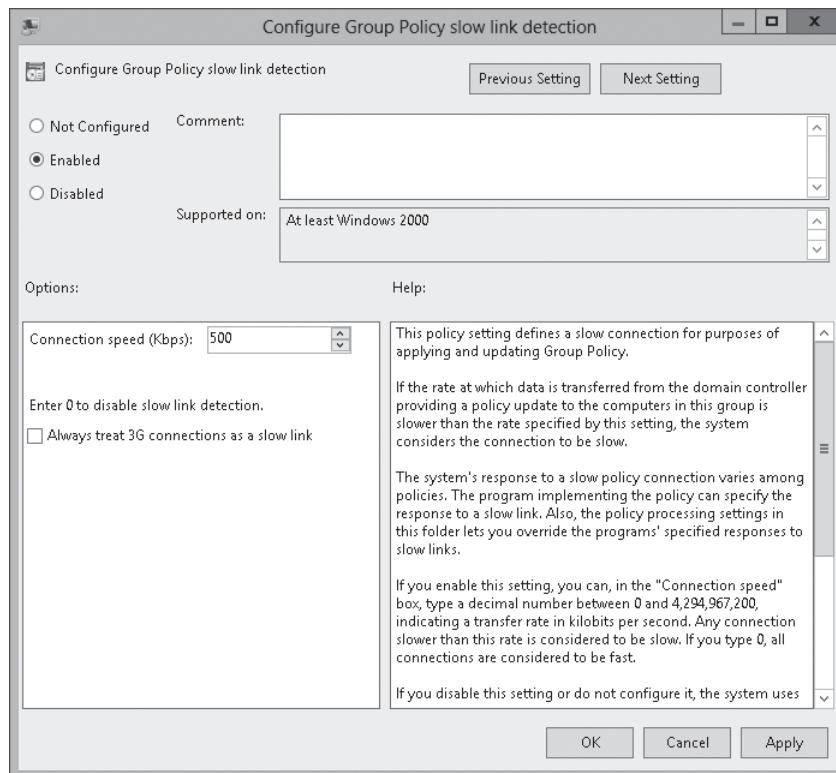
Sometimes when using group policies to perform certain tasks, group policies being executed over slow network links can affect the performance of the client computer or between a site and the corporate office of a site or the computer being configured via a GPO. By default, a link is considered slow 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

■ 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.

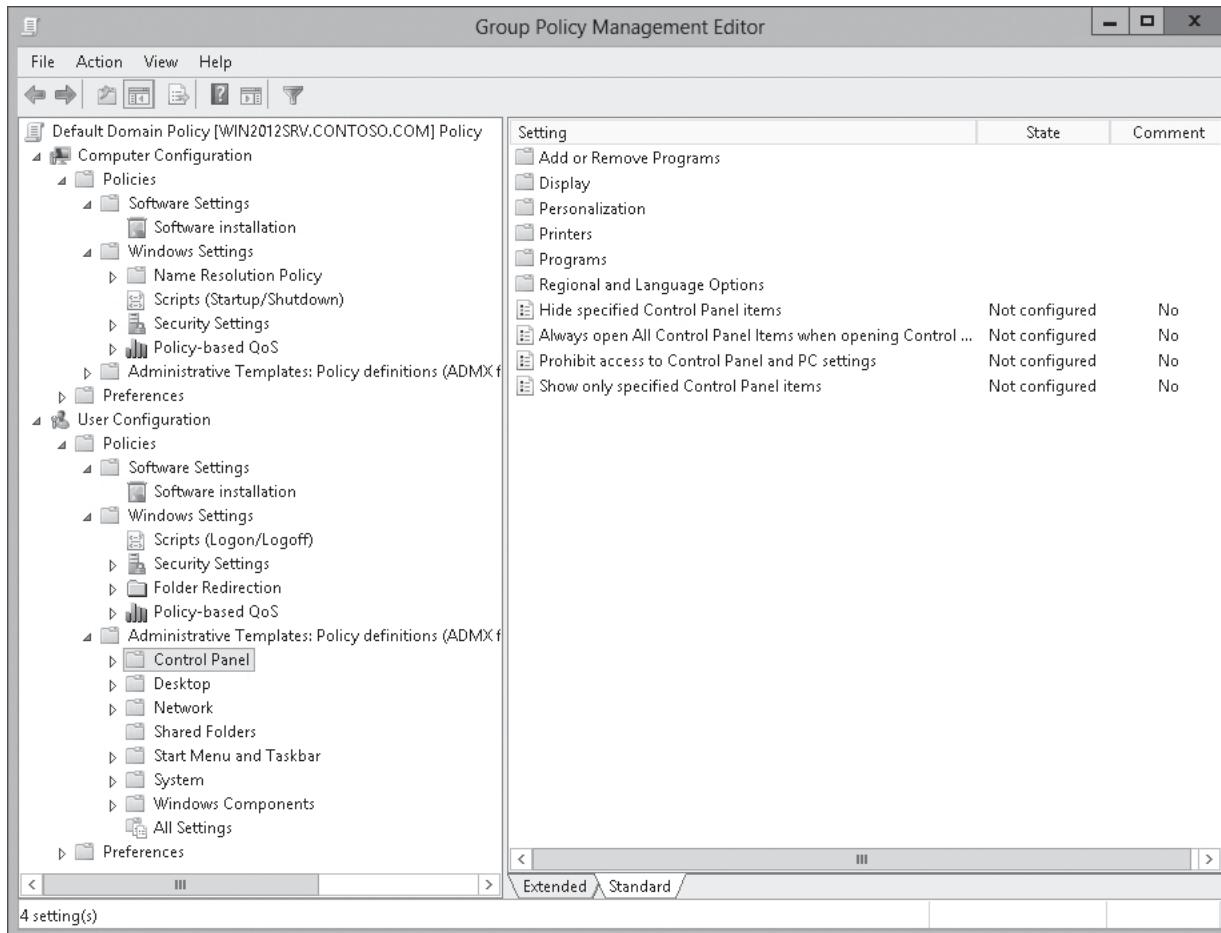
There are thousands of settings available with Group Policy. In addition, as each version of Windows is released, new settings are added to allow administrators to configure new technology that has been added to Windows, give control that was not available previously, or to give more granular control.

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](#)

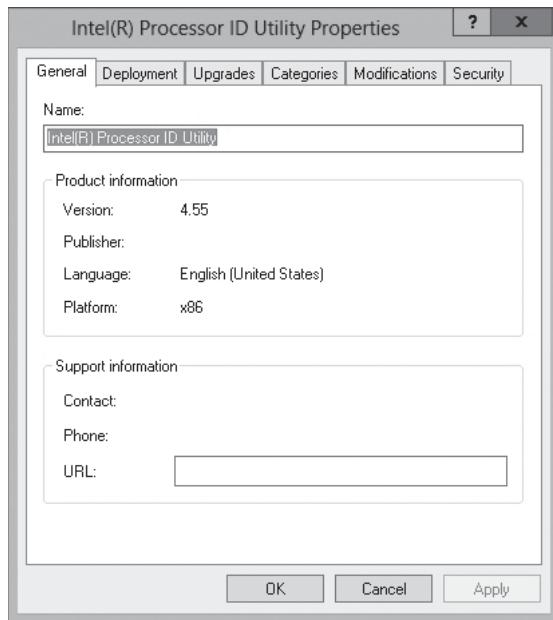
The Advanced option is used to set properties for the Windows Installer package, including published or assigned options and modifications.

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.

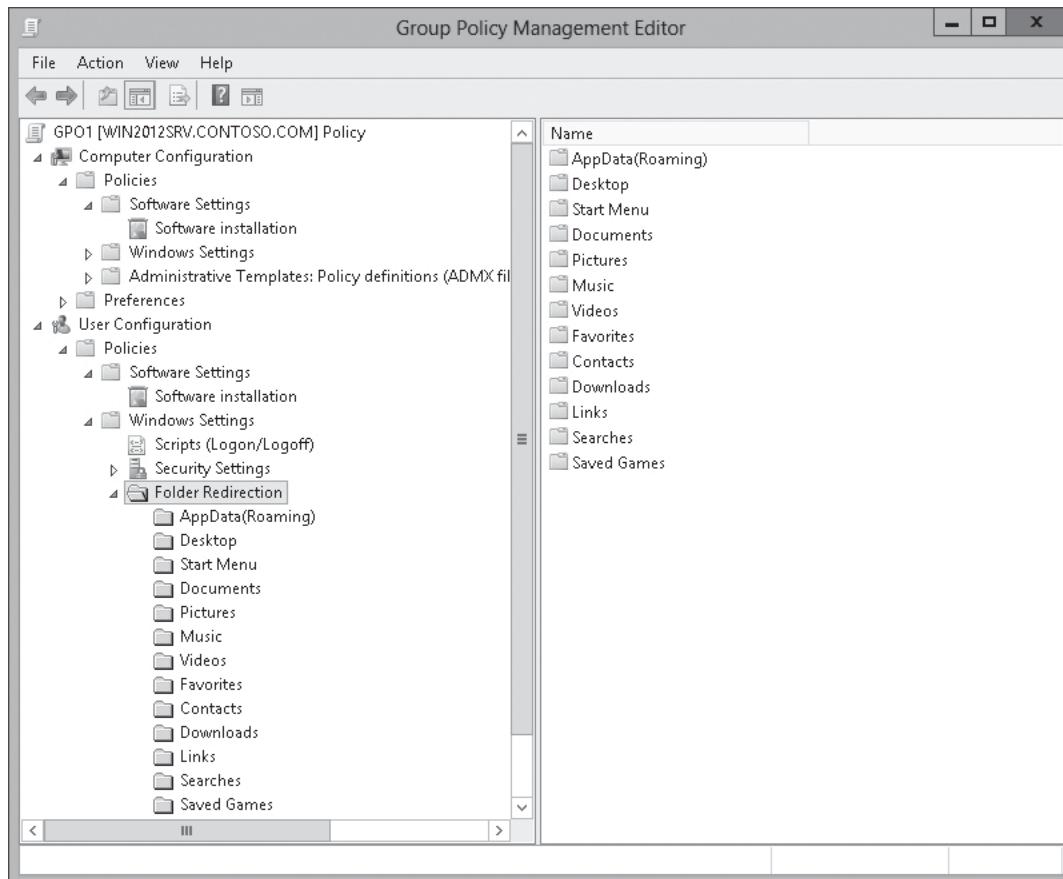
Using Folder Redirection

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 and 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/logout 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:

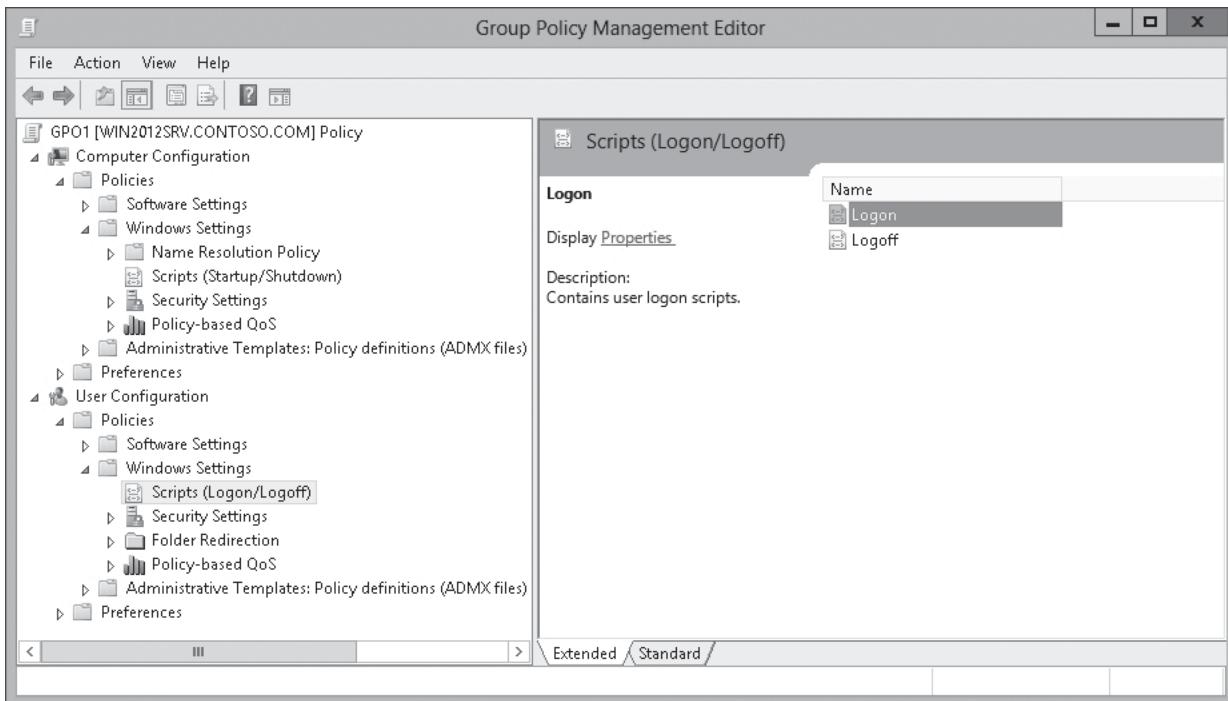
1. Create the login script.
2. Execute the script manually to make sure that the script runs and performs as planned.

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.

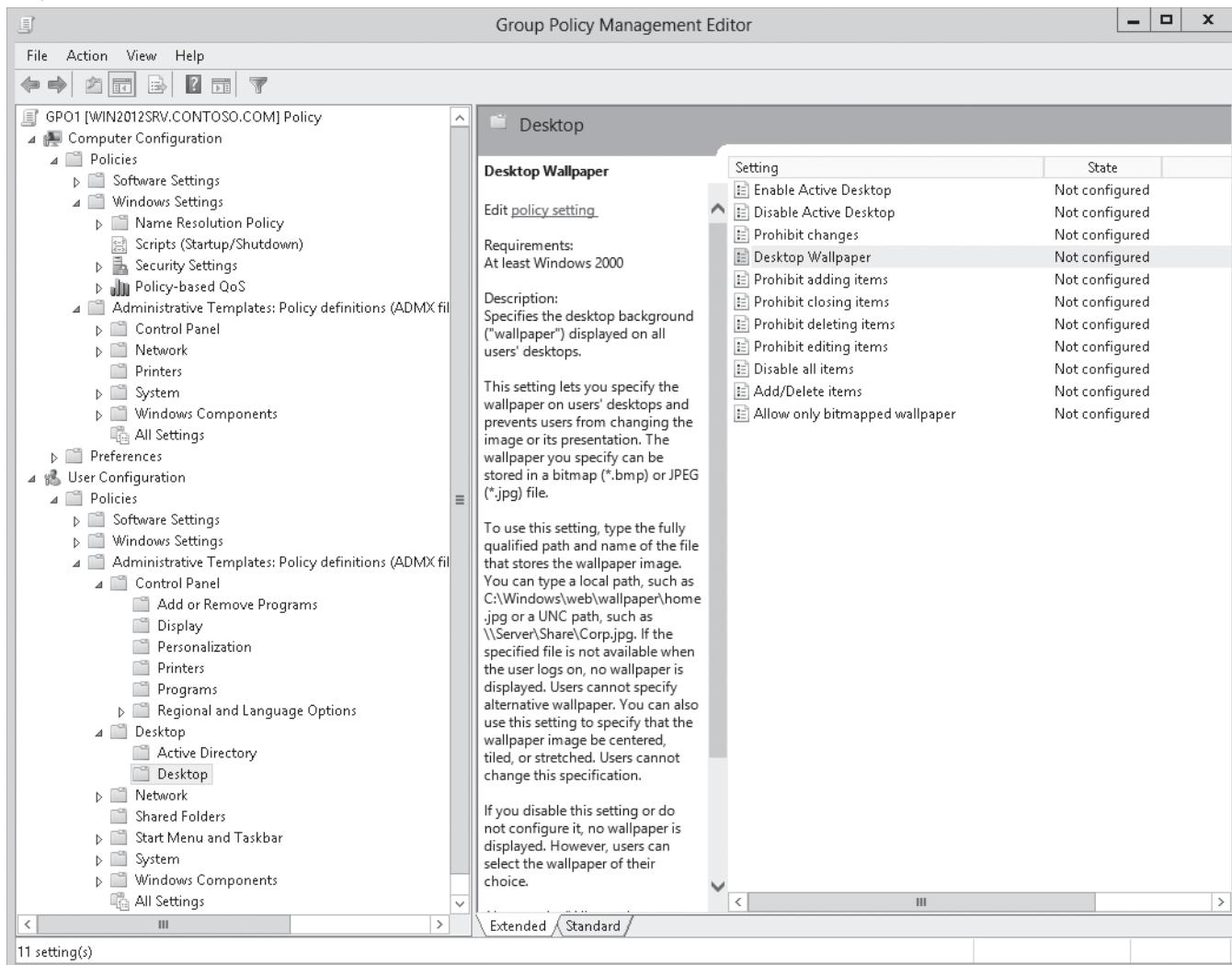
MANAGING ADMINISTRATIVE TEMPLATES

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:

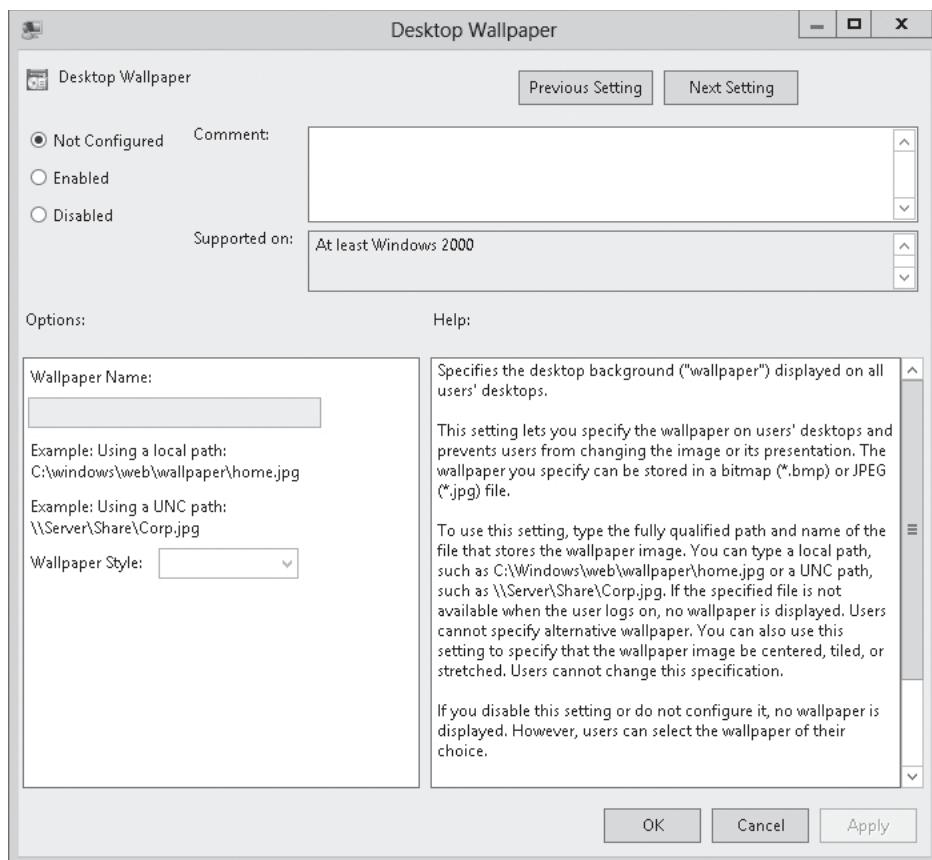
- Not Configured:** The registry key is not modified or overwritten.
- Enabled:** The registry key is modified by this setting.
- Disabled:** The Disabled settings undo a change made by a prior Enabled setting.

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.

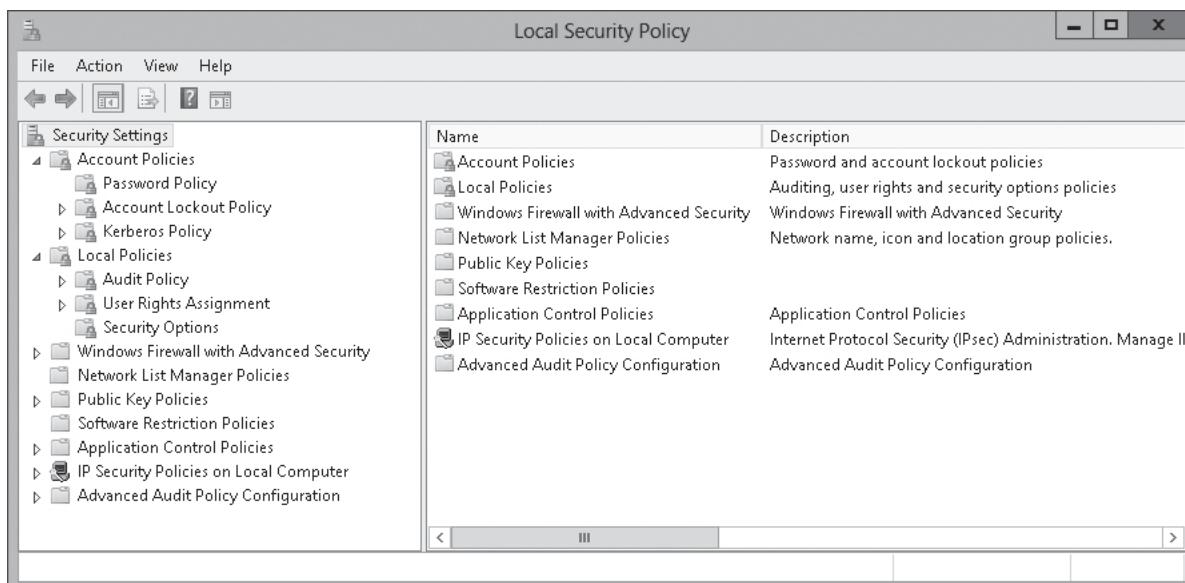
Using Security Templates

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.



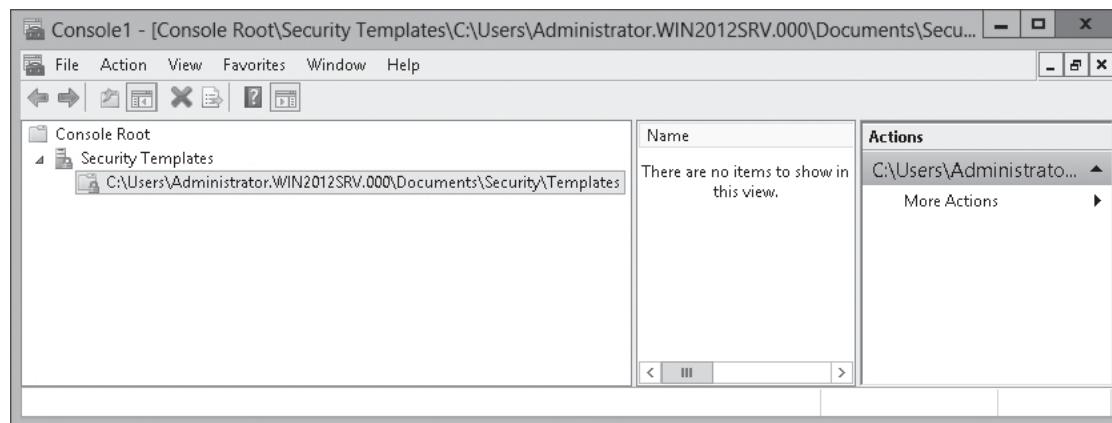
OPEN THE SECURITY TEMPLATES SNAP-IN

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?

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

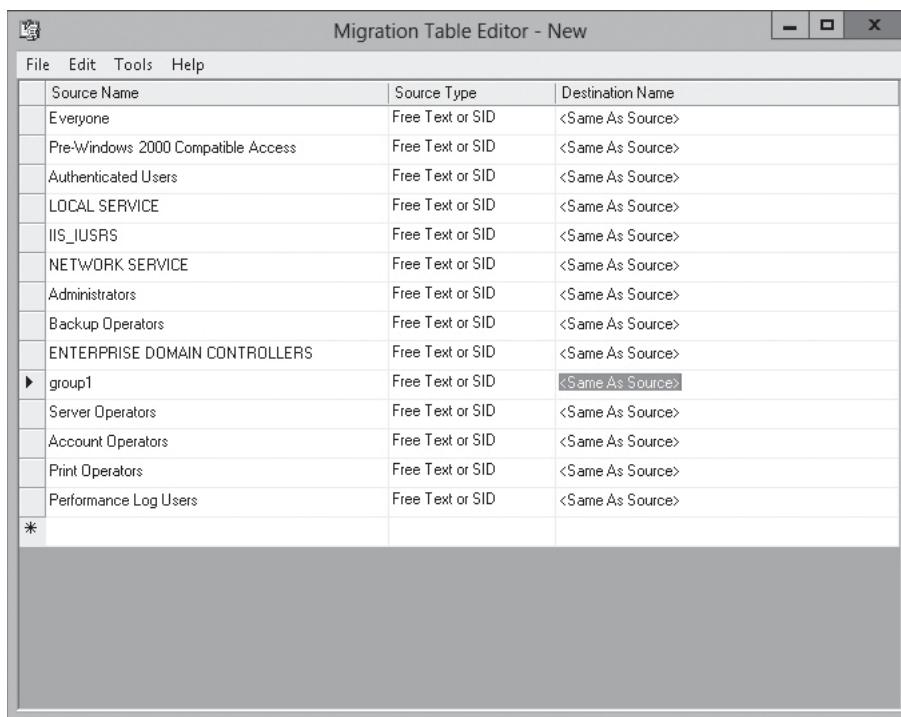
GET READY. To use a migration table while importing GPO settings, perform the following steps:

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



The screenshot shows the 'Migration Table Editor - New' window. The window has a menu bar with File, Edit, Tools, and Help. The main area is a table with three columns: Source Name, Source Type, and Destination Name. The table lists various security groups and their mappings:

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

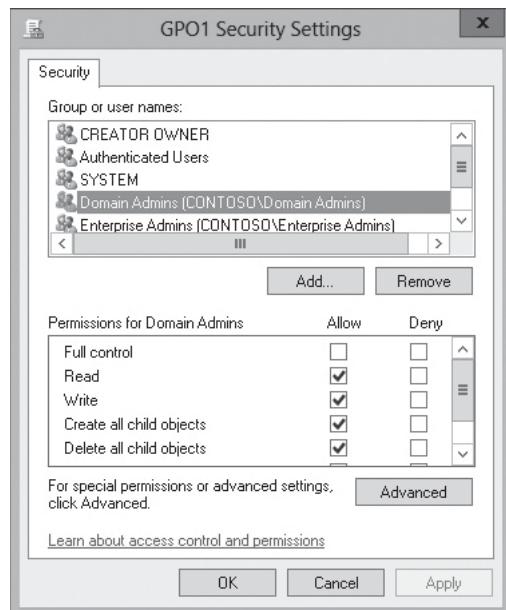
GET READY. To specify who can manage an individual GPO, perform the following steps:

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 UNC's 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

■ Using Group Policy Preferences



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 choose 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.

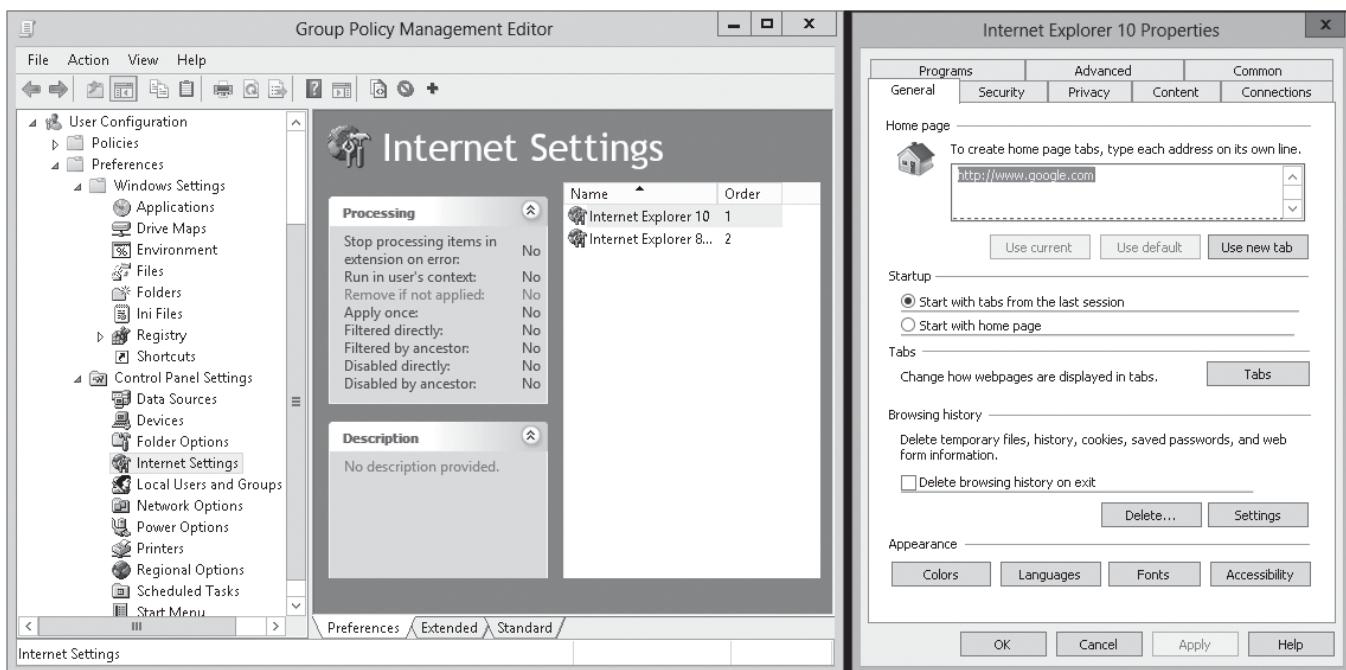
GPP can be configured on domain controllers running Windows Server 2008 or higher. By default, GPP are supported by client computers running Windows Vista SP2, Windows 7 or higher, or Windows Server 2008 or higher. To support Windows XP SP3, Windows Vista SP1, or Windows Server 2003 client computers, 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](#).

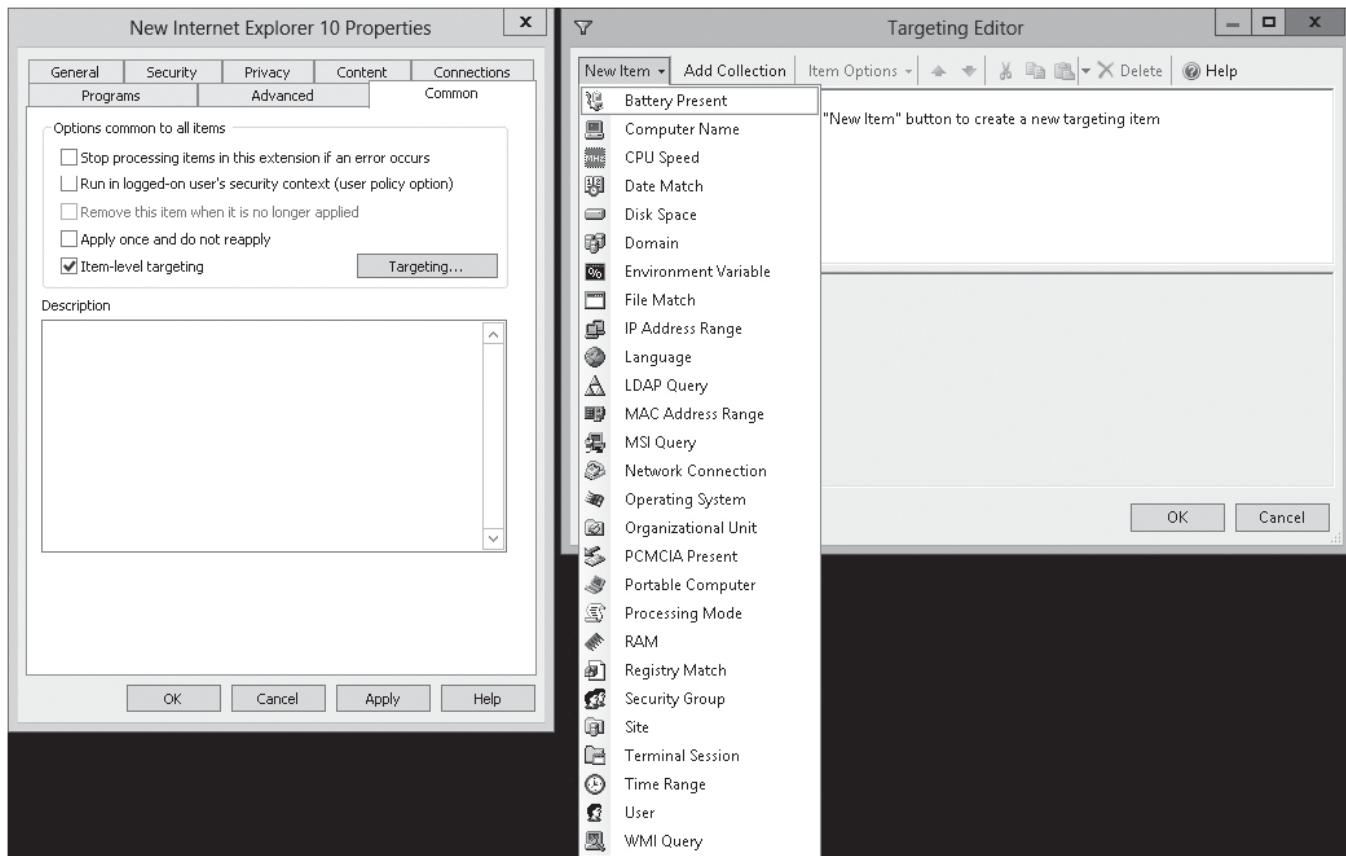
Configuring Item-Level Targeting

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

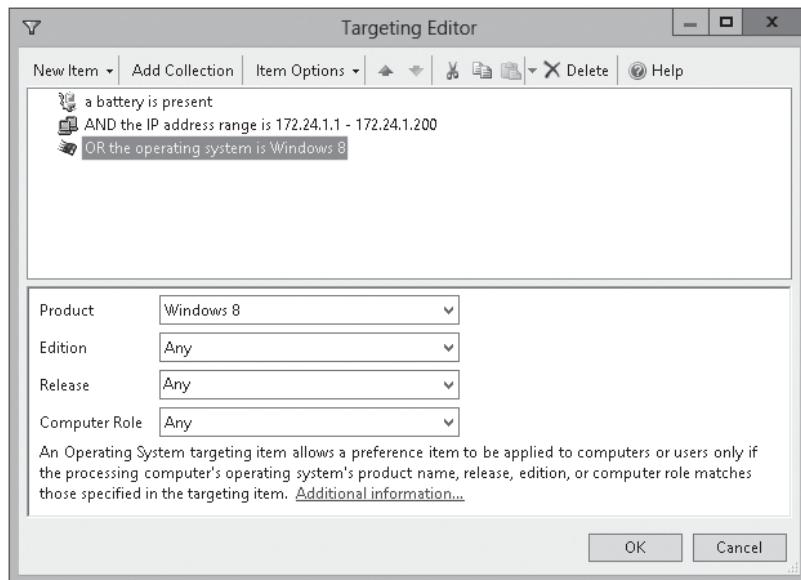


- Computer name
- CPU speed
- Date match
- Disk space
- Domain
- IP address range
- Network connection
- Operating system
- Portable computer
- RAM
- User
- Terminal session
- LDAP query
- Time range
- WMI query

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.