Microsoft

EXAM 70-646

Covers Windows Server 2008 R2

Windows Server® 2008 Server Administrator

Orin Thomas
Ian McLean

SECOND EDITION

Training Kit

Exam 70-646: Pro: Windows Server 2008 Server Administrator (2nd Edition)

OBJECTIVE	LOCATION IN BOOK
PLANNING FOR SERVER DEPLOYMENT	
Plan server installations and upgrades.	Chapter 1, Lesson 1
Plan for automated server deployment.	Chapter 1, Lesson 2
Plan infrastructure services server roles.	Chapter 2 Chapter 3 Chapter 9, Lesson 1
Plan application servers and services.	Chapter 6, Lesson 1
Plan file and print server roles.	Chapter 7
PLANNING FOR SERVER MANAGEMENT	
Plan server management strategies.	Chapter 5, Lesson 1
Plan for delegated administration.	Chapter 5, Lesson 2
Plan and implement group policy strategy.	Chapter 4
MONITORING AND MAINTAINING SERVERS	
Implement patch management strategy.	Chapter 8, Lesson 2
Monitor servers for performance evaluation and optimization.	Chapter 12
Monitor and maintain security and policies.	Chapter 8, Lesson 1 Chapter 9, Lesson 2
PLANNING APPLICATION AND DATA PROVISIONING	
Provision applications.	Chapter 6, Lesson 2
Provision data.	Chapter 10, Lesson 1
PLANNING FOR BUSINESS CONTINUITY AND HIGH AVAILABILITY	
Plan storage.	Chapter 10, Lesson 2
Plan high availability.	Chapter 11
Plan for backup and recovery.	Chapter 13

Exam Objectives The exam objectives listed here are current as of this book’s publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft’s sole discretion. Please visit the Microsoft Learning Web site for the most current listing of exam objectives: *http://www.microsoft.com/learning/en/us/Exam.aspx?ID=70-646*.

Microsoft®

Self-Paced Training Kit (Exam 70-646): Windows Server® 2008 Server Administrator (2nd Edition)

Orin Thomas
Ian McLean

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

Library of Congress Control Number: 2011929711

ISBN: 978-0-7356-4909-5

6 7 8 9 10 11 12 13 14 QG 8 7 6 5 4 3

Printed and bound in the United States of America.

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

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

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

Acquisitions Editor: Jeff Koch
Developmental Editor: Karen Szall
Project Editor: Rosemary Caperton
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Mitch Tulloch; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Sue McClung
Indexer: Jean Skipp
Cover: Twist Creative • Seattle

[2013-09-20]

This book is dedicated to my second grandchild, who is due to be born in early September 2011 and is currently known as Bump – also to Bump's Mummy and Daddy, Harjit and Drew, and of course to Bump's sister Freya, who is almost four and a big girl now.

—Ian McLean

To the awesome team at DDLS Melbourne, hope that we work together again soon!

—Orin Thomas

Contents at a Glance

Introduction *xxiii*

CHAPTER 1 Installing, Upgrading, and Deploying Windows Server 2008 R2 1

CHAPTER 2 Infrastructure Services Planning 37

CHAPTER 3 Planning Core Active Directory Infrastructure 107

CHAPTER 4 Group Policy Strategies 185

CHAPTER 5 Planning Server Administration 225

CHAPTER 6 Presentation and Application Virtualization 265

CHAPTER 7 Provisioning File and Print Servers 299

CHAPTER 8 Planning Security Policies 373

CHAPTER 9 Remote Access and Network Access Protection 433

CHAPTER 10 Provision Data and Plan Storage 473

CHAPTER 11 Clustering and High Availability 509

CHAPTER 12 Performance Evaluation and Optimization 539

CHAPTER 13 Backup and Recovery 591

Appendix *641*

Answers *645*

Index *691*

Contents

Introduction **xxiii**

System Requirements xxiv

Hardware Requirements xxiv

Software Requirements xxiv

Preparing the Computers Running Windows Server 2008 R2 Enterprise Edition xxiv

Practice Setup Instructions xxv

Using the CD xxv

How to Install the Practice Tests xxvi

How to Use the Practice Tests xxvi

How to Uninstall the Practice Tests xxvii

Acknowledgments xxviii

Support & Feedback. xxviii

Errata & Book Support xxviii

We Want to Hear from You xxviii

Stay in Touch xxviii

Chapter 1 Installing, Upgrading, and Deploying Windows Server 2008 R2 **1**

Before You Begin. 2

Lesson 1: Planning Installation and Upgrade. 3

The Differences Between Windows Server 2008 and Windows Server 2008 R2 3

Selecting the Right Edition 4

Foundation Edition 7

HPC Server 7

Server Core Installation Option 7
Physical Versus Virtual Deployment 11
Installing Windows Server 2008 R2 12
Upgrading from Windows Server 2003 13
Lesson Summary 15
Lesson Review 15

Lesson 2: Automated Server Deployment 17
Windows Server 2008 R2 Answer Files 17
Windows Deployment Services 19
Multicast, Scheduled, and Automatic Deployment 22
Rollback Preparation 26
Lesson Summary 26
Lesson Review 27

Chapter Review 34

Chapter Summary. 34

Key Terms 34

Case Scenarios. 35
Case Scenario 1: Contoso’s Migration to Windows Server 2008 35
Case Scenario 2: Tailspin Toys Automates Windows Server 2008 Deployment 35

Suggested Practices 36
Plan Server Installations and Upgrades 36
Plan for Automated Server Deployment 36

Take a Practice Test. 36

Chapter 2 Infrastructure Services Planning 37

Before You Begin. 37

Lesson 1: Planning IPv6 40
Analyzing the IPv6 Address Structure 40
IPv4-to-IPv6 Compatibility and Transition to IPv6 47
Using IPv6 Tools 55
Configuring Clients Through DHCPv6 61
Planning an IPv6 Network 63

Lesson Summary 67

Lesson Review 68

Lesson 2: Planning DNS 70

Planning Windows Server 2008 and Windows Server 2008 R2 DNS 71

Using New DNS Features and Enhancements 81

Planning a DNS Infrastructure 88

Lesson Review 96

Lesson Summary 97

Chapter Review 103

Chapter Summary 103

Key Terms 103

Case Scenarios 104

Case Scenario 1: Implementing IPv6 Connectivity 104

Case Scenario 2: Configuring DNS 104

Suggested Practices 105

Configure IPv6 Connectivity 105

Configure DNS 105

Take a Practice Test 106

Chapter 3 Planning Core Active Directory Infrastructure 107

Before You Begin 107

Lesson 1: Active Directory Directory Services 110

Planning the AD DS Server Role 110

Planning and Using RODCs 118

Planning Domain and Forest Functionality 133

Planning Forest-Level Trusts 139

Lesson Summary 143

Lesson Review 143

Lesson 2: Active Directory Certificate Services 147

Types of Certificate Authority 147

Windows Server 2008 R2 Enhancements 152

Configuring Credential Roaming 154

Configuring Autoenrollment 156

Configuring Web Enrollment Support 159

Configuring CRLs 160

Configuring an Online Responder for Certificate Services 162

Network Device Enrollment Service 165

Using Enterprise PKI to Monitor CA Health 166

Lesson Summary 168

Lesson Review 168

Chapter Review 180

Chapter Summary 180

Key Terms 181

Case Scenarios 181

Case Scenario 1: Planning an Upgrade from Windows Server 2003 to Windows Server 2008 R2 181

Case Scenario 2: Deploying Certificate Services at Coho Vineyard 182

Suggested Practices 182

Configure PSOs 182

Find Out More About RODCs 182

Configure Auditing 183

Configure Web Enrollment 183

Take a Practice Test 183

Chapter 4 Group Policy Strategies 185

Before You Begin 185

Lesson 1: Planning Group Policy Objects 188

Using Starter GPOs 188

Planning Administrative Templates 192

Lesson Summary 197

Lesson Review 197

Lesson 2: Group Policy Object Strategy 200

Planning Group Policy Strategy 200

Troubleshooting Group Policy 208

Lesson Summary 212
Lesson Review 212

Chapter Review 221

Chapter Summary 221

Key Terms 221

Case Scenarios 221

Case Scenario 1: Using Starter GPOs 222

Case Scenario 2: Planning and Documenting Troubleshooting Procedures 222

Suggested Practices 222

Use GPMC and Group Policy Management Editor 222

Examine ADMX Files 223

Examine GPO Reports 223

Examine RemoteApp Programs 223

Take a Practice Test 223

Chapter 5 Planning Server Administration 225

Before You Begin 225

Lesson 1: Server Management Technologies 227

Tools for the Administration of Windows Server 2008 and Windows Server 2008 R2 227

Remote Administration Technologies 232

Managing Event Logs 236

Lesson Summary 247

Lesson Review 247

Lesson 2: Delegating Authority 249

Delegation Policies 249

Delegation Procedures 249

Credential Delegation 253

Delegating the Management of Applications 256

Lesson Summary 258

Lesson Review 258

Chapter Review 262

Chapter Summary 262

Key Terms 262

Case Scenarios 262

Case Scenario 1: Fabrikam Event Management 263

Case Scenario 2: Delegating Rights to Trusted Users at Wingtip Toys 263

Suggested Practices 263

Plan Server Management Strategies 264

Plan for Delegated Administration 264

Take a Practice Test 264

Chapter 6 Presentation and Application Virtualization 265

Before You Begin. 265

Lesson 1: Presentation Virtualization 267

Planning Remote Desktop Infrastructure 267

Planning RD Session Host Server Software 268

RDS Licensing 268

License Server Scope 269

License Server Activation 270

RDS Client Access Licenses 271

Backing Up and Restoring a License Server 272

License Server Deployment 272

Configuring RD Session Host Servers 272

Server Properties 275

Configuring RDS with Group Policy 276

RD Web Access 277

RD Connection Broker 278

RD Gateway Server 279

Remote Desktop Virtualization Host 279

Monitoring RDS 280

Lesson Summary 281

Lesson Review 281

Lesson 2: Application Deployment and Virtualization 284

Traditional Application Deployment 284

Deploying Web Applications 285

RDS RemoteApp 288

App-V 290

Lesson Summary 291

Lesson Review 291

Chapter Review 295

Chapter Summary 295

Case Scenarios 295

Case Scenario 1: Planning an RDS Strategy for Wingtip Toys 295

Case Scenario 2: App-V at Contoso 296

Suggested Practices 296

Provision Applications 296

Plan Application Server and Services 297

Take a Practice Test 297

Chapter 7 Provisioning File and Print Servers 299

Before You Begin 299

Lesson 1: Planning Print Services Management 301

Planning the Print and Document Services Server Role 301

Using Windows Server 2008 R2 Print Enhancements 304

Managing Printers with the Print Management Console 308

Lesson Summary 318

Lesson Review 318

Lesson 2: Planning File Servers 320

Configuring a File Server 320

Using Windows Server 2008 R2 File Services Enhancements 332

Managing Access Control 346

Using FSRM to Configure Quotas, File Screen Policy, and Storage Reports 353

Lesson Summary 357

Lesson Review 358

Chapter Review 370

Chapter Summary 370

Key Terms 370

Case Scenario. 370

Planning a Windows Server 2008 R2 Upgrade 371

Suggested Practices 371

Use the Enhanced Print Management Console 371

Use the FSRM Console 371

Learn More About Windows Storage Server 2008 R2 372

Learn More About BranchCache For Network Files 372

Take a Practice Test. 372

Chapter 8 Planning Security Policies 373

Before You Begin. 373

Lesson 1: Developing Security Policies 376

Planning Server Security 376

Deploying Security Policies to Implement a Solution 384

Monitoring Server Security 391

Using the Encrypting File System 393

Lesson Summary 396

Lesson Review 396

Lesson 2: Managing Server Security 398

Deploying Updates with WSUS 398

New Features in WSUS 3.0 SP2 404

Autonomous and Replica Mode 405

Using Computer Groups 405

WSUS Client Configuration 407

Updates and Synchronization Strategies 410

Update Management and Compliance 412

Other Patch Management Tools 413

Lesson Summary 415

Lesson Review 415

Chapter Review 429

Chapter Summary 429

Key Terms 429

Case Scenarios 429

Case Scenario 1: Implementing a Security Plan for the Adatum Corporation 429

Case Scenario 2: Deploying WSUS 3.0 SP2 at Fabrikam 430

Suggested Practices 431

Monitor Server Security 431

Implement a Patch Management Strategy 431

Take a Practice Test. 431

Chapter 9 Remote Access and Network Access Protection 433

Before You Begin. 434

Lesson 1: Managing Remote Access 435

VPN Authentication 438

VPN Protocols 439

DirectAccess 442

NPS RADIUS Servers 447

Remote Access Accounting 449

Remote Desktop Gateway Servers 452

Lesson Summary 454

Lesson Review 454

Lesson 2: Firewalls and Network Access Protection 456

Windows Firewall with Advanced Security 456

Forefront Threat Management Gateway 457

Network Access Protection 459

NAP Enforcement Methods 460

DirectAccess NAP Enforcement 463

Remediation Servers 463

Monitoring-Only Mode 464

Lesson Summary 465

Lesson Review 465

Chapter Review 470

Chapter Summary. 470

Key Terms 470

Case Scenarios 471

Case Scenario 1: Remote Access at Wingtip Toys 471

Case Scenario 2: Coho Vineyard NAP 471

Suggested Practices 472

Monitor and Maintain Security Policies 472

Plan Infrastructure Services Server Roles 472

Take a Practice Test 472

Chapter 10 Provision Data and Plan Storage 473

Before You Begin. 473

Lesson 1: Provisioning Data 475

Planning Data Availability 475

Distributed File System (DFS) 478

Configuring Offline Data Access 485

Configuring Indexing in the Windows Search Service 487

Collaboration with SharePoint Foundation 2010 488

Lesson Summary 491

Lesson Review 492

Lesson 2: Planning Windows Server 2008 R2 Storage 494

Logical Unit Numbers 494

Storage Manager For SANs 496

Multipath I/O 498

Storage Explorer 499

Lesson Summary 500

Lesson Review 501

Chapter Review 505

Chapter Summary 505

Key Terms 505

Case Scenarios 505

Case Scenario 1: DFS at Wingtip Toys 506

Case Scenario 2: Provision Data at Contoso 506

Suggested Practices 506

Provision Data 506

Configure Storage 507

Take a Practice Test. 507

Chapter 11 Clustering and High Availability 509

Before You Begin. 509

Lesson 1: DNS Round Robin and Network Load Balancing. 511

Simple Availability Strategies 511

DNS Round Robin 511

Network Load Balancing 513

Managing NLB Clusters 516

NLB Port Rules 517

Comparing DNS Round Robin to Network Load Balancing 519

Lesson Summary 519

Lesson Review 520

Lesson 2: Windows Server 2008 Cluster Tools 522

Understanding Cluster Concepts 523

Installing Failover Clustering 526

Validating a Failover Cluster Configuration 526

Creating a Failover Cluster 527

Configuring Services for High Availability 528

Managing a Failover Cluster 530

Lesson Summary 531

Lesson Review 532

Chapter Review 536

Chapter Summary 536

Key Terms 536

Case Scenario. 537

Choose the Appropriate Availability Strategy 537

Suggested Practices 537

Plan for High Availability 537

Take a Practice Test. 538

Chapter 12 Performance Evaluation and Optimization 539

Before You Begin. 539

Lesson 1: Monitoring Data 542

Performance Monitoring and Reporting 542

Tracking System Reliability, Stability, and Overall Performance 554

Using the Action Center 557

Using System Tools to Investigate Processes and Services 558

Logging and Forwarding Events and Event Subscriptions 569

Lesson Summary 585

Lesson Review 585

Chapter Review 587

Chapter Summary. 587

Key Terms 587

Case Scenarios. 588

Case Scenario 1: Using Data Collector Sets and Event Forwarding 588

Case Scenario 2: Planning Monitoring on Server Computers 588

Suggested Practices 589

Use the Performance Monitoring Tools 589

Manage Event Logging 589

Investigate Process Explorer 589

Take a Practice Test. 590

Chapter 13 Backup and Recovery 591

Before You Begin. 591

Lesson 1: Backing Up Data 593

Using Shadow Copies of Shared Folders 593

Windows Server Backup 595

The Wbadmin Command-Line Tool 603

Backing Up Server Roles and Applications 606

Backing Up Computers Remotely 607

Further Considerations for Planning Backups 608

System Center Data Protection Manager 609

Lesson Summary 610

Lesson Review 610

Lesson 2: Disaster Recovery 613

Windows Server Backup Recovery Modes 613

Recovering Active Directory and Server Roles 618

Hyper-V and Disaster Recovery 625

Lesson Summary 626

Lesson Review 626

Chapter Review 638

Chapter Summary 638

Key Terms 638

Case Scenarios 639

Case Scenario 1: Wingtip Toys Backup Infrastructure 639

Case Scenario 2: Disaster Recovery at Fabrikam 639

Suggested Practices 640

Remote Backup 640

Server Restore 640

Take a Practice Test 640

Appendix 641

Answers 645

Index 691

Introduction

This training kit is designed for server and domain administrators who have two to three years of experience managing Windows servers and infrastructure in an environment that typically supports 250 to 5,000 (or even more) users in three or more physical locations and has three or more domain controllers. You will likely be responsible for supporting network services and resources such as messaging, database servers, file and print servers, a proxy server, a firewall, the Internet, an intranet, remote access, and clients. You also will be responsible for implementing connectivity requirements, such as connecting branch offices and individual users in remote locations to the corporate network and connecting corporate networks to the Internet.

NOTE **WINDOWS SERVER 2008 CERTIFICATION**

Exam 70-646 is one of three required exams for MCSA: Windows Server 2008 certification. For a limited time, it will also count towards the MCITP certification, which will be retired. Please visit the Microsoft Learning website for the most current information about Microsoft certifications: *http://www.microsoft.com/learning/*

The material covered in this training kit and on Exam 70-646 relates to the technologies in a Windows Server 2008 or Windows Server 2008 R2 network that support distributed access to web content, media, operating systems, and applications. The topics in this training kit cover what you need to know for the exam as described on the Skills Measured tab for the exam, which is available at
http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-646&locale=en-us

By using this training kit, you will learn how to do the following:

- Plan and implement the deployment of servers running Windows Server 2008 and Windows Server 2008 R2
- Plan and implement the management of servers running Windows Server 2008 and Windows Server 2008 R2
- Monitor, maintain, and optimize servers
- Plan application and data provisioning
- Plan and implement high-availability strategies and ensure business continuity

Refer to the objective mapping page in the front of this book to see where each exam objective is covered in the book.

System Requirements

The following are the minimum system requirements that your computer needs to meet to complete the practice exercises in this book and to run the companion CD. To minimize the time and expense of configuring physical computers for this training kit, it's recommended that you use Hyper-V, which is a feature of Windows Server 2008 and Windows Server 2008 R2. You can use third-party virtualization products, but the practice setup instructions in the book are written on the assumption that you are using Hyper-V.

Hardware Requirements

It is possible to complete almost all the practice exercises in this book using virtual machines rather than real server hardware. The system requirements for Windows Server 2008 R2 are listed on the following Web page: *http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx*.

If you intend to implement several virtual machines on the same computer (which is recommended), a higher specification will enhance your user experience. In particular, a computer with 8 GB of RAM and 150 GB of free disk space can host all the virtual machines specified for all the practice exercises in this book.

Software Requirements

The following software is required to complete all the practices:

- Windows Server 2008 R2 Enterprise edition
- Windows 7 Enterprise or Ultimate edition

You can obtain evaluation versions of the Windows Server 2008 R2 Enterprise edition and Windows 7 Enterprise edition from the Microsoft Download Center at the following address: *http://www.microsoft.com/Downloads/Search.aspx*.

Preparing the Computers Running Windows Server 2008 R2 Enterprise Edition

Detailed instructions for installing Windows Server 2008 R2 and installing and configuring the domain controller and member server running Windows Server 2008 R2 Enterprise edition are given in Appendix A, "Setup Instructions for Windows Server 2008 R2." The required server roles are added in the practice exercises in subsequent chapters.

Practice Setup Instructions

The exercises in this training kit require a minimum of two computers or virtual machines, as follows:

- One server running Windows Server 2008 R2 Enterprise, configured as a domain controller
- One server running Windows Server 2008 R2 Enterprise, configured as a member server

If you want to carry out all the practices and suggested practices in Chapter 4, "Group Policy Strategies," you need an additional client running Windows 7 Enterprise or Ultimate edition. All these computers can be virtual machines. You also need a second hard disk (internal or external) that is connected to your domain controller to carry out the practices in Chapter 13, "Backup and Recovery." If you are using virtual machines, this can be a virtual hard disk.

All computers must be connected physically to the same network. We recommend that you use an isolated network that is not part of your production network to do the practice exercises in this book. To minimize the time and expense of configuring physical computers, we recommend that you use virtual machines. To run computers as virtual machines on a server running Windows Server 2008 or Windows Server 2008 R2, you need to install the Hyper-V server role. Alternatively, you can use supported third-party virtual machine products.

Using the CD

The companion CD included with this training kit contains the following:

- **Practice tests** You can reinforce your understanding of how to configure Windows Server 2008 R2 by using electronic practice tests that you customize to meet your needs from the pool of Lesson Review questions in this book. Alternatively, you can practice for the 70-646 certification exam by using tests created from a pool of 200 realistic exam questions, which give you many opportunities to take practice exams to ensure that you are prepared.
- **An eBook** An electronic version (eBook) of this book is included so that you do not always have to carry the printed book with you. The eBook is in Portable Document Format (PDF), and you can view it by using Adobe Acrobat or Adobe Reader.

How to Install the Practice Tests

To install the practice test software from the companion CD to your hard disk, perform the following steps:

1. Insert the companion CD into your CD-ROM drive and accept the license agreement. The CD menu appears.

> ***NOTE*** **IF THE CD MENU DOES NOT APPEAR**
>
> **If the CD menu or the license agreement does not appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the CD-ROM for alternate installation instructions.**

2. Click Practice Tests and follow the instructions on the screen.

How to Use the Practice Tests

To start the practice test software, follow these steps:

1. Click Start, All Programs, and then Microsoft Press Training Kit Exam Prep. A window appears that shows all the Microsoft Press training kit exam prep suites that are installed on your computer.
2. Double-click the lesson review or practice test that you want to use.

> ***NOTE*** **LESSON REVIEWS VS. PRACTICE TESTS**
>
> **Select the (70-646) Windows Server 2008 R2 Server Administrator *lesson review* to use the questions from the "Lesson Review" sections of this book. Select the (70-646) Windows Server 2008 R2 Server Administrator *practice test* to use a pool of 300 questions similar to those that appear on the 70-646 certification exam.**

Lesson Review Options

When you start a lesson review, the Custom Mode dialog box appears so that you can configure your test. You can click OK to accept the defaults or you can customize the number of questions you want, how the practice test software works, which exam objectives you want the questions to relate to, and whether you want your lesson review to be timed. If you are retaking a test, you can select whether you want to see all the questions again or only the questions you missed or did not answer.

After you click OK, your lesson review starts.

- To take the test, answer the questions and use the Next, Previous, and Go To buttons to move from question to question.
- After you answer an individual question, if you want to see which answers are correct—along with an explanation of each correct answer—click Explanation.
- If you prefer to wait until the end of the test to see how you did, answer all the questions and then click Score Test. You will see a summary of the exam objectives that you chose and the percentage of questions that you got right, both overall and per objective. You can print a copy of your test, review your answers, or retake the test.

Practice Test Options

When you start a practice test, you choose whether to take the test in Certification Mode, Study Mode, or Custom Mode, which are as follows:

- **Certification Mode** This mode closely resembles the experience of taking a certification exam. The test has a set number of questions, it is timed, and you cannot pause and restart the timer.
- **Study Mode** This mode creates an untimed test, in which you can review the correct answer and the explanations for all the answer choices after you answer each question.
- **Custom Mode** This mode gives you full control over the test options so that you can customize them as you like.

The user interface when you are taking the test is basically the same in all the modes, but with different options enabled or disabled depending on the mode. The main options are discussed in the previous section, "Lesson Review Options."

When you review your answer to an individual practice test question, a "References" section is provided, which lists where in the training kit you can find the information that relates to that question and provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

How to Uninstall the Practice Tests

To uninstall the practice test software for a training kit, use the Program And Features option in the Control Panel.

> ***NOTE*** **COMPANION CONTENT FOR DIGITAL BOOK READERS**
>
> **If you bought a digital edition of this book, you can enjoy select content from the print edition's companion CD. Visit *http://go.microsoft.com/FWLink/?Linkid=219765* to get your downloadable content.**

Acknowledgments

The authors' names appear on the cover of a book, but we are only two members of a much larger team. First of all, thanks to Jeff Koch, for allowing us to update the first edition of this book, and to Karen Szall, our developmental editor. During the writing process, we worked most closely with Rosemary Caperton and Susan McClung. Rosemary and Sue, thanks for your patience with us and for making this a great book. Mitch Tulloch was our technical reviewer, and he was far more committed to the project than any reviewer we've worked with in the past. We would also like to thank Christian Holdener, of S4Carlisle Publishing Services, for his invaluable assistance in orchestrating the diverse actors in the enterprise of putting this book together. Each of our editors contributed significantly to this book, and we hope to work with them all in the future.

Support & Feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata & Book Support

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://go.microsoft.com/FWLink/?Linkid=219763

If you find an error that is not already listed, you can report it to us through the same page.

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

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

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

http://www.microsoft.com/learning/booksurvey

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

Stay in Touch

Let us keep the conversation going! We are on Twitter: *http://twitter.com/MicrosoftPress*

Preparing for the Exam

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

CHAPTER 7

Provisioning File and Print Servers

This chapter looks at the Print and Document Services and File Services server roles and describes how you can plan to meet your organization's printing, file storage, and access security needs. It discusses printer publishing and availability and looks at access permissions for both printers and files. The chapter covers file quotas and availability and describes how you can plan the deployment of the BranchCache For Network Files feature in both Distributed and Hosted Cache mode.

Exam objectives in this chapter:

- Plan file and print server roles.

Lessons in this chapter:

- Lesson 1: Planning Print Services Management **301**
- Lesson 2: Planning File Servers **320**

Before You Begin

To complete the exercises in the practice session in this chapter, you need to have done the following:

- Installed a server called VAN-DC1 running Windows Server 2008 R2 Enterprise that is configured as a domain controller in the Adatum.com domain, as described in Exercise 1 of the Appendix, "Setup Instructions for Windows Server 2008 R2."
- Optionally installed a server called VAN-SRV1 running Windows Server 2008 R2 Enterprise that is configured as a member server in the Adatum.com domain, as specified in Exercise 2 of the Appendix. This server is not required to carry out the practices in this chapter, but you may want to use it if you are trying out the new BranchCache For Network Files feature.
- Created a user account in the Adatum.com domain with the user name Kim Akers and password Pa$$w0rd, and added this account to the Domain Admins, Enterprise

Admins, and Schema Admins groups. This procedure is described in Exercise 1 of the Appendix.

- We recommend that you use an isolated network that is not part of your production network to do the practice exercises in this book. Internet access is not required for the exercises, and you do not need to configure a default gateway. To minimize the time and expense of configuring physical computers, we recommend that you use virtual machines. For example, you can create virtual machines using the Hyper-V server role.

REAL WORLD

Ian McLean

In July 1993, Microsoft introduced the new technology file system (NTFS). This was a remarkable development in its time. With its advent, folders and files could be protected from interactive as well as network users, and protection could be implemented at file level rather than folder level. I won't go into the many other developments that NTFS enabled—this isn't a history book—but I know that I have lost data on NTFS disks far less often than on FAT disks.

However, NTFS was not unalloyed good news, particularly for a network engineer (me) who was studying for his first MCSE at the time. NTFS introduced a level of complexity in calculating user permissions that almost guaranteed examination failure to those who couldn't quite understand how permissions interacted, particularly when the old No-Access permission was replaced by the more granular Deny.

Software was developed for determining resultant user permissions, but you can't take that into the examination room. My solution was much simpler. I drew three rectangular boxes next to each other. I marked the right box "File," the middle box "Folder," and the left box "Share."

Then I wrote in the NTFS permissions a user had on a file, and the permissions that the same user had on the folder that contained the file. File overrides folder, so I had my resultant NTFS permissions. If I were logged on locally, those were my permissions on the folder. I wrote the shared folder permission into the Share box. If I were accessing remotely, my permissions would be more restrictive between share and resultant NTFS. I had worked out my user permission.

I used this technique in exams and in my profession. When I became an MCT, I taught it to my students, and rectangular boxes appeared on whiteboards throughout the land. It's a simple technique. Some have even called it dumb.

It works. Try it.

Lesson 1: Planning Print Services Management

As far as the users in your organization are concerned, one of the major functions they require from a computer network is the ability to print files easily and without fuss. You need to publish printers so that your users can print to them, while at the same time controlling the use of expensive printing assets. You need to plan your print infrastructure so that urgent print jobs are completed quickly while large, non-urgent print jobs are done outside normal working hours. This lesson looks at the Print and Document Services server role and how you manage availability and access permissions and publish printers.

After this lesson, you will be able to:

- Install the Print and Document Services server role and install and manage printers and print drivers.
- Manage printer access permissions and printer availability.

Estimated lesson time: 35 minutes

Planning the Print and Document Services Server Role

As an experienced administrator, you will almost certainly be familiar with administering printers and print devices. What is new in Windows Server 2008 R2 is that the Print Services server role, introduced in Windows Server 2008, is now the Print and Document Services server role. You need to install this server role on a server to create a print server. You will install this role in the practice later in this lesson. The Print Management console has been enhanced in Windows Server 2008 R2 and is described in this lesson.

The Print and Document Services server role lets you manage print servers and printers. If you configure a server running Windows Server 2008 R2 as a print server, you reduce administrative and management workload by centralizing printer management tasks through the Print Management console.

By default, installing the Print and Document Services server role installs the Print Server role service, which lets you share printers on a network and publish them to Active Directory Directory Services (AD DS). If you want, you can install the Line Printer Daemon (LPD), which lets you print to printers connected to a UNIX server; the Distributed Scan Server role service (new to Windows Server 2008 R2), which you use to communicate with scanners that support Web Services on Devices (WSD), run scan processes, route scanned documents, and log scan-related events; and Internet Print, which lets you use a web interface to connect to and manage printers.

***NOTE* PRINTERS AND PRINT DEVICES**

A print device is a physical device that prints hard copy. A printer controls a print device. You can install several printers connected to a single print device and set different access permissions and schedules for different users. For example, if you have an expensive color print device, you might want to allow access to ordinary users only outside of normal working hours, but allow access at any time to the Managers security group. You can do this by creating two printers, both connected to the print device.

Planning the Print and Document Services server role involves analyzing current and required printing needs within an organization and configuring printer scheduling and access permissions. Do you have a department that sends very large but non-urgent jobs to a print device? In this case, you need to configure a printer that sends such jobs to a print device outside of office hours.

Does everyone in your organization need to print in color? If you give people the opportunity to print in color, they are likely to do so whether they need to or not. You cannot prevent users from habitually clicking Print several times whenever they want to print a document, or from printing out all their email messages. You can, however, set up auditing to detect high printer usage and identify those users with bad printing habits. As this book states in several places, an administrator needs to be able to solve people problems as well as technical problems.

Some of your planning decisions will be practical and pragmatic. It might be a good idea to have a print device with multiple input trays for special paper types, but it is probably a bad idea to use this device for general-purpose printing. A print device that stops and flashes an error message, thus blocking other jobs in the print queue, whenever a user specifies the wrong size of paper (which could happen easily and frequently) is also a bad choice for general printing needs. Also, you should consider using a printer pool—where a single printer controls several print devices—if you need to provide high availability of print devices.

Managing Printer Entities

If the Print and Document Services server role is installed on your server, you can manage the following entities:

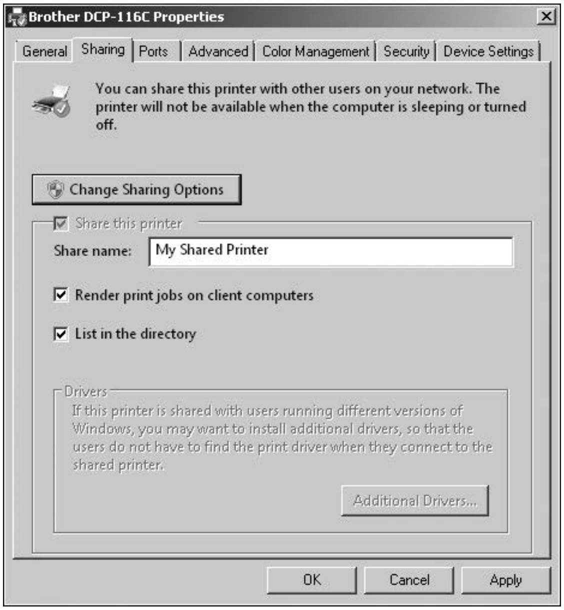
- **Print queue** A print queue is a representation of a print device. Opening a print queue displays the active print jobs and their status. If a print job at the head of the queue is not being processed (possibly because an incorrect paper size is specified), you can delete this job and allow the remainder of jobs in the queue to be processed.
- **Print spooler service** A print server has a single print spooler service. This manages all the print jobs and print queues on that server. Typically, the print spooler service starts automatically. If, however, the service has stopped for any reason, you need to restart it. A symptom of this is a print job at the head of a queue that is not being processed but cannot be deleted.

- **Printer driver** A print queue requires a printer driver to print to a print device. You need to ensure that the print driver exists on your print server, is working correctly, and is up to date.
- **Network printer port** A printer driver uses a network printer port to communicate with a physical device across a network. These ports may, for example, be TCP/IP printer ports, Line Printer Remote (LPR) ports, or standard COM and LPT ports.
- **Print server cluster** Printing is typically a mission-critical operation and you might choose to cluster your print servers to ensure high availability and failover support. Chapter 11, "Clustering and High Availability," discusses cluster administration.

Publishing Printers

If you share a printer on a network but do not publish it in Active Directory, users then need to know its network path to use it. If you do publish the printer in Active Directory, it is easier to locate. If you decide to move a printer to another print server, you do not need to change the settings on clients—you only need to change its record in Active Directory.

If a printer is shared but not published, you can publish it by selecting the List In The Directory check box on the Sharing tab of the printer's Properties dialog box, shown in Figure 7-1.



You can share this printer with other users on your network. The printer will not be available when the computer is sleeping or turned off.

☑ Share this printer

Share name: My Shared Printer

☑ Render print jobs on client computers

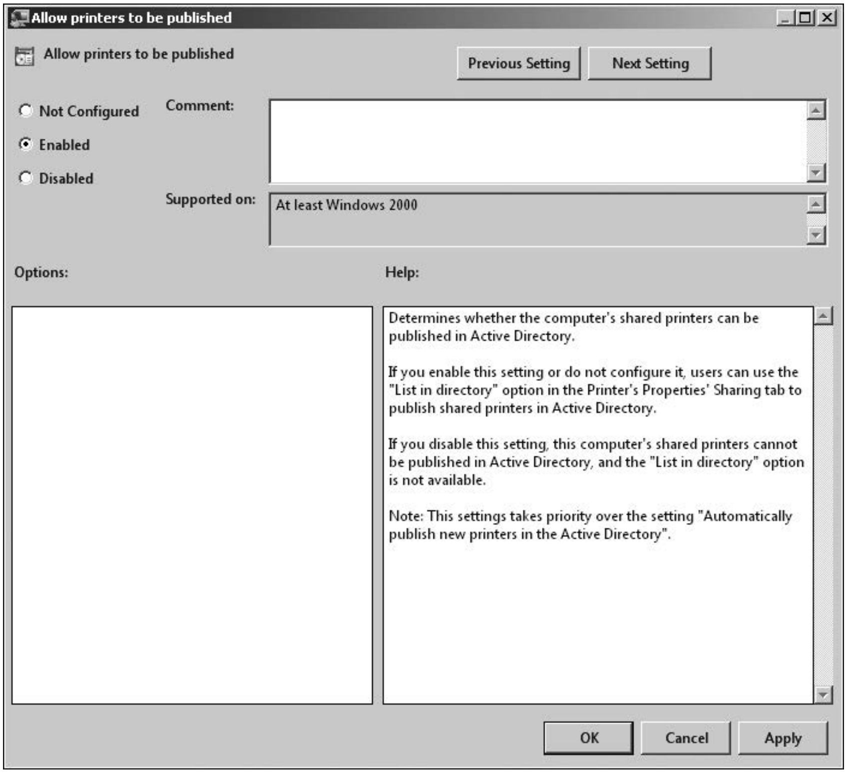
☑ List in the directory

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

FIGURE 7-1 Publishing a printer

If you add a printer on a print server running Windows Server 2008 R2 and share it, the printer is published automatically, provided that the Group Policy settings called Automatically Publish New Printers In Active Directory and Allow Printers To Be Published are enabled. Figure 7-2 shows the Allow Printers To Be Published setting. A published printer needs to be shared. If you stop sharing the printer, it is no longer published.



○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Determines whether the computer's shared printers can be published in Active Directory.

If you enable this setting or do not configure it, users can use the "List in directory" option in the Printer's Properties' Sharing tab to publish shared printers in Active Directory.

If you disable this setting, this computer's shared printers cannot be published in Active Directory, and the "List in directory" option is not available.

Note: This settings takes priority over the setting "Automatically publish new printers in the Active Directory".

FIGURE 7-2 Allowing printers to be published

Using Windows Server 2008 R2 Print Enhancements

Windows Server 2008 R2 provides users with enhanced printer and Print and Documents Services server role performance through the use of XML Paper Specification (XPS) documents, print paths, and printer drivers. It provides improved Print Management tools and, in particular, enhances the Print Management console. It also provides built-in support for WSD. It enhances efficiency and reduces the processing load on the Print Server and Documents server by performing print rendering on clients.

XPS Documents

Windows Server 2008 R2 integrates XPS throughout the print subsystem. This provides an enhanced level of efficiency, compatibility, and document quality. The XPS Document format is based on a fixed-layout document technology. The Microsoft XPS and Open Packaging Conventions (OPC) define the format, and these specifications are built on industry standards, such as XML and ZIP.

The XPS Document format provides broad platform support and is standard with Windows Vista. It is also supported by Microsoft .NET Framework 3.0 in Windows XP, Windows Vista, Windows 7, and Windows Server 2003. Cross-platform solutions are made possible by the open specifications. Many vendors of print and scan products are already developing solutions around XPS technologies to take advantage of the performance available and quality improvements to both .NET Framework 3.0 and Win32 applications.

XPSDrv printer drivers use a modular architecture that allows them to process documents in the print queue more efficiently. Windows Server 2008 R2 XPSDrv printer drivers use an architecture that extends the existing driver infrastructure with new features and capabilities while retaining compatibility with existing printers and applications. The XPSDrv printer driver architecture provides the following features:

- It supports Windows Presentation Foundation (WPF) and is also compatible with Win32-based applications.

MORE INFO **WPF**

For more information about WPF, access *http://msdn.microsoft.com/en-us/library/ms754130.aspx* and follow the links. Be aware, however, that the examination is unlikely to ask in-depth questions on this topic.

- It allows you to include custom filters that perform such functions as adding a corporate watermark or implementing quota management and print job accounting.
- It enables independent hardware vendors to share common functionalities between similar driver models. This can improve the reliability of driver components and enhance print server driver post-processing by supporting the reuse of common printer driver components.

The print architecture gives existing applications the ability to use features that can be found only in the XPSDrv printer drivers. New applications that are written to use the .NET Framework 3.0 and .NET Framework 3.5 can take advantage of all the features that are offered throughout the print path.

MORE INFO **.NET FRAMEWORK 3.0 AND .NET FRAMEWORK 3.5**

For more information about .NET Framework 3.0 and .NET Framework 3.5, including download links, see *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=10CC340B-F857-4A14-83F5-25634C3BF043&displaylang=en* and *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=333325FD-AE52-4E35-B531-508D977D32A6&displaylang=en*, respectively.

XPSDrv printer drivers provide your users with better print quality. The drivers are not limited to using only the graphics device interface (GDI) processing functions. This enables them to process graphics in alternate color spaces and to use higher-performance graphics libraries that were not available to the older, GDI-based printer drivers.

Print Paths

Windows Server 2008 R2 supports the XPS print paths that use the XPS Document format throughout the print path from the application to the printer. This makes it possible to achieve true WYSIWYG print output. Print paths in Windows Server 2008 R2 provide the following advantages:

- They eliminate the file format conversions that are common with GDI-based printer drivers. This improves print performance and printed output quality, and helps reduce the overall size of spool files.
- They provide support for advanced color spaces and technologies in the printer driver components.
- They use 32-bit-per-channel color and CMYK color space. CMYK refers to the four inks used in some color printing: cyan, magenta, yellow, and key black.
- They provide direct support for transparencies and gradients.
- They implement conversion print paths to support existing applications and printer drivers.

The Print Management Console

Print and Document Services in Windows Server 2008 R2 enables you to share printers on a network and centralize print server and network printer management tasks by using the Print Management MMC snap-in. This console, shown in Figure 7-3, helps you monitor print queues and receive notifications when print queues stop processing print jobs. It also enables you to migrate print servers and deploy printer connections using Group Policy. You access the Print Management console by clicking Print Management on the Administrative Tools menu. Note that this tool is not available unless you have installed the Remote Server Administration Tools (RSAT) or have installed the Print and Document Services server role. You install this server role in a practice later in this chapter.

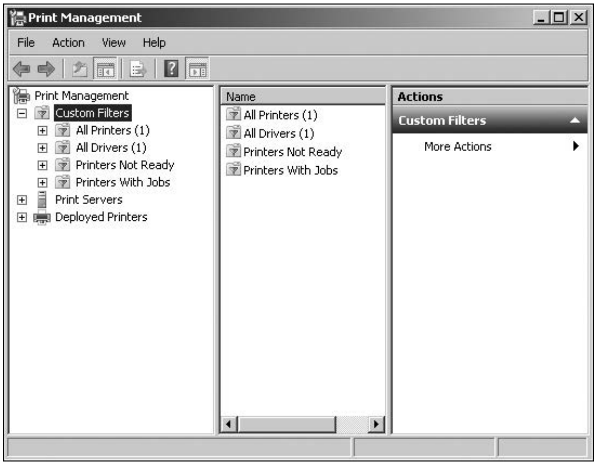


FIGURE 7-3 The Print Management console

The enhanced Windows Server 2008 R2 Print Management console includes support for print server migration from Windows 2000 Server and Windows Server 2003 to Windows Server 2008 R2. It also features an improved Network Printer Installation Wizard, which reduces the number of steps that you need to perform when adding network printers. The wizard automatically locates printers and installs the appropriate printer driver if this is available.

✓ **Quick Check**

- **What three features does the XPSDrv printer driver architecture provide in Windows Server 2008 R2?**

Quick Check Answer

- **It supports WPF.**
- **It allows you to include custom filters that perform such functions as adding a corporate watermark or implementing quota management and print job accounting.**
- **It enables independent hardware vendors to share common functionality between similar driver models.**

Web Services on Devices (WSD)

Windows Server 2008 R2 provides built-in support for WSD, which is a set of protocols for accessing and controlling services on network-connected devices. WSD makes it easier to connect, install, and use printers. Microsoft is working in collaboration with several printer manufacturers to support this protocol in its devices.

Improving Scalability

To reduce the processing load on the computer running the Print and Document Services server role, print rendering is performed on the client (in particular, on clients running Windows Vista). In some cases, performing print rendering on the client considerably reduces network bandwidth. The size of this reduction in bandwidth depends on the print job content and the Page Description Language (PDL).

The print spooler in Windows Server 2008 R2 uses remote procedure calls (RPCs) to communicate between the client and the server. Windows Server 2008 R2 significantly reduces the number of separate processing threads required for RPCs. This can greatly enhance performance in medium- to large-scale print environments.

MORE INFO **PRINT MANAGEMENT**

For more information about Print Management on computers running Windows Server 2008 R2, and also on computers running Windows Vista and Windows 7, access *http://technet.microsoft.com/en-gb/library/cc766474.aspx* and follow the links.

Managing Printers with the Print Management Console

The Print Management console is installed as part of the Print and Document Services server role in Windows Server 2008 R2. You can also install it by opening Server Manager, clicking Features in the console tree, and then clicking Add Features. You then expand Remote Server Administration Tools, expand Role Administration Tools, and select the Print And Document Services Tools check box. Click Next, and then click Install. Click Close when the tool is installed.

The Print Management console lets you implement single-seat administration in a large organization that has a number of print servers (typically a large number). When you have installed the Print Management console as part of RSAT (it is also installed by default when you add the Print and Document Services role), you can open it from the Administration Tools menu or from within Server Manager. When you have installed the Print Management console, you need to configure it to identify the printers and print servers that you want to manage. You can add printers manually, or you can scan the network to identify printers automatically by clicking Printers on the Print Management console tree, as shown in Figure 7-4.

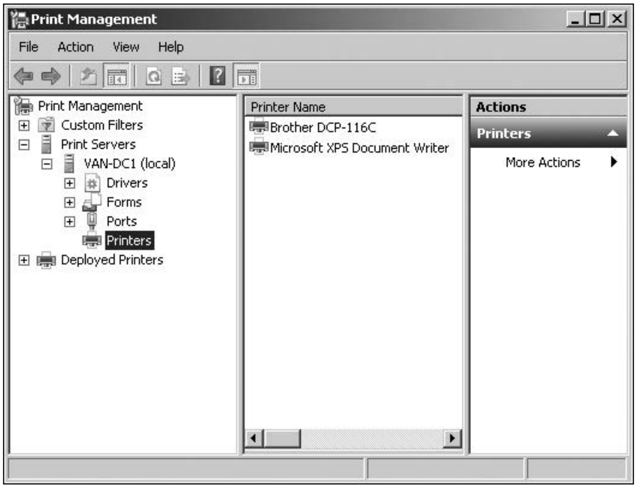
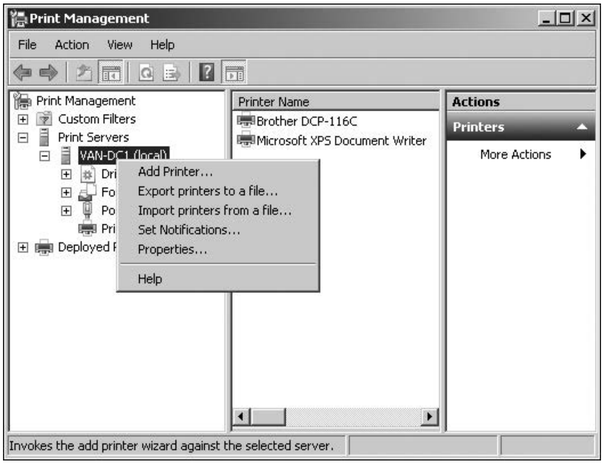


FIGURE 7-4 Scanning for printers automatically in the Print Management console

You can add a print server to the Print Management console by right-clicking Print Servers and selecting Add/Remove Servers. You can add new printers to a Windows Server 2008 R2 network by using the Add Printer wizard that was available in previous Windows versions. In Windows Server 2008 R2, this has been renamed the Network Printer Installation Wizard. The Print Management console gives you the option of running this wizard on a remote print server in both Windows Server 2008 and Windows Server 2008 R2; previously, you needed to run it locally.

To start the Network Printer Installation Wizard within the Print Management console, expand Print Servers and right-click the print server that you want to host the printer. Then click Add Printer, as shown in Figure 7-5, and follow the steps of the wizard. The Network Printer Installation Wizard lets you install a printer that is on a remote print server.



Invokes the add printer wizard against the selected server.

FIGURE 7-5 Accessing the Network Printer Installation Wizard

If you have added remote print servers to the Print Management console and configured printers on these servers, you can view, manage, and administer these printers and print servers centrally. Some of the tasks that you now can perform from the Print Management console, such as changing printer ports, adding or modifying forms, and viewing the status of printers, you previously had to carry out locally on a print server. Other tasks on the Print Management console are new, including creating custom printer filters that allow you and other administrators to view and manage selected printers based on their site, rights, and roles. The procedure to create a printer filter is described in the next section.

Creating a Printer Filter and a Print Driver Filter

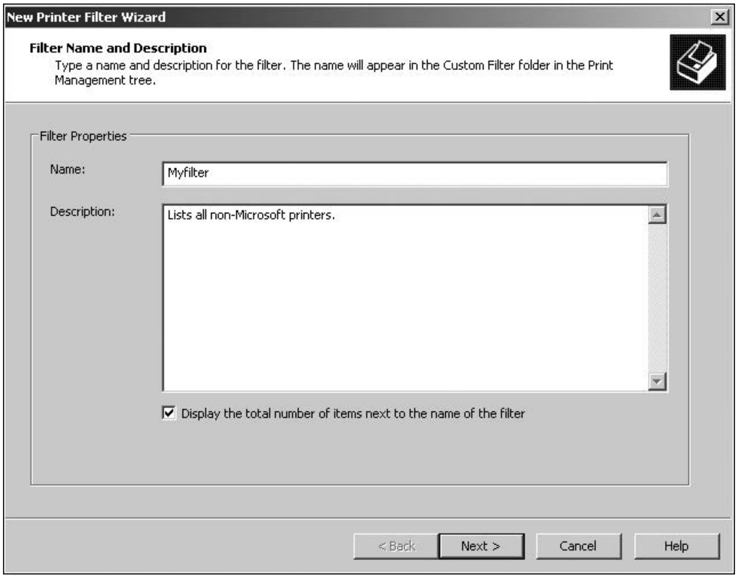
Printer filters are used to display only those printers that meet specified criteria. You can create custom printer filters that filter by manufacturer or by printer type (such as laser, color laser, and plotter). This lets you view assets by make, model, location, or configuration. For example, you could set a filter to display all the printers in a single building, regardless of the print server they use.

The Print Management console provides two default filters named Printers Not Ready and Printers With Jobs. When you create a new custom filter, you have the option to set up an email notification or to run a script when the conditions of the filter are met. The procedure to create a custom printer filter is as follows:

1. Open the Print Management console.
2. Right-click Custom Filters. Click Add New Printer Filter. This starts the New Printer Filter Wizard.
3. On the Printer Filter Name And Description page, specify a name for the printer filter. This name will appear in the Custom Printer Filters folder in the Print Management console tree.
4. If you want, type a description.

5. If you want to display the number of printers that satisfies the conditions of a filter, select the Display The Total Number Of Items Next To The Name Of The Filter check box.

6. The Filter Name And Description page should look similar to Figure 7-6. Click Next.



New Printer Filter Wizard

Filter Name and Description

Type a name and description for the filter. The name will appear in the Custom Filter folder in the Print Management tree.

Filter Properties

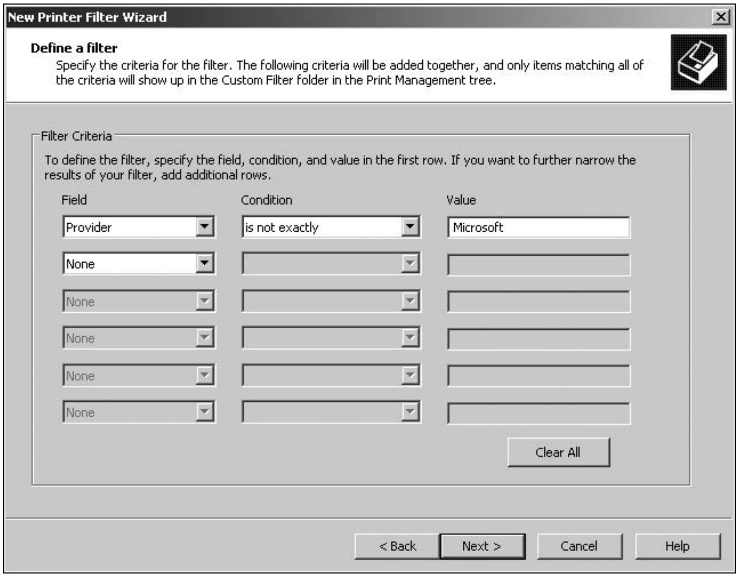
Name: Myfilter

Description: Lists all non-Microsoft printers.

☑ Display the total number of items next to the name of the filter

FIGURE 7-6 The Filter Name And Description page

7. On the Define A Printer Filter page, specify a printer status characteristic or print queue on the Field list. Specify a Condition and a Value for that condition, as shown in Figure 7-7. Click Next.



New Printer Filter Wizard

Define a filter

Specify the criteria for the filter. The following criteria will be added together, and only items matching all of the criteria will show up in the Custom Filter folder in the Print Management tree.

Filter Criteria

To define the filter, specify the field, condition, and value in the first row. If you want to further narrow the results of your filter, add additional rows.

Field	Condition	Value
Provider	is not exactly	Microsoft
None		
None		
None		
None		
None		

FIGURE 7-7 Defining a filter

8. If you want, on the Set Notifications (Optional) page, set an email notification, set a script to run, or specify both. Click Finish.
9. Click the name of the filter that you created in the Custom Filters container, as shown in Figure 7-8. View the list of printers in the middle pane.

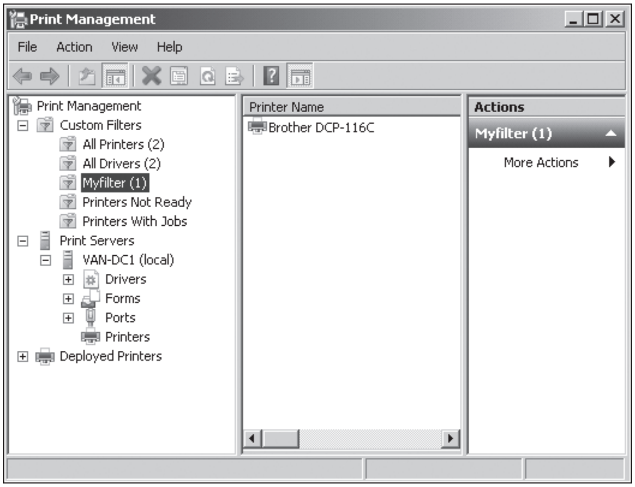


FIGURE 7-8 Viewing the printers specified by a printer filter

Similarly, you can use the Print Management console to create custom print driver filters that display only those print drivers that meet a certain set of criteria. The procedure for creating a custom print driver filter is almost identical to that for creating a custom printer filter, except that in step 2 you right-click Custom Filters and click Add New Driver Filter. You specify a name and (if you want) a description, and then select whether to display the number of items next to the filter.

As with a printer filter, you configure the print driver filter by specifying Field, Condition, and Value, and you have the option of configuring an email notification, running a script, or both.

EXAM TIP

Custom filters are new to the Print Management console and can be configured only on print servers running Windows Server 2008 or Windows Server 2008 R2.

Quick Check

- **What are the two default filters provided by the Print Management console in Windows Server 2008 R2?**

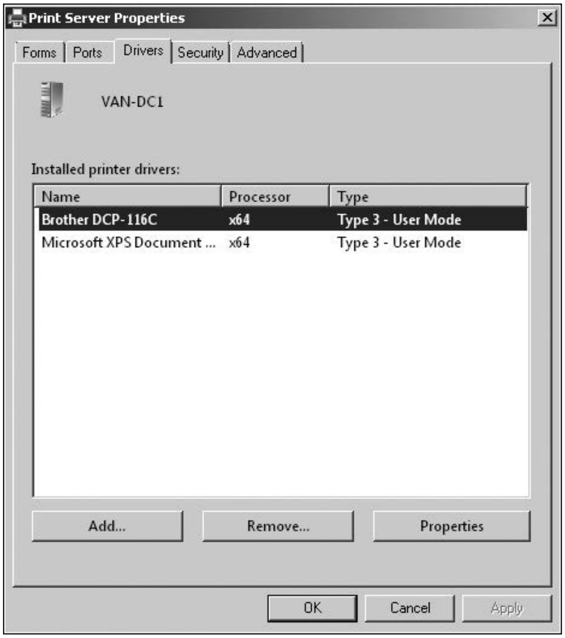
Quick Check Answer

- **Printers Not Ready and Printers With Jobs**

Managing Drivers, Ports, Forms, and Printers

You can expand any of the print servers listed in the Print Management console tree and manage drivers, ports, forms, or printers. You can also add a driver, a port, or a printer.

When you right-click Drivers and click Manage Drivers, this opens the Properties dialog box for the print server with the Drivers tab selected, as shown in Figure 7-9. You can add a new driver, remove a driver, or view the properties of any driver in the list.



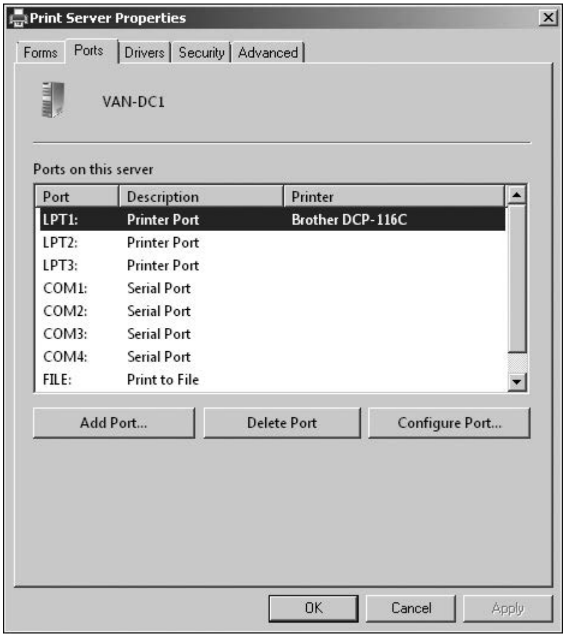
Installed printer drivers:

Name	Processor	Type
Brother DCP-116C	x64	Type 3 - User Mode
Microsoft XPS Document ...	x64	Type 3 - User Mode

FIGURE 7-9 The Drivers tab of the Print Server Properties dialog box

When you right-click Ports and click Manage Ports, this opens the Properties dialog box for the print server with the Ports tab selected, as shown in Figure 7-10. You can delete an existing port, add a new port, or configure a selected port. To configure a port, click Configure Port, enter a value (in seconds) for the transmission timeout retry interval, and then click OK.

When you right-click Forms and click Manage Forms, this opens the Properties dialog box for the print server with the Forms tab selected. When you select the Create A New Form check box, you can give the form a name and specify paper size and print area margins, as shown in Figure 7-11. When you are satisfied with your configuration, you click Save Form to create the form. Note that the Delete button becomes active only if you have already saved one or more custom forms and select a custom form on the Forms tab. You cannot delete standard forms from this tab.

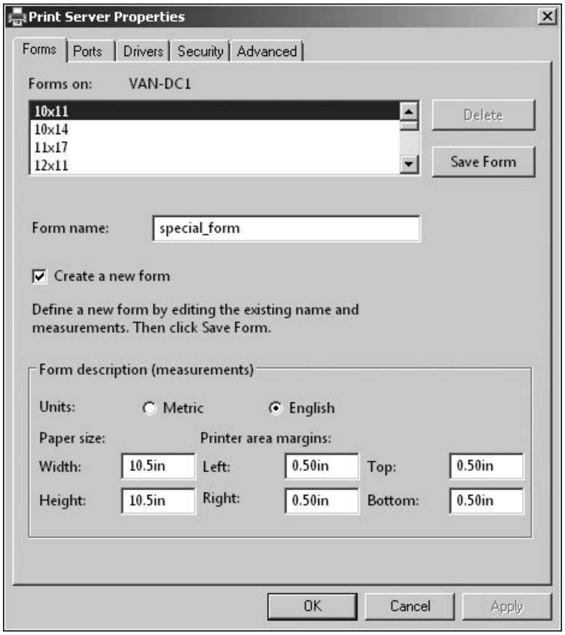


VAN-DC1

Ports on this server

Port	Description	Printer
LPT1:	Printer Port	Brother DCP-116C
LPT2:	Printer Port	
LPT3:	Printer Port	
COM1:	Serial Port	
COM2:	Serial Port	
COM3:	Serial Port	
COM4:	Serial Port	
FILE:	Print to File	

FIGURE 7-10 The Ports tab of the Print Server Properties dialog box



Forms on: VAN-DC1

10x11
10x14
11x17
12x11

Form name: special_form

☑ Create a new form

Define a new form by editing the existing name and measurements. Then click Save Form.

Form description (measurements)

Units: ○ Metric ● English

Paper size:		Printer area margins:			
Width:	10.5in	Left:	0.50in	Top:	0.50in
Height:	10.5in	Right:	0.50in	Bottom:	0.50in

FIGURE 7-11 The Forms tab of the Print Server Properties dialog box

When you right-click Printers under a print server, you can add a printer or show or hide Extended view. If you choose to show Extended view, then more details are given for any printer that you select in the Print Management console. You can view the print jobs currently running on the printer and access the printer Web page (if one exists). Figure 7-12 shows Extended view details for a selected printer.

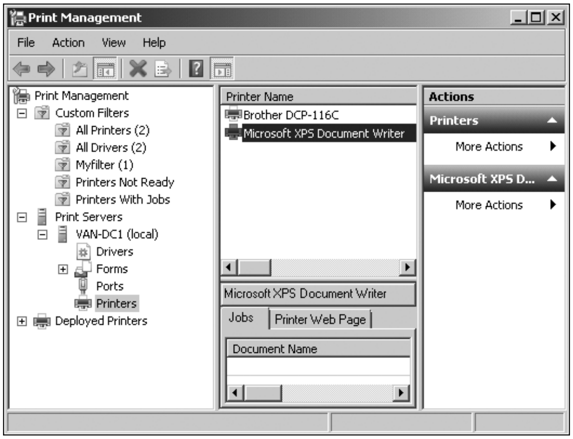
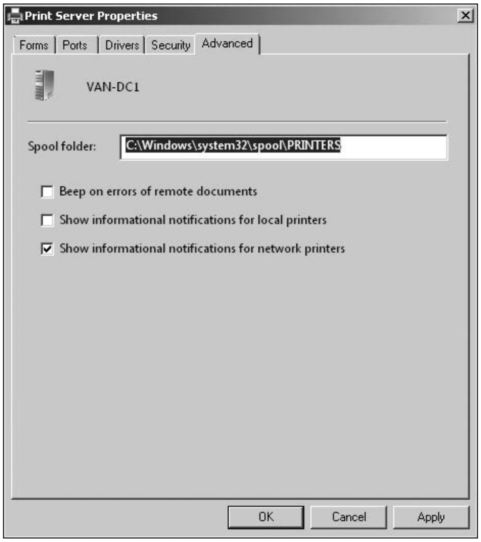


FIGURE 7-12 Showing Extended view

You can also access the Properties dialog box for a print server by right-clicking the server in the Print Management console tree and clicking Properties. By default, this accesses the Advanced tab, shown in Figure 7-13. On this tab, you can change the location of the print spool folder and select whether an audible warning will be generated if an error is detected on a remote document and whether to show informational notifications for local printers, remote printers, or both.



Spool folder: C:\Windows\system32\spool\PRINTERS

☐ Beep on errors of remote documents

☐ Show informational notifications for local printers

☑ Show informational notifications for network printers

FIGURE 7-13 The Advanced tab of the Print Server Properties dialog box

Planning and Managing Security and Access Permissions

To secure a print server and control access to specific printers, you must consider what rights users and groups should have. As an experienced administrator, you have probably configured permissions for both files and printers. You should be aware that you should grant permissions to groups rather than individual users, and you should use explicit Deny permissions as sparingly as possible.

You have probably dealt with the situation where a user who should have access to a printer does not and (more difficult to diagnose) where a user who should not have access to a printer does. Setting permissions and debugging permission configuration are common administrative tasks.

Planning permissions is a much more difficult task. Should you configure two print drivers for an expensive print device, so that the Managers security group has full-time access while the Everyone security group has access only at off-peak times? How should you plan access to color printers or A3 printers? What type of auditing and monitoring should you set up so you can identify users with bad printing habits (such as sending a job to a printer several times if it does not immediately appear on the print device)? Should you use printer pools to handle heavy print traffic?

EXAM TIP

Remember that you can have several printers controlling a single print device and giving different groups different levels and times of access. You can also have several print devices controlled by a single print driver so that they form a printer pool.

The Security tab of the Print Server Properties dialog box lets you configure access settings for all printers on the print server, as well as to the print server itself. You are probably aware of the print permissions available, but they are listed here to remind you:

- **Print** This permission is assigned to the Everyone group by default. The user can connect to a printer and send documents. Members of the Administrators, Print Operators, and Server Operators groups also have explicit Print permission.
- **Manage Documents** This permission is assigned explicitly to members of the Creator Owner group and is the only permission assigned to that group. Members of the Administrators, Print Operators, and Server Operators groups are granted the Manage Documents permission but are also granted the Manage Printers permission. The user can pause, resume, restart, cancel, and rearrange the order of documents submitted by all other users. A user who has only the Manage Documents permission, however, cannot send documents to the printer or control the status of the printer.
- **Manage Printers** This permission is assigned to members of the Administrators, Print Operators, and Server Operators groups. The user can perform the tasks associated with the Print permission and has complete administrative control of the printer. The user can pause and restart the printer, change spooler settings, share a printer, adjust printer permissions, and change printer properties.

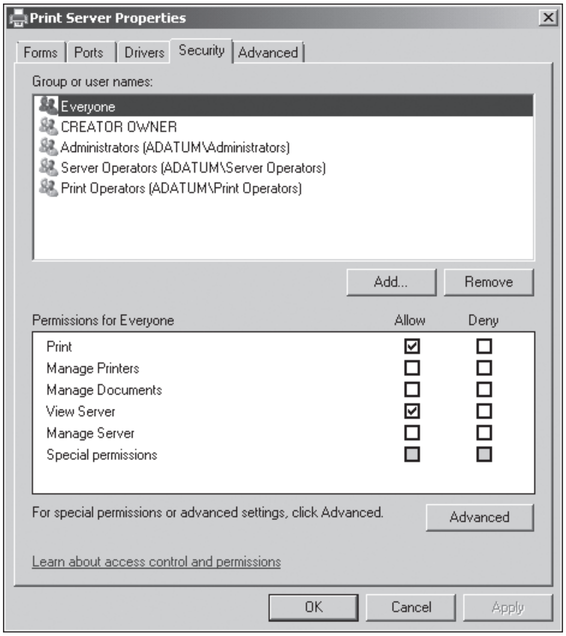
The Security tab of the Print Server Properties dialog box also lets you assign permissions to the server itself. The View Server permission allows a user to view the print server. Without the View Server permission, a user cannot see printers that are managed by the server, and for this reason, this permission is given to members of the Everyone group.

The Manage Server permission lets users create and delete print queues (with already installed drivers), add or delete ports, and add or delete forms. By default, the Administrators, Server Operators, and Print Operators groups are granted this permission. A standard user who is granted this permission is called a delegated print administrator.

MORE INFO **ASSIGNING DELEGATED PRINT ADMINISTRATOR AND PRINTER PERMISSION SETTINGS**

For more information about delegating print server management, see *http://msdn.microsoft.com/en-us/library/ee524015(WS.10).aspx*.

Figure 7-14 shows the Security tab of the Print Server Properties dialog box and the permission settings for the Everyone group. A group or an individual user can be specifically allowed permission, although as a best practice individual users should inherit permissions through group membership.



Group or user names:

- Everyone
- CREATOR OWNER
- Administrators (ADATUM\Administrators)
- Server Operators (ADATUM\Server Operators)
- Print Operators (ADATUM\Print Operators)

Permissions for Everyone	Allow	Deny
Print	☑	□
Manage Printers	□	□
Manage Documents	□	□
View Server	☑	□
Manage Server	□	□
Special permissions	□	□

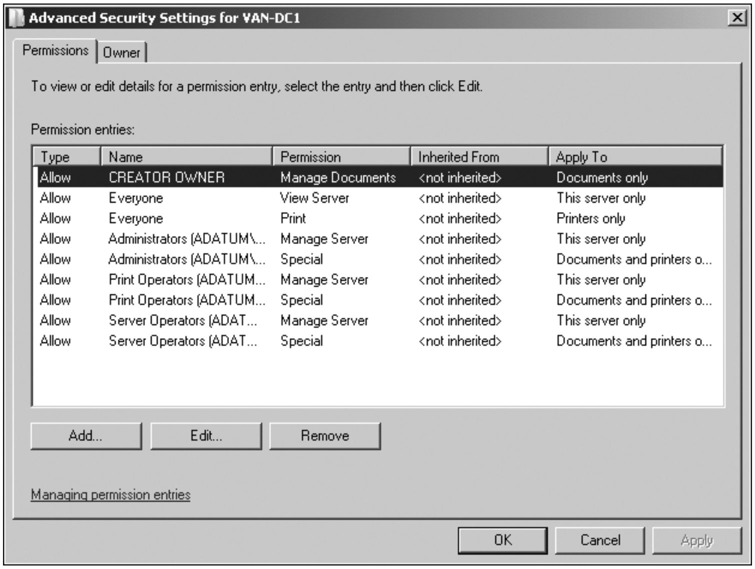
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

FIGURE 7-14 The Security tab of the Print Server Properties dialog box

A user or group can also be specifically denied permission. A user who has been specifically denied a permission, or who is a member of a group that has been specifically denied a permission, cannot be granted the permission through being a member of other groups. For this reason, the explicit Deny permission should be used as seldom as possible, and any instance should be documented carefully.

If appropriate, you can grant special permissions to a user or a group by allocating a non-standard combination of the available permissions. To confer special permissions to a user or security group, select the user or group in the Security tab and then click Advanced. The Advanced Security Settings dialog box, shown in Figure 7-15, allows you to configure permissions for a listed group or user by selecting the group or user and clicking Edit. You can also add a group or user and edit its permissions.



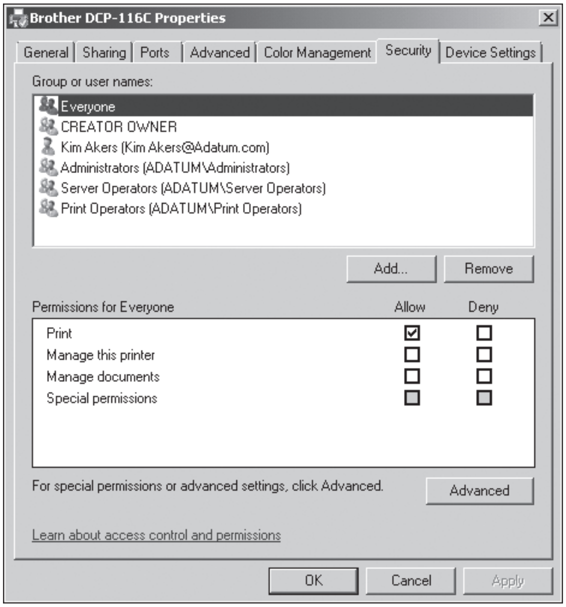
To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	CREATOR OWNER	Manage Documents	<not inherited>	Documents only
Allow	Everyone	View Server	<not inherited>	This server only
Allow	Everyone	Print	<not inherited>	Printers only
Allow	Administrators (ADATUM\...	Manage Server	<not inherited>	This server only
Allow	Administrators (ADATUM\...	Special	<not inherited>	Documents and printers o...
Allow	Print Operators (ADATUM...	Manage Server	<not inherited>	This server only
Allow	Print Operators (ADATUM...	Special	<not inherited>	Documents and printers o...
Allow	Server Operators (ADAT...	Manage Server	<not inherited>	This server only
Allow	Server Operators (ADAT...	Special	<not inherited>	Documents and printers o...

FIGURE 7-15 The Advanced Security Settings dialog box

In addition to granting permissions on a print server, you can configure permissions on an individual printer. Permissions specifically configured at the printer level override permissions inherited from the print server configuration. You can assign Print, Manage Documents, and Manage Printers permissions to groups or users, and you can configure and assign special permissions. As with all permission configurations, it is good practice to confer permissions to groups rather than individual users and to be very sparing in the use of explicit Deny and special permissions. The Security tab of a printer's Properties dialog box is shown in Figure 7-16.



Group or user names:

- Everyone
- CREATOR OWNER
- Kim Akers (Kim Akers@Adatum.com)
- Administrators (ADATUM\Administrators)
- Server Operators (ADATUM\Server Operators)
- Print Operators (ADATUM\Print Operators)

Permissions for Everyone	Allow	Deny
Print	☑	□
Manage this printer	□	□
Manage documents	□	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

FIGURE 7-16 The Security tab of a printer's Properties dialog box

Lesson Summary

- When you install the Print and Document Services server role, you can install and manage printers and print drivers, add and manage ports, and configure forms.
- The Print Management console provides single-seat management of printers on remote print servers on your network.
- You can configure printer and server permissions on the Print Server Properties dialog box. You can configure permissions to an individual printer on the printer's Properties dialog box.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Planning Print Services Management." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE **ANSWERS**

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

1. When you install the Print and Document Services server role, you can use the Print Management console to carry out a number of jobs remotely that previously you needed to do locally on the print server that held the printer. The console also introduces features that were not available in Windows versions earlier than Windows Server 2008. Which of the following tasks is new to the Print Management console?

   A. Changing printer ports

   B. Viewing the printer status

   C. Adding or modifying forms

   D. Creating custom printer filters

2. Which permission, assigned by default to the Creator Owner security group, allows a user to pause, resume, restart, cancel, and rearrange the order of documents submitted by all other users, but does not permit the user to send documents to the printer or control the status of the printer?

   A. Print

   B. Manage Documents

   C. Manage Printers

   D. Manage Server

3. Jeff Hay is a standard user. You want him to be a delegated print administrator on the print server DEN-PRS1. What permission do you grant him?

   A. Manage Server

   B. View Server

   C. Manage Documents

   D. Manage Printers

4. If you add and share a printer on a print server running Windows Server 2008 R2, the printer is published automatically, provided that two Group Policy settings are enabled. What are these settings? (Each answer forms part of the solution. Choose two.)

   A. Disallow Installation Of Printers Using Kernel Mode Drivers

   B. Always Render Print Jobs On The Server

   C. Automatically Publish New Printers In Active Directory

   D. Pre-Populate Printer Search Location Text

   E. Allow Printers To Be Published

Lesson 2: Planning File Servers

Your users need to be able to create files and save these files where they can be retrieved easily. You, on the other hand, need to ensure that users cannot read confidential files unless they are allowed to. You need to control usage so that users cannot clog the network with high numbers of large files. This lesson discusses file server configuration, file access permissions, quotas, storage availability, and the new BranchCache For Network Files feature introduced by Windows Server 2008 R2.

After this lesson, you will be able to:

- Plan your file and folder infrastructure and install the role services that you require to implement this plan.
- Manage file access permissions and storage availability.
- Plan and implement file quotas.
- Use the new BranchCache For Network Files feature.

Estimated lesson time: 45 minutes

Configuring a File Server

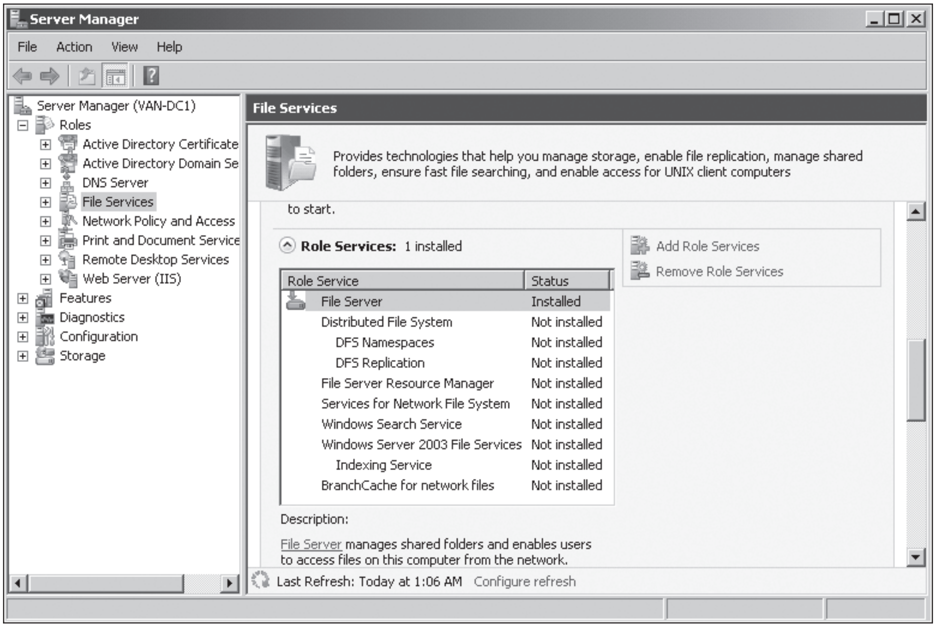
A file server provides a central network location where users can store files and share them with other users on the network. If a user requires a file that typically is accessed by many users, such as a company policy document, she should be able to access the file remotely. For the purposes of centralized administration, backup and restore, and the implementation of shadow copies, you need to store user files on a file server rather than on individual computers, although users typically also need to have the facility of working with their files offline.

You configure a server running Windows Server 2008 R2 as a file server by adding the File Services role, which consists of a number of role services. The File Server role service is installed automatically if you share a folder on the server. Figure 7-17 shows the role services that you can install as part of the File Services role.

As part of your planning process, you need to decide what role services you require and how these should be configured. The temptation is to install everything just in case you need it. Resist this temptation. The more services you install on a server, the more pressure you put on limited resources and the larger the footprint for attack.

The Role Services server role provides the following role services:

- Share And Storage Management (provided by File Server), which includes Disk Management, which in turn enables you to configure shadow copies
- Distributed File System (DFS), which includes DFS Namespaces (DFSN) and DFS Replication (DFSR)
- File Server Resource Manager (FSRM)



Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

to start.

Role Services: 1 installed

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed
Services for Network File System	Not installed
Windows Search Service	Not installed
Windows Server 2003 File Services	Not installed
Indexing Service	Not installed
BranchCache for network files	Not installed

Description:

File Server manages shared folders and enables users to access files on this computer from the network.

Last Refresh: Today at 1:06 AM Configure refresh

FIGURE 7-17 Role services provided by the File Services server role

- Services For Network File System
- Windows Search Service
- Windows Server 2003 File Services, which includes the legacy Indexing Service
- BranchCache For Network Files, which is new in Windows Server 2008 R2

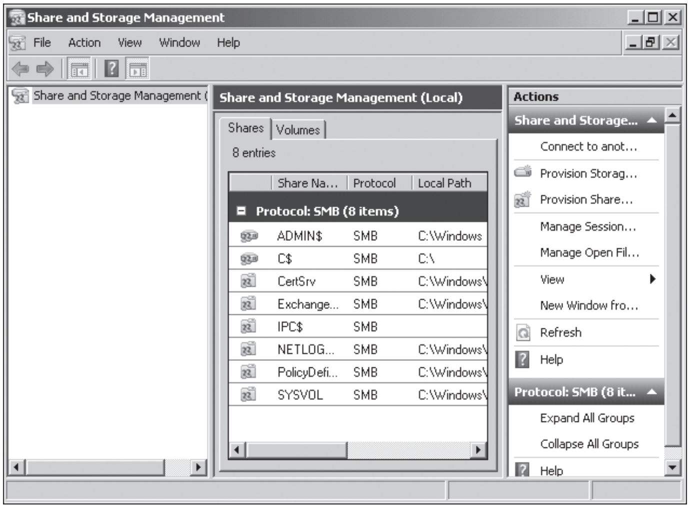
NOTE **OPTIONAL FEATURES**

Often the Windows Server Backup, Storage Manager for SANs, Failover Clustering, and Multipath I/O (MPIO) features are installed at the same time as the role services provided by the File Services server role. Chapter 13, "Backup and Recovery," and Chapter 10, "Provision Data and Plan Storage," discuss these features.

Share and Storage Management

Share And Storage Management is installed by default with the File Server role service. You can access the Share And Storage Management console through Server Manager or directly from Administrative Tools. It uses the Microsoft Server Message Block (SMB) 2.0 protocol to share the content of folders and to manage shared folders.

Figure 7-18 shows the Share And Storage Management console (accessed from Administrative Tools rather than from Server Manager) and lists the shared folders on the VAN-DC1 domain controller. Your domain controller might have additional shares if you created them when you were experimenting with your network.



8 entries

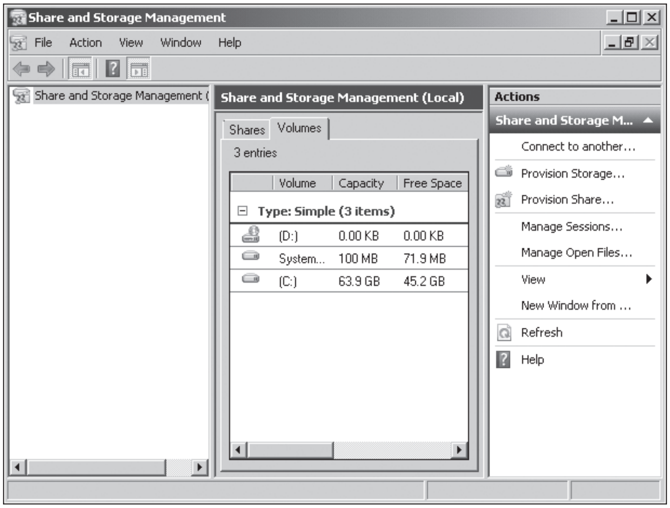
Share Na...	Protocol	Local Path
Protocol: SMB (8 items)		
ADMIN$	SMB	C:\Windows
C$	SMB	C:\
CertSrv	SMB	C:\Windows\
Exchange...	SMB	C:\Windows\
IPC$	SMB	
NETLOG...	SMB	C:\Windows\
PolicyDefi...	SMB	C:\Windows\
SYSVOL	SMB	C:\Windows\

FIGURE 7-18 The Share And Storage Management console

MORE INFO **THE SMB PROTOCOL**

If you want to learn more about the SMB protocol, as well as the Common Internet File System (CIFS) protocol that is a dialect of the SMB protocol, see *http://msdn2.microsoft.com/en-us/library/aa365233.aspx*. However, the examination is unlikely to ask you detailed questions about this protocol.

You can manage volumes and disks by using the Share And Storage Management console, as shown in Figure 7-19. Again, the volumes on your VAN-DC1 domain controller might differ from those seen here.

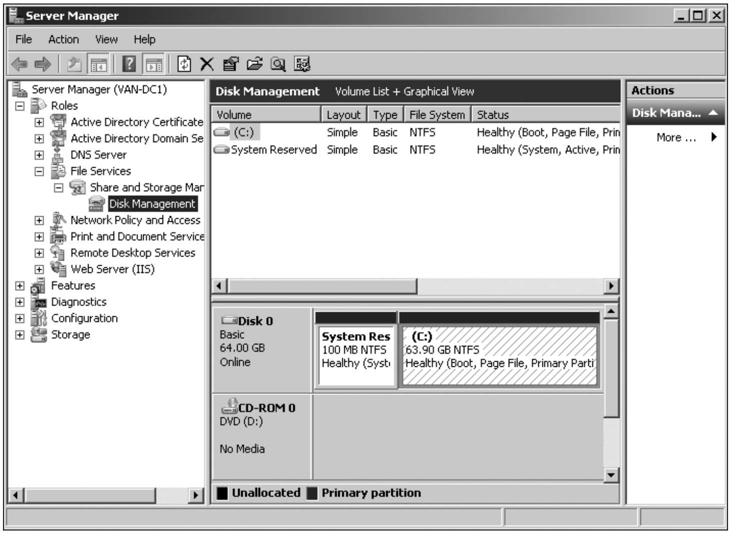


3 entries

Volume	Capacity	Free Space
Type: Simple (3 items)		
(D:)	0.00 KB	0.00 KB
System...	100 MB	71.9 MB
(C:)	63.9 GB	45.2 GB

FIGURE 7-19 Managing volumes

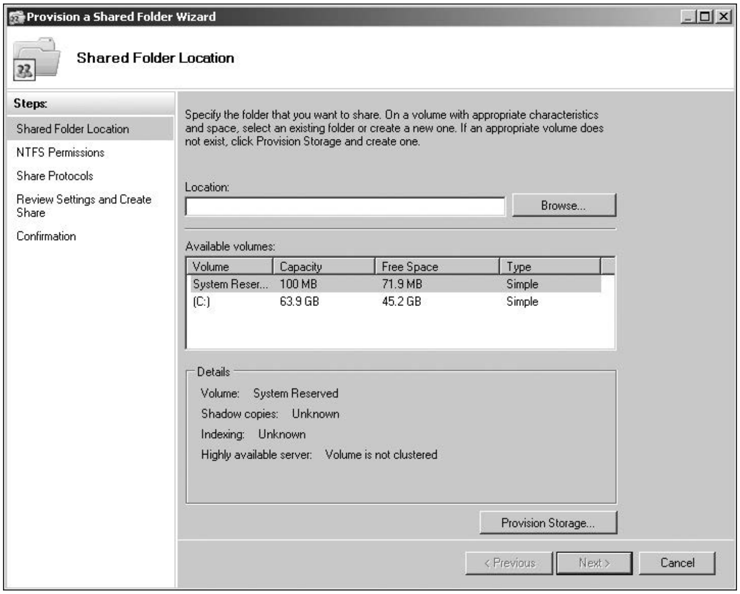
If you access Share And Storage Management from Server Manager, you can access the Disk Management console, shown in Figure 7-20. Again, the disks in your VAN-DC1 domain controller might differ from those seen here.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Prin
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Prin

FIGURE 7-20 Managing disks

You can share the content of folders and volumes on a server running Windows Server 2008 or Windows Server 2008 R2 over the network by using the Provision A Shared Folder Wizard, which you can access by selecting Provision Share from the Actions pane in the Share And Storage Management console. Figure 7-21 shows this wizard, which guides you through the steps required to share a folder or volume and configure its properties.



Specify the folder that you want to share. On a volume with appropriate characteristics and space, select an existing folder or create a new one. If an appropriate volume does not exist, click Provision Storage and create one.

Location:

Available volumes:

Volume	Capacity	Free Space	Type
System Reser...	100 MB	71.9 MB	Simple
(C:)	63.9 GB	45.2 GB	Simple

Details

Volume: System Reserved

Shadow copies: Unknown

Indexing: Unknown

Highly available server: Volume is not clustered

FIGURE 7-21 The Provision A Shared Folder Wizard

You can use the Provision A Shared Folder Wizard to do the following:

- Specify a folder or volume to share, or create a new folder to share.
- Specify the network sharing protocol used to access the shared resource.
- Change the local NTFS permissions for the folder or volume you are sharing.
- Configure the share access permissions, user limits, and offline access to files in the shared resource.
- Publish the shared resource to a DFS namespace.

If you have installed the Services For Network File System role service, you can specify Network File System (NFS)–based access permissions for the shared resource. If you have installed the File Server Resource Manager role service, you can apply storage quotas to the new shared resource and limit the type of files that can be stored in it.

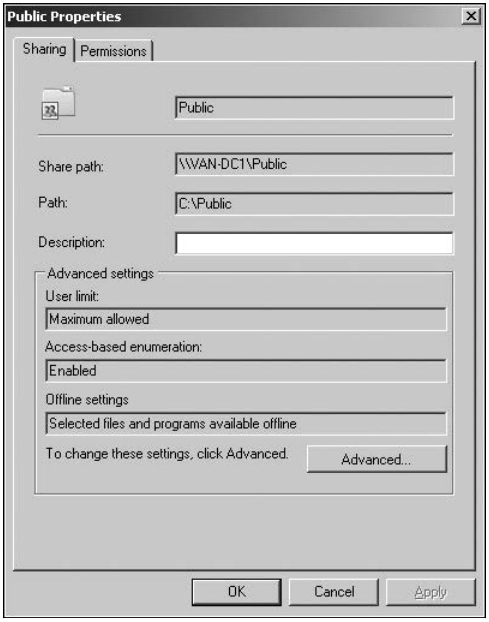
You can use Share And Storage Management to stop sharing a resource by selecting the resource on the Shares tab (shown previously in Figure 7-18) and clicking Stop Sharing in the Actions pane. If a folder or volume is shared for access by both the SMB and the NFS protocols, you need to stop sharing for each protocol individually. Before you stop sharing a folder or volume, you need to ensure that it is not in use by using the Manage Sessions and Manage Open Files features of Share And Storage Management. These features are described later in this section.

You can also use Share And Storage Management to view and modify the properties of a shared folder or volume, including the local NTFS permissions and the network access permissions for that shared resource. To do this, you again select the shared resource on the Shares tab and select Properties in the Actions pane (or right-click the shared resource and then click Properties). Figure 7-22 shows the Properties dialog box for a Public folder that has been shared. Clicking Advanced on the Sharing tab lets you configure user limits and caching and disable or enable access-based enumeration (ABE). ABE is enabled by default and lets you hide files and folders from users who do not have access to them. The Permissions tab lets you specify share and NTFS permissions.

NOTE **ADMINISTRATIVE SHARES**

You cannot modify the access permissions of folders or volumes shared for administrative purposes, such as C$ and ADMIN$.

If you want to view and close open sessions and open files—for example, if you intend to stop sharing a resource—you can click Manage Sessions or Manage Open Files as appropriate in the Share And Storage Management Actions pane. Figure 7-23 shows the Manage Sessions dialog box.



Public

Share path: \\VAN-DC1\Public

Path: C:\Public

Description:

Advanced settings

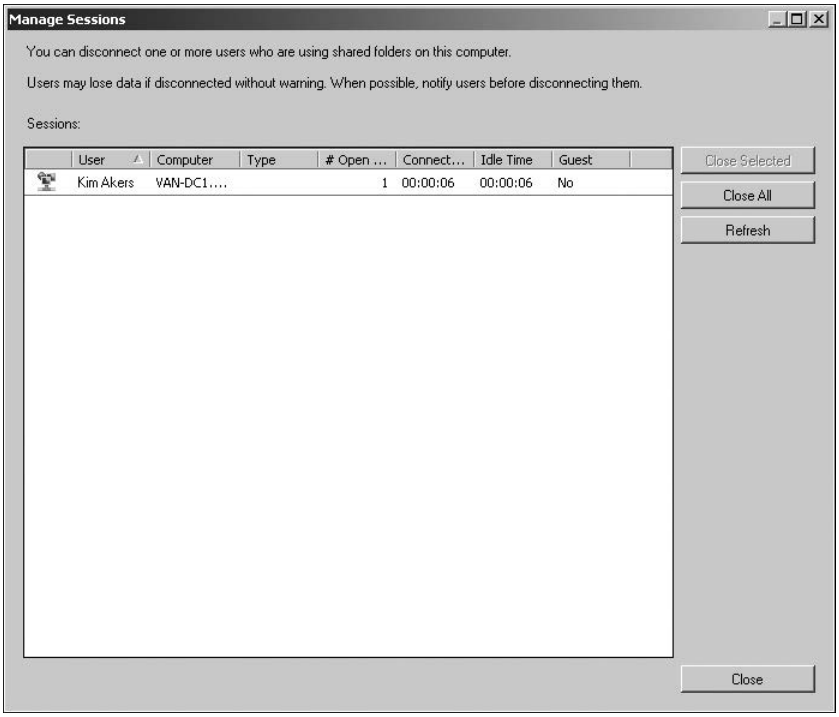
User limit: Maximum allowed

Access-based enumeration: Enabled

Offline settings: Selected files and programs available offline

To change these settings, click Advanced.

FIGURE 7-22 The Properties dialog box for a shared resource



You can disconnect one or more users who are using shared folders on this computer.

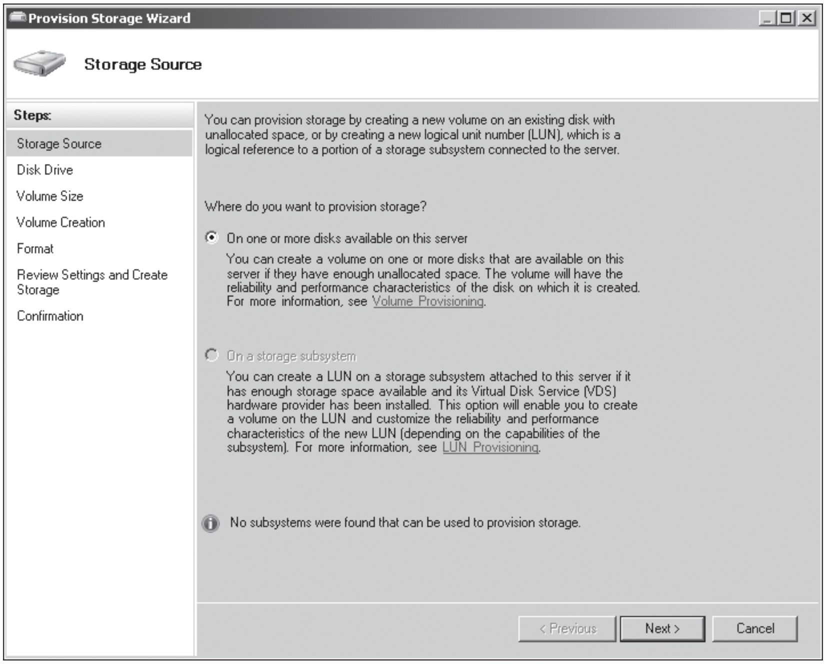
Users may lose data if disconnected without warning. When possible, notify users before disconnecting them.

Sessions:

User	Computer	Type	# Open ...	Connect...	Idle Time	Guest
Kim Akers	VAN-DC1....		1	00:00:06	00:00:06	No

FIGURE 7-23 The Manage Sessions dialog box

Share And Storage Management enables you to provision storage on disks on your server running Windows Server 2008 or Windows Server 2008 R2, or on storage subsystems that support Virtual Disk Service (VDS). The Provision Storage Wizard, shown in Figure 7-24, guides you through the process of creating a volume on an existing disk or on a storage subsystem, such as a storage area network (SAN), attached to your server. You access this wizard from Share And Storage Management by clicking Provision Storage on the Actions pane.



You can provision storage by creating a new volume on an existing disk with unallocated space, or by creating a new logical unit number (LUN), which is a logical reference to a portion of a storage subsystem connected to the server.

Where do you want to provision storage?

● On one or more disks available on this server

You can create a volume on one or more disks that are available on this server if they have enough unallocated space. The volume will have the reliability and performance characteristics of the disk on which it is created. For more information, see Volume Provisioning.

○ On a storage subsystem

You can create a LUN on a storage subsystem attached to this server if it has enough storage space available and its Virtual Disk Service (VDS) hardware provider has been installed. This option will enable you to create a volume on the LUN and customize the reliability and performance characteristics of the new LUN (depending on the capabilities of the subsystem). For more information, see LUN Provisioning.

No subsystems were found that can be used to provision storage.

FIGURE 7-24 The Provision Storage Wizard

If you create a volume on a storage subsystem, the wizard enables you to create a Logical Unit Number (LUN) to host that volume. You can also use the wizard to create a LUN, and use the Disk Management console (shown previously in Figure 7-20) to create the volume later.

NOTE **RUNNING THE PROVISION STORAGE WIZARD**

You can run the Provision Storage Wizard only if your server can access disks with unallocated space or storage subsystems with available storage for which a VDS hardware provider is installed. Also, you can create a volume only on a disk that is online. Chapter 10 discusses storage provisioning in more detail.

Provided that you have the available disk or storage subsystem resources, the Provision Storage Wizard can perform the following functions:

- Choose the disk on which the volume is created.
- Specify the volume size.

- Assign a drive letter or a mount point.
- Format the volume. (You can also do this from the Disk Management console.)

You can use Share And Storage Management to monitor and manage volumes on your server. The tool enables you to perform the following operations:

- Extend the size of a volume.
- Format a volume.
- Delete a volume.
- Change volume properties, including compression, security, offline availability, and indexing.
- Access disk tools for error checking, defragmentation, and backup.

LUNs

A LUN refers to a portion of a storage subsystem. It can include a disk, a section of a disk, a whole disk array, or a section of a disk array. LUNs simplify storage management by providing logical identifiers through which you can assign access and control privileges.

You can use the Provision Storage Wizard in Share And Storage Management to create LUNs on Fibre Channel and iSCSI disk drive subsystems connected to your server. You can then assign the LUN to your server or to other servers on the network. While creating the LUN, you can also create a volume on that LUN and format it. Alternatively, you can create the LUN first and the volume later.

If you want to create a LUN on a disk storage subsystem, you need to ensure that all the following requirements are met:

- **The storage subsystem supports VDS.**
- **The VDS hardware provider for the storage subsystem is installed on the server.**
- **Storage space is available on the subsystem.**
- **The storage subsystem is attached directly to the server or is accessible over the network.**

If you need to assign a LUN to a server or cluster other than the server on which you run the Provision Storage Wizard, you need to configure the server connections by using Storage Manager for SANs. (See Chapter 10 for more information about this.) If you want to assign the LUN to a cluster, ensure that each server in the cluster is a member of only one cluster and has been configured by installing Failover Clustering. Also, if you enable multiple Fibre Channel ports or iSCSI Initiator adapters for LUN access, make sure that that the server supports MPIO.

NOTE **STORAGE MANAGER FOR SANS**

Storage Manager for SANs is not installed by default. You can install it by clicking Add Features in the Features node in Server Manager.

MORE INFO **ISCSI**

For more information about iSCSI, access *http://download.microsoft.com/download/a/e/9/ae91dea1-66d9-417c-ade4-92d824b871af/uguide.doc* and download the Users Guide. Note, however, that the exam is unlikely to test iSCSI in depth.

MORE INFO **MPIO**

For more information about MPIO, see *http://technet.microsoft.com/en-us/library/ee619734(WS.10).aspx*.

MORE INFO **SHARE AND STORAGE MANAGEMENT**

For more information about Share and Storage Management, open the command prompt and enter hh storagemgmt.chm.

Distributed File System

DFS is considerably enhanced in Windows Server 2008 and Windows Server 2008 R2 and is installed as a role service under File Services. This topic is discussed in detail in Chapter 10 and is introduced only briefly here. DFS consists of two technologies, DFSN and DFSR, that you can use (together or independently) to provide fault-tolerant and flexible file sharing and replication services.

DFSN lets you group shared folders on different servers (and in multiple sites) into one or more logically structured namespaces. Users view each namespace as a single shared folder with a series of subfolders. The underlying shared folders structure is hidden from users, and this structure provides fault tolerance and the ability to connect users automatically to local shared folders, when available, instead of routing them over wide area network (WAN) connections.

DFSR provides a multimaster replication engine that lets you synchronize folders on multiple servers across local or WAN connections. It uses the Remote Differential Compression (RDC) protocol to update only those files that have changed since the last replication. You can use DFS Replication in conjunction with DFS Namespaces or by itself.

File Server Resource Manager

FSRM is a role service that you can install as part of File Services in Windows Server 2008 R2. When you install the role service you can access tools that enable you to understand, control, and manage the quantity and type of data stored on your servers. You can use FSRM to place quotas on folders and volumes, actively screen files, and generate storage reports. Details of the facilities available from FSRM are given later in this lesson. You install the FSRM server role in a practice later in this chapter.

Services For Network File System

You can install Services For Network File System as a role service under File Services. NFS provides a file sharing solution for organizations with a mixed Windows and UNIX environment. Services For Network File System lets you transfer files between computers running Windows Server 2008 or Windows Server 2008 R2 and the UNIX operating system by using the NFS protocol. The Windows Server 2008 and Windows Server 2008 R2 versions of Services For NFS support the following enhancements:

- **Active Directory lookup** Identity management for the UNIX extension of the Active Directory schema includes the UNIX user identifier (UID) and group identifier (GID) fields. This enables Server For NFS and Client For NFS to refer to Windows-to-UNIX user account mappings directly from Active Directory Domain Services (AD DS). Identity management for UNIX simplifies mapping user accounts from Windows to UNIX in AD DS.
- **64-bit support** You can install Services For NFS on all editions of Windows Server 2008, including 64-bit editions, and on all editions of Windows Server 2008 R2.
- **Enhanced server performance** Services For NFS includes a file filter driver, which significantly reduces server file access latencies.
- **UNIX special device support** Services For NFS provides support for UNIX special devices based on the *mknod* (make a directory, a special file, or a regular file) function.

> ***MORE INFO*** **MKNOD**
>
> **For more information on the *mknod* function, see *http://www.opengroup.org/onlinepubs/009695399/functions/mknod.html*. However, the exam is unlikely to ask about UNIX functions.**

- **Enhanced UNIX support** Services For NFS supports the following UNIX versions: Sun Microsystems Solaris version 9, Red Hat Linux version 9, IBM AIX version 5L 5.2, and Hewlett Packard HP-UX version 11i.

> ***NOTE*** **WINDOWS SERVER 2008 R2 ENHANCEMENTS**
>
> **The Services For NFS role service is enhanced in Windows Server 2008 R2 and supports netgroups, which you can use to support network-wide named groups of hosts. The role service is also enhanced to support the Remote Procedure Call Security_Generic Security Services (RPCSEC_GSS) protocol, which enables applications to take advantage of the Generic Security Services_Application Programming Interface (GSS_API) to verify authentication and integrity. It lets you use Windows Management Instrumentation (WMI) for remote NFS management and makes an unmapped UNIX user option available for NFS shares.**

MORE INFO **SERVICES FOR NFS**

For more information about Services For NFS, including the enhancements introduced by Windows Server 2008 R2, open the command prompt and enter hh nfs__lh.chm.

✓ **Quick Check**

- **What are the three main tasks that FSRM enables you to perform?**

Quick Check Answer

- **FSRM enables you to place quotas on folders and volumes, actively screen files, and generate storage reports.**

Windows Search Service

The Windows Search Service role service enables you to perform fast file searches on a server from clients that are compatible with Windows Search. It creates an index of the most common file and non-file data types on your server, such as email, contacts, calendar appointments, documents, photographs, and multimedia. Indexing files and data types enables you to perform fast file searches on your server running Windows Server 2008 or Windows Server 2008 R2 from clients running Windows Vista or Windows 7, or from clients running Windows XP with Windows Desktop Search installed.

Windows Search Service replaces the Indexing Service feature that was provided in Windows Server 2003. Although you have the option of installing the Windows Server 2003 File Services role service—including the Indexing Service—as part of the File Services server role on a server running Windows Server 2008 or Windows Server 2008 R2, you cannot install Indexing Services if you choose to install Windows Search Service.

When you install Windows Search Service, you are given the option to select the volumes or folders that you want to index. Microsoft recommends that you select a volume rather than a folder only if that volume is used exclusively for hosting shared folders.

Windows Server 2003 File Services

The File Services role in Windows Server 2008 or Windows Server 2008 R2 includes the role services that are compatible with Windows Server 2003. If you want, you can include the legacy Indexing Service that catalogs contents and properties of files on local and remote computers. Note that if you install the Windows Search Service, you cannot install the legacy Indexing Service.

In Windows Server 2008, you also have the option of installing the File Replication Service (FRS), which enables you to synchronize folders with file servers that use FRS. However, Microsoft recommends that where possible, you should use the DFSR service. In Windows Server 2008 R2, FRS has been replaced by DFSR for replicating DFS folders and for replicating the SYSVOL folder. The option to install the FRS role service is not available in Windows Server 2008 R2.

BranchCache For Network Files

The BranchCache For Network Files role service helps you reduce WAN utilization and enhance the responsiveness of network applications when users in branch office locations access content held in a central office. This role service is new to Windows Server 2008 R2 and is therefore discussed in detail later in this lesson.

Optional Features

If you want, you can install the following additional features to complement the role services in the File Services role:

- **Windows Server Backup** Windows Server Backup provides a reliable method of backing up and recovering the operating system, certain applications, and files and folders stored on your server.

> ***MORE INFO*** **WINDOWS SERVER BACKUP**
>
> **For more information, open the command prompt and enter hh backup.chm.**

- **Storage Manager for SANs** Storage Manager for SANs lets you provision storage on one or more Fibre Channel or iSCSI storage subsystems on a SAN.

> ***MORE INFO*** **STORAGE MANAGER FOR SANS**
>
> **For more information about SANs, open the command prompt and enter hh sanmgr.chm.**

- **Failover Clustering** The Failover Clustering feature enables multiple servers to work together to increase the availability of services and applications. If one of the clustered servers (or nodes) fails, another node provides the required service through failover.

> ***MORE INFO*** **FAILOVER CLUSTERS IN WINDOWS SERVER 2008 R2**
>
> **For more information about failover clusters and the enhancements introduced in Windows Server 2008 R2, access *http://technet.microsoft.com/en-us/library/ff182338(WS.10).aspx* and follow the links.**

- **MPIO** MPIO, introduced earlier in this lesson, provides support for multiple data paths between a file server and a storage device (known as multipathing). You can use MPIO to increase data availability by providing redundant connections to storage subsystems. Multipathing can also load-balance I/O traffic and improve system and application performance.

Using Windows Server 2008 R2 File Services Enhancements

Windows Server 2008 R2 helps you manage data more effectively, as well as more efficiently. It provides features that help you gain insight into organizational data and reduce the cost of data storage, maintenance, and management. It assists you to enforce company policies and mitigate the risks of leaking data.

File Classification Infrastructure

File Classification Infrastructure (FCI) in Windows Server 2008 R2 helps you manage your data more effectively, reduce costs, and mitigate risks. It provides a built-in solution for file classification that allows you to automate manual processes with predefined policies based on the business value of the data.

File systems on servers running previous operating systems stored files and allowed access based on user permissions. They did not, however, classify files according to their business value. When you have no indication about the business value of data in a file, it is difficult to make decisions about when stale files should expire or which files require a higher level of protection. By being able to both automatically and manually classify files according to predefined rules, you can manage organizational data more effectively and decide what should be retained and where it should be stored.

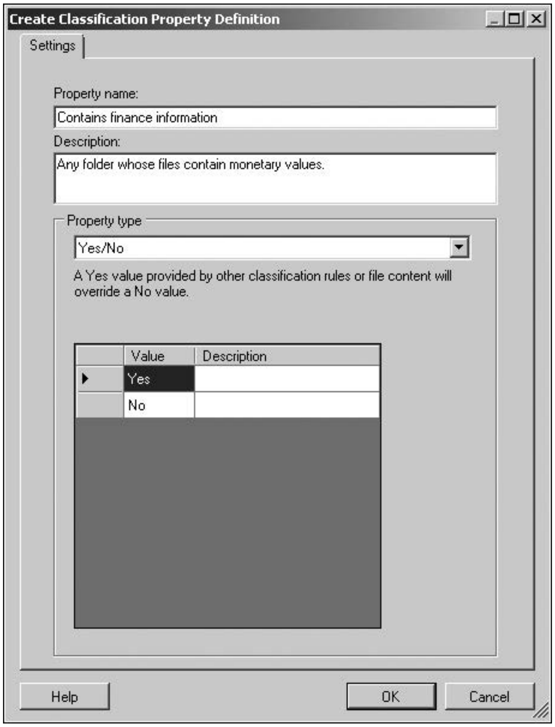
You can access Classification Properties and Classification Rules under Classification Management in the FSRM MMC snap-in and use the functionality built into Windows Server 2008 R2 to classify files based on content and location so that the files can be protected and managed more effectively based upon business value. An organization's files can be classified to enable you to perform the following tasks:

- Identify sensitive data on public servers.
- Configure automated expiration of stale data.
- Use custom IT scripts. For example, you can use a script to move low-business-value files to cheaper storage hardware.
- Integrate with third-party storage software solutions.

Figure 7-25 shows the Create Classification Property Definition dialog box. If you click Classification Rules, you can create a new classification rule or configure a classification schedule. Figure 7-26 shows a classification schedule configured on the Automatic Classification tab of the File Server Resource Manager Options dialog box, which you access by clicking Classification Rules under Classification Properties in the FSRM MMC snap-in and then clicking Configure Classifications Schedule in the Actions pane.

MORE INFO **FCI**

For more information about FCI, see *http://www.microsoft.com/windowsserver2008/en/us/FCI.aspx*.



Property name: Contains finance information

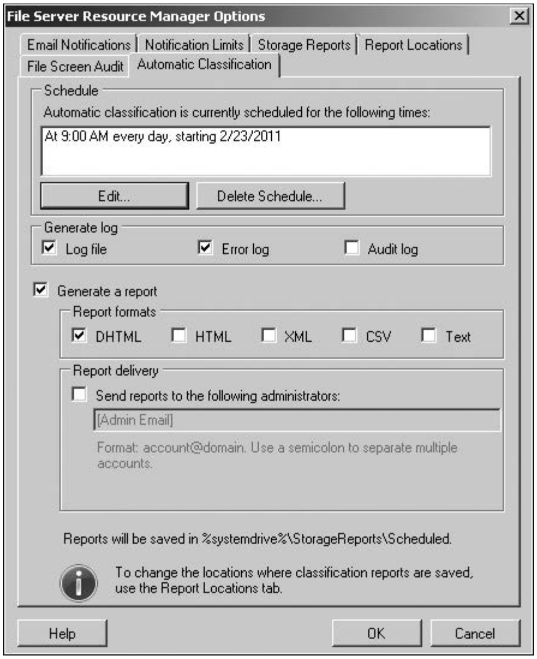
Description: Any folder whose files contain monetary values.

Property type: Yes/No

A Yes value provided by other classification rules or file content will override a No value.

	Value	Description
▸	Yes	
	No	

FIGURE 7-25 The Create Classification Property Definition dialog box



Schedule

Automatic classification is currently scheduled for the following times:

At 9:00 AM every day, starting 2/23/2011

Generate log

☑ Log file ☑ Error log □ Audit log

☑ Generate a report

Report formats

☑ DHTML □ HTML □ XML □ CSV □ Text

Report delivery

□ Send reports to the following administrators:

[Admin Email]

Format: account@domain. Use a semicolon to separate multiple accounts.

Reports will be saved in %systemdrive%\StorageReports\Scheduled.

To change the locations where classification reports are saved, use the Report Locations tab.

FIGURE 7-26 Configuring a classification schedule

Distributed File Management

Windows Server 2008 R2 file services include DFSR and DFSN, introduced earlier in this lesson, to provide customers with better access to data and simplified access to files and shares across a network-wide infrastructure. DFSR efficiently and bidirectionally replicates partial file changes to keep multiple file copies in synchronization. DFSN makes file shares easier to locate and more resilient by enabling users to access their data without regard to the physical file server(s) on which the files reside. Replicated copies and transparent redirection enable your users to be more productive because their data is closer to them and highly available.

DFS is discussed in more detail in Chapter 10. Briefly, DFS technologies offer WAN-friendly replication as well as simplified, highly available access to geographically dispersed files. DFS is enhanced and operates more efficiently in Windows Server 2008 R2. It provides the following benefits:

- Better access to data
- Simplified access to files
- Increased productivity and data availability
- Support for failover clusters
- Read-only replicated folders

MORE INFO **DFS MANAGEMENT IN WINDOWS SERVER 2008 R2**

For more information about the DFS management facilities provided by Windows Server 2008 R2, see *http://technet.microsoft.com/en-gb/library/cc732006.aspx*.

Disk Management

You use the Disk Management console, described earlier in this lesson, to manage hard disks and the volumes or partitions that they contain. You can initialize disks, create volumes, and format volumes with the FAT, FAT32, or NTFS file system. Disk Management enables you to perform most disk-related tasks without restarting the system or interrupting users, and most configuration changes take effect immediately.

The following Disk Management features are provided by Windows Server 2008 R2:

- **More efficient disk partition creation** When you right-click a volume, you can choose directly from a shortcut menu whether to create a basic, spanned, or striped partition.
- **Disk conversion options** If you add more than four partitions to a basic disk, you are prompted to convert the disk to dynamic or to the GUID partition table (GPT) partition style.
- **The ability to extend and shrink partitions** You can extend and shrink partitions directly from the Disk Management console.

MORE INFO **DISK MANAGEMENT IN WINDOWS SERVER 2008 R2**

For more information about the disk management facilities provided by Windows Server 2008 R2, see *http://technet.microsoft.com/en-gb/library/cc771097.aspx*.

FSRM

As mentioned earlier in this lesson, the FSRM role service installs the Classification Management console. In Windows Server 2008 R2, FSRM delivers better-managed file services across Common Internet File System/Server Message Block (CIFS/SMB) and NFS. By centralizing several different file service utilities available in previous Windows Server operating systems, FSRM provides a single management interface that lets you manage all the file allocation, quota, and sharing options in one place. Windows Server 2008 R2 FSRM provides built-in reporting, which lets you determine how your file-serving resources can be used for management, audit, and planning purposes, and offers the following advantages:

- Better-managed file services
- Improved control and compliance over files
- Insight into how your file servers are being used

Using the FSRM MMC snap-in to configure quotas and file screen policy is discussed later in this lesson.

MORE INFO **FSRM IN WINDOWS SERVER 2008 R2**

For more information about the facilities provided by Windows Server 2008 R2 FSRM, see *http://technet.microsoft.com/en-gb/library/cc732431.aspx*.

Removable Storage

You can use the Removable Storage component to track removable storage media easily and to manage the libraries that contain them. Removable Storage labels, catalogs, and tracks media; controls library drives, slots, and doors; and provides drive-cleaning operations. It works with data-management programs, such as Backup, which manage the data stored on the media. Removable Storage makes it possible for multiple programs to share the same storage media resources and organizes all the media in your libraries into different media pools. It also moves media between media pools to provide the amount of data storage that your applications require.

Microsoft has removed Removable Storage Manager (RSM) from Windows Server 2008 R2 in favor of new archiving technology. The Ntbackup utility is not available in Windows Server 2008 R2, and it is currently impossible to restore files or folders or entire volumes from old archives created with Ntbackup on Windows Server 2008 and previous versions of Windows unless you download and install the Windows NT Backup Restore Utility for Windows 7 and for Windows Server 2008 R2. This is available at *http://support.microsoft.com/kb/974674*.

MORE INFO REMOVABLE STORAGE IN WINDOWS SERVER 2008 R2

For more information about Removable Storage in Windows Server 2008 R2, access *http://technet.microsoft.com/en-gb/library/cc772263(WS.10).aspx* and follow the links.

Services For NFS

As stated earlier in this lesson, Services For NFS is a role service that you can install as part of the File Services server role. It includes Server For NFS and Client For NFS and provides a file-sharing solution for organizations that have a mixed Windows and UNIX environment. Services For NFS enables you to transfer files between servers running Windows Server 2008 R2 and UNIX operating systems using the NFS protocol. The Windows Server 2008 R2 version of Services For NFS offers the following improvements:

- **Simplified administration** The configuration for supporting NFS clients has been simplified by the introduction of the Unmapped UNIX User Access feature.
- **Active Directory lookup** The Identity Management for UNIX Active Directory schema extension includes UNIX UID and GID fields. This enables Server For NFS and Client For NFS to look up Windows-to-UNIX user account mappings directly from AD DS.
- **Enhanced server performance** Services For NFS includes a file filter driver. This significantly reduces access latencies when accessing common server files.
- **UNIX special device support** Services For NFS supports UNIX special devices.
- **Enhanced UNIX support** Services For NFS supports Sun Microsystems Solaris version 9, Red Hat Linux version 9, IBM AIX version 5L 5.2, and Hewlett Packard HP-UX version 11i. NFS security is enhanced with the Kerberos protocol.

MORE INFO SERVICES FOR NFS IN WINDOWS SERVER 2008 R2

For more information about Services For NFS in Windows Server 2008 R2, see *http://technet.microsoft.com/en-gb/library/cc753495.aspx*.

Shadow Copies of Shared Folders

Shadow Copies of Shared Folders provides point-in-time copies of files that are located on shared resources. It enables users to access shared files and folders as they existed at points of time in the past. Accessing previous versions of files, or shadow copies, lets users recover files that were accidentally deleted (or recent versions of such files), recover from accidentally overwriting a file, and compare versions of a file while working.

The following is a list of the aspects that are part of the Shadow Copies of Shared Folders managed entity in Windows Server 2008 R2:

- **Volume Snapshot driver integrity** Shadow Copies of Shared Folders uses the Volume Snapshot driver (Volsnap.sys) to create shadow copies in Windows Server 2008 R2. This driver uses storage space allocated on a volume to maintain a snapshot of the contents of the shared folders. This storage space is called the Diff Area.
- **Diff Area integrity** A snapshot is a block-level set of information that represents the differences between the current content and content from a previous point in time. Shadow Copies of Shared Folders allocates the Diff Area storage space on a volume to maintain snapshots of the contents of shared folders. The integrity of existing and new snapshots depends on the integrity of the Diff Area.
- **Volume Revert operations** Shadow Copies of Shared Folders enables you to return a volume to the state that it was in when a shadow copy was created.

NOTE **REVERTING A VOLUME**

When you revert a volume, all changes made to files and folders on the volume since the shadow copy was created are lost.

MORE INFO **SHADOW COPIES IN WINDOWS SERVER 2008 R2**

For more information about shadow copies of shared folders in Windows Server 2008 R2, see *http://technet.microsoft.com/en-us/library/dd364797(WS.10).aspx*.

Share and Storage Management

Share and Storage Management, discussed earlier in this lesson, provides a centralized location where you can manage folders and volumes that are shared on the network and volumes in disks and storage subsystems. You can use the Provision A Shared Folder Wizard to share the content of folders and volumes on your server over your network. Share and Storage Management enables you to provision storage on disks that are available on your server, or on storage subsystems that support VDS.

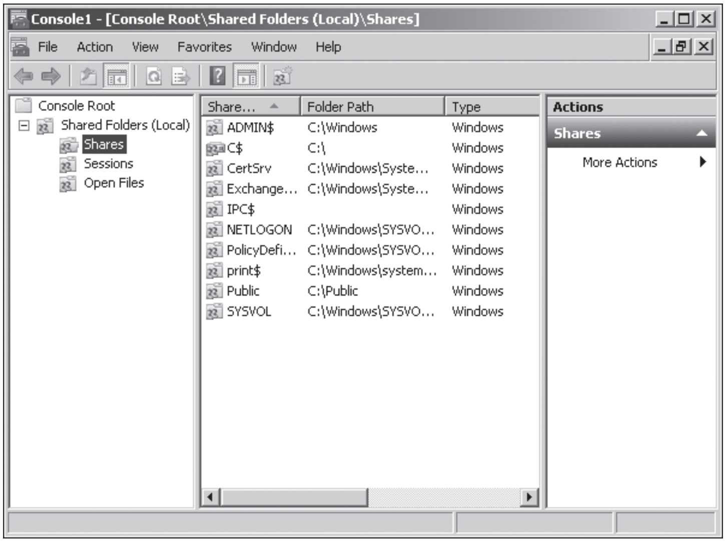
The wizard guides you through the process of creating a volume on an existing disk, or on a storage subsystem attached to your server. If the volume is created on a storage subsystem, the wizard also guides you through the process of creating a LUN to host that volume. You also have the option of creating the LUN and then using Disk Management to create the volume. Share and Storage Management also helps you monitor and manage the volumes that you have created, along with any other volumes that are available on your server.

MORE INFO **SHARE AND STORAGE MANAGEMENT IN WINDOWS SERVER 2008 R2**

For more information about Share and Storage Management in Windows Server 2008 R2, access *http://technet.microsoft.com/en-gb/library/cc731574.aspx* and follow the links.

Shared Folders

In Windows Server 2008 R2, you can use the Shared Folders MMC snap-in, shown in Figure 7-27, to manage file shares centrally on a computer. This enables you to create file shares, set permissions, and view and manage open files and users connected to file shares on the computer.



Share...	Folder Path	Type
ADMIN$	C:\Windows	Windows
C$	C:\	Windows
CertSrv	C:\Windows\Syste...	Windows
Exchange...	C:\Windows\Syste...	Windows
IPC$		Windows
NETLOGON	C:\Windows\SYSVO...	Windows
PolicyDefi...	C:\Windows\SYSVO...	Windows
print$	C:\Windows\system...	Windows
Public	C:\Public	Windows
SYSVOL	C:\Windows\SYSVO...	Windows

FIGURE 7-27 The Shared Folders MMC snap-in

MORE INFO **SHARED FOLDERS IN WINDOWS SERVER 2008 R2**

For more information about the Shared Folders MMC snap-in in Windows Server 2008 R2, access *http://technet.microsoft.com/en-gb/library/cc770406.aspx* and follow the links.

Storage Explorer

A fabric is a network topology in which devices are connected to each other through one or more high-efficiency data paths. In the case of a Fibre Channel fabric, the network includes one or more Fibre Channel switches that allow servers and storage devices to connect to each other through virtual point-to-point connections. For iSCSI fabrics, the network includes one or more Internet Storage Name Service (iSNS) servers that provide discoverability and partitioning of resources. Storage Explorer enables you to view and manage the Fibre Channel and iSCSI fabrics that are available in your SAN.

The Storage Explorer console, shown in Figure 7-28, can display detailed information about servers connected to the SAN, as well as components in the fabrics such as host bus adapters (HBAs), Fibre Channel switches, and iSCSI Initiators and targets. You can also perform administrative tasks on an iSCSI fabric—for example, you can log on to iSCSI targets, configure iSCSI security, add iSCSI target portals, add iSNS servers, and manage discovery domains and discovery domain sets.

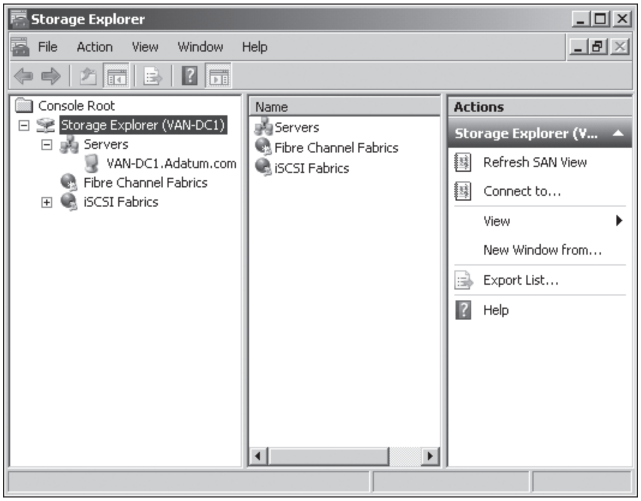


FIGURE 7-28 The Storage Explorer console

MORE INFO **DISCOVERY DOMAINS AND DISCOVERY DOMAIN SETS**

For more information about discovery domains and discovery domain sets, see *http://technet.microsoft.com/en-us/library/cc753442.aspx*.

MORE INFO **STORAGE EXPLORER IN WINDOWS SERVER 2008 R2**

For more information about the Storage Explorer console in Windows Server 2008 R2, see *http://technet.microsoft.com/library/cc731884.aspx*.

Storage Manager for SANs

The Storage Manager for SANs console lets you create and manage LUNs on Fibre Channel and iSCSI disk drive subsystems that support VDS in your SAN. Using LUNs simplifies the management of storage resources in your SAN because LUNs serve as logical identifiers through which you can assign access and control privileges.

As described previously in this lesson, a LUN is a logical reference to a portion of a storage subsystem. A LUN can comprise a disk, a section of a disk, a whole disk array, or a section of a disk array in the subsystem.

MORE INFO **STORAGE MANAGER FOR SANS IN WINDOWS SERVER 2008 R2**

For more information about the Storage Manager for SANs console in Windows Server 2008 R2, access *http://technet.microsoft.com/en-gb/library/cc771378.aspx* and follow the links.

Quick Check

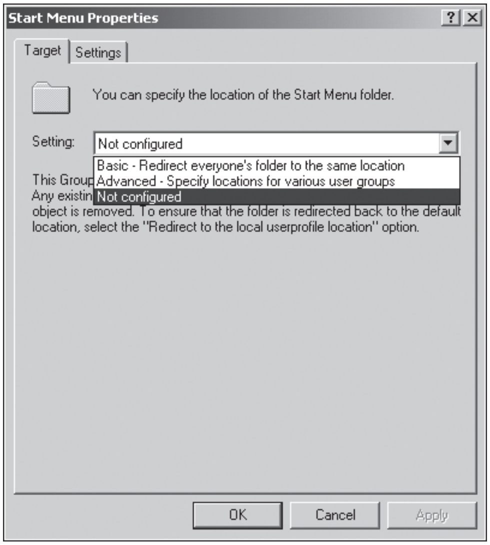
- **What tool enables you to view and manage the Fibre Channel and iSCSI fabrics that are available in a SAN?**

Quick Check Answer

- Storage Explorer

Folder Redirection

Folder Redirection lets you redirect the path of a folder to a new location, such as a directory on a network file share. Users can then work with files on a file server as if these files were stored on a local drive on their clients. The documents in the folder are available to a user from any client on the network. Folder Redirection is a Group Policy setting and can be configured for any Group Policy object (GPO) that has User Configuration enabled. You can right-click any of the folders, click Properties, and configure the redirection options. Figure 7-29 shows the redirection options available for the Start Menu folder.


Start Menu Properties
?
Target
Settings
Basic - Redirect everyone's folder to the same location
Advanced - Specify locations for various user groups
Not configured
OK
Cancel
Apply

You can specify the location of the Start Menu folder.

Setting: Not configured

This Group
Any existin
object is removed. To ensure that the folder is redirected back to the default location, select the "Redirect to the local userprofile location" option.

FIGURE 7-29 Redirection options for the Start Menu folder

Folder Redirection is not a new feature, but Windows Server 2008 R2 includes the following enhancements:

- The ability to redirect more folders in the user profile folders than in earlier Windows operating systems. These include the Contacts, Downloads, Favorites, Links, Music, Saved Games, Searches, and Videos folders.
- The ability to apply settings for redirected folders to clients running earlier versions of Windows.

- The option to have the Music, Pictures, and Videos folders follow the Documents folder.
- The ability to redirect the Start Menu folder to a specific path for all users.

MORE INFO **FOLDER REDIRECTION IN WINDOWS SERVER 2008 R2**

For more information about Folder Redirection, especially the enhancements introduced by Windows Server 2008 R2, see *http://technet.microsoft.com/en-us/library/cc732275.aspx*.

The Offline Files Feature

Offline files enable users such as mobile workers and branch office employees to access files that are available on a shared network resource and continue to work with network files when the computer is not connected to the network.

The Offline Files feature maintains a local cache of remote files and folders on your computer, so that they are available to users when they are working offline. Users can access these files in the same way that they accessed them online because the shared network resource paths and namespaces are preserved. The cache also speeds up the access to these files and folders over a slow connection.

When a network connection is restored, any changes that a user made while working offline are updated to the network by default. Any changes a user makes while working on a slow link are synchronized automatically with the version on the server at regular intervals as a background task.

The major enhancement to the Offline Files feature in Windows Server 2008 R2 is significantly improved file access over WANs, resulting in an improved network file experience for remote users. Other enhancements include the following:

- Fast First Logon
- Usually Offline Support With Background Sync
- Exclusion List
- Transparent Caching

MORE INFO **THE OFFLINE FILES FEATURE IN WINDOWS SERVER 2008 R2**

For more information about enhancements to the Offline Files feature in Windows Server 2008 R2, see *http://technet.microsoft.com/en-us/library/ff183315(WS.10).aspx*.

BranchCache For Network Files

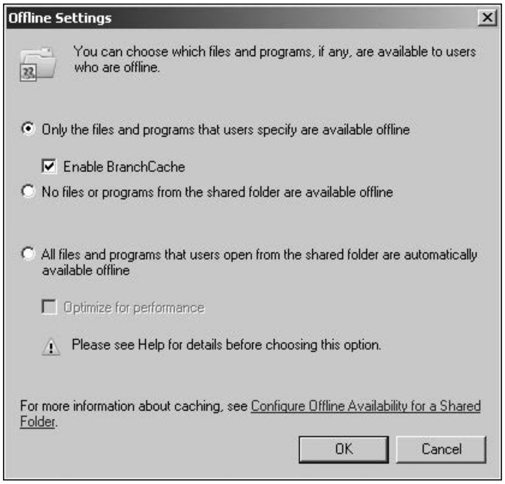
As mentioned previously in this lesson, BranchCache For Network Files is a role service that can be installed as part of the File Services server role in Windows Server 2008 R2. This role service was not available in previous versions of Windows Server. BranchCache For Network Files helps reduce WAN utilization and enhances the responsiveness of network applications when users in branch office locations access content held in a central office.

The role service caches, within a branch office, a copy of the content that is retrieved from a web server or file server at a central location such as a head office. If another client in the branch requests the same content, that client can download it directly from the local branch network without needing to retrieve the content over the WAN. You install the BranchCache For Network Files role service in a practice later in this chapter.

Users at branch offices can experience poor performance when they use network applications that connect to servers over a WAN connection. It might take a significant amount of time for a branch office user to open a large file on a shared folder located on a server at the central office—and remember that user expectations are now such that even a few seconds can seem like a long time. For instance, a user viewing a video through a web browser might have to wait an appreciable period of time before the video loads.

If BranchCache For Network Files is used, a branch office user should experience the same level of service as a user at the central office. The first branch office client to download data from a web server or file server (known as the *content server*) caches a copy on the local branch network. Subsequent clients download the locally cached copy of the content from within the branch after it is authenticated and authorized by the content server.

BranchCache For Network Files is designed to work with existing network and security infrastructures and supports IPv4, IPv6, and end-to-end encryption methods such as SSL and IPSec. It ensures that the most up-to-date content version is served and that clients are authorized by the content server before they can retrieve content from within the branch. BranchCache For Network Files requires that clients are running Windows 7 with the BranchCache feature enabled, and that web servers and file servers are running Windows Server 2008 R2 with the BranchCache For Network Files role service installed. You can enable BranchCache For Network Files for a shared folder by accessing the Properties dialog box for that folder and clicking Offline Settings on the General tab. Figure 7-30 shows the Offline Settings dialog box with Enable BranchCache selected.



Offline Settings

You can choose which files and programs, if any, are available to users who are offline.

● Only the files and programs that users specify are available offline

☑ Enable BranchCache

○ No files or programs from the shared folder are available offline

○ All files and programs that users open from the shared folder are automatically available offline

□ Optimize for performance

Please see Help for details before choosing this option.

For more information about caching, see Configure Offline Availability for a Shared Folder.

FIGURE 7-30 Enabling BranchCache For Network Files

Depending on the cache location, BranchCache For Network Files can operate in one of the following modes:

- **Hosted Cache** This mode deploys a computer running Windows Server 2008 R2 as a host in the branch office. Clients are configured with the fully qualified domain name (FQDN) of the host computer so that they can retrieve content from the hosted cache. If the content is not available in the hosted cache, it is retrieved from the content server over the WAN and then stored in the hosted cache for access by subsequent clients.
- **Distributed Cache** This mode typically is used in branch offices with fewer than 50 users. In Distributed Cache mode, a local client running Windows 7 keeps a copy of the content and makes it available to other authorized clients. This eliminates the need for a server in the branch office. However, Distributed Cache mode works across only a single subnet (unlike Hosted Cache mode). This means that the content needs to be retrieved over the WAN for each subnet in the branch office. Also, clients that disconnect from the network (for example, clients that hibernate) cannot, while disconnected, provide content when requested.

To reduce bandwidth, BranchCache For Network Files sends content metadata to clients, which in turn retrieve the content from within the branch. The content metadata is significantly smaller than the actual content. Prior to sending content metadata, the server authorizes the client. The content server needs to send the content metadata to each client to ensure that the client always receives hashes for the most up-to-date content.

The content is broken into blocks. A block hash is computed for each block. A segment hash is also computed on a collection of blocks. Content metadata is primarily composed of block hashes and segment hashes. The hash algorithm that is used is SHA 256. The compression ratio achieved is approximately 2,000 to 1; that is, the size of the metadata is approximately 2,000 times smaller than the size of the original data itself.

MORE INFO **SHA 256**

If you have a professional interest in secure hash algorithms and want to learn more about SHA 256, see *http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf.* Be aware, however, that the exam will not test hash algorithms in the depth described in this document.

Segment hashes help reduce the total number of lookups performed for given content (compared to looking up every block). When a client needs to retrieve data from the hosted cache or from another client, it downloads the content in units defined by block hashes.

NOTE **MINIMUM SIZE OF CONTENT CACHED**

The minimum size of content that BranchCache For Network Files caches is 64 KB. When content is less than 64 KB, data is directly retrieved from the content server through the WAN.

Windows Storage Server 2008 R2

Windows Storage Server 2008 R2 offers the same file services that are included in Windows Storage Server 2008, along with additional file services and enhancements. It is built upon Windows Server 2008 R2 and provides a platform for network-attached storage (NAS) appliances. The Windows Storage Server 2008 R2 family—Windows Storage Server 2008 R2 Enterprise edition, Windows Storage Server 2008 R2 Standard edition, and Windows Storage Server 2008 R2 Workgroup edition—offers advanced storage solutions to all sizes of organizations and includes storage technologies such as file deduplication (the removal of duplicate files and data) and an iSCSI software target for unified file services and block I/O storage.

MORE INFO **MICROSOFT ISCSI INITIATOR IN WINDOWS SERVER 2008 R2**

For more information about the Microsoft iSCSI Initiator in Windows Server 2008 R2, see *http://technet.microsoft.com/en-us/library/dd878522(WS.10).aspx*.

Windows Storage Server 2008 R2 provides simplified deployment and management of individual appliances and dual-node, highly available storage clusters. Windows Storage Server 2008 R2 Enterprise edition includes wizards that enable automated two-node failover cluster setup.

Single Instance Storage (SIS) reduces the amount of storage used by data by replacing multiple identical copies with logical links to a single source copy, hence performing file deduplication. SIS now supports 128 volumes on a single server. Windows Storage Server 2008 R2 includes a set of Windows PowerShell cmdlets to manage SIS, such as Install-SisVolume, Enable-SisVolume, and Get-SisVolume.

MORE INFO **POWERSHELL CMDLETS TO MANAGE SIS**

For more information about the PowerShell cmdlets that manage SIS in Windows Storage Server 2008 R2, see *http://technet.microsoft.com/en-us/library/gg278036.aspx*.

Windows Storage Server 2008 R2 enables file access over a network using the SMB and NFS protocols. It uses DFS and DFSR to implement a unified namespace and file-replication for data publishing to satellite offices. You can administer Windows Storage Server 2008 R2 remotely from Windows Internet Explorer using an ActiveX control, and from non-Microsoft browsers using a Java Remote Desktop Protocol (RDP) control. Windows Storage Server 2008 R2 provides a cost-effective, reliable, and scalable solution to challenges about how file data is accessed, moved, and managed. It offers the following file service features:

- **Distributed access to file services** Windows Storage Server 2008 R2 file services enable you to provide better access to files, which typically are distributed widely across an organizational network. Distributed access increases storage management efficiency. Regardless of platform or location, data is more quickly accessible and easier to manage.

- **Centralized management of file services** Centralized file services management provides controls that exclude unwanted data and management tools that improve the management of wanted data. These tools centralize management and reduce administrative overhead while simultaneously providing information about file infrastructures. This information helps you to meet requirements for file service availability and compliance more efficiently.
- **Cost-effective scalability and increased productivity** Windows Storage Server 2008 R2 file services enable you to expand IT services and support a growing base of users affordably and efficiently.

These improved file service features are implemented by means of the following file service components that are introduced by Windows Storage Server 2008 R2 (and Windows 7):

- **SMB version 2.1** The SMB 2.1 protocol is faster and more efficient than previous versions of SMB. SMB 2.1 is also optimized for low-bandwidth connectivity and improved for better flexibility, compatibility, and resiliency for clients running Windows 7.
- **NFS** The NFS protocol enables organizations with heterogeneous environments to consolidate their file-sharing resources on Windows Storage Server 2008 R2. It enables computers running both Windows and non-Windows operating systems to share data easily.
- **DFS** DFSR and DFSN provide organizations with better access to data and simplified access to files and shares across a network-wide infrastructure. DFS also extends traditional file serving by making file shares easier to locate and more resilient.
- **FSRM** This server role provides a single management interface that delivers better-managed file services across CIFS/SMB and NFS and improves control and compliance over files. FSRM also provides built-in reporting that lets you determine how your file-serving resources are used for auditing and planning purposes.
- **FCI** This feature automates classification processes to help you manage your data more effectively. Your organization can save money and reduce risk by storing and retaining files based on their business value or impact, and FCI provides expiration, custom tasks, and reporting.

The File Server Migration Toolkit

When you migrate from a previous version of Windows Server to Windows Server 2008 R2, you need to ensure that permissions are set properly, and that the way users access files and the file naming conventions are preserved. The Microsoft File Server Migration Toolkit (FSMT) is a downloadable toolkit that contains two step-by-step wizards to help you migrate existing file servers to Windows Server 2008 R2. You can download the FSMT at *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d00e3eae-930a-42b0-b595-66f462f5d87b&displaylang=en*.

Managing Access Control

Access control is the process of permitting users, groups, and computers to access objects on the network or on a computer. It involves permissions, permission inheritance, object ownership, user rights, and auditing.

Permissions define the type of access granted to a user or group for an object. When a folder or volume is shared over a network and users access its contents remotely (as is the case with files on a file server), share or shared folder permissions apply to these users. A folder or file on an NTFS volume also has NTFS permissions, which apply whether it is accessed locally or across the network. Access permissions to files on a file server are typically a combination of NTFS permissions and the shared folder permissions set on the folder or folder hierarchy that contains the files. Printer objects have associated print permissions.

Every container and object on a network has associated (or attached) access control information defined within a security descriptor. This controls the type of access allowed to users and security groups. Permissions defined within an object's security descriptor are associated with, or assigned to, specific users and security groups. Each assignment of permissions to a user or group is represented in the system as an access control entry (ACE). The entire set of permission entries in a security descriptor is known as a permission set, or access control list (ACL).

You can set NTFS permissions for objects such as files, Active Directory objects, registry objects, or system objects such as processes. You set NTFS permissions on the Security tab of the object's Properties dialog box, sometimes known as the Access Control User Interface. Permissions can be granted to individual users, security groups, computers, and other objects with security identifiers in the domain. It is a good practice to assign permissions to security groups rather than to individual users.

The permissions attached to an object depend on the type of object. For example, the permissions that can be attached to a file are different from those that can be attached to a printer or to a registry key. When you set permissions, you specify the level of access for groups and users. For example, you can let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file.

Microsoft states that permission inheritance allows administrators to assign and manage permissions easily and ensures consistency of permissions among all objects within a given container. Inheritance automatically causes objects within a container to inherit all the inheritable permissions of that container. For example, child folders by default inherit the permissions of their parent, and files within a folder have their permissions set automatically depending upon folder permissions.

Undoubtedly, inheritance is convenient when configuring permissions. You can block folder inheritance and assign explicit rather than inherited permissions to child objects. You can change file permissions so that some files in a folder can have different access permissions than others. This gives you a lot of flexibility, but it also can lead to complexity, so inheritance can make permissions more difficult to manage rather than easier. As with all administrator tasks, the key is to plan carefully to avoid exceptions. You should also limit the use of explicit Deny permissions. If a user is a member of a group that has a Deny permission, or if the user has been explicitly denied a permission, she will be denied that permission no matter what other groups she is a member of.

An owner is assigned to an object when that object is created—typically, an object is owned by the user that creates it, so files saved in a Documents folder in a user profile are owned by that user. The owner of the object can always change the permissions on an object.

MORE INFO **OBJECT OWNERSHIP**

For more information on object ownership, see *http://technet.microsoft.com/en-us/library/cc732983(WS.10).aspx*.

User rights grant specific privileges and logon rights to users and security groups. You can assign specific rights to group accounts or to individual user accounts. These rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories.

User rights are different from permissions because user rights apply to user accounts and permissions are attached to objects. Although you can apply user rights to individual user accounts, it is good practice to apply them to security groups rather than to individual users. You can administer user rights through the Local Security Settings MMC snap-in.

You can audit successful or failed access to objects on a per-user basis. You select which object's access to audit by using the Access Control User Interface, but first, you must enable the Audit Policy by selecting Audit Object Access under Local Policies in the Local Security Settings snap-in. You can then view these security-related events in the Security log in Event Viewer.

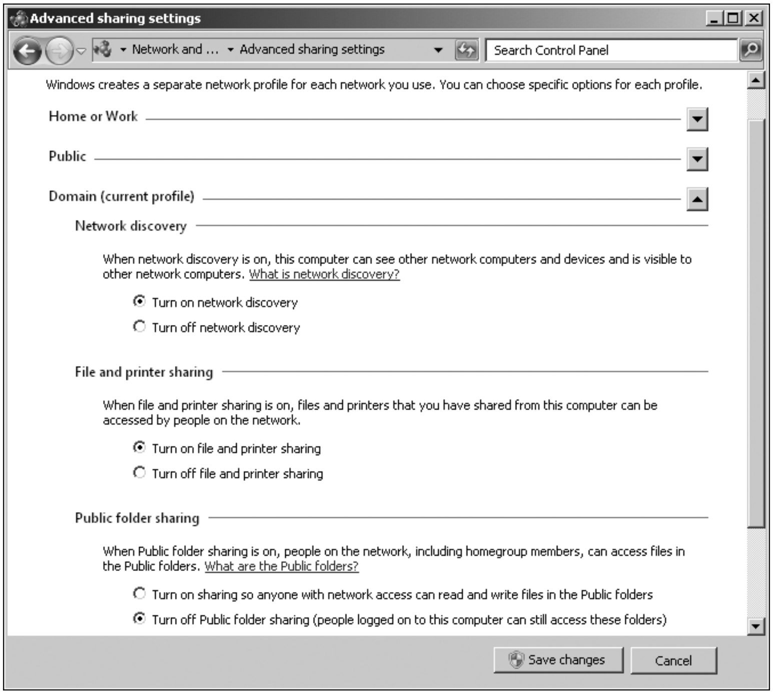
MORE INFO **SECURITY AUDITING**

For more information on security auditing, see *http://technet.microsoft.com/en-us/library/cc771475(WS.10).aspx*.

Configuring Access Permissions

By default, File Sharing is enabled and Public Folder Sharing is disabled on a computer running Windows Server 2008 or Windows Server 2008 R2. You can enable and disable these features by clicking Change Advanced Sharing Settings in the Network And Sharing Center, which you can access through the Control Panel. Figure 7-31 shows the Advanced Sharing Settings dialog box.

You can also open the MMC and add the Shared Folders snap-in. If you then right-click Shares and select New Share, the Create A Shared Folder Wizard starts. This wizard lets you specify the path to a folder you want to share, the name of the share, and the shared folder access permissions.



Advanced sharing settings

Network and ... ▸ Advanced sharing settings

Search Control Panel

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public

Domain (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery

○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing

○ Turn off file and printer sharing

Public folder sharing

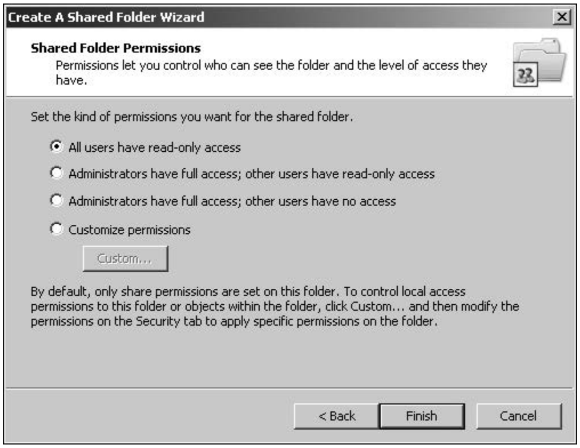
When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

○ Turn on sharing so anyone with network access can read and write files in the Public folders

● Turn off Public folder sharing (people logged on to this computer can still access these folders)

FIGURE 7-31 The Advanced Sharing Settings dialog box

On the Shared Folder Permissions page of the wizard, shown in Figure 7-32, you can specify standard shared folder permissions—for example, All Users Have Read-Only Access (the default) or Administrators Have Full Access; Other Users Have Read-Only Access. You can also select Customize Permissions and click Custom to set custom permissions. Figure 7-33 shows the Customize Permissions dialog box. The wizard also lets you configure offline settings. You can share a folder or a volume.



Create A Shared Folder Wizard

Shared Folder Permissions

Permissions let you control who can see the folder and the level of access they have.

Set the kind of permissions you want for the shared folder.

● All users have read-only access

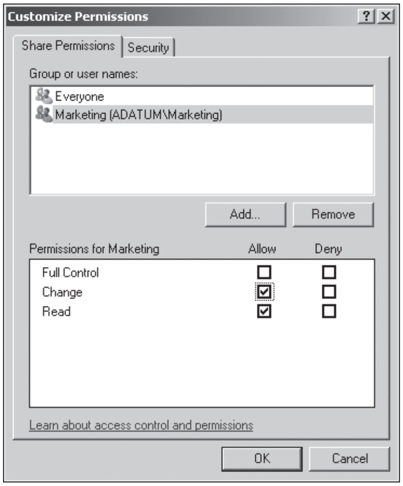
○ Administrators have full access; other users have read-only access

○ Administrators have full access; other users have no access

○ Customize permissions

By default, only share permissions are set on this folder. To control local access permissions to this folder or objects within the folder, click Custom... and then modify the permissions on the Security tab to apply specific permissions on the folder.

FIGURE 7-32 The Shared Folder Permissions page



Group or user names:

- Everyone
- Marketing (ADATUM\Marketing)

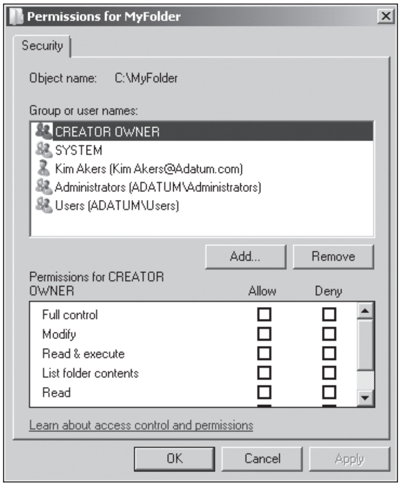
Permissions for Marketing	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

FIGURE 7-33 The Customize Permissions dialog box

EXAM TIP

The default standard shared folder permission in Windows Server 2008 R2 is All Users Have Read-Only Access. In Windows Server 2008, the default is to grant administrators full control and all other users read-only access.

If you choose to customize permissions, you can also access a Security tab that lets you set NTFS permissions by selecting a user or group and clicking Edit. For users who access folders on a server over a network (the vast majority of users), access permissions are a combination of shared folder and NTFS permissions. Figure 7-34 shows the Security tab on which you can configure NTFS permissions.



Object name: C:\MyFolder

Group or user names:

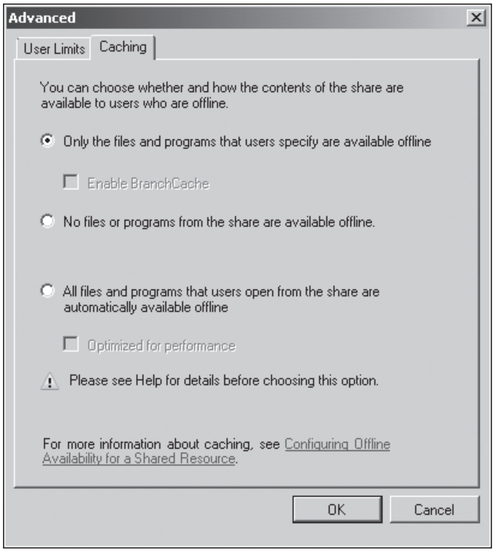
- CREATOR OWNER
- SYSTEM
- Kim Akers (Kim Akers@Adatum.com)
- Administrators (ADATUM\Administrators)
- Users (ADATUM\Users)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

FIGURE 7-34 Configuring NTFS permissions by clicking Edit on the Security tab

You can also create and provision a shared folder by using the Share And Storage Management MMC snap-in. You click Provision Share in the Actions pane and specify the path to the folder that you want to share and provision. This starts the Provision A Shared Folder Wizard. The wizard lets you modify the default NTFS permissions if you want. You can then select the protocol over which users can access the shared folder—SMB, NFS, or both. Note that you can specify NFS only if you have installed the Services For NFS role service.

You then have the option of clicking Advanced, which lets you set a user limit, disable user-based enumeration, and reconfigure offline settings. Figure 7-35 shows the caching options available for offline settings.



You can choose whether and how the contents of the share are available to users who are offline.

● Only the files and programs that users specify are available offline

□ Enable BranchCache

○ No files or programs from the share are available offline.

○ All files and programs that users open from the share are automatically available offline

□ Optimized for performance

⚠ Please see Help for details before choosing this option.

For more information about caching, see Configuring Offline Availability for a Shared Resource.

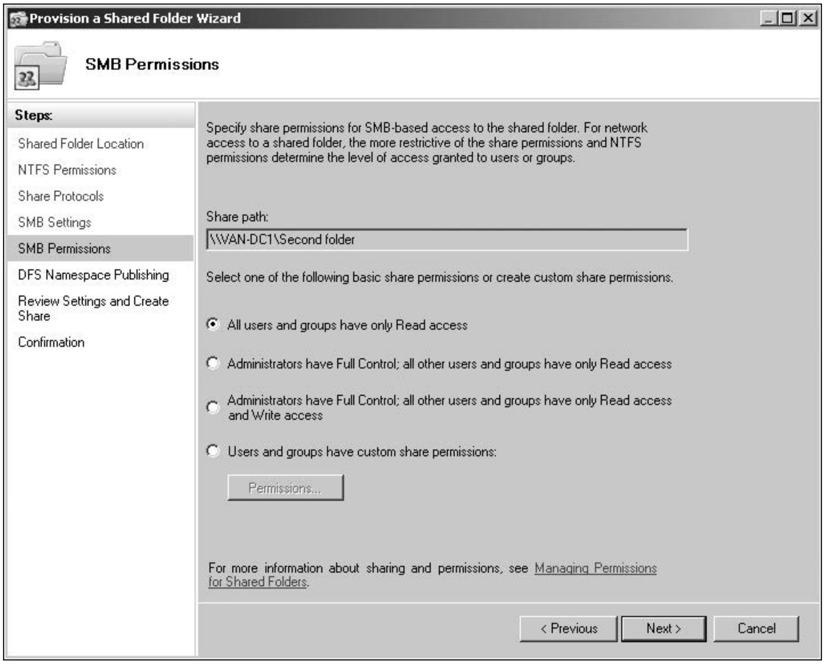
FIGURE 7-35 Caching options

If you are configuring SMB permissions (which is typically the case), you can either choose one of three standard shared folder permission configurations or to customize these permissions. The SMB Permissions page is shown in Figure 7-36. If you choose to customize shared folder permissions, the wizard presents you with a dialog box very similar to the Customize Permissions dialog box in the Create A Shared Folder Wizard, which was shown earlier in Figure 7-33.

NOTE **SMB AND NTFS PERMISSIONS**

If your SMB permissions differ from your NTFS permissions for the same shared folder, then the more restrictive set of permissions applies.

The wizard then prompts you to publish the share in a DFS namespace. Note that you cannot do this unless you have installed the appropriate role services. Finally, the wizard summarizes your settings, and you click Create to create the share.



Provision a Shared Folder Wizard

SMB Permissions

Steps:
- Shared Folder Location
- NTFS Permissions
- Share Protocols
- SMB Settings
- SMB Permissions
- DFS Namespace Publishing
- Review Settings and Create Share
- Confirmation

Specify share permissions for SMB-based access to the shared folder. For network access to a shared folder, the more restrictive of the share permissions and NTFS permissions determine the level of access granted to users or groups.

Share path:
\\VAN-DC1\Second folder

Select one of the following basic share permissions or create custom share permissions.

● All users and groups have only Read access

○ Administrators have Full Control; all other users and groups have only Read access

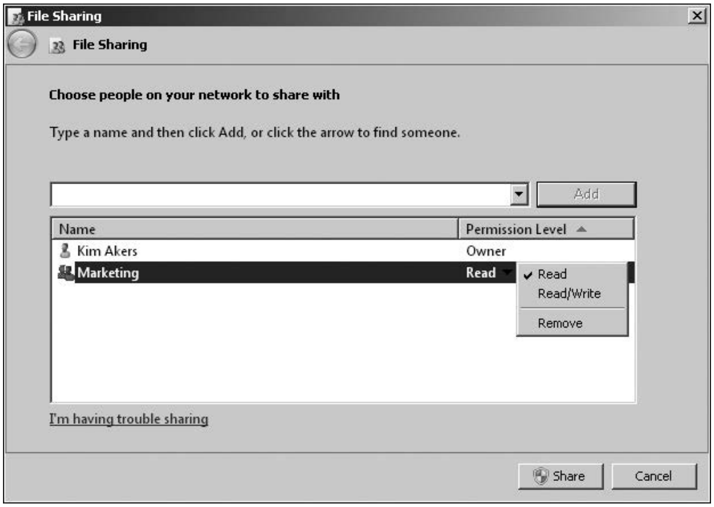
○ Administrators have Full Control; all other users and groups have only Read access and Write access

○ Users and groups have custom share permissions:

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

FIGURE 7-36 The SMB Permissions page

You can also share a folder manually and set shared folder and NTFS permissions by right-clicking a folder or volume in Windows Explorer or My Computer and clicking Properties. If you choose to share a folder by this method, you will see a dialog box similar to that shown in Figure 7-37. If you click the Security tab on the folder's Properties dialog box, you can configure NTFS permissions using a dialog box similar to that provided by the Create A Shared Folder and Provision A Shared Folder wizards.



File Sharing

File Sharing

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Kim Akers	Owner
Marketing	Read

FIGURE 7-37 Sharing a folder manually

Combining Share and NTFS Permissions

Files, folders, and other objects typically are accessed across a network, such as when they are held on a file server. ACEs, however, are applied at both the share level (share permissions) and at the file system level (NTFS permissions). This means that you need to remember to change permissions in two different places.

For example, if you want members of the Managers security group to be able to add, edit, and delete files in a folder called Reports, when previously they could only view them, you would change the NTFS permission for the security group to Modify. However, if the share permission of the folder is Read and you forget to change this, group members will still only be able to view the contents of the files.

One solution to this problem is to grant everyone full access at the share level and to assign restrictive NTFS permissions. The NTFS permissions are then the effective permissions because they are more restrictive. However, many administrators are not happy about assigning nonrestrictive share permissions. The security best practice in this situation is to use (at most) the Change share permission.

To figure out what permissions a security group has on a file, you first figure out the effective NTFS permissions, remembering that any explicit permissions that are set at the file level override the folder permissions. You then compare share and NTFS permissions; the effective permissions are the more restrictive of the two. This process becomes even more complex when you want to figure out access permissions for a user that might be a member of several security groups.

You can figure out a user's effective permissions manually. This is a tedious process, but it gets easier with practice. Currently, no Windows Server 2008 or Windows Server 2008 R2 tool exists to automate the process, but you should consider downloading Server Share Check from the Windows Server 2003 Resource Kit. This tool can be used on servers running Windows Server 2008 or Windows Server 2008 R2. You can download this resource kit at *http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en*.

MORE INFO **SERVER SHARE CHECK**

For more information on Server Share Check, see *http://searchwindowsserver.techtarget.com/tip/Checking-access-permissions-with-Server-Share-Check*. Also, you need to become a member of SearchWindowsServer.com, but membership is free. If you cannot access this URL or do not want to register with this site, search the Internet for "Server Share Check."

Using FSRM to Configure Quotas, File Screen Policy, and Storage Reports

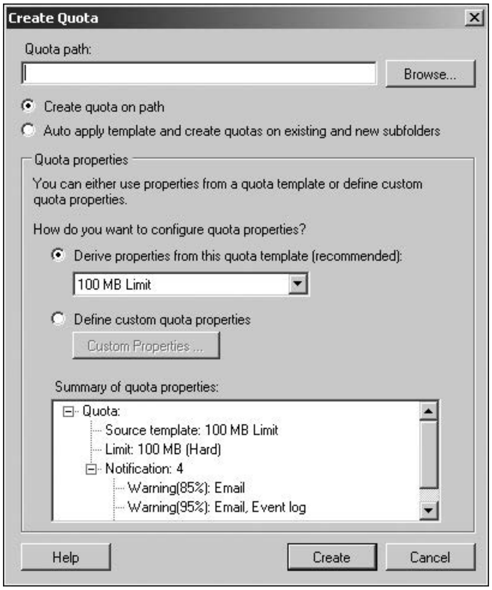
Windows Server 2008 and Windows Server 2008 R2 offer enhanced quota management. You can apply quotas to folders as well as volumes, and you have a set of quota templates that you can use to create quotas quickly and easily. You can create a custom quota or derive a quota from an existing template.

Microsoft recommends deriving quotas from templates. This simplifies the management of quotas because you can update automatically all quotas that are based on a specific template by editing that template. You then have the option of updating the settings of any quotas that you created by using the template. You can also exclude specified quotas from this update. For example, if you created a quota from a template and then manually changed some of its settings, you might not want to update that quota when you change the template because you could lose these settings.

You can create an auto-apply quota and assign a quota template to a parent volume or folder. Quotas based on that template are then automatically generated and applied to each of the existing subfolders and to any subfolders that you create in the future.

Creating Quotas

If the FSRM File Services server role is installed, you can use the FSRM MMC snap-in to create quotas. The Create Quota dialog box is shown in Figure 7-38. Note that you will be unable to access this box if you have not installed the appropriate server role, which you will do in the practice later in this chapter. You can also choose to create a quota from a template, which you also will do in the practice.



Create Quota

Quota path:

● Create quota on path
○ Auto apply template and create quotas on existing and new subfolders

Quota properties

You can either use properties from a quota template or define custom quota properties.

How do you want to configure quota properties?

● Derive properties from this quota template (recommended):
100 MB Limit
○ Define custom quota properties

Summary of quota properties:

```
⊟ Quota:
    Source template: 100 MB Limit
    Limit: 100 MB (Hard)
  ⊟ Notification: 4
      Warning(85%): Email
      Warning(95%): Email, Event log
```

FIGURE 7-38 The Create Quota dialog box

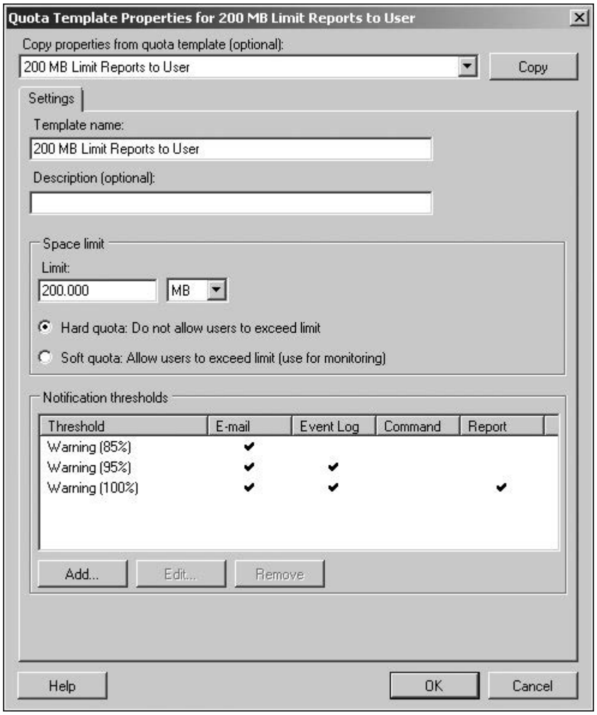
You specify a path to the volume or folder for which you want to create the quota and then specify whether you want to create a quota only on that path or whether a template-based quota will be generated and applied to existing and new subfolders on the path of the parent volume or folder automatically. To specify the latter action, select Auto Apply Template And Create Quotas On Existing And New Subfolders.

Typically, you would select Derive Properties From This Quota Template (Recommended) and select a template. You can define custom quota properties if you want, but this is not recommended. You can select templates that specify the quota size that is allocated to each user and whether the quota is hard or soft. A hard quota cannot be exceeded. A user can exceed a soft quota, but exceeding the quota limit typically generates a report, in addition to sending an email notification and logging the event. Soft quotas are used for monitoring. Quota templates include the following:

- **100 MB Limit** This is a hard quota. It emails the user and specified administrators if the 100 percent quota limit has been reached and writes an event to the event log.
- **200 MB Limit Reports To User** This is a hard quota. It generates a report, sends emails, and writes an event to the event log if the 100 percent quota limit has been reached.
- **200 MB Limit With 50 MB Extension** Technically, this is a hard quota because it performs an action when the user attempts to exceed the limit rather than merely monitoring the exceeded limit. The action is to run a program that applies the 250 MB Extended Limit template and effectively gives the user an additional 50 MB. Emails are sent and the event is logged when the limit is extended.
- **250 MB Extended Limit** The 250-MB limit cannot be exceeded. Emails are sent and the event is logged when the limit is reached.
- **Monitor 200 GB Volume Usage** This is a soft quota that can be applied only to volumes. It is used for monitoring.
- **Monitor 50 MB Share** This is a soft quota that can be applied only to shares. It is used for monitoring.

You can also configure templates to send emails and write to the event log if a defined percentage of the quota is reached. Figure 7-39 shows the properties of the 200 MB Limit Reports To User template.

When you have created a quota or an auto-apply quota, you can edit it. Figure 7-40 shows a Quota Properties box. You can change the Quota Template, Space Limit, and Notifications Thresholds and add a label. You can add new Notification Thresholds and specify what action should be taken if a threshold is reached. For example, you can specify whether an email is sent to the user and to one or more specified administrators. You can also specify a command, generate a report, and specify whether the event is to be logged. If you edit quota settings or create a custom quota, you can use the quota to create a new template.



Quota Template Properties for 200 MB Limit Reports to User

Copy properties from quota template (optional): 200 MB Limit Reports to User

Template name: 200 MB Limit Reports to User

Description (optional):

Space limit

Limit: 200.000 MB

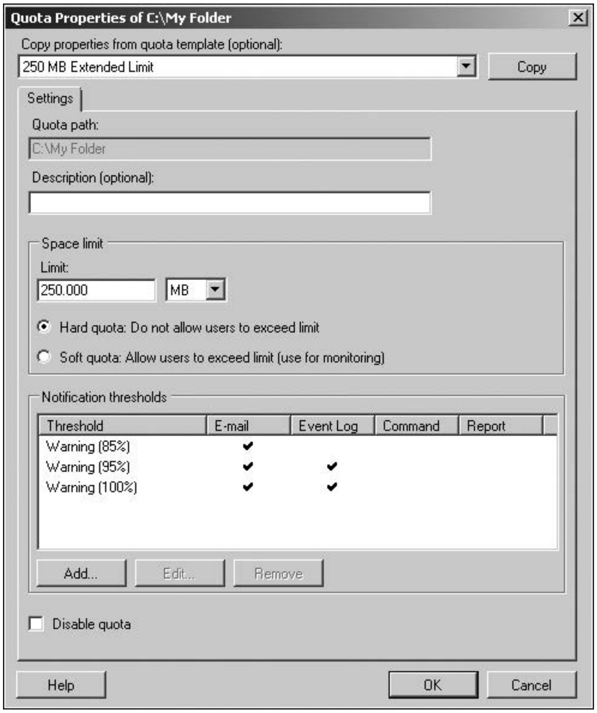
● Hard quota: Do not allow users to exceed limit

○ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

Threshold	E-mail	Event Log	Command	Report
Warning (85%)	✓			
Warning (95%)	✓	✓		
Warning (100%)	✓	✓		✓

FIGURE 7-39 Properties of the 200 MB Limit Reports To User template



Quota Properties of C:\My Folder

Copy properties from quota template (optional): 250 MB Extended Limit

Quota path: C:\My Folder

Description (optional):

Space limit

Limit: 250.000 MB

● Hard quota: Do not allow users to exceed limit

○ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

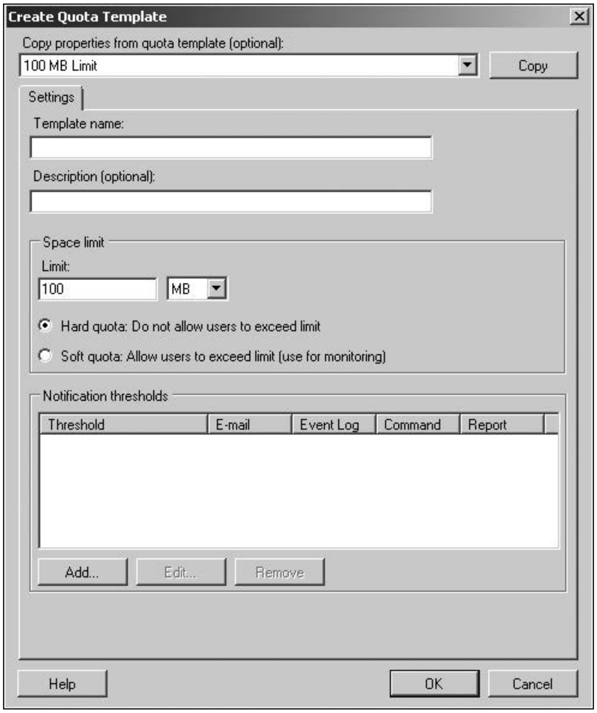
Threshold	E-mail	Event Log	Command	Report
Warning (85%)	✓			
Warning (95%)	✓	✓		
Warning (100%)	✓	✓		

□ Disable quota

FIGURE 7-40 Quota properties

Creating Templates

If none of the supplied templates is suitable for your purposes, you can create a new template. If you like, you can copy settings from an existing template and edit them, or you can specify new settings. Figure 7-41 shows the Create Quota Template dialog box. Many of the settings are similar to those that you can configure when editing a quota.



Copy properties from quota template (optional): 100 MB Limit

Template name:

Description (optional):

Space limit

Limit: 100 MB

● Hard quota: Do not allow users to exceed limit

○ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

Threshold	E-mail	Event Log	Command	Report

FIGURE 7-41 Creating a quota template

Managing File Screens

You can use FSRM to create and manage file screens that control the types of files that users can save and generate notifications when users attempt to save unauthorized files. You can also define file screening templates that you can apply to new volumes or folders and use across your organization.

FSRM also enables you to create file screening exceptions that extend the flexibility of the file screening rules. You could, for example, ensure that users do not store music files in personal folders, but you could allow storage of specific types of media files, such as training files that comply with company policy. You could also create an exception that allows members of the senior management group to save any type of file they want (provided that they comply with legal restrictions).

You can also configure your screening process to notify you by email when an executable file is stored on a shared folder. This notification can include information about the user who stored the file and the file's exact location.

EXAM TIP

File screens are not included specifically on the objectives for the exam. You should know what they are, what they do, and that you can manage them from FSRM. You probably will not come across detailed questions about file screen configuration.

Managing Storage Reports

FSRM provides a Storage Reports Management node. This enables you to generate storage-related reports, such as reports about duplicate files, the largest files, which files are accessed most frequently, and which files are seldom accessed. It also lets you schedule periodic storage reports, which help you identify trends in disk usage, and monitor attempts to save unauthorized files.

For example, you could schedule a report to run at midnight every Sunday and provide you with information about the most recently accessed files from the previous two days. This lets you monitor weekend storage activity and plan server downtime so that it has a minimum impact on users who connect from home over the weekend.

You could use the information in a report that identifies duplicate files so that you can reclaim disk space without losing data, and you could create other reports that enable you to analyze how individual users are using shared storage resources.

MORE INFO **FSRM**

For more information about FSRM, open the command prompt and enter hh fsrm.chm.

Lesson Summary

- The File Server role service in the File Services server role is installed by default and allows access to the Share And Storage Management MMC snap-in. This in turn provides access to the Provision A Stored Folder Wizard and lets you configure access control and manage shared folders, volumes, open sessions, and open files. The Shared Folders MMC snap-in also enables you to share a folder and set permissions.
- If you want, you can install the DFS, FSRM, Services For NFS, Windows Search Service, and BranchCache For Network Files role services. DFS includes DFSN and DFSR. You can also install the Windows Server 2003 File Services server role to create compatibility with earlier versions of Windows.
- The FSRM console lets you configure quotas and file screens and generate storage reports. You can set quotas on shared folders as well as volumes.
- BranchCache For Network Files caches files downloaded from a central location on a computer in a branch office. Other computers in the branch that need to access these files can then do so locally.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Planning File Servers." The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE*** **ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.**

1. Which of the following wizards can you access from the Share And Storage Management console?
   - **A.** Provision A Shared Folder Wizard
   - **B.** New Namespace Wizard
   - **C.** Create Quota Wizard
   - **D.** Create File Screen Wizard
2. You have not installed any additional role services for the File Services server role; only the default File Server role service is installed. You start the Provision A Shared Folder Wizard. All your volumes are formatted with NTFS. Which of the following tasks can you carry out by using the wizard? (Each answer is a complete solution. Choose three.)
   - **A.** Specify a folder to share.
   - **B.** Create a new folder to share.
   - **C.** Specify the network sharing protocol that is used to access the shared resource.
   - **D.** Change the local NTFS permissions for the folder or volume that you are sharing.
   - **E.** Publish the shared resource to a DFS namespace.
3. Which of the following quota templates, available by default, creates a soft quota that can be applied only to volumes?
   - **A.** 100 MB Limit
   - **B.** 200 MB Limit Reports To User
   - **C.** Monitor 200 GB Volume Usage
   - **D.** Monitor 50 MB Share Usage
4. Which mode of which server role deploys a computer running Windows Server 2008 R2 as a host in a branch office? The host stores files downloaded from a central location across a WAN so that other clients in the branch can access these files locally.
   - **A.** FSRM in Hosted Cache mode
   - **B.** FSRM in Distributed Cache mode

C. BranchCache For Network Files in Distributed Cache mode

D. BranchCache For Network Files in Hosted Cache mode

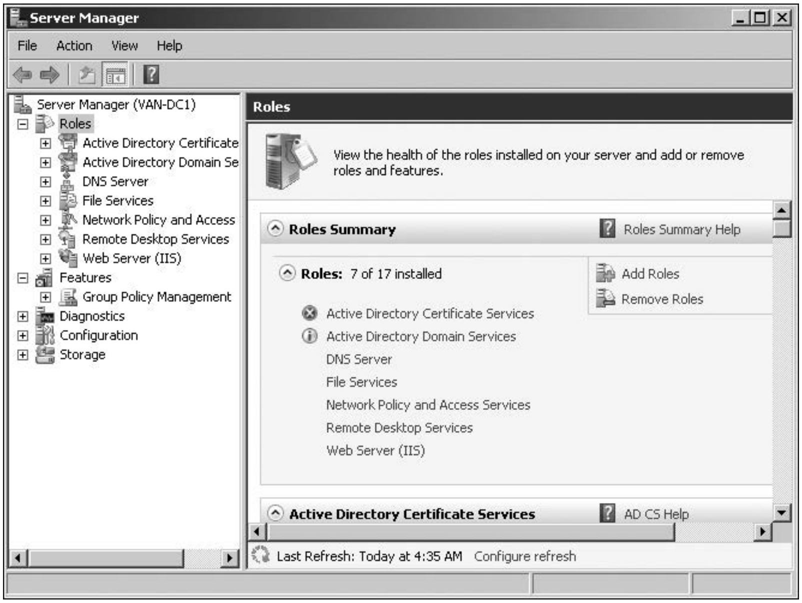
PRACTICE Adding the Print and Document Services Server Role

In this practice, you add the Print and Document Services server role and the Internet Printing role service. Here, you log on to the domain controller interactively. In a production network, you typically would access the domain controller remotely from your administrator workstation.

EXERCISE Installing the Print and Document Services Server Role

In this exercise, you install the Print and Document Services server role. This lets you share (or publish) printers on a network. To complete the exercise, follow these steps:

1. Log on to VAN-DC1 with the Kim Akers account and, if necessary, open Server Manager.
2. In the console tree, expand Server Manager. Locate the Roles Summary in the right pane, as shown in Figure 7-42. Check that the Print and Document Services role is not listed. If this role is listed, it is installed, and you do not need to complete the rest of this exercise.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 7 of 17 installed

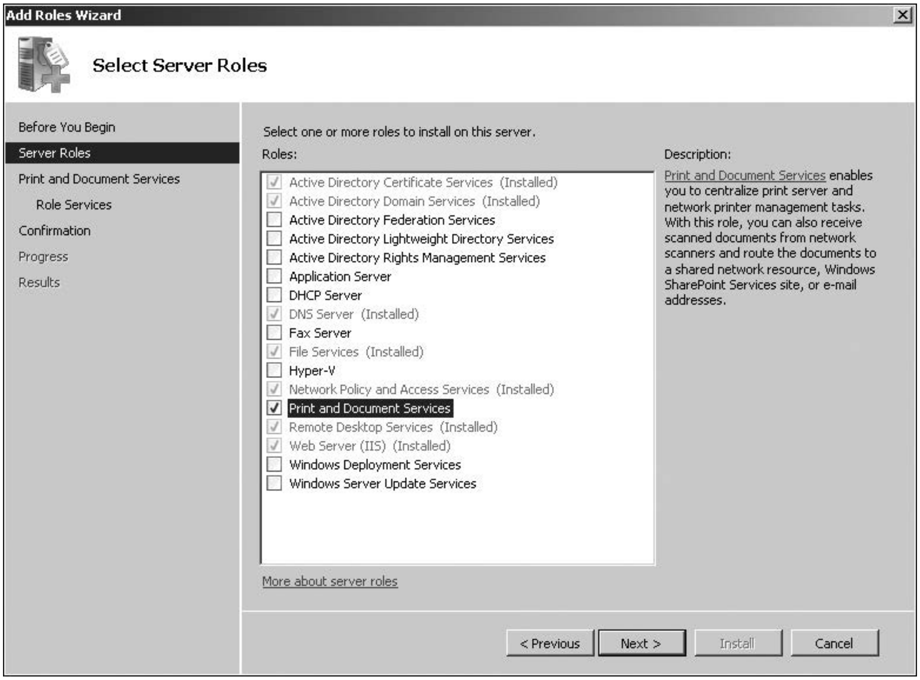
- Active Directory Certificate Services
- Active Directory Domain Services
- DNS Server
- File Services
- Network Policy and Access Services
- Remote Desktop Services
- Web Server (IIS)

Last Refresh: Today at 4:35 AM

FIGURE 7-42 Reading the list of installed roles under Roles Summary

3. Click Add Roles. The Add Roles Wizard starts. If the Before You Begin page appears, click Next.

4. On the Select Server Roles page, select Print And Document Services, as shown in Figure 7-43. Click Next.



Select one or more roles to install on this server.

Roles:

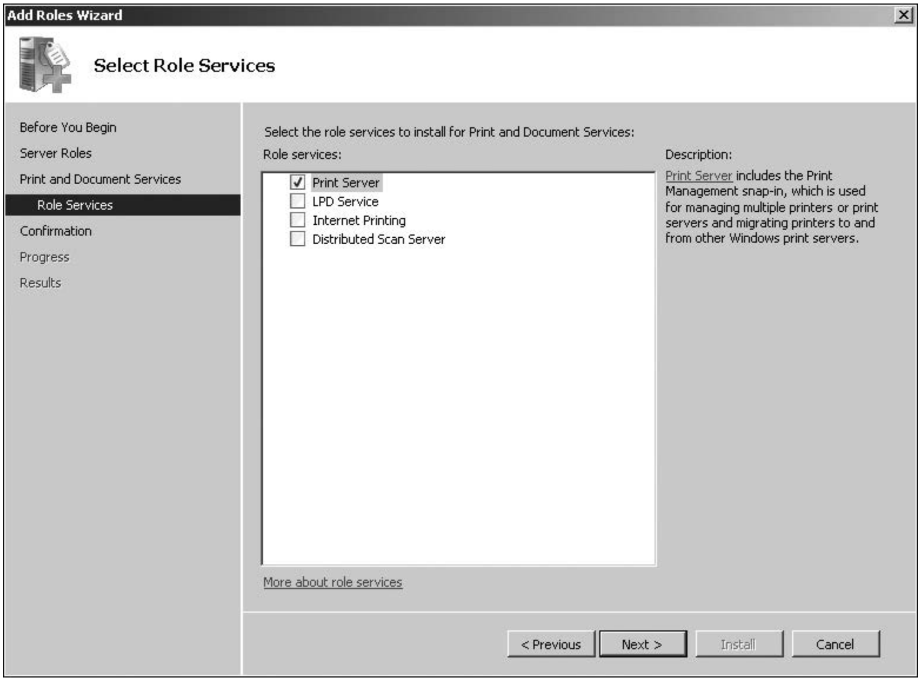
- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ☑ File Services (Installed)
- □ Hyper-V
- ☑ Network Policy and Access Services (Installed)
- ☑ Print and Document Services
- ☑ Remote Desktop Services (Installed)
- ☑ Web Server (IIS) (Installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Print and Document Services enables you to centralize print server and network printer management tasks. With this role, you can also receive scanned documents from network scanners and route the documents to a shared network resource, Windows SharePoint Services site, or e-mail addresses.

FIGURE 7-43 Selecting Print and Document Services

5. Read the information under Introduction To Print And Document Services and under Things To Note. If you want, you can also click the links to the Help files. Click Next.
6. On the Select Role Services page, shown in Figure 7-44, Print Server should be selected by default. Select Internet Printing. If the Add Role Services Required For Internet Printing dialog box appears, click Add Required Role Services. Click Next on the Select Role Services page.
7. If the Web Server (IIS) page appears, read the information presented and then click Next.
8. The Select Role Services page should now look similar to Figure 7-45, and it should show that the Web Server role service is already installed. If this server role is not installed, select Web Server. Click Next.



Select the role services to install for Print and Document Services:

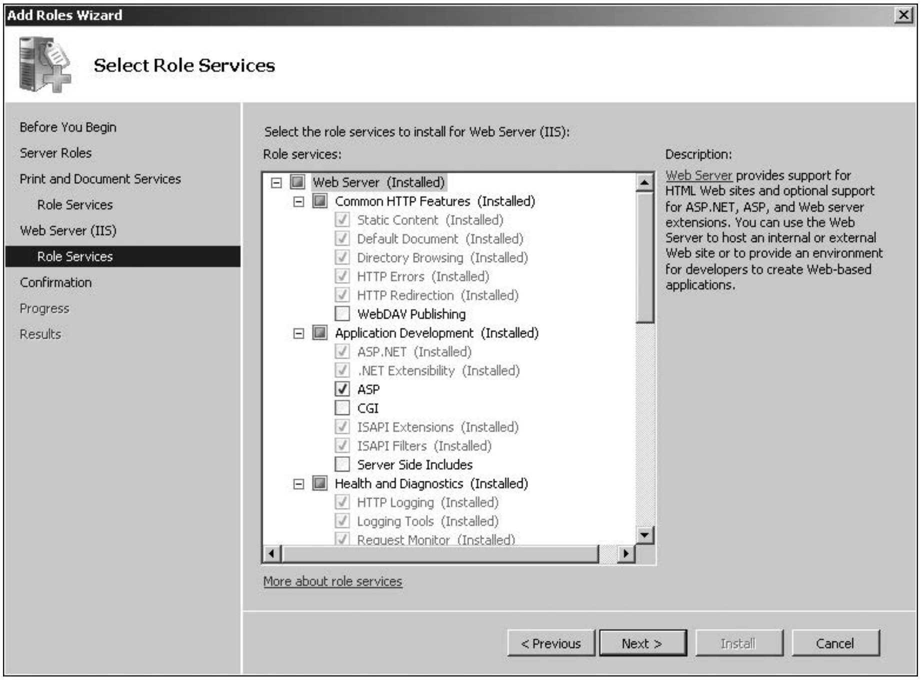
Role services:

- ☑ Print Server
- ☐ LPD Service
- ☐ Internet Printing
- ☐ Distributed Scan Server

Description:

Print Server includes the Print Management snap-in, which is used for managing multiple printers or print servers and migrating printers to and from other Windows print servers.

FIGURE 7-44 Print Server, selected by default



Select the role services to install for Web Server (IIS):

Role services:

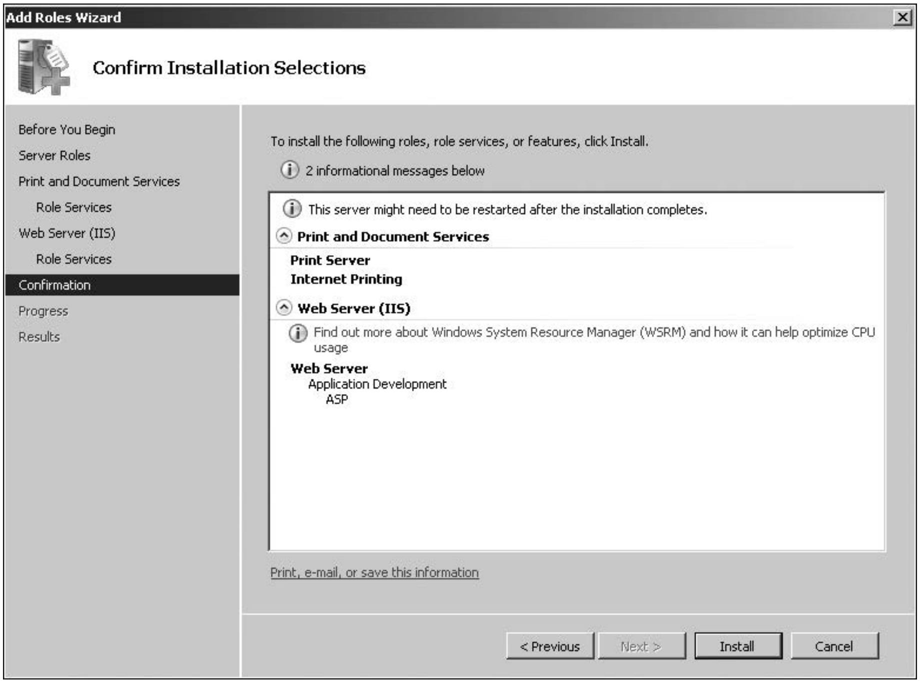
- ▣ Web Server (Installed)
  - ▣ Common HTTP Features (Installed)
    - ☑ Static Content (Installed)
    - ☑ Default Document (Installed)
    - ☑ Directory Browsing (Installed)
    - ☑ HTTP Errors (Installed)
    - ☑ HTTP Redirection (Installed)
    - ☐ WebDAV Publishing
  - ▣ Application Development (Installed)
    - ☑ ASP.NET (Installed)
    - ☑ .NET Extensibility (Installed)
    - ☑ ASP
    - ☐ CGI
    - ☑ ISAPI Extensions (Installed)
    - ☑ ISAPI Filters (Installed)
    - ☐ Server Side Includes
  - ▣ Health and Diagnostics (Installed)
    - ☑ HTTP Logging (Installed)
    - ☑ Logging Tools (Installed)
    - ☑ Request Monitor (Installed)

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

FIGURE 7-45 The Web Server role service, already installed

9. Read the information on the Confirm Installation Selections page, which should look similar to Figure 7-46. Note that you might need to reboot your server when installation is complete. Click Install.



To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

Print and Document Services

Print Server
Internet Printing

Web Server (IIS)

Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server
Application Development
ASP

FIGURE 7-46 The Confirm Installation Selections page

10. Click Close when installation completes. Check that Print And Document Services is now listed under Roles Summary in Server Manager.

11. Save any unsaved files and close all open windows. Reboot VAN-DC1 if prompted to do so.

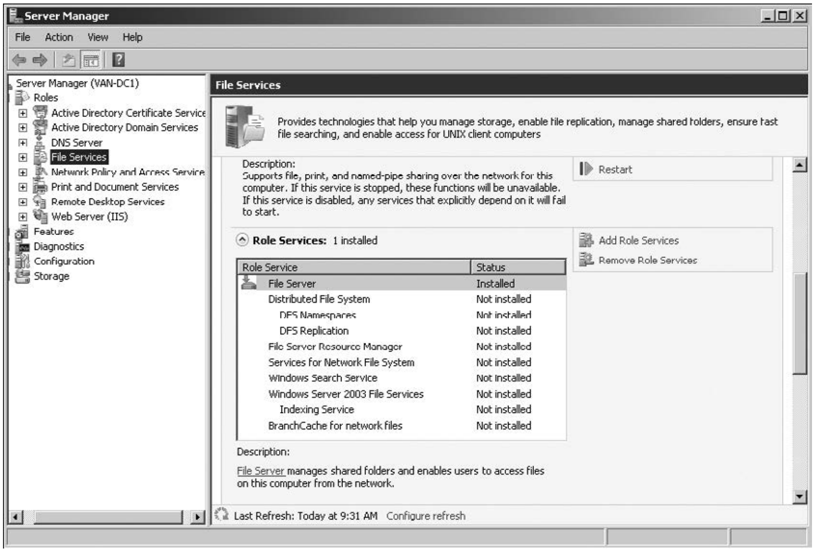
PRACTICE Adding Role Services to the File Services Server Role and Configuring a Quota

In this practice, you add selected role services to the File Services server role on your domain controller, VAN-DC1. You then create a shared folder on that domain controller and configure a quota for that folder. As with the previous practice, you will log on to VAN-DC1 interactively. In a production network, you typically would access the domain controller remotely.

EXERCISE 1 Adding Role Services to the File Services Server Role

In this exercise, you open Server Manager and add selected role services to the File Services server role. You do not add any of the optional features associated with this server role. The folder C:\Public should exist on your domain controller by default—if it is not, create it before you start this exercise. To complete the exercise, follow these steps:

1. If necessary, log on to VAN-DC1 with the Kim Akers account, share the C:\Public folder with default permissions, and open Server Manager.
2. Expand Roles and click File Services. In the right pane, locate the list of Role Services, as shown in Figure 7-47.



Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Description:
Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

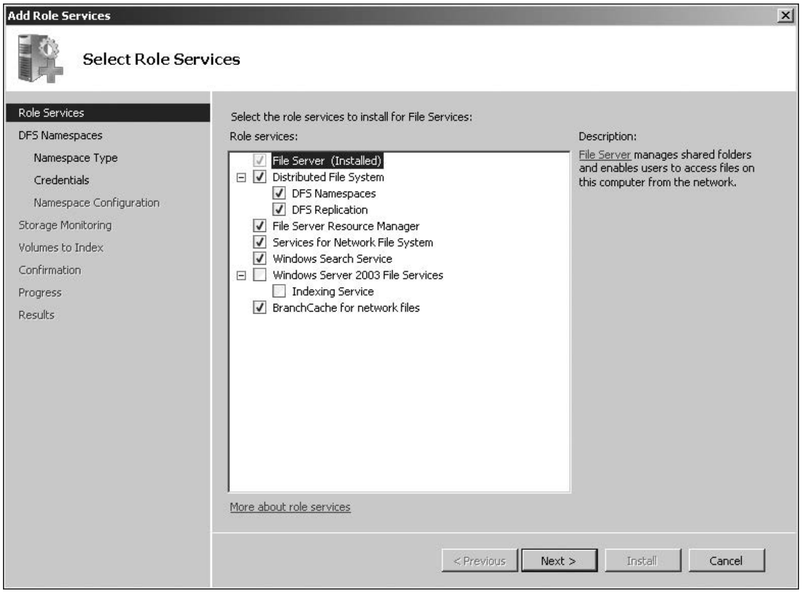
Role Services: 1 installed

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed
Services for Network File System	Not installed
Windows Search Service	Not installed
Windows Server 2003 File Services	Not installed
Indexing Service	Not installed
BranchCache for network files	Not installed

Description:
File Server manages shared folders and enables users to access files on this computer from the network.

FIGURE 7-47 Role services that can be added to the File Services role

3. Click Add Role Services.
4. In the Select Role Services dialog box, select all uninstalled role services except the Windows Server 2003 File Services and its associated Indexing Service, as shown in Figure 7-48.



Select the role services to install for File Services:

Role services:

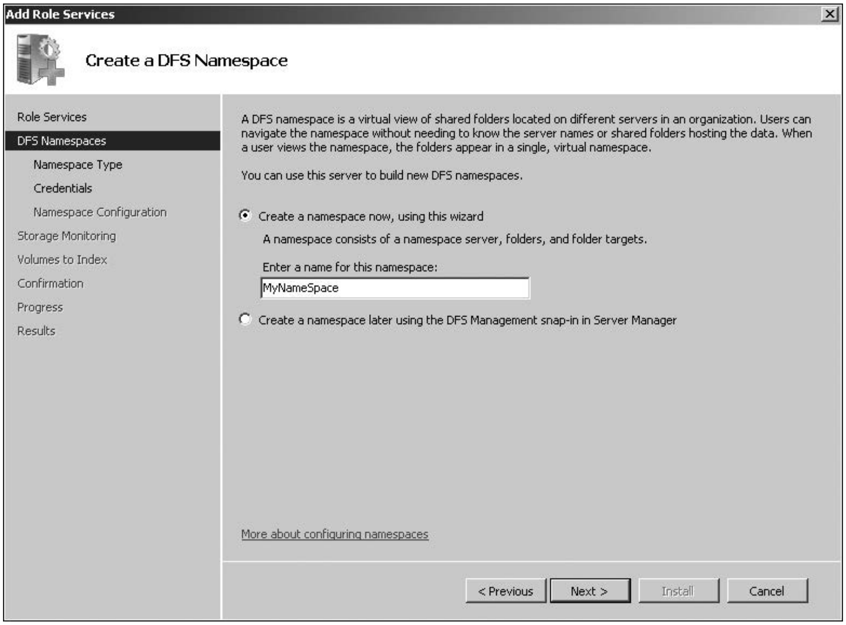
- ☑ File Server (Installed)
- ☑ Distributed File System
  - ☑ DFS Namespaces
  - ☑ DFS Replication
- ☑ File Server Resource Manager
- ☑ Services for Network File System
- ☑ Windows Search Service
- ☐ Windows Server 2003 File Services
  - ☐ Indexing Service
- ☑ BranchCache for network files

Description:
File Server manages shared folders and enables users to access files on this computer from the network.

FIGURE 7-48 Selecting role services

5. Click Next.

6. Call the DFS namespace **MyNameSpace**, as shown in Figure 7-49. Click Next.



Add Role Services

Create a DFS Namespace

A DFS namespace is a virtual view of shared folders located on different servers in an organization. Users can navigate the namespace without needing to know the server names or shared folders hosting the data. When a user views the namespace, the folders appear in a single, virtual namespace.

You can use this server to build new DFS namespaces.

● Create a namespace now, using this wizard

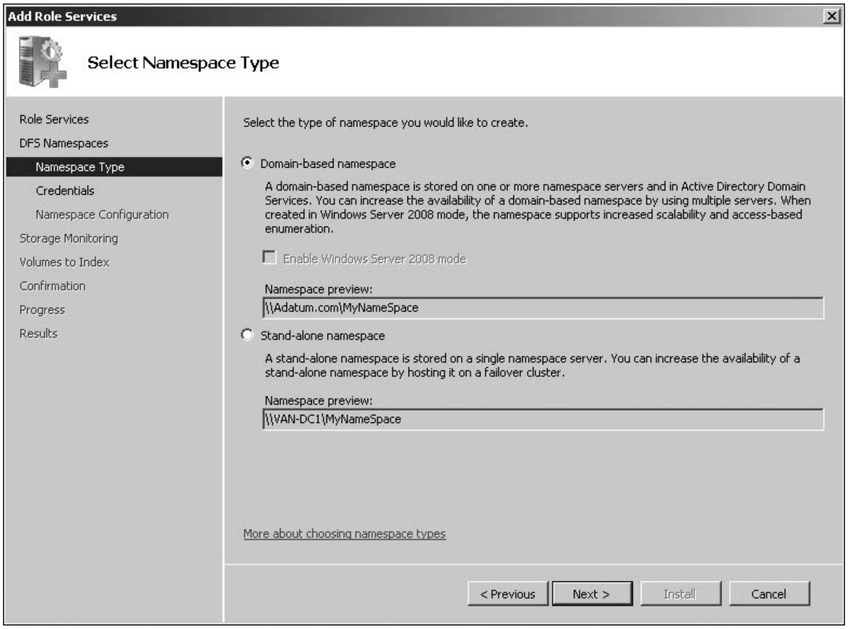
A namespace consists of a namespace server, folders, and folder targets.

Enter a name for this namespace: MyNameSpace

○ Create a namespace later using the DFS Management snap-in in Server Manager

FIGURE 7-49 Specifying a DNS namespace

7. Specify a domain-based namespace (the default), as shown in Figure 7-50. Click Next.



Add Role Services

Select Namespace Type

Select the type of namespace you would like to create.

● Domain-based namespace

A domain-based namespace is stored on one or more namespace servers and in Active Directory Domain Services. You can increase the availability of a domain-based namespace by using multiple servers. When created in Windows Server 2008 mode, the namespace supports increased scalability and access-based enumeration.

□ Enable Windows Server 2008 mode

Namespace preview: \\Adatum.com\MyNameSpace

○ Stand-alone namespace

A stand-alone namespace is stored on a single namespace server. You can increase the availability of a stand-alone namespace by hosting it on a failover cluster.

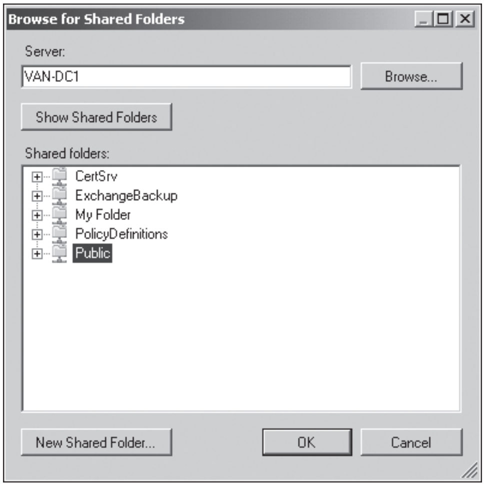
Namespace preview: \\VAN-DC1\MyNameSpace

FIGURE 7-50 Specifying a DNS namespace type

NOTE **DOMAIN-BASED AND STAND-ALONE NAMESPACES**

Chapter 10 discusses domain-based and stand-alone namespaces.

8. On the Provide Credentials To Create A Namespace page, click Select. Specify the user name and password for the Kim Akers account, and then click OK. Click Next.
9. In the Configure Namespace dialog box, click Add. Click Browse in the Add Folder To Namespace dialog box.
10. In the Browse For Shared Folders dialog box, click Show Shared Folders. Ensure that Public is selected, as shown in Figure 7-51. Click OK.

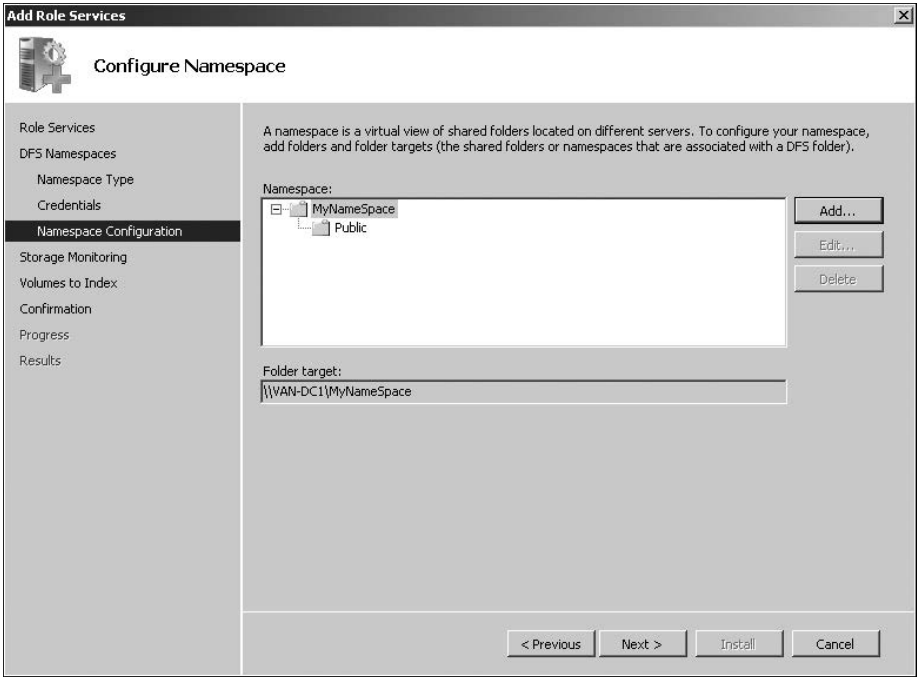


Server: VAN-DC1

Shared folders: Public

FIGURE 7-51 Selecting a shared folder

11. By default, the corresponding folder in your namespace takes the same name as the shared folder you selected. Click OK to accept this default.
12. Your Configure Namespace wizard page should look similar to Figure 7-52. Click Next.
13. In the Configure Storage Usage Monitoring page, select your C: volume, as shown in Figure 7-53. Your volume size and usage probably will differ from what is shown here. Do not change the default options. Click Next.



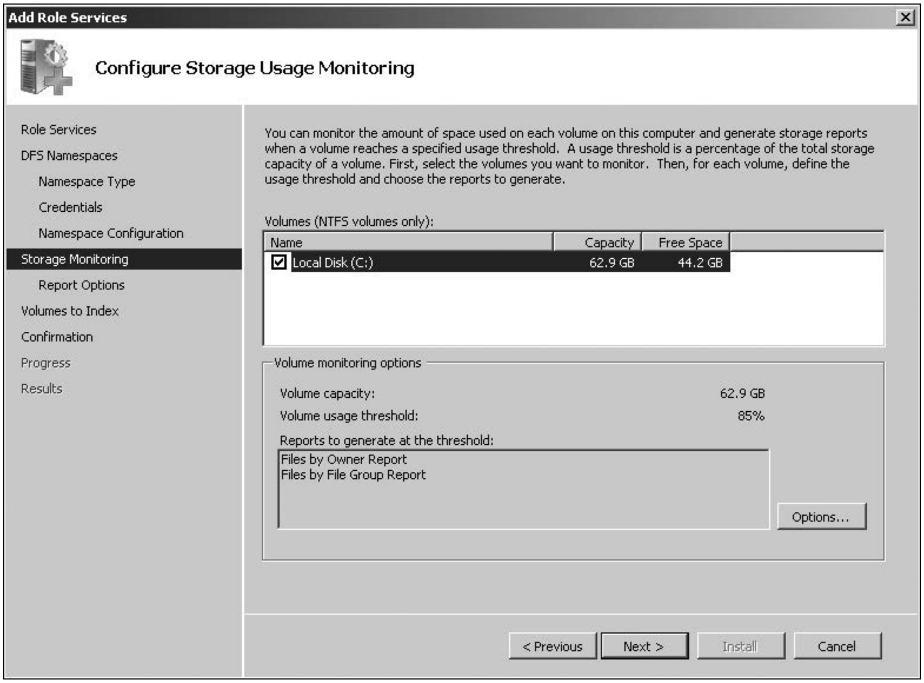
A namespace is a virtual view of shared folders located on different servers. To configure your namespace, add folders and folder targets (the shared folders or namespaces that are associated with a DFS folder).

Namespace:

```
⊟ MyNameSpace
   └ Public
```

Folder target: \\VAN-DC1\MyNameSpace

FIGURE 7-52 Configuring a namespace



You can monitor the amount of space used on each volume on this computer and generate storage reports when a volume reaches a specified usage threshold. A usage threshold is a percentage of the total storage capacity of a volume. First, select the volumes you want to monitor. Then, for each volume, define the usage threshold and choose the reports to generate.

Volumes (NTFS volumes only):

Name	Capacity	Free Space
☑ Local Disk (C:)	62.9 GB	44.2 GB

Volume monitoring options

Volume capacity: 62.9 GB

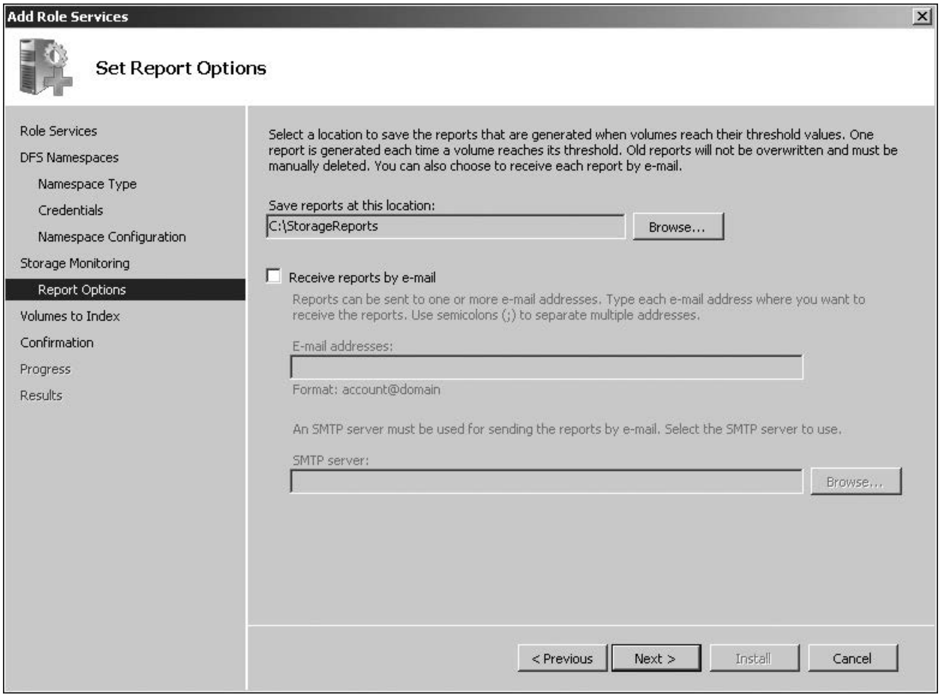
Volume usage threshold: 85%

Reports to generate at the threshold:

Files by Owner Report
Files by File Group Report

FIGURE 7-53 Configuring storage usage monitoring

14. The Set Report Options page should look similar to Figure 7-54. Click Next to accept the default settings.



Select a location to save the reports that are generated when volumes reach their threshold values. One report is generated each time a volume reaches its threshold. Old reports will not be overwritten and must be manually deleted. You can also choose to receive each report by e-mail.

Save reports at this location: C:\StorageReports [Browse...]

☐ Receive reports by e-mail

Reports can be sent to one or more e-mail addresses. Type each e-mail address where you want to receive the reports. Use semicolons (;) to separate multiple addresses.

E-mail addresses:

Format: account@domain

An SMTP server must be used for sending the reports by e-mail. Select the SMTP server to use.

SMTP server: [Browse...]

FIGURE 7-54 Configuring report options

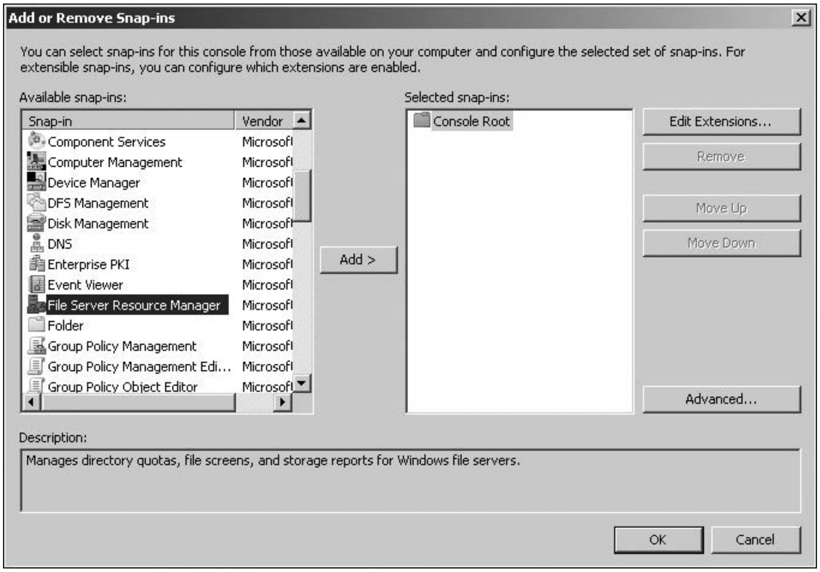
15. Choose to index a volume that does not contain your operating system. If the only volume on your server is C:, do not index any volumes. Click Next.
16. Check your installation selections. If you are satisfied with them, click Install.
17. When installation completes, click Close.

EXERCISE 2 Configure a Quota

In this exercise, you create a shared folder on domain controller VAN-DC1 and configure a quota for that folder. If you prefer, you can access the File Server Resource Manager tool from the Administrative Tools menu rather than adding the snap-in to the MMC.

1. If necessary, log on to VAN-DC1 with the Kim Akers account.
2. Create a folder named My Folder in the root of your C: drive and share it, giving the Everyone group Read Access. If you are unsure how to do this, refer to Lesson 2.
3. On the Start menu, click Run. Enter **mmc**.
4. If necessary, click Yes to close the User Account Control (UAC) dialog box.
5. In the MMC, click File. Click Add/Remove Snap-In.

6. Click File Server Resource Manager, as shown in Figure 7-55. Click Add, and then click OK.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Component Services	Microsof
Computer Management	Microsof
Device Manager	Microsof
DFS Management	Microsof
Disk Management	Microsof
DNS	Microsof
Enterprise PKI	Microsof
Event Viewer	Microsof
File Server Resource Manager	Microsof
Folder	Microsof
Group Policy Management	Microsof
Group Policy Management Edi...	Microsof
Group Policy Object Editor	Microsof

Selected snap-ins:

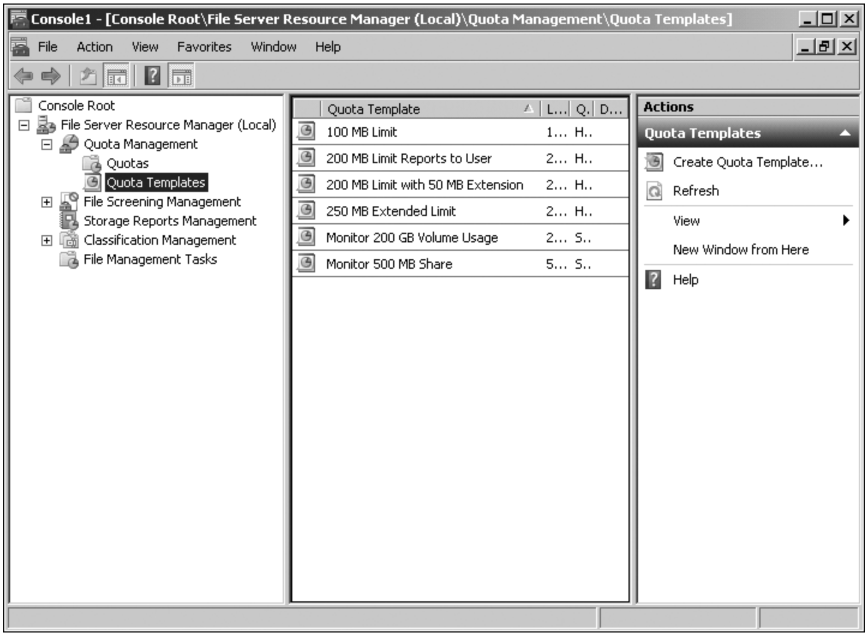
Console Root

Description:

Manages directory quotas, file screens, and storage reports for Windows file servers.

FIGURE 7-55 Adding the File Server Resource Manager snap-in

7. Expand File Server Resource Manager (Local), expand Quota Management, and then click Quota Templates, as shown in Figure 7-56.



Console1 - [Console Root\File Server Resource Manager (Local)\Quota Management\Quota Templates]

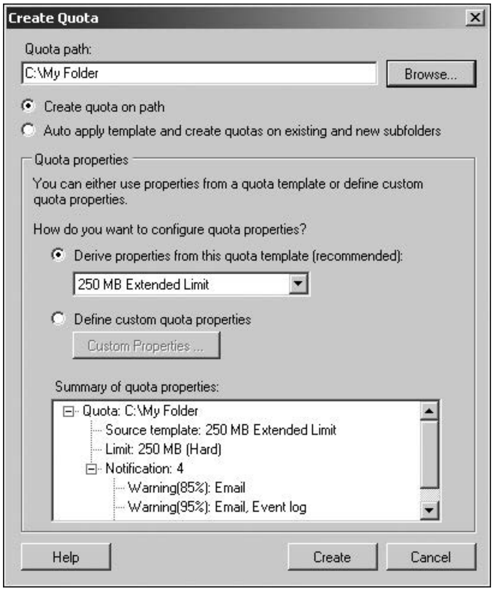
- Console Root
  - File Server Resource Manager (Local)
    - Quota Management
      - Quotas
      - Quota Templates
    - File Screening Management
    - Storage Reports Management
    - Classification Management
    - File Management Tasks

Quota Template	L...	Q.	D...
100 MB Limit	1...	H..	
200 MB Limit Reports to User	2...	H..	
200 MB Limit with 50 MB Extension	2...	H..	
250 MB Extended Limit	2...	H..	
Monitor 200 GB Volume Usage	2...	S..	
Monitor 500 MB Share	5...	S..	

FIGURE 7-56 Accessing the quota templates

8. Click 250 MB Extended Limit, and then, in the Actions pane, click Create Quota From Template.

9. In the Create Quota dialog box, click Browse and browse to C:\My Folder. Click OK. The dialog box should look similar to Figure 7-57.



Create Quota

Quota path: C:\My Folder

● Create quota on path

○ Auto apply template and create quotas on existing and new subfolders

Quota properties

You can either use properties from a quota template or define custom quota properties.

How do you want to configure quota properties?

● Derive properties from this quota template (recommended): 250 MB Extended Limit

○ Define custom quota properties

Summary of quota properties:

```
⊟ Quota: C:\My Folder
    Source template: 250 MB Extended Limit
    Limit: 250 MB (Hard)
  ⊟ Notification: 4
      Warning(85%): Email
      Warning(95%): Email, Event log
```

FIGURE 7-57 Selecting a shared folder on which to apply the quota

10. Click Create.

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenario. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- The Print and Document Services server role lets you manage printers, print drivers, print queues, and printer permissions, both on locally installed printers and on printers installed on other print servers on your network.
- The role services in the File Services server role let you configure access control; manage shared folders, volumes, open sessions, and open files; manage DFS, DFSN, and DFSR; configure quotas and file screens; generate storage reports; configure offline file settings; configure indexing; and implement the caching of files in branch offices.

Key Terms

The following terms were introduced in this chapter. Do you know what they mean?

- Access control entry (ACE)
- Access control list (ACL)
- Access control
- Caching
- DFS Namespace (DFSN)
- DFS Replication (DFSR)
- Distributed File System (DFS)
- Offline file
- Quota

Case Scenario

In the following case scenario, you will apply what you have learned about provisioning file and print servers. You can find answers to these questions in the "Answers" section at the end of this book.

Planning a Windows Server 2008 R2 Upgrade

You are a senior administrator at Blue Yonder Airlines. All the company's servers run Windows Server 2008, and all its clients run Windows 7. The company's network infrastructure consists of a central office and a number of branch offices in distant locations that currently access files on a central office server through WAN links. Sometimes it can take an unacceptable length of time for a large file to download. All the branch offices are small (typically using between 10 and 15 clients), and all the computers in each branch office are on a single subnet. The company plans to upgrade all its domain controllers and some of its member servers at its central office to Windows Server 2008 R2. Answer the following questions:

1. The technical director is concerned with the slow transfer of files to branch offices. She wants to know if installing Windows Server 2008 R2 will improve the situation. What do you tell her?
2. There is no budget for upgrading servers at branch offices. How will this affect branch office caching?
3. The financial director is concerned that files currently can be classified by criteria such as size, what folders they are stored in, and when they were last updated. He asks you if the planned expenditure will assist in classifying files by other criteria, such as the business value of the information they contain. What do you tell him?
4. The technical director is also concerned about the time it takes and the number of steps that are required to install network printers. She wants to know if it is worthwhile to install Windows Server 2008 R2 on a computer running the Print Services server role. What do you tell her?

Suggested Practices

To help you master the examination objectives presented in this chapter, complete the following tasks.

Use the Enhanced Print Management Console

- You can become familiar with a tool only through practice. Use the enhanced Print Management console provided in Windows Server 2008 R2 and become familiar with the various wizards that it provides. If you also have access to a computer running Windows Server 2008, compare the printer management facilities provided by both operating systems and note the differences if you want.

Use the FSRM Console

- You may be familiar with the facilities provided through the FSRM role service in Windows Server 2008, and these continue to be implemented in Windows Server 2008 R2. This role service is not significantly changed, but it remains important, and the exam is likely to ask about quotas, file screening, and report generation. Ensure that you are familiar with the FSRM console.

- Arguably, the most significant feature implemented by the FSRM role service is the facility to implement quotas. Make sure that you are familiar with the process of configuring quotas, that you are familiar with the various standard quota templates available, and that you can distinguish between hard and soft quotas.

Learn More About Windows Storage Server 2008 R2

- Windows Storage Server 2008 R2 is based on Windows Server 2008 R2, and you should know about it. It is described only briefly in this chapter. Look for articles in online technical magazines and on TechNet.

Learn More About BranchCache For Network Files

- BranchCache For Network Files is new to Windows Server 2008 R2. Read any online articles and discussions you can discover, including TechNet articles.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **PRACTICE TESTS**

For details about all the practice test options available, see the "How to Use the Practice Tests" section in this book's Introduction.

CHAPTER 9

Remote Access and Network Access Protection

You can use VPNs to allow remote users to connect to your organization's internal network resources, whether they are using a hotel wireless hotspot in Gundagai or are connecting through an ADSL connection in Canberra. When you plan how to provision VPN access, you need to take into account a host of factors. You need to know how your organization's external firewall will be configured, the operating system used by the client, and the types of resources that remote clients will need to access.

Network Access Protection (NAP) allows you to restrict network access on the basis of client health. Put simply, NAP allows you to enforce a rule that if the client is not up to date with patches and antivirus definitions, you can block it from getting full access to the network. In this chapter, you will learn how to configure and deploy NAP and the various methods that are available to deal with noncompliant computers. You will also learn how to plan and deploy Windows Server 2008 R2 remote access services to ensure that your organization's clients can connect to your internal resources no matter where in the world they are.

Exam objectives in this chapter:

- Plan infrastructure services server roles.
- Monitor and maintain security and policies.

Lessons in this chapter:

- Lesson 1: Managing Remote Access **435**
- Lesson 2: Firewalls and Network Access Protection **456**

Before You Begin

To complete the exercises in the practice in this chapter, you need to have done the following:

- Complete the setup tasks outlined in Appendix A, "Setup Instructions for Windows Server 2008 R2."

No additional configuration is required for this chapter.

REAL WORLD

Orin Thomas

Traditional models of networks and firewalls had all the bad stuff "out there" and all the safe stuff "in here." Today, however, the internal network can be as hostile an environment as the Internet. In the past, every computer that connected to the network was stationary, and very few people took their workstations home with them. But today, most computers sold are laptops, and increasing numbers of people take their primary computer with them when they leave the office for the day. Unfortunately, once people take their computers out of the protected glasshouse that is your internal network, all sorts of bad things can happen to them. Malware, which might have been blocked by the external firewall, will be inadvertently downloaded on the home ADSL connection. Computers that you were able to keep completely healthy when they were under your control are now exposed on a daily basis to all manner of Internet nasties. The biggest problem is that after those computers go out of your safe environment, they are brought back into work the next day and are plugged into your organizational network. Technologies such as Windows Firewall with Advanced Security and NAP go some distance toward protecting hosts on your internal network from whatever "the cat drags in" on a regular basis when the people you work with bring their computers back from home. When you plan your organizational security strategy, don't assume that hosts that have a local IP address are any safer than hosts with an Internet IP address unless they've gone through some process, such as NAP, to provide evidence that they are secure.

Lesson 1: Managing Remote Access

If your organization is going to allow workers to telecommute, you need to provide those workers with some way to access resources on your organization's internal network. In this lesson, you will learn how to plan the deployment of VPN servers to allow remote access to your internal network from locations that are external to your organization's network. You will also learn about DirectAccess, a technology available with Windows 7 and Windows Server 2008 R2 that dramatically simplifies the remote access process from the user perspective. The lesson will also cover traditional remote access protocols, including Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPsec), Secure Socket Tunneling Protocol (SSTP), and another technology new to Windows Server 2008 R2 called IKEv2.

After this lesson, you will be able to:

- Plan remote access infrastructure server roles.
- Monitor and maintain remote access security policies.
- Implement remote access technologies, including IKEv2 VPNs and DirectAccess.

Estimated lesson time: 60 minutes

The Routing and Remote Access Service (RRAS) role service is available as part of the Network Policy And Access Services server role. You should deploy the Remote Access Service (RAS) component of the RRAS role service when you want to provide either of the following resources to your network environment:

- VPN remote access server
- Dial-up remote access server

In this lesson, you will learn how to configure and monitor a VPN remote access server running Windows Server 2008 and Windows Server 2008 R2. To install the RRAS role service, use the Add Roles Wizard and then select Network Policy And Access Services. RRAS is a role service within this role. As an alternative, open an elevated Windows PowerShell prompt on a computer running Windows Server 2008 R2 and issue the following commands:

```
Import-Module ServerManager
Add-WindowsFeature NPAS-RRAS-Services
```

To remove RRAS completely from a server running Windows Server 2008 R2, issue the command:

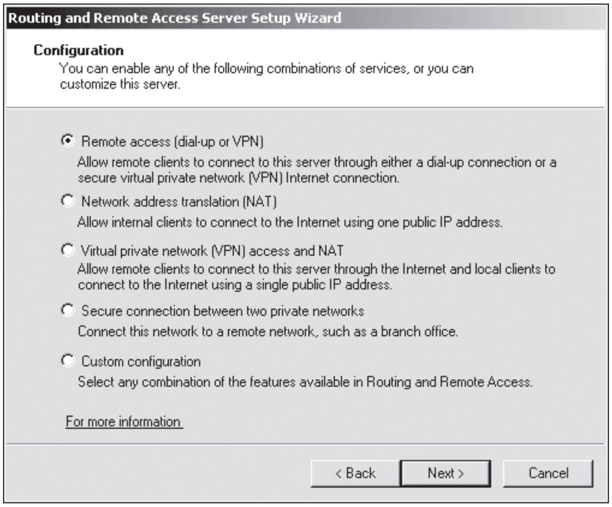
```
Remove-WindowsFeature NPAS
```

NOTE **PREVIOUS INSTALLATIONS OF RRAS**

If you have installed and configured RRAS before, you may need to reset the configuration to get RRAS to perform other functions. To do this, issue the following commands: `netsh ras set conf confstate=disabled` **and then** `net stop "Routing and Remote Access"`**.**

Once installed, you must configure RAS manually. Only members of the local Administrators group are able to configure the RAS. In domain environments, you should perform this action using a user account that is a member of the Domain Admins group. If your user account is not a member of the Domain Admins security group, organize a domain admin to add the RAS server account manually to the RAS And IAS Servers domain security group. It is not necessary to add the RAS server to this group if the RAS server will be using local authentication or authenticating against a Remote Authentication Dial-In User Service (RADIUS) server.

To enable Remote Access, open the Routing and Remote Access console from the Administrative Tools menu, right-click the computer running Windows Server 2008 R2 that you want to host this role, and then click Configure And Enable Routing And Remote Access. Performing this action starts the Routing And Remote Access Server Setup Wizard. The configuration page of this wizard, shown in Figure 9-1, allows you to select the combination of services that this particular server will provide. The Remote Access (Dial-Up Or VPN) option is selected when you want to provide either remote access option or both options to clients outside your organization.



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

● Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

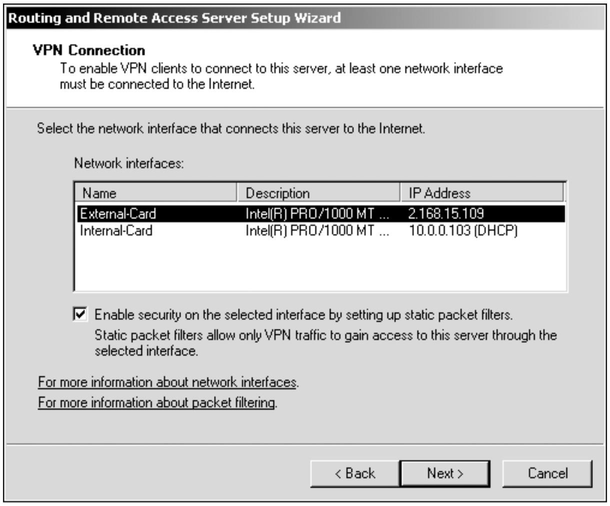
○ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

○ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.

FIGURE 9-1 The Routing And Remote Access Server Setup Wizard

If you have chosen to install a VPN server, you will need to specify which network interface connects to the Internet on the VPN Connection page shown in Figure 9-2. This will be the interface that has the public IP address, rather than the interface that has the private IP address. If additional network adapters are installed on the server that hosts the RAS role after the RAS server is deployed, they can be configured for use with RAS using the RRAS console. If the computer running Windows Server 2008 R2 has fewer than two network adapters, you will not be able to perform a standard VPN server setup and will need to perform a custom configuration instead.



VPN Connection

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
External-Card	Intel(R) PRO/1000 MT ...	2.168.15.109
Internal-Card	Intel(R) PRO/1000 MT ...	10.0.0.103 (DHCP)

☑ Enable security on the selected interface by setting up static packet filters.

Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

For more information about network interfaces.

For more information about packet filtering.

FIGURE 9-2 Installing the RAS

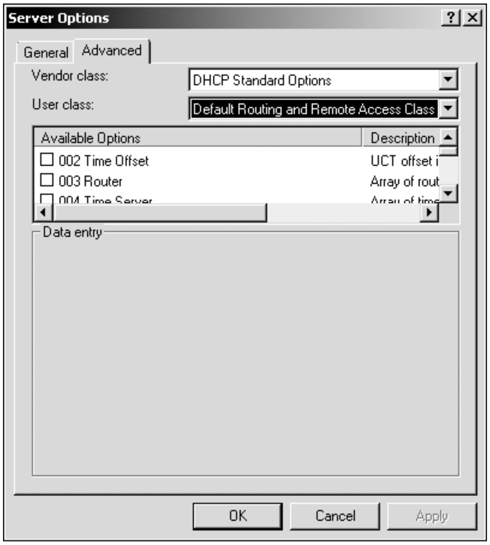
When you configure a remote access server, the process applies packet filters that allow only VPN protocols to the Internet interface. This means that the server is limited to providing VPN access. If you have deployed other services on the server that will host the RAS role, you will need to configure new packet filters to allow this traffic to the server. As a deployment strategy, you should seriously consider keeping the RAS server separate from other services.

After you identify the external interface, the next step in configuring the RAS role is specifying how to assign IP addresses to clients. You can do this in several ways:

- Client addresses can be leased from a DHCP server within the organization.
- The RAS server can generate the addresses itself.
- You can specify a range of addresses to assign to connecting clients.

When using your organization's DHCP infrastructure, the RAS server will lease blocks of 10 addresses, requesting new blocks if previously requested blocks are all currently in use.

DHCP servers running Windows Server 2008 and Windows Server 2008 R2 have a predefined user class, known as the Default Routing And Remote Access Class. This class allows administrators to assign specific options only to Routing And Remote Access clients. This class is configured through the Advanced tab of DHCP Server Options, as shown in Figure 9-3.



Vendor class: DHCP Standard Options

User class: Default Routing and Remote Access Class

Available Options	Description
☐ 002 Time Offset	UCT offset i
☐ 003 Router	Array of rout
☐ 004 Time Server	Array of time

FIGURE 9-3 The RRAS DHCP class

The next step in configuring an RAS server is determining how authentication will occur. You can configure the RAS server to perform authentication against Active Directory Domain Services (AD DS) or the local account database, or you can configure the RAS server as a RADIUS client and allow the RADIUS server to perform the authentication and authorization of client connection requests. You will learn more about RADIUS options later in this lesson. After you have performed these steps, the RAS server will be functional.

VPN Authentication

A VPN is an extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. A client connects to a public network, such as the Internet, and initiates a VPN connection to a remote server. This remote server is usually located on the perimeter network of the organization that the client wants to connect to. After the connection is made, an encrypted tunnel forms between the client and the VPN server. This encrypted tunnel carries local area network (LAN) traffic between the client and the remote network that the client is connected to. Clients are connected to the network in the same way that they would be if they were in the office. Instead of a network cable connecting them to a switch somewhere in the office, a virtual cable in the form of a VPN tunnel connects them to their organization's network infrastructure.

The following authentication protocols can be used by a computer running Windows Server 2008 or Windows Server 2008 R2 to authenticate incoming VPN connections. These protocols are listed in order from most secure to least secure:

- **Extensible Authentication Protocol-Transport Level Security (EAP-TLS)** This is the protocol that you deploy when your VPN clients are able to authenticate using smart cards or digital certificates. EAP-TLS is not supported on stand-alone servers and can be implemented only when the server hosting the RAS role service is a member of an AD DS domain.

- **Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2)** This protocol provides mutual authentication and allows for the encryption of both authentication data and connection data. MS-CHAPv2 is enabled by default in Windows Server 2008 and Windows Server 2008 R2.
- **Challenge Handshake Authentication Protocol (CHAP)** An older authentication method that encrypts authentication data using MD5 hashing. CHAP does not support the encryption of data and is used most often to provide compatibility with older, non-Microsoft clients.
- **Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP)** A version of CHAP that has been ported to the EAP framework. This authentication protocol supports encryption of authentication data through MD5 hashing and is generally used to provide compatibility with non-Microsoft clients.
- **Shiva Password Authentication Protocol (SPAP)** A weakly encrypted authentication protocol that does not support the encryption of connection data.
- **Password Authentication Protocol (PAP)** When this protocol is used, authentication data is not encrypted, but is passed across the network in plain text. Does not support the encryption of protection data.

The authentication process always attempts to negotiate the use of the most secure authentication protocol. The default authentication protocol used for VPN clients connecting to a Windows Server 2008 and Windows Server 2008 R2 VPN is MS-CHAPv2.

VPN Protocols

Windows Server 2008 R2 supports four different VPN protocols: Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec), Secure Socket Tunneling Protocol (SSTP), and IKEv2. The factors that will influence the protocol you choose to deploy in your own network environment include client operating system, certificate infrastructure, and how your organization's firewall is deployed.

PPTP

PPTP connections can only be authenticated using MS-CHAP, MS-CHAPv2, EAP, and PEAP. PPTP connections use MPPE to encrypt PPTP data. PPTP connections provide data confidentiality but do not provide data integrity or data origin authentication. It is possible to use PPTP with certificates if EAP-TLS is selected as the authentication protocol, although the advantage of PPTP over the other VPN protocols supported by Windows Server 2008 and Windows Server 2008 R2 is that it does not require certificates be installed on the client making the connection. With PPTP, you do not need to be concerned about shared secrets or computer certificates or ensuring that the appropriate Certificate Authority (CA) is trusted. PPTP is often used with non-Microsoft operating systems.

MORE INFO **PPTP**

For more information on configuring PPTP-based remote access, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ff687676(WS.10).aspx.*

L2TP/IPsec

L2TP connections use encryption provided by IPsec. L2TP/IPsec is the protocol that you need to deploy if you are supporting remote access clients running Microsoft Windows XP because such clients cannot use SSTP. L2TP/IPsec provides per-packet data origin authentication, data integrity, replay protection, and data confidentiality.

L2TP/IPsec connections use two levels of authentication. Computer-level authentication occurs either using digital certificates issued by a CA trusted by the client and VPN server or through the deployment of preshared keys. PPP authentication protocols are then used for user-level authentication. L2TP/IPsec supports all the VPN authentication protocols available on Windows Server 2008 and Windows Server 2008 R2.

MORE INFO **L2TP/IPSEC**

To learn more about L2TP/IPsec, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ff687761(WS.10).aspx.*

SSTP

SSTP is a VPN technology that made its debut with Windows Server 2008 and is available in Windows Server 2008 R2. SSTP VPN tunnels allow traffic to pass across firewalls that block traditional PPTP or L2TP/IPsec VPN traffic. SSTP works by encapsulating PPP traffic over the Secure Sockets Layer (SSL) channel of the Secure Hypertext Transfer Protocol (HTTPS). Expressed more directly, SSTP piggybacks PPP over HTTPS. This means that SSTP traffic passes across TCP port 443, which is almost certain to be open on any firewall between the Internet and a public-facing web server on an organization's perimeter network.

The PPP of SSTP allows for the deployment of advanced authentication methods such as EAP-TLS, which is used most commonly with smart cards. The SSL component of SSTP provides the VPN tunnel with encryption, enhanced key negotiation, and integrity checking. This means data transferred using this method is encoded and that it is possible to detect whether someone has attempted to intercept the contents of the tunnel between the source and destination points.

When planning for the deployment of SSTP, you need to take into account the following considerations:

- SSTP is supported only with Windows Server 2008, Windows Server 2008 R2, Windows 7, and Windows Vista with SP1.
- SSTP requires that the client trust the CA that issues the VPN server's SSL certificate.

- The SSL certificate must be installed on the server that will function as the VPN server prior to the installation of RRAS; otherwise, SSTP will not be available.
- The SSL certificate subject name and the host name that external clients use to connect to the VPN server must match, and the client running Windows 7 or Windows Vista SP1 must trust the issuing CA.
- SSTP does not support tunneling through web proxies that require authentication.
- SSTP does not support site-to-site tunnels. (PPTP and L2TP, however, do.)

MORE INFO **SSTP**

For more information on SSTP, consult the following TechNet article: ***http://technet.microsoft.com/en-us/library/ff687819(WS.10).aspx*****.**

IKEv2

IKEv2 is a VPN protocol that is new to Windows 7 and Windows Server 2008 R2. This protocol is not present in previous versions of Windows, and clients running Windows 7 will be able to use this protocol only if the remote access server is running Windows Server 2008 R2. IKEv2 has the following properties:

- Supports IPv6.
- Has a VPN Reconnect feature.
- Supports EAP and computer certificates for client-side authentication. This includes the Microsoft: Protected EAP (PEAP), Microsoft: Secured Password (EAP-MSCHAP v2), and Microsoft Smart Card Or Other Certificate options in the user interface.
- IKEv2 does not support PAP, CHAP, or MS-CHAPv2 (without EAP) as authentication protocols. IKEv2 supports data origin authentication, data integrity, replay protection, and data confidentiality.
- IKEv2 uses UDP port 500.
- When you configure a new Windows 7 VPN connection with the default settings, the client will attempt to make an IKEv2 connection first.
- IKEv2 requires a client running Windows 7 and an RRAS server running Windows Server 2008 R2.

The benefit of using IKEv2 over other protocols is that it supports VPN Reconnect. When you connect to a VPN server using the PPTP, L2TP/IPsec, or SSTP protocol and you suffer a network disruption, you can lose your VPN connection and need to restart it. This often involves reentering your authentication credentials. If you are transferring a file, downloading email, or sending a print job, and something interrupts your connection, you need to start over from the beginning. VPN Reconnect allows clients running Windows 7 to reconnect automatically to a disrupted VPN session even if the disruption has lasted for up to 8 hours.

VPN Reconnect uses the IKEv2 tunneling protocol with the *.mobike* extension. The *.mobike* extension allows VPN clients to change their Internet addresses without having to renegotiate authentication with the VPN server. For example, a user might be using a VPN connection to his corporate network while connected to a wireless network at an airport coffee shop. As the time of his flight's departure approaches, he moves from the coffee shop to the airport lounge, which has its own Wi-Fi network. With VPN Reconnect, the user's VPN connection is reestablished automatically when he achieves Internet connectivity with the new network. With a traditional VPN solution, this user would have to reconnect manually once he connected to the new wireless network in the airport lounge, and any existing operations occurring across the VPN would be lost. Unlike DirectAccess, which only some editions of Windows 7 support, all editions of Windows 7 support IKEv2 with VPN Reconnect.

MORE INFO **IKEV2**

For more information on setting up IKEv2 VPNs, consult the following TechNet article: ***http://technet.microsoft.com/en-us/library/ff687731(WS.10).aspx.***

✓ **Quick Check**

- **Which clients support SSTP?**

Quick Check Answer

- **Clients running Windows Vista SP1 and Windows 7 support SSTP.**

DirectAccess

DirectAccess is an always-on, IPv6, IPsec VPN connection. If a properly configured computer is able to connect to the Internet, DirectAccess automatically connects that computer to a properly configured corporate network. DirectAccess differs from the VPN solutions outlined earlier in the following ways:

- The connection process is automatic and does not require user intervention or logon. The DirectAccess connection process starts from the moment the computer connects to an active network. From the user's perspective, the computer always has access to the corporate intranet, whether she is sitting at her desk or when she has just connected to a Wi-Fi hotspot at a beachside cafe. Traditionally, users must initiate VPN connections to the corporate intranet manually.
- DirectAccess is bidirectional, with servers on the intranet being able to interact with the client running Windows 7 in the same way that they would if the client was connected to the LAN. In many traditional VPN solutions, the client can access the intranet, but servers on the intranet cannot initiate communication with the client.
- DirectAccess provides administrators with greater flexibility in controlling which intranet resources are available to remote users and computers. Administrators can

integrate DirectAccess with NAP to ensure that remote clients remain up to date with virus definitions and software updates. Administrators can also apply connection security policies to isolate servers and hosts.

The DirectAccess process is automatic. It requires no intervention on the part of the person who is logging on to the computer running Windows 7. A portable computer that is taken home and connected to a home Internet network can still receive software and Group Policy updates from servers on the corporate network even if the user has not logged on. Clients running Windows 7 use the following process to establish a DirectAccess connection:

1. The client running Windows 7 configured with DirectAccess connects a network. This occurs prior to user logon when the client running Windows 7 first connects to the network.
2. During the network identification phase, whenever a computer running Windows 7 detects that it is connecting to a new network or resuming a connection to an existing network, the client attempts to connect to a specially configured intranet website. An administrator specifies this website address when configuring DirectAccess on the DirectAccess server. If the client can contact the website, Windows 7 concludes that it has connected to the corporate network and no further action is necessary.
3. If the client running Windows 7 is unable to contact the specially configured intranet website, the client attempts to determine whether a native IPv6 network is present. If a native IPv6 network is present and the client has been assigned a public IPv6 address, DirectAccess makes a direct connection to the DirectAccess server across the Internet.
4. If a native IPv6 network is not present, Windows 7 attempts to establish an IPv6 over IPv4 tunnel using first the 6to4 and then the Teredo transition technologies.
5. If the client running Windows 7 cannot establish a Teredo or 6to4 connection due to an intervening firewall or proxy server, the client running Windows 7 attempts to connect using IP-HTTPS. IP-HTTPS encapsulates IPv6 traffic over an HTTPS connection. IP-HTTPS is likely to work because few firewalls that allow connections to the Internet block traffic on TCP port 443.
6. The DirectAccess IPsec session is established when the client running Windows 7 and the DirectAccess server authenticate with each other using computer certificates. DirectAccess supports only certificate-based authentication.
7. The DirectAccess server checks the appropriate AD DS group to verify that the computer and user have authorization to connect using DirectAccess.
8. The DirectAccess client now has access to appropriately configured resources on the corporate network.

Table 9-1 summarizes DirectAccess client configurations and the corresponding method of communicating using IPv6 with the DirectAccess server. When you configure the DirectAccess server, you configure it to support all these different connection methods. You do this because you cannot be certain of what conditions exist on the remote network from which the DirectAccess client is attempting to connect. IP-HTTPS is tried last because it provides a poorer performance compared to the other connection methods.

TABLE 9-1 DirectAccess Connection Methods

CLIENT NETWORK CONNECTION	DIRECTACCESS CONNECTION METHOD
Public IPv6 Address	Public IPv6 Address
Public IPv4 Address	6to4
Private (NAT) IPv4 Address	Teredo
Client unable to connect through firewall, but is connected to the Internet	IP-HTTPS

Only domain-joined clients running Windows 7 Enterprise and Ultimate editions support DirectAccess. You cannot use DirectAccess with other editions of Windows 7 or earlier versions of Windows, such as Windows Vista or Windows XP. When configuring a client for DirectAccess, you must add the client's domain computer account to a special security group. You specify this security group when running the DirectAccess wizard on the DirectAccess server.

Clients receive their DirectAccess configuration through Group Policy. This differs from traditional VPN configuration, where connections are configured manually or distributed through the Connection Manager Administration Kit (CMAK). Once you have added the computer's client account to the designated security group, you need to install a computer certificate on the client for the purpose of DirectAccess authentication. An organization needs to deploy Active Directory Certificate Services (AD CS) so that clients can enroll automatically with the appropriate certificates.

You configure DirectAccess primarily by configuring the DirectAccess server. When you configure the DirectAccess server, you also end up configuring the necessary Group Policy objects (GPOs) that support DirectAccess. Prior to installing DirectAccess, you should ensure that the DirectAccess server meets the following requirements:

- The computer needs to have Windows Server 2008 R2 installed and be a member of a domain.
- This server must have two network adapters.
- One of these network adapters needs to have a direct connection to the Internet. You must assign this adapter two consecutive public IPv4 addresses.
- The second network adapter needs a direct connection to the corporate intranet.
- The computer needs digital certificates to support server authentication. This includes having a computer certificate that matches the fully qualified domain name (FQDN) that is assigned to the IP addresses on the DirectAccess server's external network interface.

You should also create at least one global security group in AD DS that you use with DirectAccess. You can give this group any name that you like, although it is easier to keep track of it if you give it a DirectAccess-related name. It is possible to create and specify multiple DirectAccess-related security groups if necessary. You create multiple groups when you need to differentiate access to segments of the corporate intranet.

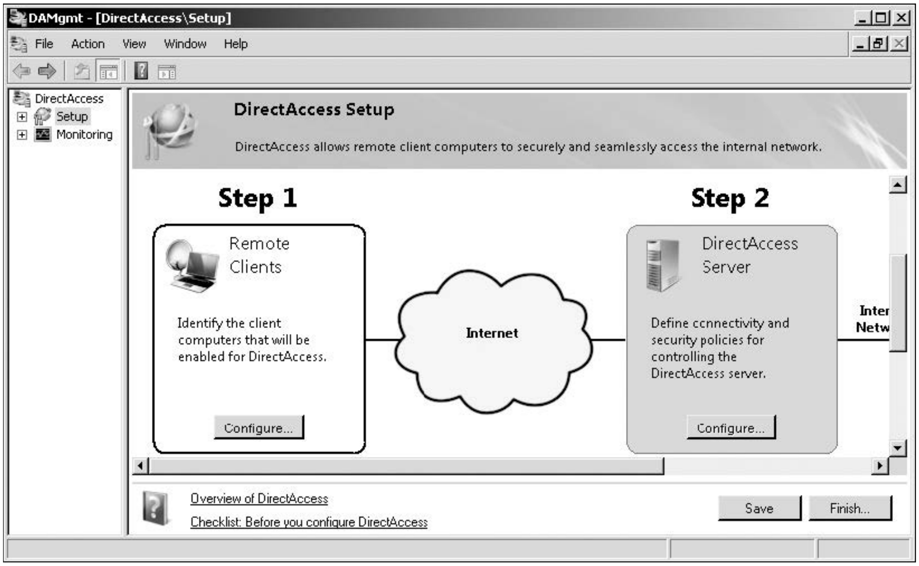
To install DirectAccess on a server running Windows Server 2008 R2, add the DirectAccess Management Console feature using the Add Features Wizard or the following PowerShell command:

```
Add-WindowsFeature DAMC
```

Installing the DirectAccess Management console allows you to configure and manage DirectAccess features. Installing the DirectAccess Management console also requires that you add the Group Policy Management feature. The Group Policy Management feature is necessary because the DirectAccess setup wizard creates DirectAccess-related GPOs that configure DirectAccess clients. You need to run the DirectAccess Setup wizard with a user account that has permission to create and apply GPOs in the domain.

After you have installed the DirectAccess Management console, you can configure the DirectAccess server. To do this, perform the following steps:

1. Open the DirectAccess Management console from the Administrative Tools menu on the computer running Windows Server 2008 R2. This console is shown in Figure 9-4.



DirectAccess allows remote client computers to securely and seamlessly access the internal network.

Identify the client computers that will be enabled for DirectAccess.

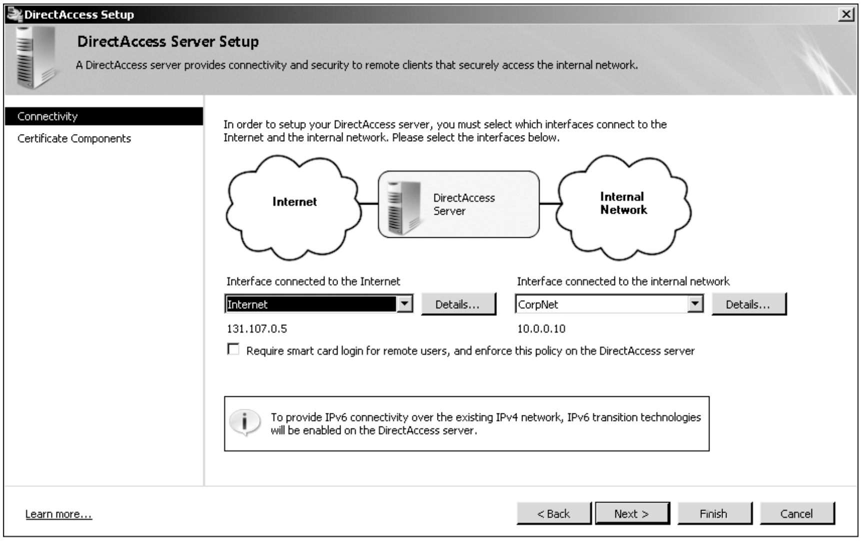
Define connectivity and security policies for controlling the DirectAccess server.

FIGURE 9-4 DirectAccess Management console

2. Select the Setup node. In the details pane, in the Remote Clients area, click Configure. This opens the DirectAccess Client Setup dialog box. Click Add and then specify the name of the security groups to which you add computer accounts when you want to

grant access to DirectAccess to specific clients running Windows 7. These groups can have any names.

3. Use the DirectAccess Server Setup item to specify which interface is connected to the Internet and which interface is connected to the internal network. Performing this step will enable IPv6 transition technologies on the DirectAccess server, as shown in Figure 9-5. You use this item to specify the CA that client certificates must ultimately come from, either directly or through a subordinate CA. You also must specify the server certificate used to secure IP-HTTPS traffic.



DirectAccess Setup

DirectAccess Server Setup

A DirectAccess server provides connectivity and security to remote clients that securely access the internal network.

- Connectivity
- Certificate Components

In order to setup your DirectAccess server, you must select which interfaces connect to the Internet and the internal network. Please select the interfaces below.

Interface connected to the Internet: Internet ▼ Details...
131.107.0.5

Interface connected to the internal network: CorpNet ▼ Details...
10.0.0.10

□ Require smart card login for remote users, and enforce this policy on the DirectAccess server

To provide IPv6 connectivity over the existing IPv4 network, IPv6 transition technologies will be enabled on the DirectAccess server.

FIGURE 9-5 DirectAccess Server Setup

4. On the Infrastructure Server Setup page, you specify the location of the internal website (known as the Network Location Server) that DirectAccess clients attempt to contact to determine whether they are connected to the corporate intranet or a remote location. You must ensure that you secure this website with a web server certificate. You also use this dialog box to specify which DNS servers and domain controllers the DirectAccess clients are able to contact for authentication purposes.

5. The final step involves specifying which resources on the corporate intranet are accessible to DirectAccess clients. The default setting is to allow access to all resources. In more secure environments, it is possible to use isolation policies to limit the contact to the membership of specific security groups. For example, you might create a security group and add the computer accounts of some file servers and mail servers, but not others.

6. When you click Finish, DirectAccess interfaces with a domain controller and creates two new GPOs in the domain. The first of these is targeted at the security groups that contain the computer accounts of DirectAccess clients. The second GPO is targeted at the DirectAccess server itself.

DirectAccess relies upon several other components in a Windows Server 2008 R2 network infrastructure. The domain in which you install the DirectAccess server must also have the following:

- At least one domain controller running Windows Server 2008 R2 and a DNS server on the internal network
- A server running Windows Server 2008 or later with AD CS installed, either as an Enterprise Root CA or an Enterprise Subordinate CA

To make internal network resources available to remote DirectAccess clients, you need to do one of the following:

- Ensure that all internal resources that will be accessed by DirectAccess support IPv6.
- Deploy ISATAP on the intranet, which allows intranet servers and applications to be reached by tunneling IPv6 traffic over an IPv4 intranet.
- Deploy a NAT-PT device, which allows hosts that support only IPv4 addresses to be accessible to DirectAccess clients using IPv6.

All application servers that DirectAccess clients access need to allow ICMPv6 traffic in Windows Firewall with Advanced Security (WFAS). You can accomplish this by enabling the following firewall rules using Group Policy:

- Echo Request – ICMPv6-in
- Echo Request – ICMPv6-out

The following ports on an organization's external firewall must be open to support DirectAccess:

- **UDP port 3544** Enables Teredo traffic
- **IPv4 protocol 41** Enables 6to4 traffic
- **TCP port 443** Allows IP-HTTPS traffic
- **ICMPv6 and IPv4 protocol 50** Required when remote clients have IPv6 addresses

> ***MORE INFO*** **DIRECTACCESS**
>
> **To learn more about DirectAccess, consult the following TechNet article:** ***http://technet.microsoft.com/en-us/network/dd420463.aspx*****.**

NPS RADIUS Servers

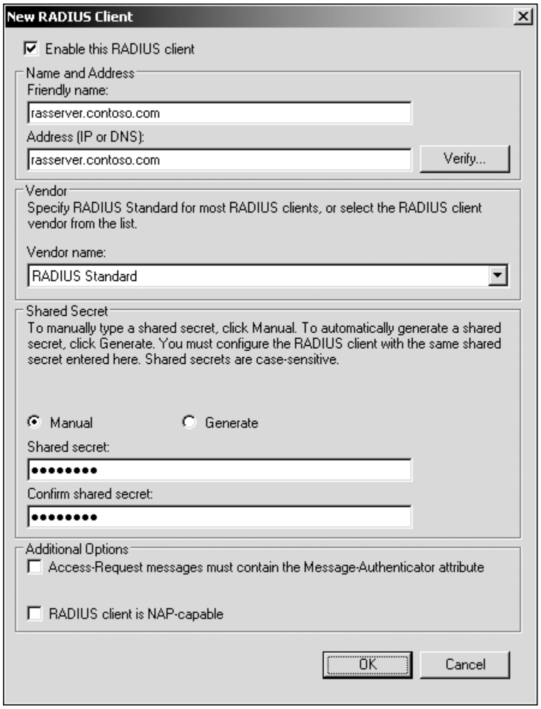
In addition to its ability to provide RRAS gateways, Network Policy Server (NPS) can function as a RADIUS server and as a RADIUS client, which also is known as a RADIUS proxy. When an organization has more than one remote access server, an administrator can configure a server that has NPS installed as a RADIUS server and then configure all remote access servers as RADIUS clients. The benefit of doing this is that network policy management is centralized rather than requiring management on a per-remote-access-server basis.

When RADIUS is used as an authentication provider for RAS servers, the connection request is sent in a RADIUS request message format to a RADIUS server. The RADIUS server performs the authentication and authorization and then passes this information back to the RAS server. The RADIUS server must be a member of an AD DS domain, but the RAS VPN server passing authentication requests to the RADIUS server can be a stand-alone computer.

NPS and RADIUS clients

RADIUS clients are network access servers such as VPN servers, wireless access points, and 802.1x authenticating switches. Although the computers that access these network access servers are called *remote access clients*, they are not considered RADIUS clients. RADIUS clients provide network access to other hosts.

To configure a RADIUS client using NPS, open the Network Policy Server console from the Administrative Tools menu. Right-click RADIUS Clients and then click New RADIUS Client. This will open the dialog box shown in Figure 9-6.



New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: rasserver.contoso.com

Address (IP or DNS): rasserver.contoso.com

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

FIGURE 9-6 Configuring a new RADIUS client

Configuration involves providing the following information:

- Friendly Name
- Address (IP or DNS)
- Vendor Name (with more than 20 separate vendors available in this drop-down menu)
- Shared Secret (configured using the NPS snap-in on the RADIUS client)

MORE INFO **RADIUS CLIENTS**

For more information about configuring RADIUS clients, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/cc754033.aspx*.

NPS as a RADIUS Proxy

RADIUS proxies route RADIUS messages between remote access servers configured as RADIUS clients and the RADIUS servers that perform authentication, authorization, and accounting. When configured as a RADIUS proxy, an NPS will record information in the accounting log about the messages that it passes on from RAS clients to the RADIUS servers. NPS functions as a RADIUS client when it is configured as a RADIUS proxy.

You should deploy NPS as a RADIUS proxy when you need to provide authentication and authorization for accounts from other AD DS forests. The NPS RADIUS proxy uses the realm name (which identifies the location of the user account) portion of a user name to forward the request to a RADIUS server in the target forest. This allows connection attempts for user accounts in one forest to be authenticated for the network access server in another forest. Using a RADIUS proxy for inter-forest authentication is not necessary when both forests are running at the Windows Server 2003 functional level or higher and a forest trust exists.

You should also deploy NPS as a RADIUS proxy when you need authentication and authorization to occur against a database other than the Windows account database. Connection requests that match a specific realm name are forwarded to a RADIUS server, often running on a platform other than Windows, that accesses a separate database of user accounts and authorization data. Hence, you would deploy NPS as a RADIUS proxy when authentication and authorization have to occur against a RADIUS server that uses Novell Directory Services or one that runs on UNIX.

A final reason to consider the deployment of NPS as a RADIUS proxy server is when you need to process a large number of connection requests between RAS RADIUS clients and RADIUS servers. An NPS RADIUS proxy can load balance traffic across multiple RADIUS servers—something that is difficult to configure when dealing with just RADIUS clients and RADIUS servers.

MORE INFO **RADIUS PROXIES**

To learn more about RADIUS proxies, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/cc731320.aspx*.

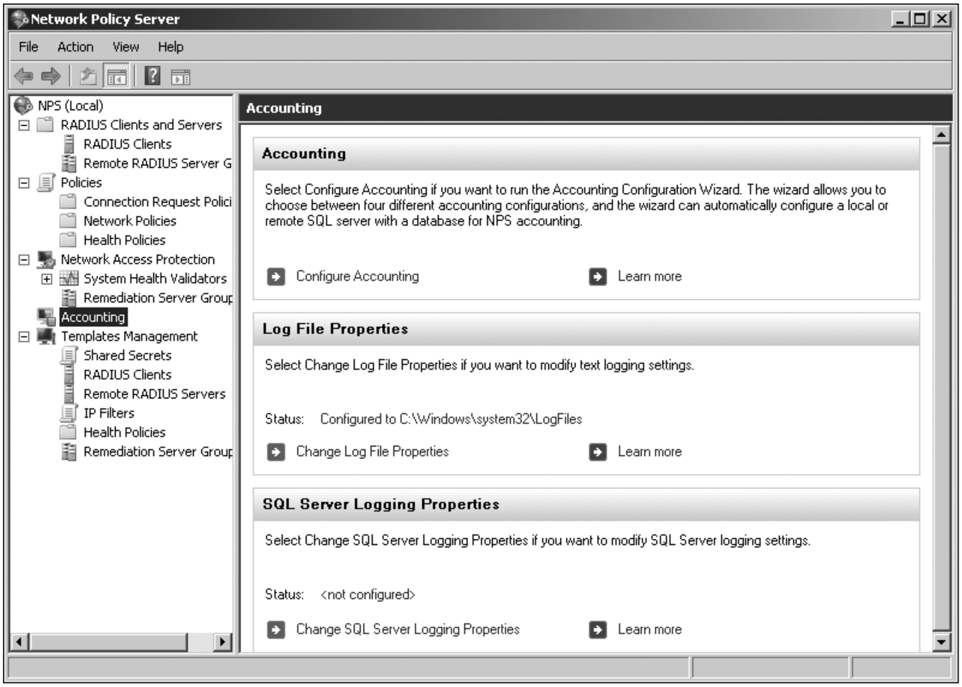
Remote Access Accounting

You can configure NPS to perform RADIUS accounting. RADIUS accounting allows you to keep track of who is connecting and who has failed to connect to your RADIUS infrastructure. You can use NPS accounting to monitor the following information:

- User authentication requests
- Access-Accept messages

- Access-Reject messages
- Accounting requests and responses
- Periodic status updates

As Figure 9-7 shows, you have two separate ways of recording log data. Logs can be stored locally or written to a database in Microsoft SQL Server 2005 SP1, SQL Server 2008, or SQL Server 2008 R2. Locally written logs are suitable if you have a small number of remote access clients. If you have a significant number of remote access clients, writing data to a SQL Server database will provide you with a much better way of managing what is likely to be a mountain of information.



Accounting

Select Configure Accounting if you want to run the Accounting Configuration Wizard. The wizard allows you to choose between four different accounting configurations, and the wizard can automatically configure a local or remote SQL server with a database for NPS accounting.

Log File Properties

Select Change Log File Properties if you want to modify text logging settings.

Status: Configured to C:\Windows\system32\LogFiles

SQL Server Logging Properties

Select Change SQL Server Logging Properties if you want to modify SQL Server logging settings.

Status: <not configured>

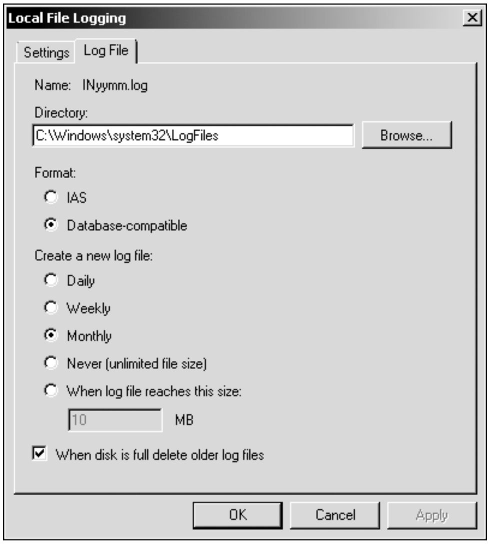
FIGURE 9-7 The Accounting node of the NPS console

Local File Logging

NPS log files can be written in two formats: IAS and database-compatible. The default format is database-compatible. The frequency at which new log files are created should be adjusted to suit your organization's needs. The benefit of having a single file of unlimited size is that locating a specific event is simpler, because you have to search for only one log file. The drawback of larger log files is that on systems where a log of NPS accounting data is logged, the log files can become huge, making the process of opening them and searching them difficult.

Although logs are written by default to the %Systemroot%/System32/LogFiles folder, Microsoft recommends that you keep log files on a partition separate from the operating system and application or file share data. Log files, unless strictly monitored, have a way of filling all available disk space. If this happens on a critical partition, the server could become unavailable. It is very important to note that NPS accounting data logs are not deleted automatically. You can configure the log retention policy to ensure that older log files are deleted automatically when the disk is full. This works best when log files are written to an isolated partition, so that the only impact of a disk that is full of NPS log files is on the storage of existing NPS log files. If NPS log files must be stored on a partition with other data or on the same volume as the operating system, you should consider writing a script that automatically removes logs when they reach a certain age.

Log files can be written to remote shares. This is done by specifying the UNC path of the share. If you configure this option, it will be necessary to ensure that the share permissions are configured to allow the account that writes the logs to write data to the shared folder. The Log File tab of the Local File Logging properties dialog box is shown in Figure 9-8.



Name: INyymm.log

Directory: C:\Windows\system32\LogFiles

Format:
○ IAS
● Database-compatible

Create a new log file:
○ Daily
○ Weekly
● Monthly
○ Never (unlimited file size)
○ When log file reaches this size:
10 MB

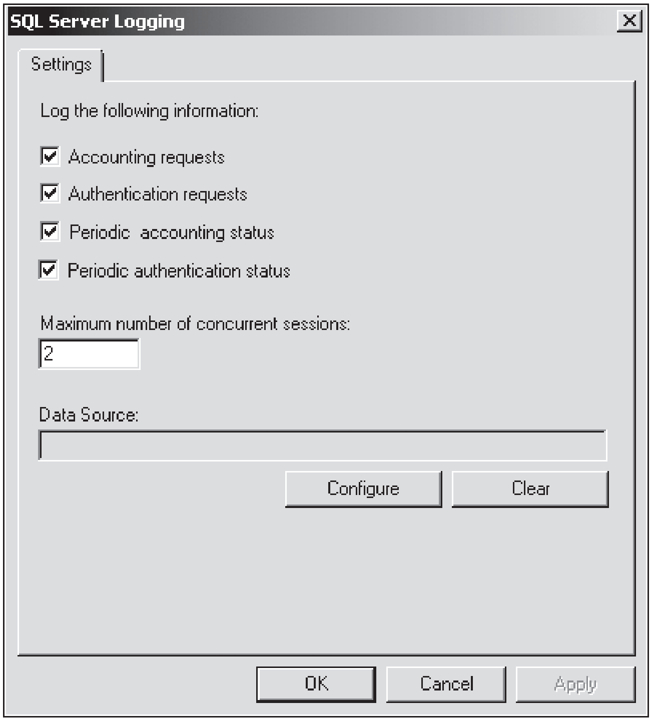
☑ When disk is full delete older log files

FIGURE 9-8 Configure local NPS logging

Configure SQL Server Logging

The alternative to logging NPS accounting data locally is to have it written to a computer running SQL Server that is installed either locally or on the local network. NPS sends data to the *report_event* stored procedure on the target computer running SQL Server. This stored procedure is available on SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.

You can configure which NPS accounting data is sent to the computer running SQL Server by selecting options in the SQL Server Logging properties dialog box shown in Figure 9-9. Clicking Configure in this dialog box allows you to specify the properties of the data link to the computer running SQL Server. When configuring the data link properties for the SQL Server connection, you must provide the server name, the method of authentication that will be used with the computer running SQL Server, and the database on the computer running SQL Server that you will use to store the accounting data. Just as it is a good idea to have a separate partition on a computer to store NPS accounting data, it is a good idea to have a separate database that stores NPS accounting data.



SQL Server Logging

Settings

Log the following information:

☑ Accounting requests

☑ Authentication requests

☑ Periodic accounting status

☑ Periodic authentication status

Maximum number of concurrent sessions:
2

Data Source:

FIGURE 9-9 Configure NPS logging to SQL Server

MORE INFO **NPS CHANGES IN WINDOWS SERVER 2008 R2**

For more information about the changes to NPS in Windows Server 2008 R2, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd365355(WS.10).aspx.*

Remote Desktop Gateway Servers

Remote Desktop Gateway (RD Gateway) servers allow Remote Desktop Protocol (RDP) over HTTPS connections to RDP servers located on protected internal networks to clients on the Internet. This functionality allows clients on the Internet to access RemoteApp applications, standard Remote Desktop Server sessions, and remote desktop sessions to appropriately configured clients.

NOTE **TERMINOLOGY CHANGE**

On computers running Windows Server 2008, Remote Desktop Services is called *Terminal Services* and RD Gateway is referred to as *TS Gateway*.

An advantage of RD Gateway is that you do not need to set up RAS VPNs to grant access to resources. Instead of having to deploy client connection kits to everyone in the organization that needs to be able to access resources from the Internet side of the firewall, you can email them an RDP shortcut file and allow them to connect with their clients running Windows XP SP2, Windows Vista, or Windows 7. RD Gateway is essentially an SSL VPN that is restricted to RDP. With a regular VPN connection, you can access all resources directly once connected (in theory, anyway). For example, a VPN can be used to connect to internal file shares and shared printers. With RD Gateway, you can access an RDS server or remote desktop session and, through that, access resources such as shared drives and printers.

Follow these steps to configure an RD Gateway server:

1. Install the RD Gateway Role Service on a computer running Windows Server 2008 R2 that is located on a screened subnet. The perimeter firewall should be configured so that the RD Gateway server is accessible on port 443.
2. Obtain an SSL certificate. The certificate name must match the name that clients use to connect to the server. Install the certificate on the server and then use the RD Gateway Manager console to map the server certificate. It is important that you only use RD Gateway Manager to map the SSL certificate. If you use another method, the RD Gateway server will not function properly.
3. Configure Remote Desktop Connection Authorization Policies (RD-CAPs) and Remote Desktop Resource Authorization Policies (RD-RAPs). (These are covered in the next section.)

MORE INFO **RD GATEWAY CONFIGURATION**

To learn more about configuring RD Gateway, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/cc772479.aspx*.

Connection Authorization Policies

Remote Desktop Connection Authorization Policies (RD-CAPs) specify which users are allowed to connect through the RD Gateway server to resources located on your organization's internal network. This is usually done by specifying a local group on the RD Gateway server or a group within AD DS. Groups can include user or computer accounts. You can also use RD-CAPs to specify whether remote clients use password or smart-card authentication to access internal network resources through the RD Gateway server. You can use RD-CAPs in conjunction with NAP; this scenario is covered in more detail in Lesson 2, "Firewalls and Network Access Protection."

Resource Authorization Policies

Remote Desktop Resource Authorization Policies (RD-RAPs) are used to determine the specific resources on an organization's network that an incoming RD Gateway client can connect to. When you create an RD-RAP, you specify a group of computers that you want to grant access to and the group of users that you will allow this access to. For example, you could create a group of computers called AccountsComputers that will be accessible to members of the Accountants user group. To be granted access to internal resources, a remote user must meet the conditions of at least one RD-CAP and at least one RD-RAP.

Lesson Summary

- SSTP piggybacks PPP over HTTPS. The SSL certificate installed on the RAS server must match the host name that the SSTP client is connecting to. SSTP can be used only by clients running Windows 7 and Windows Vista SP1. SSTP cannot be used for site-to-site tunnels.
- IKEv2 VPNs can be used only by clients running Windows 7 that are connected to VPN servers running Windows Server 2008 R2. IKEv2 VPNs support the VPN Reconnect feature.
- DirectAccess is an always-on IPv6 remote access technology. DirectAccess is supported only on Windows 7 Enterprise and Ultimate editions and requires a DirectAccess server running Windows Server 2008 R2.
- NPS servers can be configured to write accounting data to local log files or to computers running SQL Server that have the *report_event* stored procedure available.
- RADIUS proxies are a useful way of load balancing requests from RAS servers to RADIUS servers.
- RD Gateway servers provide another method of remote access, allowing clients running Windows Vista to connect to RDP servers using port 443.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Managing Remote Access." The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE*** **ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.**

1. Which of the following VPN protocols would you deploy if your firewall blocked all traffic from the Internet except traffic on TCP ports 25, 80, and 443?

   A. L2TP/IPsec

   B. SSTP

C. PPTP

D. IKEv2

2. Users at your organization have all been issued laptops running Windows 7 Enterprise edition. These users often need to place their computers into hibernation and do not want to have to reauthenticate to access their VPN connection when they resume using them. Which of the following VPN protocols allows users to reconnect to a VPN session that they initiated in the last few hours when they resume from hibernation?

   A. L2TP/IPsec

   B. SSTP

   C. PPTP

   D. IKEv2

3. Which of the following clients can connect to your organization's VPN server running Windows Server 2008 R2 if the only ports that are available for VPN connections are ports 25, 80, and 443? (Each answer is a complete solution. Choose all that apply.)

   A. Windows Vista with SP1

   B. Windows 7

   C. Windows XP Professional with SP3

   D. Microsoft Windows 2000 Professional with SP2

4. Servers VPN1, VPN2, and VPN3 host the RAS server role and accept incoming VPN connections from clients on the Internet. Server NPS1 is configured as a RADIUS server using the NPS server role. Servers VPN1, VPN2, and VPN3 use NPS1 to authenticate incoming connections. Server SQL1 is a computer running Windows Server 2008 R2 that has SQL Server 2008 R2 installed. You want to improve your ability to search through RADIUS accounting data. Which of the following strategies should you pursue?

   A. Configure VPN1, VPN2, and VPN3 so that NPS accounting data is forwarded to SQL1.

   B. Configure VPN1, VPN2, and VPN3 so that NPS accounting data is forwarded to NPS1.

   C. Configure SQL1 so that NPS accounting data is forwarded to server NPS1.

   D. Configure NPS1 so that NPS accounting data is forwarded to server SQL1.

5. Computers running which of the following operating systems are able to use DirectAccess to access your organization's internal network from locations on the Internet?

   A. Windows XP Professional with SP3

   B. Windows Vista Enterprise edition

   C. Windows 7 Enterprise edition

   D. Windows 7 Home Premium edition

Lesson 2: Firewalls and Network Access Protection

You deploy NAP on your network as a method of ensuring that computers accessing important resources meet certain client health benchmarks. These benchmarks include (but are not limited to) having the most recent updates applied, having antivirus and anti-spyware software up to date, and having important security technologies such as Windows Firewall configured and functional. In this lesson, you will learn how to plan and deploy an appropriate NAP infrastructure and enforcement method for your organization.

After this lesson, you will be able to:

- Plan NAP server roles.
- Monitor and maintain NAP policies.

Estimated lesson time: 60 minutes

Windows Firewall with Advanced Security

The simplest method of enforcing a standardized firewall configuration across an organization is to use Group Policy. You can configure inbound and outbound rules, as well as enable and disable Windows Firewall with Advanced Security for specific profiles, through the Computer Configuration/Policies/Windows Settings/Windows Firewall With Advance Security node of Group Policy.

You can configure new rules based on a specific program, port, or predefined rule. Rules can be applied to inbound and outbound traffic. In many domain environments, administrators use outbound rules as a way of blocking the use of specific programs such as file sharing or instant messaging programs. Although the best way to block this sort of traffic is to stop the software from being installed in the first place or restricting its use with AppLocker policies, many domain environments have users with laptops that are taken on and off the network. In some cases, laptop users are given local administrative control over their computers. Applying firewall rules to each computer through Group Policy allows administrators to block programs that may use SSL tunnels to get around perimeter firewall configuration.

MORE INFO **CONFIGURE WINDOWS FIREWALL THROUGH GROUP POLICY**

To learn more about configuring Windows Firewall with Advanced Security through Group Policy, consult the following TechNet article*: http://technet.microsoft.com/en-us/library/ff602918(WS.10).aspx*.

Domain Isolation

Windows Firewall with Advanced Security can be used to create connection security rules that secure traffic by using IPsec. Domain isolation uses an AD DS domain, domain membership, and Windows Firewall with Advanced Security Group Policy settings to enforce a policy that forces domain member computers to accept incoming communication requests only from other computers that are members of the same domain. When enforced, computers that are members of the domain are isolated from computers that are not members of the domain. It is important to remember that in domain isolation scenarios, isolated computers can initiate communication with hosts outside the domain, such as web servers on the Internet. However, they will not respond when network communication is initiated from a host outside the domain.

Domain isolation policies are applied through the Computer Configuration/Policies/ Windows Settings/Security Settings/Windows Firewall with Advanced Security node of a GPO by accessing the Connection Security Rules item.

MORE INFO **DOMAIN ISOLATION**

To learn more about domain isolation, consult the following TechNet article: ***http://technet.microsoft.com/en-us/library/cc730709(WS.10).aspx.***

Server Isolation

Server isolation works in a similar way to domain isolation except that instead of applying to all computers within a domain, a server isolation policy applies only to a specific set of servers in a domain. You do this by placing the computer accounts of the servers that will be isolated in a specific OU and then applying a GPO that has an appropriately configured connection security rule to that OU. When enforced, only computers that are members of the domain are able to communicate with the isolated servers. This can be an effective way of protecting servers when you must grant network access to third-party computers. The third-party computers are able to access some network resources, such as intranet web and DNS servers, but you can isolate specific network resources, such as file servers and databases, by configuring server isolation policies.

MORE INFO **SERVER ISOLATION**

To learn more about domain isolation, consult the following TechNet article: ***http://technet.microsoft.com/en-ca/library/cc770626(WS.10).aspx.***

Forefront Threat Management Gateway

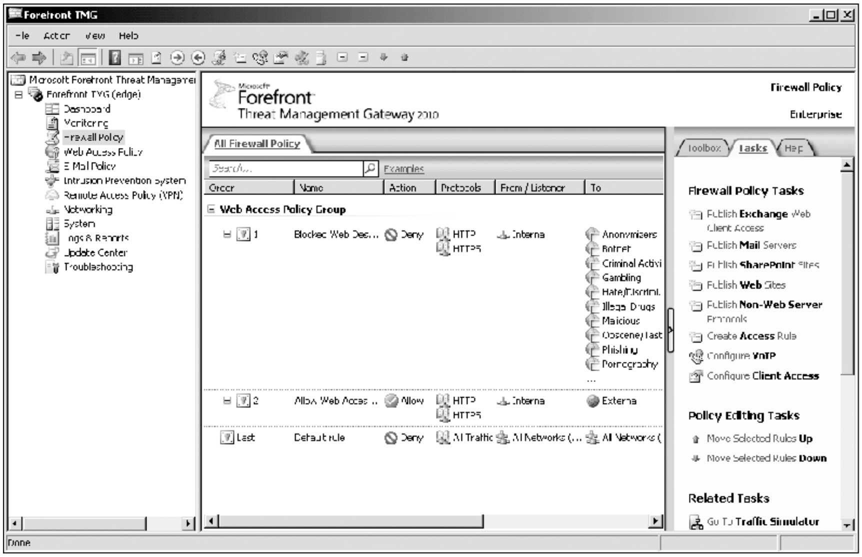
While Windows Firewall with Advanced Security is an appropriate solution to protect individual servers, you should look toward a more fully featured firewall, such as Microsoft Forefront Threat Management Gateway (TMG) 2010, as a solution between your organization's perimeter network and the Internet. Perimeter networks are networks that exist between the Internet and an organization's internal network. Organizations host resources that need to be available to the Internet on perimeter networks. This allows them to provide an external firewall to protect the resource and then also to provide a firewall between the perimeter network and the internal network as a second layer of protection. In most configurations, traffic can pass from the Internet to the perimeter network and back, or from the internal network to the perimeter network and back, but never directly from the internal network to the Internet without passing in some way across the perimeter network.

Forefront TMG 2010 includes the following advanced features:

- Packet inspection and application filtering
- Intrusion Prevention System (IPS)
- Secure proxy
- Web filtering based on URL or URL category (for example, filtering sports or entertainment websites)
- Web traffic monitoring
- HTTPS inspection
- Publish reverse proxy services to the Internet, such as websites, Microsoft Outlook Web Access, and Microsoft SharePoint sites including SSL bridge functionality
- Create site-to-site VPNs
- The ability to publish VPN servers to the Internet

You can install Forefront TMG 2010 on computers running Windows Server 2008 with SP2 or Windows Server 2008 R2. When you install Forefront TMG 2010, the installation routine automatically installs the Network Policy Server, RRAS, and Active Directory Lightweight Directory Services (AD LDS) roles and role services.

Usually, you would install Forefront TMG on a computer that has two network cards, with one computer connected to the Internet and the other network adapter connected to your perimeter or internal network. It is possible to deploy Forefront TMG on a computer with a single network adapter, but in general, you would do this only when you have deployed an additional perimeter firewall solution. ForeFront TMG is the latest version of the product once known as Microsoft Internet Security and Acceleration (ISA) Server. You manage Forefront TMG using the Forefront TMG console, shown in Figure 9-10.



Order	Name	Action	Protocols	From / Listener	To
Web Access Policy Group					
1	Blocked Web Des...	Deny	HTTP HTTPS	Internal	Anonymizers Botnet Criminal Activi Gambling Hate/Discrimi. Illegal Drugs Malicious Obscene/Tast Phishing Pornography ...
2	Allow Web Acces...	Allow	HTTP HTTPS	Internal	External
Last	Default rule	Deny	All Traffic	All Networks (...	All Networks (

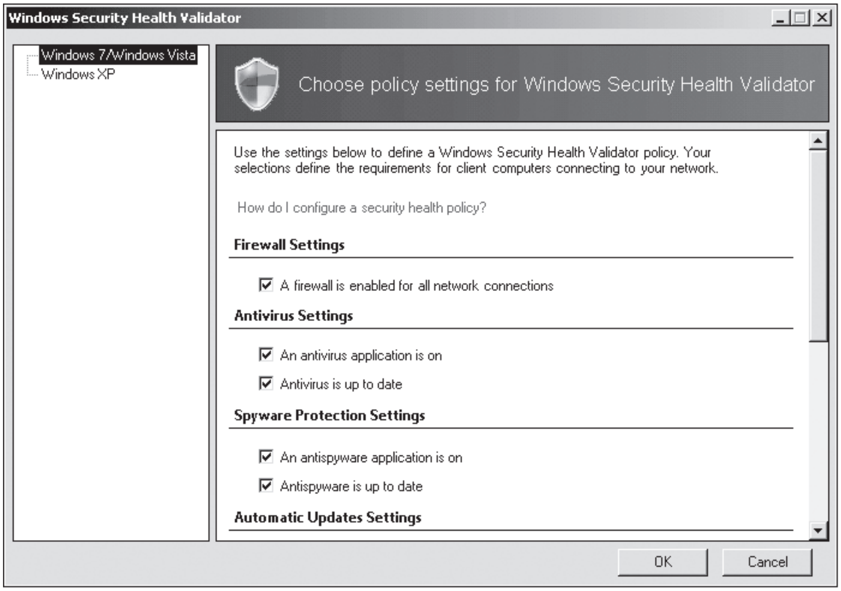
FIGURE 9-10 The Forefront TMG console

MORE INFO **FOREFRONT TMG 2010**

To learn more about Forefront TMG 2010, consult the following TechNet website: ***http://technet.microsoft.com/en-us/library/ff355324.aspx.***

Network Access Protection

Network Access Protection (NAP) is a technology that allows you to restrict network access on the basis of a client's health. System Health Agents (SHAs) and System Health Validators (SHVs) are the components that validate a computer's health against a configured set of benchmarks. The SHV specifies which benchmarks the client must meet. The SHA is the component against which those benchmarks are tested. The SHVs in Windows 7, Windows Vista, and Windows XP can be configured through the System Health Validators node under NAP in the NPS. Figure 9-11 shows the settings that you can configure for the SHV in Windows 7 and Windows Vista.



Windows Security Health Validator

Windows 7/Windows Vista
Windows XP

Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

How do I configure a security health policy?

Firewall Settings

☑ A firewall is enabled for all network connections

Antivirus Settings

☑ An antivirus application is on

☑ Antivirus is up to date

Spyware Protection Settings

☑ An antispyware application is on

☑ Antispyware is up to date

Automatic Updates Settings

FIGURE 9-11 An SHV in Windows 7 and Windows Vista

Third-party organizations can provide SHAs and SHVs that you can use with their own products and NAP. Deploying third-party SHAs and SHVs involves installing the SHA components on all clients and the SHV on the computer running Windows Server 2008 or Windows Server 2008 R2 that hosts the Network Policy Server server role. Once installed, you create a new health policy that uses the new SHV as a compliance benchmark. A health policy can call on multiple SHVs. For example, you might create a health policy that requires all conditions on the SHV on Windows 7 or Windows Vista and the Fabrikam SHV to be met before a client is granted access to all network resources.

MORE INFO **SHVS**

For more information about SHVs, consult the following article on TechNet: ***http://technet.microsoft.com/en-us/library/dd314150(WS.10).aspx.***

NAP Enforcement Methods

When a computer is found to be noncompliant with the enforced health policy, NAP enforces limited network access. This is done through an Enforcement Client (EC). Windows 7, Windows Vista, Windows XP SP3, Windows Server 2008, and Windows Server 2008 R2 include NAP EC support for IPsec, IEEE 802.1X, Remote Access VPN, and DHCP enforcement methods. Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008 R2 also support NAP enforcement for RD Gateway connections.

NAP enforcement methods can be used either individually or in conjunction with each other to limit the network access of computers that are found not to be in compliance with configured health policies. Hence, you can apply the remote access VPN and IPsec enforcement methods to ensure that internal clients and clients coming in from the Internet are granted access to resources only if they meet the appropriate client health benchmarks.

IPsec NAP Enforcement

IPsec enforcement works by applying IPsec rules. Only computers that meet health compliance requirements are able to communicate with each other. IPsec enforcement can be applied on a per-IP address, per-TCP port number, or per-UDP port number basis. For example: You can use IPsec enforcement to block RDP access to a web server so that only computers that are healthy can connect to manage that server but allow clients that do not meet health requirements to connect to view Web pages hosted by the same web server.

IPsec enforcement applies after computers have received a valid IP address, either from DHCP or through static configuration. IPsec is the strongest method of limiting network access communication through NAP. Where it might be possible to subvert other methods by applying static addresses or switching ports, the IPsec certificate used for encryption can be obtained by a host only when it passes the health check. No IPsec certificate means that communication with other hosts that encrypt their communications using a certificate issued from the same CA is impossible.

To deploy IPsec enforcement, a network environment must have a Windows Server 2008 or 2008 R2 Health Registration Authority (HRA) and a Windows Server 2008 or Windows Server 2008 R2 CA. Clients must be running Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, or Windows XP SP3, all of which include the IPsec EC.

MORE INFO **IPSEC ENFORCEMENT POLICIES**

To learn more about configuring policies for IPsec enforcement, consult the following TechNet page: ***http://technet.microsoft.com/en-us/library/cc771899.aspx.***

802.1X NAP Enforcement

802.1X enforcement uses authenticating Ethernet switches or IEEE 802.11 Wireless Access Points. These compliant switches and access points grant unlimited network access only to computers that meet the compliance requirement. Computers that do not meet the compliance requirement are limited in their communication by a restricted access profile. Restricted access profiles work by applying IP packet filters or virtual local area network (VLAN) identifiers. This means that hosts that have the restricted access profile are allowed only limited network communication. This limited network communication generally allows access to remediation servers. You will learn more about remediation servers later in this lesson.

An advantage of 802.1X enforcement is that the health status of clients is assessed constantly. Connected clients that become noncompliant will be placed under the restricted access profile automatically. Clients under the restricted access profile that become compliant will have that profile removed and will be able to communicate with other hosts on the network in an unrestricted manner. For example, suppose that a new antivirus update comes out. Clients that have not checked the update server recently are put under a restricted access profile until they check the server and retrieve the update. Once the check has been performed successfully, the clients are returned to full network access.

A computer running Windows Server 2008 or Windows Server 2008 R2 with the Network Policy Server role is necessary to support 802.1X NAP enforcement. It is also necessary to have switch or Wireless Access Point hardware that is 801.1X-compliant. Clients must be running Windows 7, Windows Vista, Windows Server 2008 R2, Windows Server 2008, or Windows XP SP3 because only these operating systems include the EAPHost EC.

MORE INFO **802.1X ENFORCEMENT**

To learn more about 802.1X enforcement, consult the following TechNet page: *http://technet.microsoft.com/en-us/library/cc770861.aspx*.

VPN NAP Enforcement

VPN enforcement is used on connecting VPN clients as a method of ensuring that clients granted access to the internal network meet system health compliance requirements. VPN enforcement works by restricting network access to noncompliant clients through the use of packet filters. Rather than being able to access the entire network, incoming VPN clients that are noncompliant have access only to the remediation server group.

As is the case with 802.1X enforcement, the health status of a connected client is monitored continuously. If a client becomes noncompliant, packet filters restricting network access will be applied. If a noncompliant client becomes compliant, packet filters restricting network access will be removed. VPN enforcement requires an existing remote access infrastructure and an NPS server. The enforcement method uses the VPN EC, which is included with Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

MORE INFO **VPN ENFORCEMENT**

To learn more about VPN enforcement, consult the following TechNet page: ***http://technet.microsoft.com/en-us/library/cc753622.aspx*.**

DHCP NAP Enforcement

DHCP NAP enforcement works by providing unlimited-access IPv4 address information to compliant computers and limited-access IPv4 address information to noncompliant computers. Unlike VPN and 802.1X enforcement methods, DHCP NAP enforcement is applied only when a client lease is obtained or renewed. Organizations using this method of NAP enforcement should avoid configuring long DHCP leases because this will reduce the frequency at which compliance checks are made.

To deploy DHCP NAP enforcement, you must use a DHCP server running Windows Server 2008 or Windows Server 2008 R2 because this includes the DHCP Enforcement Service (ES). The DHCP EC is included in the DHCP Client service on Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

The drawback of DHCP NAP enforcement is that you can get around it by configuring a client's IP address statically. Only users with local administrator access can configure a manual IP, but if your organization gives users local administrator access, DHCP NAP enforcement may not be the most effective method of keeping these computers off the network until they are compliant.

MORE INFO **DHCP ENFORCEMENT**

To learn more about DHCP enforcement, consult the following TechNet page: ***http://technet.microsoft.com/en-us/library/cc733020.aspx*.**

✓ Quick Check

1. **Which NAP enforcement method uses VLANs?**
2. **Which NAP enforcement methods can you get around by configuring a static IP address?**

Quick Check Answer

1. **The 802.1X NAP enforcement method uses VLANs.**
2. **You can get around the DHCP NAP enforcement method by configuring a static IP address.**

RD Gateway NAP Enforcement

RD Gateway NAP enforcement ensures that clients running Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008 R2 located on the Internet that are connecting to an RD Gateway meet health compliance requirements before the RD Gateway allows connections to RDP servers on the internal network. To configure RD Gateway for NAP, you must perform the following basic steps:

1. Enable NAP health policy checking on the RD Gateway server by configuring the RD Gateway server to request that clients send a statement of health.
2. Remove any existing RD-CAPs. It is not necessary to remove existing RD-RAPs.
3. Configure a Windows SHV on the RD Gateway server by editing the properties of the Windows SHV in the Network Policy Server console on the RD Gateway server.
4. Create NAP Policies on the RD Gateway server using the Configure NAP Wizard. You will need to create two health policies (one for compliant and one for noncompliant computers), a connection request policy, and three network policies (compliant, noncompliant, and non-NAP-capable).

MORE INFO **RD GATEWAY ENFORCEMENT**

For more information on using NAP with RD Gateway enforcement, consult the following TechNet page: *http://technet.microsoft.com/en-us/library/cc771213.aspx.*

DirectAccess NAP Enforcement

You can incorporate NAP into your DirectAccess infrastructure as a way of ensuring that clients that are attempting to connect using DirectAccess from remote networks will be successful only if they meet network health requirements. Using NAP with DirectAccess requires similar infrastructure to the NAP IPsec enforcement method. It is necessary to ensure that your organization has at least one HRA as well as CAs that are configured to support NAP, NAP health policy servers, and necessary remediation servers. If your remediation and HRA servers are on the Intranet, you'll need to perform the following steps:

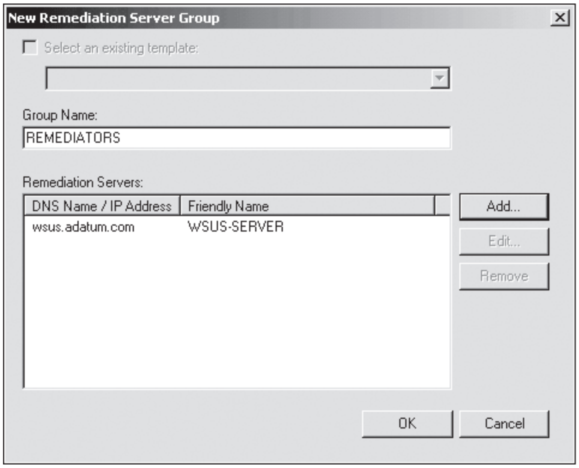
- Add the IPv6 addresses of the HRA and remediation servers to the list of management servers when running the DirectAccess Setup Wizard.
- Configure the intranet tunnel rule in the DirectAccess server GPO to require health certificates.

MORE INFO **DIRECTACCESS WITH NAP**

For more information on DirectAccess with NAP enforcement, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ff528477(WS.10).aspx.*

Remediation Servers

Remediation servers generally host software updates and antivirus and anti-spyware definition files and are used to bring a client that has not passed a health check up to date. Remediation servers are accessible from the restricted networks that noncompliant clients are relegated to when they do not pass system health checks. Remediation servers allow these clients to be brought into compliance so that they can have unrestricted access to the network. Remediation server groups are added through the Remediation Server Group node of the Network Policy Server console, as shown in Figure 9-12.



New Remediation Server Group

□ Select an existing template:

Group Name: REMEDIATORS

Remediation Servers:

DNS Name / IP Address	Friendly Name
wsus.adatum.com	WSUS-SERVER

FIGURE 9-12 Remediation Server Group node

Monitoring-Only Mode

While you usually use NAP to restrict access to noncompliant clients, when you deploy NAP for the first time, you should use NAP in monitoring-only mode. This is because when you start out, you are likely to have a large number of noncompliant clients and if you enforce NAP policies right at the start, a large number of the computers that you are responsible for managing will be unable to access the network. By using monitoring-only mode, you can get a good idea about how many clients in your organization do not comply with current health policies. You can then take steps to correct these problems on the clients so that when you do enforce NAP, only a small number of clients will be forced into remediation.

MORE INFO **NO ENFORCEMENT**

To learn more about configuring NAP for monitoring rather than enforcement, consult the following TechNet article: ***http://technet.microsoft.com/en-us/library/dd314142(WS.10).aspx.***

MORE INFO **HOST CREDENTIAL AUTHORIZATION PROTOCOL**

Host Credential Authorization Protocol (HCAP) allows the integration of NAP with Cisco's Network Admission Control technology. HCAP allows the NPS server running on Windows Server 2008 and Windows Server 2008 R2 to perform authorization for Cisco 802.1X access clients. To learn more about HCAP, consult the following TechNet page: ***http://technet.microsoft.com/en-us/library/cc732681.aspx.***

Lesson Summary

- An SHV is a set of conditions that a computer must meet to be considered healthy. An SHA is what the NPS server checks with to determine whether a connecting client meets all the conditions of the SHV.
- The four methods of NAP enforcement that can be applied to Windows Server 2008 R2, Windows Server 2008, Windows 7, Windows Vista, and Windows XP SP3 clients are IPsec, DHCP, VPN, and 802.1X enforcement. You can use RD Gateway NAP only with Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008 R2.
- NPS servers are installed as a part of the Network Policy And Access Services role. These servers are where you configure health policies and SHVs that dictate the health compliance benchmark.
- Domain isolation allows you to use IPsec to limit network communication to computers that are members of a specific domain.
- Forefront TMG 2010 is an advanced firewall application that can be installed on servers running Windows Server 2008 and Windows Server 2008 R2. It is often installed between a perimeter network and the Internet.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, “Firewalls and Network Access Protection.” The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE* ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the “Answers” section at the end of the book.**

1. You want only healthy computers on your network to be able to connect to a computer running Windows Server 2008 used as an intranet web server role for management tasks, but you want to allow all clients, healthy or unhealthy, to be able to access Web pages on the same servers. Which of the following NAP enforcement methods should you implement without having to configure the firewall or IP address restrictions on the intranet server running Windows Server 2008?

   A. IPsec

   B. 802.1X

   C. DHCP

   D. VPN

2. Your network contains a mixture of Windows Vista SP1 and Windows XP SP3 clients. You want to enable NAP enforcements for the clients running Windows Vista SP1. Clients running Windows XP SP3 should not be subjected to NAP enforcement. Which of

the following strategies should you pursue? (Each answer forms a part of the solution. Choose two.)

A. Create a network policy that specifies the operating system as a condition.

B. Create a VLAN for all clients running Windows XP.

C. Configure the network policy to allow computers running Windows Vista to bypass the health check.

D. Configure the network policy to allow computers running Windows XP to bypass the health check.

3. Your organization has one domain controller running Windows Server 2003, named 2K3DC, and one domain controller running Windows Server 2008, named 2K8DC. The domain functional level is Windows Server 2003. DNS is installed on a stand-alone computer named DNS1 running Windows Server 2003 R2. DHCP is installed on a stand-alone computer named DHCP1 running Windows Server 2003 R2. NPS is installed on a computer named NPS1 running Windows Server 2008. Which of the following computers must you upgrade if you want to use DHCP NAP enforcement?

A. 2K3DC

B. DNS1

C. DHCP1

D. NPS1

4. Which of the following server roles must be available on your network if you plan to configure IPsec rules so that only healthy computers can connect to each other? (Each answer forms a part of the solution. Choose two.)

A. HRA

B. Windows Server 2008 CA

C. Windows Server 2008 DHCP server

D. HCAP server

5. Other than 802.1X-compatible switches, which of the following components must be deployed in your network environment to support 802.1X NAP enforcement? (Choose two; each solution forms a complete answer.)

A. The NPS server role on a computer running Windows Server 2008

B. A RADIUS proxy server

C. EAPHost EC on clients

D. The HCAP server role on a computer running Windows Server 2008

PRACTICE Installing and Configuring NAP with DHCP Enforcement

In this set of practices, you will configure Windows Server 2008 R2 with the Network Policy Server role to support NAP with the DHCP.

EXERCISE 1 Network Policy Server Installation and DHCP Configuration

In this exercise, you will install the NPS server role on server VAN-DC1. To complete this practice, perform the following steps:

1. Log on to server VAN-DC1 with the Kim_Akers user account.
2. Open an elevated PowerShell session and issue the following commands to ensure that the DHCP and NPS role services, if installed, are removed from the server. If these roles are present, it will be necessary to reboot the server, log in, restart PowerShell, and import the ServerManager module again.

   ```
   Import-Module ServerManager
   Remove-WindowsFeature DHCP, NPAS
   ```

3. From the elevated PowerShell session, issue the following commands to install DHCP and the NPS server roles:

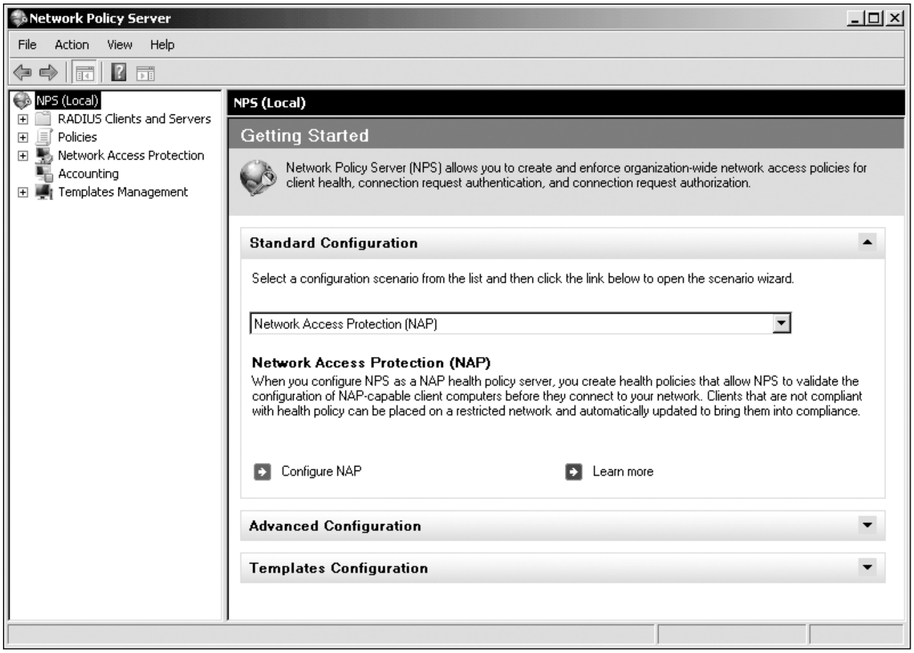
   ```
   Add-WindowsFeature DHCP, NPAS
   ```

4. From the Administrative Tools menu, click DHCP. The DHCP console will open. Right-click the DHCP node and then click Manage Authorized Servers. Click Authorize. In the Authorize DHCP Server dialog box, enter the name **VAN-DC1** and then click OK. Verify that the IP address of the DHCP server matches 10.10.0.10, and then click OK. Highlight VAN-DC and then click OK.
5. Open the Services console. Set the properties of the DHCP Server service to start automatically. Start the service.
6. In the DHCP console, expand the IPv4 node under van-dc.adatum.com and then delete the scope Alpha Scope.
7. Select and right-click the IPv4 node under van-dc.adatum.com, and then click New Scope. This will start the New Scope Wizard. Click Next.
8. On the Scope Name page, enter the scope name **NAP_Scope**. Click Next.
9. Set the start IP address as **10.100.0.1** and the end IP address as **10.100.0.254**. Set the Subnet Mask Length at **24**. Click Next three times.
10. On the Configure DHCP Options page, select the No, I Will Configure These Options Later option, and then click Next. Click Finish.

EXERCISE 2 Configure NPS

In this exercise, you will configure NPS. To complete this practice, perform the following steps:

1. From the Administrative Tools menu, click Network Policy Server. The Network Policy Server console will open.
2. On the Getting Started page, shown in Figure 9-13, click Configure NAP.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

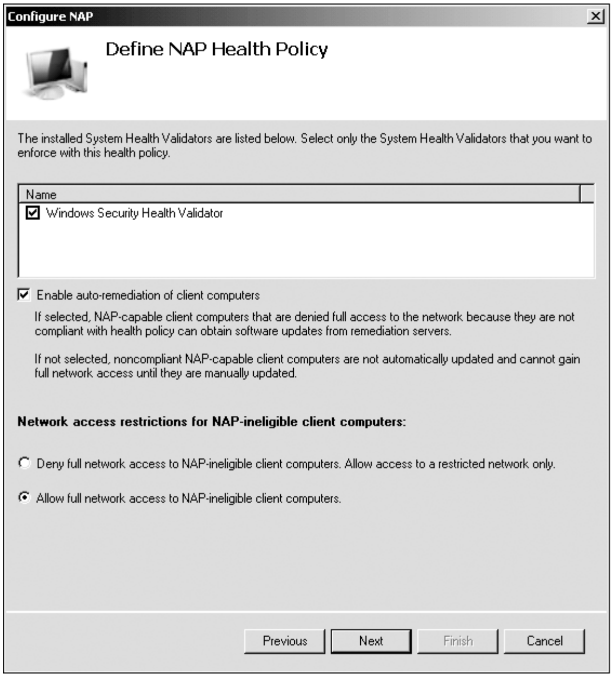
FIGURE 9-13 NPS NAP Getting Started page

3. On the Select Network Connection Method For Use With NAP page, use the drop-down menu to select Dynamic Host Configuration Protocol (DHCP), and then click Next.
4. On the RADIUS Clients page, click Next.
5. On the DHCP Scopes page, click Add. In the Specify The Profile Name That Identifies Your DHCP Scope box, type **NAP_Scope** and click OK. Click Next.
6. On the Configure Machine Groups page, click Next.
7. On the Specify A NAP Remediation Server Group And URL page, click Next.
8. On the Define NAP Health Policy page, clear the Enable Auto-Remediation Of Client Computers option and select Allow Full Network Access To NAP-Ineligible Client Computers, as shown in Figure 9-14. Click Next, and then click Finish.

EXERCISE 3 Configure SHV

In this exercise, you will configure an SHV to support your NAP DHCP deployment. To complete this practice, perform the following steps:

1. In the Network Policy Server console, navigate to the Network Access Protection/System Health Validators/Windows Security Health Validator/Settings node. In the details pane, right-click Default Configuration and then click Properties. This will open the Windows Security Health Validator dialog box.



Configure NAP

Define NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

Name
☑ Windows Security Health Validator

☑ Enable auto-remediation of client computers

If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.

If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

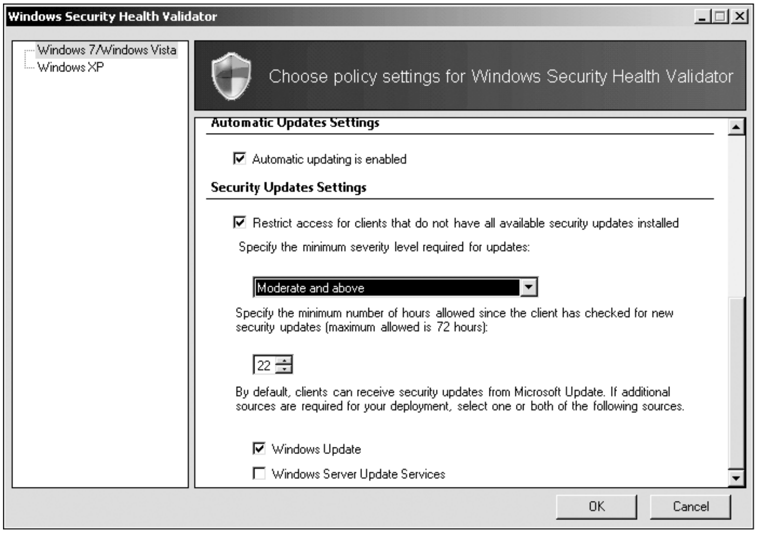
Network access restrictions for NAP-ineligible client computers:

○ Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.

● Allow full network access to NAP-ineligible client computers.

FIGURE 9-14 NAP Health Policy

2. In the details pane of the Windows Security Health Validator dialog box, scroll down to the Security Updates Settings section. Enable the Restrict Access For Clients That Do Not Have All Available Security Updates Installed option and change the severity level to Moderate And Above, as shown in Figure 9-15.



Windows Security Health Validator

Choose policy settings for Windows Security Health Validator

Automatic Updates Settings

☑ Automatic updating is enabled

Security Updates Settings

☑ Restrict access for clients that do not have all available security updates installed

Specify the minimum severity level required for updates:

Moderate and above

Specify the minimum number of hours allowed since the client has checked for new security updates (maximum allowed is 72 hours):

22

By default, clients can receive security updates from Microsoft Update. If additional sources are required for your deployment, select one or both of the following sources.

☑ Windows Update

☐ Windows Server Update Services

FIGURE 9-15 Configuring severity level

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenarios. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- VPN servers running Windows Server 2008 and Windows Server 2008 R2 support the PPTP, L2TP/IPsec, and SSTP protocols. SSTP can be used only by computers running Windows Vista or Windows 7.
- VPN servers running Windows Server 2008 R2 support IKEv2 VPNs. VPNs using IKEv2 support automatic reconnection, but they can be used only by computers running Windows 7.
- DirectAccess is an always-on IPv6 remote access solution. It requires a computer running Windows Server 2008 R2 and supports only clients running Windows 7 Enterprise and Ultimate editions.
- You can configure a computer running Windows Server 2008 or Windows Server 2008 R2 to function as a RADIUS server, RADIUS proxy, or RADIUS client.
- The four methods of local NAP enforcement are IPsec, DHCP, VPN, and 802.1X enforcement. You can also configure NAP enforcement for RD Gateway and DirectAccess.

Key Terms

The following terms were introduced in this chapter. Do you know what they mean?

- DirectAccess
- EAP-TLS
- IKEv2
- L2TP/IPsec
- PPP
- PPTP
- SSTP
- RADIUS
- VPN

Case Scenarios

In the following case scenarios, you will apply what you have learned about planning server installs and upgrades. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Remote Access at Wingtip Toys

Wingtip Toys has branch office locations in Sydney and Melbourne, Australia. The branch office firewalls are configured to let traffic from the Internet through only to hosts on the screened subnet on TCP ports 25, 80, and 443. An RD Gateway server has been installed on the screened subnet at the Sydney location. A multihomed computer running Windows Server 2008 R2 with the Remote Access role installed will be deployed on the Melbourne screened subnet next week. Given this information, provide answers to the following questions:

1. What type of policy should you configure to limit access at the Sydney location to a list of authorized users?
2. When the Melbourne server is deployed, what VPN protocol would you use to provide access if you are not able to modify the existing firewall rules?
3. What sort of NAP enforcement should you use in the Melbourne location?

Case Scenario 2: Coho Vineyard NAP

You are in the process of improving network security at Coho Vineyard's head office. Coho Vineyard has 20 servers running Windows Server 2008 R2 and 400 clients running Windows 7 Enterprise edition. As a part of this process, you intend to deploy NAP, but must deal with the following design constraints:

- Management at Coho want to do a six-month trial before they commit to purchasing any new hardware. The pilot program should allow NAP to be tested and ensure that noncompliant clients are remediated.
- If the pilot program proves to be successful, NAP should be implemented in such a way that unhealthy clients are blocked from accessing the network at the switch level.
- Coho Vineyard does not have the necessary hardware infrastructure at this time to implement switch-level network access demarcation, but the hardware will be purchased at the conclusion of a successful pilot program.
- Several of Coho Vineyard's legacy third-party systems do not support the IPsec protocol.

With this information in mind, answer the following questions:

1. Which NAP method should be used at Coho Vineyard during the pilot program?
2. Which NAP method should be used at Coho Vineyard once the pilot program is deemed successful?
3. What steps should you take to allow for remediation?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Monitor and Maintain Security Policies

Do all the practices in this section.

- Practice 1: Configure an RD Gateway server on a stand-alone computer running Windows Server 2008 R2 that has two network cards, one connected to a public network such as the Internet, and the other connected to the internal network.
- Practice 2: Configure and test an RD-RAP and RD-CAP.

Plan Infrastructure Services Server Roles

Do all the practices in this section.

- Practice 1: Create a server isolation policy using Windows Firewall with Advanced Security.
- Practice 2: Configure IPsec enforcements so that only healthy clients on the network are able to communicate with each other.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **PRACTICE TESTS**

For details about all the practice test options available, see the section "How to Use the Practice Tests" in this book's Introduction.

Index

Symbols and Numbers

- !SAC console, 232
- % (percent symbol), 45, 55
- .adml files, 194, 196
- .admx files, 194
- .NET Framework, 305
- / (slash) notation, 41
- 32-bit processors, 15, 159, 523
- 64-bit Extended Unique Identifier (EUI-64) address, 43
- 64-bit processors, 6, 14, 159, 329, 523
- 6to4 tunneling, 54, 443–44, 447
- 802.1X standard, 461

A

- AAAA (quad-A) records, 76, 81, 87–88, 513
  - configuring, practice exercise, 100
- Access control, 346–52
- Access control entry (ACE), 346, 352
- Access control list (ACL), 130, 346
- Access Control User Interface, 346–47
- Access permissions
  - file, 324, 346–51
  - Group Policy Management Editor, 206
  - printer, 302, 315–17
- Access, distributed
  - to file services, 344
- Accessed-based enumeration, 480–81
- Account Logon Events, 392
- Account Management category, 388, 392
- Accounts
  - administrator, 254, 380–81, 399
  - audit levels settings, 386
  - lockout policies, 126–29
  - managed service, 4
  - Read-only domain controllers (RODCs), creating, 120–21, 123–25
  - user, 254, 419–22
  - WSUS, 399
- Action Center, 557–58
- Activation
  - clock, resetting, 13
  - keys, 24–25
  - license server, 270–71
  - proxy, 25
  - volume, 24–25
  - Windows Deployment Services (WDS), 24–25
  - Windows Server 2008 R2, 13
- Active Directory
  - backing up, 607
  - lookups, 329, 336
  - recovering, 617–25
- Active Directory Administrative Center, 112–16
- Active Directory Certificate Services (AD CS)
  - administrative roles, 149–50
  - autoenrollment, configuring, 156–58
  - Certificate Authorities (CAs) types, 147–49
  - certificate revocation lists (CRLs), 160–61
  - credential roaming, configuring, 154–55
  - deploying, 182
  - deploying, practice exercise, 175–76
  - DirectAccess authentication for, 444
  - features and enhancements, 152–53
  - Online Responder, configuring, 162–64
  - web enrollment, configuring, 159
- Active Directory Database Mounting Tool, 623
- Active Directory Domain Services (AD DS)
  - auditing, 130–32
  - data mining tool, 111, 129
  - diagnostics, 547
  - domain functional levels available in, 133–34
  - GlobalNames DNS zone integration with, 83
  - Installation Wizard, 112, 122–23
  - objects, restoring, 618–21
  - planning, 70
  - printers to, publishing, 301
  - restartable, 111
  - Windows Server 2008, 111
- Active Directory Federation Services (AD FS), 142–43

Active Directory Lightweight Directory Services (AD LDS), 111, 129
Active Directory Module for Windows PowerShell, 597, 623–25
Active Directory Recycle Bin, 112, 117–18
  enabling, 138–39, 172
Active Directory Rights Management Services (AD RMS), 7
Active Directory Sites and Services, 125
Active Directory Users and Computers (ADUC) tool, 112, 120, 125–30
Active Directory Web Services (AD WS), 114
Add Features Wizard, 188
Add Windows Feature cmdlet, 227
Address configuration
  automatic, 47
  manual, 52
  multicast, 21, 534
  stateful, 44, 61
Address ranges, 40
Address Resolution Protocol (ARP), 48
Address space, 39–40, 47
Address structure
  global unicast, 42–43
  IPv6, 40–42
  multicast, 46
  Teredo, 49
Addresses
  aggregatable, 42–43, 48
  APIPA, 39–40
  autoconfigured, 44
  compatibility, 49–52
  DNS Round Robin, 511–12
  DNS Server, 62
  Internetwork Packet Exchange (IPX), 45
  IP, assigning client, 437
  IPv4-compatible, 49, 53
  IPv4-mapped, 49
  IPv6, 41–47
  ISATAP, 51–52
  MAC, 43, 47–48, 515
  manually configuring compatibility, 52
  Network Load Balancing (NLB) cluster, 513
  network, identifying and process connections, 563–64
  Teredo, 49
ADM (Administrative Template) files, 188, 194
Admin event logs, 243
Administration, role-based
  Certificate Services, 149–50
Administrative Template (ADM) files, 188, 194
Administrative Templates settings, 192–94
Administrator accounts, 254, 380–81, 399
Administrator mode, Authorization Manager, 257
ADMX files, 188, 194–96
  creating, central store for, practice exercise, 215–17
adprep/rodcprep command, 120
ADSI Edit MMC snap-in
  PSOs, creating, 126
ADUC. *See* Active Directory Users and Computers (ADUC) tool
Advanced Encryption Services (AES), 135
Advanced Sharing Settings, 347
Aggregatable addresses, 42–43, 48
Aging settings, 92–93
Alerts, 132, 205, 381, 549–50, 569
Algorithms, 137
Allow Remote Start Of Unlisted Programs policy, 202–4
Allow Time Zone Redirection policy, 204
Always Show Desktop on Connection policy, 204
Analytic event logs, 243
Answer files, 17–19, 112, 123
Anycast addresses, 42
APIPA (Automatic Private IP Addressing), 39–40
Application deployment. *See* Deployment
Application Virtualization (APP-V), 265, 284, 290–91
  deploying, 296
Applications
  backing up, 606
  configuring, for high availability, 528–30
  delegating management of, 256–58
  event logs, 237
  recovering, 614–15
  requirements, identifying, 64–66
  types of, supported by failover clusters, 522
Applications and Services Logs, 237, 242–43, 571
AppLocker, 4
APP-V. *See* Application Virtualization (APP-V)
Arrays
  Online Responder, 162, 164
  redundant, of inexpensive disks, 477, 494–95
  storage, 496
Attacks, external, 382–83
Audit credentials subcategory, 388
Audit Logon Events, 392
Audit policies, 386–90
Audit Policy category, 389
Audit Policy Group Policy container, 379
Audit Process Tracking policy, 393
Auditing, 111, 130–32, 377–80
  account creation, practice exercise, 417–19
  objects, access to, 347
  printers, usage of, 302
  security, 347, 391–93
Auditing Policy policy, 393
Auditing System Events policy, 393
Authentication
  802.1X standard, 461
  delegated, 253–55
  DHCP, 462
  DirectAccess, 444, 463
  distributed, 142

Forest-Wide Authentication, 141
IPsec, 440
L2TP, 440
protocols, 438–39
RAS server, 438
RD Gateway, 462–63
Selective Authentication, 141
selective cross-forest, 135
server, 273
VPN, 438–39, 461–62
Authentication mechanism assurance (AMA), 111, 135
Authoritative restores, 618–22
practice exercise, 634–36
Authority delegation, 249–58
Authority Information Access (AIA), 164
Authorization
connection policies, 453–54
distributed, 142
role-based, 137
Authorization Manager, 135, 257–58
Auto-casts, 23
Autoconfiguration, address, 43, 61. *See also* Stateless address configuration
Autoenrollment
configuring, 156–58
group policy settings, 157–58
purpose of, 148
Automated server deployment, 17
Automated System Recovery (ASR) Backup, 26
Automatic approval, 410–11
Automatic Private IP Addressing (APIPA), 39–40
Automatic service principle name (SPN) management, 111
Automatic tunneling, 53–54
Autonomous mode, 405
Autounattended.xml file, 17–20
Availability
application, 511
data, 331, 475–76
DNS Round Robin, 511–13
failover cluster, 331, 528–30
file, 328–30, 486
folder, 321, 337–38
high, defined, 509
Network Load Balancing (NLB), 513–19
printer, 302–3
storage, 321, 336

B

Backbone routers, 48
Background Intelligent Transfer Service (BITS), 401–2
Background zone loading, 81–82
Backups, 26, 321, 331, 335
byte-level, 609
differential, 602
incremental, 596, 601
manual, 602
offsite, 608
performance optimization, 602
remote, 607–8
restoring, practice exercise, 637
scheduled, 598–1
unscheduled, 602
Bare Metal Recovery, 615–17
Baselines, 541–42
Best Practices Analyzer, 112
Bidirectional connectivity, 442
BIND servers, 94
Bitlocker, 394–95
Bitlocker To Go, 394
BITS (Background Intelligent Transfer Service), 401–2
Block hashes, 343
Boot images, 24
BootP-enabled routers, 62
Branch office zones, 81
Branch offices
content, caching downloaded, 341–43
name resolution, 89
replication groups for, 482
RODCs (read-only domain controllers) installation, 118–19, 123–25
BranchCache, 4, 331, 341–43, 404
Breadcrumb bar, 115
Business strategies
data management and, 332–334
documenting requirements, 67

C

CA Administrator, 149–50
Cache
clearing, 78
destination, 58
minimum size of, 343
neighbor, 57
Caching
file, 585
negative, 78
offline settings, 350
transparent, 341
web proxy, 162
Capacity, adding server, 278
Capture images, 24
Case scenarios
Active Directory Certificate Services (AD CS), deploying, 182
application strategy, choosing appropriate, 537
APP-V, deploying, 296
backup infrastructure, 639
data collector sets and event forwarding, 588
data provisioning, 506
DFS (Distributed File System), 506
disaster recovery, 639–40
DNS configuration, 104
event management, 263
IPv6 connectivity implementation, 104
NAP deployment, 471
planning monitoring on server computers, 588–89
remote access, 471
Remote Desktop Services (RDS) deployment, planning, 295–96
rights delegation, 263

Case scenarios, *continued*
- security plans, implementing, 429–30
- Starter GPOs, using, 222
- troubleshooting procedures, planning and documenting, 222
- Windows Server 2003 to Windows Server 2008 R2 upgrade, 181
- Windows Server 2008 automated deployment, 35
- Windows Server 2008 migration, 35
- Windows Server 2008 R2 upgrade, planning, 371
- Windows Server Update Services (WSUS) SP2, 430

Categories element, 196

Central store
- ADMX files, 194
- creating, for ADMX files, 215–17

Centralized replication topology, 84

Centralized WINS topology, 84

Certificate Authorities (CAs)
- administrative roles, 149–50
- autoenrollment, configuring, 148, 156–58
- certificate revocation lists (CRLs), 160–62
- credential roaming policy, 154–55
- enrollment, across forests, 153–54
- Enterprise, 147–48
- health monitoring of, using Enterprise PKI snap-in, 166–67
- high-volume, 154
- Online Responder, configuring, 162–64
- root, installing, 151–52
- Standalone, 147–49
- types of, 147–49
- web enrollment, 153, 159

Certificate Enrollment Policy Web Service, 152–53

Certificate Enrollment Web Service, 152–53

Certificate Manager, 149–50, 160

Certificate names, 148

Certificate revocation lists (CRLs), 160–62

Certificate templates, 147, 156–58

Certificates
- digital, 438
- renewal of, 157–58
- self-signed, 394
- SSL, 440–41, 453

Challenge Handshake Authentication Protocol (CHAP), 439

Change Action Center Settings dialog box, 557–58

Claims, 142

Classification, 332, 345

Classless Interdomain Routing (CIDR), 39

Client access licenses, 268–72

Client For Network File System (NFS), 329, 336

Client workstation name resolution, 83

Clients
- DHCPv6, configuring, 61–63
- DirectAccess, 447
- RADIUS, configuring, 448–49
- roaming, updating, 409

Client-side extension (CSE) processing, 202

Clipboard redirection policy, 205

Cluster operation modes, 515–16

Cluster.exe, 530

Clusters. *See also* Failover Clustering feature
- DNS Round Robin, 511–13
- domain-based namespaces, 479–81
- failover, 479, 516–17, 522–31
- LUNs, assigning, 327
- Network Load Balancing (NLB), 513–19, 533–35
- Network Load Balancing (NLB) operation modes, 514–15
- print server, 303

Cmdlets, 116–17, 227, 344

Collaboration, Sharepoint Foundation 2010, 488–90

Collector computer, 240–42

Collector-initiated log subscription, 240–42, 574–76

Colon (), 41

Colon-hexadecimal format, 41

Column Explorer, 114

Command Line Interface (CLI) commands, 57

Command prompt, 57, 550–51

Command-line tools, 112, 231
- netdom.exe, 135

Commands
- adprep/rodcprep, 120
- cluster.exe, 530
- control-intl.cpl, 9
- control-timedate.cpl, 9
- dsacls.exe, 249–50, 253, 261
- eventvwr, 569
- Find, 125
- Get-Eventlog, 245
- gpupdate, 201, 212
- installation, 19
- IPv6, displaying configuration, 55
- ldifde, 126, 621
- netstat-r, 60
- nslookup, 61, 79–80
- nslookup ls -d, 79
- oclist.exe, 10, 227
- ocsetup.exe, 10, 227
- pathping-d, 59
- perfmon, 543, 552, 554
- ping, 58
- resmon, 561
- route print, 58, 60
- services.msc, 568
- site ids, obtaining, 56
- tracert-d, 59
- wbadmin, 596–97
- wecutil, 575
- winrm, 574–76

Commit (MB) Handles field, 560

Commit Limit, 567

Common Internet File System/ Server Message Block (CIFS/SMB), 335

Compatibility
- addresses, 49–52
- check, 14–15
- IPv4-to-IPv6, 47–50

Compliance, 72, 412, 414

Computer Configuration settings
- Administrative Templates settings, 190
- disabling, 201

Computer health check, 551

Computers
- assigning to groups, 405–7
- credential delegation, 253–55

Conditional forwarders, 70, 75

Cone flags, 49

Cone NATs, 49, 51

Configuration
- DHCPv6 client, 61–63
- IPv6, verifying, 55–57

Configuration Data Collector, 549–50

Configure Custom Alert Text policy, 205

Configured tunneling transition, 53

Connections Group Policy node, 276–77

Connectivity
- authorization policies, 453–54
- automatic, 443
- bidirectional, 442
- checking, 58
- DirectAccess, using, 442–47
- IPv6, verifying, 57–59
- network, troubleshooting, 208, 212
- troubleshooting, 59
- virtual machine, 279
- VPN Reconnect, 441–42

Constrained delegation, 135, 254

Containers, 115, 126

Content metadata, 343

control-intl.cpl command, 9

control-timedate.cpl command, 9

Convergence, heartbeat and, process, 514

Core processing, Group Policy settings, 202, 211–12

Counters, performance
- adding, 543–45
- adding, practice, 579–82
- adding, to Data Collector Sets, 547, 549
- graphs for, updating, 544
- RD Session Host server-specific, 280

CPU usage, 559

Create A Basic Task Wizard, 572

Create Cluster Wizard, 524

Create New Data Collector Wizard, 549

Credential delegation, 253–55

Credential roaming, 154–55

CryptoAPI 2.0 diagnostics, 145

Cryptography, 162

Custom views, 239, 391, 570

D

-d command line switch, 59

Data
- availability, planning, 475–76
- backing up, 593–10
- filtering, in Resource Monitor, 563
- recovering, 614–15
- viewing read-only, 129

Data collaboration, Sharepoint Foundation 2010, 488–90

Data Collector Sets (DCSs), 546–51
- creating, 548, 550–51
- customizing, 548–50
- editing, 550
- starting and stopping, 551
- types of, 549

Data delivery, real-time, 48

Data management and business strategies, 332–34

Data mining tools, 129–30

Data Protection Manager (DPM), 609–10

Data provisioning, 488–90
- case scenario, 506

Data recovery strategies, 129–30

Data snapshots, 129–30

Database Availability Groups, 5, 510

Datacenter Edition, 5–6, 12, 14

dcpromo command, 71, 112, 122

Debug event logs, 243

Debugging tools, Group Policy, 209–11

Deduplication, file, 344

Default gateways, 40, 45, 58–59

Default Routing and Remote Access Class, 437

Delegation, 74, 249–58
- authority, 249–58
- blocking, 254–56
- constrained, 135, 254
- credential, 253–55
- custom, 251
- existing, modifying, 252–53
- IIS (Internet Information Services) configuration, 256–57
- of administrative privileges, 251–52
- of read-only domain controller installation, 123–25
- printer server management, 316
- procedures, 249–50
- resetting a, using a dsacls command, practice exercise, 261
- role-based, 256

Delegation of Control Wizard, 249–51

Delta CRLs (certificate revocation lists), 161

Deny permission, 346

Deployment
- APP-V, 290–91
- automated server, 17
- certificate, 180
- Group Policy, 284–85
- Network Access Protection (NAP), 152–53
- Network Load Balancing (NLB), 513–14
- of read-only domain controllers (RODCs), 118–19
- physical versus virtual, 11–12

Deployment, *continued*
- RemoteApp Manager tool, 288–89
- scheduled, 23
- single server, 400
- traditional, 284
- web, 285–86

Deployment Workbench, 17
Desktop display, remote, 204
Desktop Experience, 207–8
Desktop wallpaper removal, 205
Destination cache, 58
Detailed Tracking category, 388
Developer mode, Authorization Manager, 257
Device and Resource Redirection policy, group policy settings, 276
DFS (Distributed File System), 135, 478
- benefits of, 334, 345
- managing, 483–85
- role service, 328

DFS Namespace (DFSN)
- access-based enumeration, 481
- choosing, 479–80
- configuring, practice exercise, 502
- creating, 478–79
- function of, 328
- servers, 478–80
- servers, adding, practice exercise, 502

DFS Replication (DFSR), 89
- configuring, 482–83
- function of, 328
- servers, 528
- zone type selection, 92

DFSN. *See* DFS Namespace (DFSN)
DFSR. *See* DFS Replication (DFSR)
DHCP (Dynamic Host Configuration Protocol)
- address configuration, 47
- functions of, 40
- NAP enforcement, 64–65, 462
- NAP enforcement, practice exercise, 467
- Routing and Remote Access Service (RRAS), 62
- servers, 5, 20, 437, 528
- virtualization, 62

DHCPv6
- address configuration, 47
- client configuration, 61–63
- NAP enforcement, 65
- servers, 62
- similarities to DHCP, 62

Diagnostic Policy Service (DPS), 205
Diagnostics
- Active Directory Domain Services (AD DS), 547
- CryptoAPI 2.0, 167
- Network, 572–73
- system, 546, 551–52

Dial-up remote access server, 435
Diff Area, 337
DirectAccess, 4, 442–47
- connections, specifying, 446
- differences from VPN, 442–444
- NAP enforcement, 463
- ports, list of, 447
- security groups, 445
- servers, 444–47

DirectAccess Management console, 445–46
Directory services, 108–9
Directory Services Restore Mode (DSRM)
- booting methods, 619–20
- in authoritative restore process, 618–19

Disable Port Range filtering mode, 518
Disaster recovery, 613–26
- Active Directory, 617–25
- case scenario, 639–40
- data, 614–15
- Hyper-V and, 625–26
- offsite backups, 608
- roles and role services, 617–625
- servers, 615–17

Discover images, 24
Discovery domain sets, 338–39
Discovery domains, 338–39
Discovery scope, license server, 269
Disk Diagnostic Configure Execution Level policy, 205
Disk management, 322–23, 334–35, 495–96
Disk Management console, 322–23, 326–27, 495
Disk mirroring, 477
Disk space requirement, 15
Disk storage, 327–28
Disk striping, 477
Distinguished name (DN), 115
Distributed Cache mode, 343
Distributed File System. *See* DFS (Distributed File System)
Distributed File System Replication. *See* DFS Replication (DFSR)
Distributed Scan Server role service, 301
Distributed Transaction Coordinator (DTC), 528
Distribution groups, universal, 135
DLL (dynamic-link library) files, 565–66
DNS (Domain Name System)
- administering, 77–78
- configuration, 61
- configuration, AAAA (quad-A) records, practice exercise, 100
- forwarding, 70, 74–75, 91–92
- infrastructure, 70, 88, 90, 94
- namespace, planning a, 88–90
- record types, 76

DNS Manager MMC snap-in, 77–78
DNS Recursive Name Server, 61
DNS Round Robin, 278, 509, 511–13
- advantages and disadvantages of, 514, 519
- entries, creating, 513
- netmask ordering, 409
- netmask ordering, verifying status, 512

DNS server
- addresses, 62
- file-backed, 72
- managing, 77–78
- RODCs (read-only domain controllers) installation, 120–21
- root hints for, 93–94

dnscmd tool, 77, 83, 88

Do Not Allow Clipboard Redirection policy, 205

Do Not Display Initial Configuration Tasks Window Automatically At Logon policy, 205

Do Not Display Server Manager Automatically At Logon policy, 205

Documenting requirements, IPv6 implementation, 66–67

Domain Admins group, 128, 436

Domain controllers. *See also* Read-only domain controllers (RODCs)
- domain functional levels and, table of supported, 134
- forest functional levels and, table of supported, 136
- locations for ADMX files on, 195
- recovering full servers on, 622

Domain functional levels, 119, 133–35
- domain controllers, supported, table of, 134
- features enabled by, table of, 135
- raising, 138

Domain isolation, 456–57

Domain management tool, 135

Domain Name System (DNS). *See* DNS (Domain Name System)

Domain namespaces, 479–81

DomainDNSZones, 81

Domains
- discovery scope, 269
- renaming, 137
- viewing Active Directory objects in, 114

Downstream servers, 401, 404–405, 413

DPM (Data Protection Manager), 609–10

Drainstop, 517

Drivers
- file filter, 329, 336
- print, 312
- Volume Snapshot, 337
- XPSDrv printer, 305

DS Access category, 388, 392

dsacls.exe command, 249–50, 253
- delegation, resetting a, using, practice exercise, 261

dsamain.exe (data mining tool), 129

Dsamin.exe, 623

Dual stack transition method, 52–53

Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)

Dynamic Least Queue Depth, load balancing policy, 499

Dynamic-link library (DLL) files, 565–66

DynamicObject class, 137

E

EAP-MD5 CHAP (Extensible Authentication Protocol-Message Digest 5 Challenge handshake Authentication Protocol), 439

EAP-TLS (Extensible Authentication Protocol-Transport Level Security) protocol, 438–39, 441

Emergency Management Services (EMS), 231–32

Enable-ADOptionalFeature cmdlet, 138–39

Enabling
- Active Directory Recycle Bin, 138–39, 172
- credential roaming policy, 154–55
- Remote Access for VPN, 436
- Shadow Copies of Shared Folders feature, 593–94

Encrypting File System (EFS), 393–94, 606

Encryption, 64, 135, 236, 273–74

Enforce Removal Of Remote Desktop Wallpaper policy, 205

Enforcement Client (EC), 460. *See also* Network Access Protection (NAP)

Enterprise Certificate Authorities (CAs), 147–48

Enterprise Edition, 5, 10, 12, 14

Enterprise PKI tool, 166–67

Enumeration, accessed-based, 480–81

Equal_Per_Session WSRM policy, 281

Equal_Per_User WSRM policy, 281

EUI-64 (Extended Unique Identifier 64-bit), 43

Event forwarding, 391, 573
- case scenario, 588

Event logs, 236–45
- application, 237
- applications and services, categories of, 242–43
- archiving, 244
- filtering, 238
- forwarded events, 237, 241, 573
- helper class, 573
- informational, 573
- logging methods, 450–52
- managing, 244–45
- security, 132, 237, 377–80, 391
- setup, 237
- size of, setting, 237
- storage, 244
- subscription. *See* Subscriptions, event log
- system, 237
- task notification, 239–40
- viewing, 239, 243–44

Event subscriptions.
    See Subscriptions, event log
Event Trace Data Collector, 549–50
Event Viewer, 569–78
    Application and Service Logs, 237, 242–43
    categories, 569–70
    custom views, 239, 391, 570
    customizing, 570
    logs, 237, 570–71
    remote computers, connecting to, 243–44
    security monitoring, 377–80
    Windows Network Diagnostics, using with, 572–73
Events
    Account Logon, 392
    attaching tasks to, 239–40
    Audit Logon, 392
    system, 237
eventvwr command, 569
Expiration notification policy, 158
Explicit tunnels, 53
Extended Unique Identifier (EUI-64) addresses, 43
Extensible Authentication Protocol-Message Digest 5 Challenge handshake Authentication Protocol (EAP-MD5 CHAP), 478
Extensible Authentication Protocol-Transport Level Security (EAP-TLS) protocol, 438–39, 441
Extension headers, 48
External trusts, 140
Extranets, 153

F

Fabric, 338, 499–500
Failback policy, load balancing policy, 499
Failover Cluster Manager console, 522, 524, 530–31
Failover clustering, 5, 509–10, 514–17, 522
Failover Clustering feature
    clusters in, creating, 527–28
    function of, 331
    installing, 526
    LUN assignment, 327
    roles services, 321
Failover, load balancing policy, 499
Failure audits, 438
Farms, 278–79
Fast First Logon, 341
FCI (File Classification Infrastructure), 332, 345
fe8 address lookup, 43
fec0 address lookup, 44
ff address prefix, 46
Fibre Channel, 327, 331, 338–39, 497, 499, 609
File Classification Infrastructure (FCI), 332, 345
File Replication Service (FRS), 330
File screens, 356–57
File Server, 528
File Server Resource Manager (FSRM)
    advantages of, 335
    classification management, 332
    file screening, 356–57
    functions of, 328–30
    quotas, creating, 353–54
    role service, 324, 345
    storage reports, 357
File servers, 320–21
File Service Migration Toolkit (FSMT), 345
File Services
    DFS (Distributed File System), 328
    server role, 320–21
    Windows Server 2003, 330–31
    Windows Server 2008 R2, 332–36
    Windows Storage Server 2008 R2, 344–45
File sharing, 338, 484
File Transfer Protocol (FTP), 287-88
File-backed DNS server, 72
File-backed zone data, 82
Files
    access permissions for, 324, 346
    availability of, 328–30, 486
    deduplication, 344
    indexing, 487
    offline, 341, 350, 485–86
    recovering, 613–14
    restoring, practice exercise, 632–34
    screening, 328
Filtering
    in Event Viewer, 570, 572
    in Resource Monitor, 563–64
Filtering modes, 517–19
Filters
    custom, 309–11
    event log, 238
    packet, 437, 461
    password, 128–29
    print, 309–11
    print driver, 311
    replication, editing, 483–85
    subscription, 241
Find command, Active Directory Sites and Services, 125
Fine-grained password policies, 126–29. *See also* Passwords
Firewalls, 233, 386, 447, 456
Flags field, 46
Flash devices, booting from, 13
Folder Redirection, group policy settings, 340–41
Folders
    content, sharing, 323
    recovering, 613–14
    replication, 482–83
    restoring, 632–34
    selecting, for indexing, 487
    sharing manually, 351
    viewing shared properties of, 324
Forefront Threat Management Gateway (TMG), 457–59
Forensic analysis, 380, 383–86
Forest functional levels
    in Windows Server 2008, 135–36

ForestDNSZones, 81
Forests
- Certificate Authorities (CAs)
  - enrollment across, 153–154
- discovery scope, 269
- functional levels, 119, 133, 135–38
- GlobalNames DNS zone deployment, 95–96
- trusts, 137, 139–41, 153–54

Forest-Wide Authentication, 141
Format Prefix (FP)
- global unicast, 42
- link-local address, 43
- multicast addresses, 46

Forms, managing, 312
Forward lookup zones, 71, 92–93
Forwarded Events event log, 237, 241, 573
Forwarders, 70, 74–75, 91–92, 94–95
Forwarding computers, 574
Foundation Edition, Windows Server 2008 R2, 4, 7–8
FQDNs (fully qualified domain names), 89, 95–96
FSRM. *See* File Server Resource Manager (FSRM)
FTP (File Transfer Protocol), 287–88
Full Server Recovery, 615–17
Full-cone NATs, 51
Full-mesh topology, 84, 485
Fully qualified domain names (FQDNs), 89, 95–96
Functional levels, 119. *See also* Domain functional levels; *also* Forest functional levels
- password account management and, 128
- planning, 133–38
- raising, 138
- raising/upgrading, practice exercise, 170–71
- servers and, 133

G

Generic Security Services_ Application Programming Interface (GSS_API), 329
Get-Eventlog command, 245
Global security groups, password policies for, 128–29
Global System Access Auditing category, 390
Global unicast addresses, 42–43
GlobalNames zone, 70, 82–83, 95–96
Glue records, 74
GPMC. *See* Group Policy Management Console (GPMC)
GPOs. *See* Group Policy objects (GPOs)
GPOTool.exe, 209
GPResult.exe tool, 209, 219
gpupdate command, 201, 212
Graphs, performance monitoring, 544–45, 559–60, 566–67
Group ID, 47
Group Manager settings, 253
Group Policy
- ADMX files, 188, 194–96, 215–17
- collector-initiated subscriptions, configuring, 242
- configuring, 276–77
- for assigning computers, 406–7
- for autoenrollment, configuring, 157–58
- Online Certificate Status Protocol (OCSP) settings, 164–65
- Remote Desktop Services (RDS), configuring with, 276–77
- security monitoring, 380
- strategy, planning, 200–2
- Windows Firewall With Advanced Security snap-in, 456
- WSUS client configuration, 407

Group Policy Management Console (GPMC), 210–11, 445
- installation, 188
- installation, practice exercise, 214–15
- recovering objects, 622

Group Policy Management Editor, 377
- access permissions, 206
- Administrative Templates, 192–94
- ADMX files, 194, 196
- audit policies in, 386–90
- Group Policy structure, 202
- unconfigured settings, disabling, 201

Group Policy objects (GPOs)
- backing up, 191, 607
- creating and configuring, practice exercise, 217–218
- multiple, creating, 190
- processing, 202
- refreshing, 201
- reports, generating, practice exercise, 218
- restoring, 622
- strategy, 200

Group Policy Results Wizard, 209
Group Policy settings
- editing, 192
- new in Windows Server 2008 R2, 202–7
- troubleshooting, 208–12
- verifying, practice exercise, 219–20

Group Policy Starter GPO Editor policy, 206
Groups
- conversion, 135
- nesting, 135
- password account policies for, 127–28
- Password Setting Objects (PSOs) for, 128–29
- printer access permissions for, 315–17
- replication, 482–83

Groups, *continued*
- security, creating, practice exercise, 419–22
- shadow, 128
- universal distribution, 135
- updates deployment using, 405–6

H

Handles, 560, 565–66
Hard quotas, 354
Hardware redundancy
- data availability through, 475
- rules for, 476–77

Hardware requirements
- Datacenter Edition, Windows Server 2008 R2, 5–6
- Enterprise Edition, Windows Server 2008 R2, 5
- IPv6 network, 63–64
- Server Core, 8
- Standard Edition, Windows Server 2008 R2, 6
- Windows Web Server 2008 R2, 6

Hash algorithms, 343
Header size, 48
Heartbeat and convergence process, 514
Helper class events, 573
High Availability Wizard, 528–30
Host addresses, 47, 61
Host bus adapter (HBA) ports, 497
Host Credential Authorization Protocol (HCAP), 464
Hosted cache mode, 343
Hub and spoke topology, 84–86, 485
Hyper-V
- Dynamic Memory, 4, 625
- failover cluster, 12
- RD Virtualization Host, 279
- virtual machine hosting, 529

I

I/O, load balancing policies for, 499
IA64 processors, 3
iCMPv6, 447
ICMPv6 (Internet Control Message Protocol for IPv6) messages, 48, 58
Idle sessions, 275, 277
IGMP multicast mode, 515
IIS (Internet Information Services), 256–57, 284
IIS (Internet Information Services) Manager, 286–87
IIS 7.5 (Internet Information Services 7.5), 4, 7, 284, 286–88
IKEv2 protocol, 441–42
Images, Windows Deployment Services (WDS), 24, 32–33
Indexing files, 487
Indexing Service, 330, 487
inetOrgPerson objects, 128, 135, 137
Informational events, 573
Infrastructure Master Flexible Single-Master (IM FSMO), 138
Initial Configuration Tasks window, 205
Installation, unattended
- creating files for, 17–19
- running, 18–22

Integrated zones, 70, 92
Interfaces
- identification, 43, 55
- IPv6 address, 41–43, 56–57
- router, default, 58

Internet Assigned Numbers Authority (IANA), 39
Internet Control Message Protocol for IPv6 (ICMPv6) messages, 48, 58
Internet Explorer, certificate web enrollment, 159
Internet Information Services (IIS), 256–57, 284
Internet Information Services (IIS) Manager, 286–87
Internet Information Services 7.5 (IIS 7.5), 4, 7, 284, 286–88
Internet Key Exchange (IKEv2), 441–42
Internet Protocol version 4 (IPv4). *See* IPv4 (Internet Protocol version 4)
Internet Protocol version 6 (IPv6). *See* IPv6
Internet Security Protocol. *See* IPsec
Internet Storage Name Service (iSNS), 338, 499, 528
Internet, certificate enrollment over, 153
Internetwork Packet Exchange (IPX) addresses, 45
Intra-Site Automatic Tunnel Addressing Protocol. *See* ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
IP Security. *See* IPsec
ipconfig command-line tool, 55, 58, 61, 78
IP-HTTPS, 443–44
IPsec
- domain isolation and, 456
- encryption, 64, 236
- L2TP protocol, 440
- NAP enforcement, 154, 460
- Policies Management snap-in, 59
- troubleshooting connectivity, 59

IPSec6 tool, 60
IPv4 (Internet Protocol version 4)
- addresses, 42, 44–45, 49
- configurations, releasing/renewing, 78
- interoperability, need for, 40, 63–64
- IPv6, 47–48, 52–54
- ISATAP addresses and, 51–52
- protocol 41, 447
- protocol 50, 447

IPv4-compatible addresses, 49, 53
IPv4-mapped addresses, 49
IPv6
- AAAA (quad-A) records, 76, 81, 87–88, 513
- AAAA (quad-A) records, configuring, practice exercise, 100

advantages over IPv4, 47
connectivity, troubleshooting, 59
DirectAccess connection method, 444
implementation, 55–58, 66–67
interoperability, 40
IPv4-to-IPv6 compatibility, 49–52
network connectivity tools, 51
networks, planning, 63–67
routing tables, 48, 60–61
support for Windows Server 2008 DNS Server, 81
tools, 55–56
transition strategies, 46–47, 52–54
IPv6 address structure, 40–42
DNS server support for, 61, 81
prefixes, 41
syntax, 41
types of addresses, 41–45
Windows Server 2008 R2 support for, 87–88
IPX addresses, 45
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
addresses, 51–52
practice exercise, 99–100
tunneling, 54
iSCSI, 327–28, 338, 499–500, 609
iSCSI Initiator, 344, 497
iSNS (Internet Storage Name Service), 338, 499, 528
Isolation, domain, 456–57
Itanium-based systems, 6, 14

K

KCC (Knowledge Consistency Checker), 137
Kerberos authentication protocol, 135, 140, 142, 156, 162
Kernel Memory (MB), 560
Key Management Services (KMS), 24–25
Knowledge Consistency Checker (KCC), 137

L

L2TP/IPsec protocol, 440
Language-neutral resources (.admx files), 194–96
Language-specific resources (.adml files), 194, 196
Last Interactive Logon information, 135
Layer-3 switches, 62
LDAP Data Interchange Format (LDIF), 621
ldifde command, 126, 621
Libraries, Sharepoint, 488–90
License server
activation, methods of, 270–271
backing up, 272
deployment, 272
discovery scope, 269
restoring, 272
Licensing
Datacenter Edition, 5, 12
Enterprise Edition, Windows Server 2008 R2, 5, 12
Remote Desktop Services (RDS) client, 268–72
Standard Edition, 5
Licensing Group Policy node, 276
Lightweight Directory Access Protocol (LDAP), 115
Line Printer Daemon (LPD), 301
Linked-value replication, 137
Link-local addresses, 43, 45
Load balancing, 207, 278–79, 499. *See also* Network Load Balancing (NLB)
Local File Logging, 450–51
Local Security Settings, 347
Log subscriptions. *See* Subscriptions, event log
Logging
event forwarding and subscriptions, 569–78
password synchronization, 207
performance data, 548
Logical Unit Numbers. *See* LUNs (Logical Unit Numbers)
Logman utility, 550–51
Logon rights, remote, changing, 232
Logon time stamp update, 135
Logon/Logoff category, 389
Logs. *See* Event logs
Lookups
Active Directory, 329, 336
forward, 71, 91–92
nslookup, 61, 79–80
reverse, 70, 77, 87–88
reverse, practice exercise, 101–2
Windows-to-UNIX, 329, 336
Loopback addresses, IPv6, 45
LUNs (Logical Unit Numbers)
assigning, 327–28
creating, 327, 337
deleting, 495
Fibre Channel, 497
iSCSI, 497
managing, 495
Provision Storage Wizard, 326
Storage Manager for SANs, 339
types of, 494–95
unassigning, 495

M

MAK (Multiple Activation Key), 24–25
MAK Independent Activation, 25
MAK Proxy Activation, 24–25
Malware, 386
Manage Open Files feature, 324
Manage Sessions feature, 324
Management packs, 112, 246, 609
Memory usage, 280, 560–61, 564
Message Queuing, 529
Messages, archiving, 558
Metadata, 343
Microsoft Application Virtualization (App-V). *See* Application Virtualization (APP-V)
Microsoft Baseline Security Analyzer, 414
Microsoft Bitlocker, 394–95

Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2), 439
Microsoft Deployment Toolkit (MDT), 17
Microsoft Desktop Optimization Pack (MDOP), 290
Microsoft Dynamic DNS (DDNS), 70
Microsoft Forefront Threat Management Gateway (TMG), 457–59
Microsoft Management Console (MMC) snap-ins
  custom, creating, 228–29
  deploying, 235
  enhancements, 122, 125–29
  Server Core remote connection, 7
Microsoft Report Viewer, Redistributable, 399
Microsoft Server Message Block (SMB) protocol, 321–22
Microsoft Sharepoint Foundation 2010, 488–90
Microsoft SQL Server, failover clustering, 5
Microsoft System Center Operations Manager 2007 R2, 245–246, 380
Microsoft System Center Operations Manager 2007 R3, 1
Microsoft System Center Operations Manager 2010, 609
Microsoft System Center Virtual Machine Manager 2008 R2, 246
Mirror of stripes, 477
mknod function, 329
MMC. *See* Microsoft Management Console (MMC)
Modules, 565
Monitoring
  performance, 542–45
  remote access, 449–50
  soft quotas for, 354
  System Center Operations Manager 2007 R2, 112, 245–46
  with Network Access Protection (NAP), 464
Most Recently Used (MRU) lists, 114
MPIO (Multipath I/O), 321, 327, 331, 498–99
Multicast addresses, 21, 42, 46–47
  configuration, 534
Multicast cluster operation modes, 514–16
Multicast mode, 514–15
Multicast transmission, 22–23
Multinetting, 41
Multipath I/O (MPIO), 321, 327, 331, 498–99
Multiple Activation Key (MAK), 24–25
Multiple host filtering mode, 518
Multiple-instance applications, 522

N

Name resolution
  client workstation, 83, 87
  failed, 78
  for UNIX systems, 94
  importance of, 71
  in dynamic environments, 92–93
  in remote locations, 92
  NetBIOS, using WINS, 70
  single-label, 81–83
  zone replication, 75
Namespaces. *See also* DFS Namespace (DFSN)
  Domain Name System (DNS), 88–90
  policy, 196
  types of, 479–80
  Windows Server 2008, 480
NAP. *See* Network Access Protection (NAP)
NATs (Network Address Translations), 39–40, 49, 51
Navigation, Active Directory Administrative Center, 113–15
ND (Neighbor Discovery) protocol, 43, 48
Negative caching, 78
Neighbor cache, 57
Neighbor Discovery (ND) protocol, 43, 48
NetBIOS (Network Basic Input/Output System), 70
NetBIOS Extended User Interface (NetBEUI), 70
NetBT (NetBIOS over TCP/IP), 82
Netdom.exe, 135
Netgroups, 329
Netmask ordering, 409, 512
netsh (network shell) commands, 55–57, 105
  and netsh interface ipv6 add v6v4tunnel, 51
  netsh interface ipv6 6to4, 51
  netsh interface ipv6 add dnsserver, 52, 57, 61
  netsh interface ipv6 add route, 61
  netsh interface ipv6 delete destinationcache, 58
  netsh interface ipv6 delete neighbors, 57
  netsh interface ipv6 delete route, 61
  netsh interface ipv6 isatap, 51
  netsh interface ipv6 set address, 52, 56
  netsh interface ipv6 set interface, 57
  netsh interface ipv6 set route, 61
  netsh interface ipv6 show address, 55–56
  netsh interface ipv6 show destinationcache, 58
  netsh interface ipv6 show dnsservers, 61, 80

- netsh interface ipv6 show neighbors, 55, 57
- netsh interface ipv6 show route, 58, 60

netstat-r command, 60

Network Access Protection (NAP), 433, 459–64
- DCHP integration with, 64-65
- deployment, 152–53
- enforcement, 64–65, 154, 279, 460–63
- high-volume CAs and, 154
- in Windows Server 2008 R2 Foundation Edition, 7
- monitoring-only mode, 464
- remediation servers, 463
- scopes, 61–62

Network adapters, 436, 513

Network Address Translations (NATs), 39–40, 49, 51

Network Basic Input/Output System (NetBIOS), 70

Network Device Enrollment Service, 165–66

Network Diagnostics, 572–73

Network File System (NFS)
- Client For, 329, 336
- protocols, 324, 345
- Server For, 329, 336

Network filtering mode, 518

Network Information Service (NIS), 206

Network Load Balancing (NLB)
- advantages and disadvantages of, 509, 514, 519
- clusters, 513–19, 533–35
- deployment, 513–14
- heartbeat and convergence process, 514
- multicast mode, 514–15
- port rules, 517–19
- RD Connection Broker, 278
- removing, from the NLB cluster, practice exercise, 535
- traffic management, 517–19
- unicast mode, 514–15

Network Policy Server (NPS)
- 802.1X standard, 461
- configuring, practice exercise, 467–68
- installation, practice exercise, 467–68
- log files, 450–51
- RADIUS, 447–50
- remediation servers, 463

Network print port, 303

Network Printer Installation Wizard, 307–8

Network Service Access Point (NSAP) addresses, 45

Networks
- IPv6, planning, 63–67
- perimeter, 438, 453, 457
- private, connecting, 233–34
- security for, 64–66
- usage of, 561

New Replicated Folders Wizard, 482–83

New Technology File System (NTFS), 300, 349, 352

Next Level Aggregator (NLA), 42

NFS. *See* Network File System (NFS)

No Majority Disk Only quorum model, 524

Node and Disk Majority quorum model, 524

Node and File Share Majority quorum model, 524

Node Majority quorum model, 523

Nodes, 42, 49, 276–77

Non-administrators, remote administration tools for, 235–36

Nonce requests, 162

None filtering mode, 518

No-nonce requests, 162

Notepad, 9

Notification
- AD DS enhancement, 112
- event log task, 239–40
- expiration, 158
- file screening, 356
- print queue, 306, 309
- printer, 314
- quota limit, 354

NPS. *See* Network Policy Server (NPS)

NSAP addresses, 45

nslookup command, 61, 79–80

nslookup ls -d command, 79

NT LAN Manager (NTLM) authentication, 236

NTBackup, 598

Ntbackup utility, 335

Ntdsutil tool, 129–30, 621

NTFS (New Technology File System), 300, 349, 352

NTLM (NT LAN Manager) authentication, 236

O

Object Access category, 389, 392

Object ownership, 346–47

Objects, Active Directory
- auditing, 131–32
- restoring, 117–18, 618–22, 624–25
- searching for, 116

oclist.exe command, 10, 227

ocsetup.exe command, 10, 227

Offline files, 341
- caching options, 350
- settings, configuring, 485–86
- settings, configuring, practice exercise, 504

Offsite backups, 608

Online Certificate Status Protocol (OCSP), 162–65

Online Responder
- arrays, 164
- Certificate Authority configuration resolution, 167
- configuring, for Certificate Services, 162–63
- deploying, 163–64
- deploying, practice exercise, 176–79
- managing, 163

Online Responder management console, 163
Operating System Recovery, 615–17
Operational event logs, 243
Optimize Backup Performance dialog box, 596
Option tag 60, 20
Organizational units (OUs)
  password account policies for, setting, 128–29
  Password Setting Objects (PSOs) for, 128
Other Server, 529
Override Referral Ordering, 481
Overview tab, Resource Monitor, 562

P

Packet filters, 437, 461
Page Description Language (PDL), 307
Paging file use, 560
Partitions
  application directory, 119–21
  defined, 71
  Logical Unit Number (LUN), 495
  managing, 334–35
  NFTS, 19
  silo, 290
Password Authentication Protocol (PAP), 439
Password policies
  administrative level, 127
  enabling, practice exercise, 172–74
  fine-grained, 126–29
  replication. *See* Password Replication Policy
  service account, 127
  user-level, 127
Password Replication Policy, 111, 119–23, 125–26
Password Settings Container (PSC) object class, 126
Password Settings Objects (PSOs)
  creating, 126
  creating, practice exercise, 172–74
  groups and, 128–29
  Precedence attribute, 129
Passwords
  account, setting policies for, 126–29
  default settings, 126
  Directory Services Restore Mode (DSRM), 620
  filters for, 128–29
  in answer files, 112, 123
  management of, 129
  management of, practice exercise, 260–61
  read-only domain controller, 119
  synchronization, 206–7
Patch management tools, 413–14
pathping-d command, 59
Payload identification, 48
Peer caching, 401–2
Per device CALs, 271
Per user CALs, 271
Percent (%) symbol, 45, 55
perfmon command, 543, 552, 554
Performance
  backup, 602
  monitoring, 542–45
  server, 336
  system, data collection set, 546
Performance Counter Alert, 549
Performance Counter Data Collector, 549–50
Performance counters
  adding, 543–45
  adding, practice exercise, 579–82
  adding, to Data Collector Sets, 547, 549
  graphs for, updating, 544
  RD Session Host server-specific, 280
Performance Monitor tool, 543, 550
Perimeter networks, 438, 453, 457
Permission inheritance, 346–47
Permissions, 112, 120, 346
  assigning, Certificate Services, 149
  autoenrollment, 156
  certificate template, 147
  customizing, 348–49
  folder and volume access, 324
  for remote backup, 607
  NTFS (New Technology File System), 352
  physical versus virtual deployment considerations, 12
  printer access, 315–17
  remote logon, changing, 232
  setting, 120, 129
  share, 352
  user, determining, 352
Physical Memory (MB), 560
ping command, 58
PKI (Public key infrastructure), 149, 151, 166–67
Pointer record (PTR), 40, 101–2
Point-to-Point Protocol (PPP), 440
Point to Point Tunneling Protocol (PPTP), 439–40
Policies. *See also* Administrative Templates
  Allow Remote Start Of Unlisted Programs policy, 202–4
  Allow Time Zone Redirection policy, 204
  Always Show Desktop on Connection policy, 204
  Configure Custom Alert Text policy, 205
  Device and Resource Redirection policy, 276
  Disk Diagnostic Configure Execution Level policy, 205
  Do Not Allow Clipboard Redirection policy, 205
  Do Not Display Initial Configuration Tasks Window Automatically At Logon policy, 205
  Do Not Display Server Manager Automatically At Logon policy, 205

  - Enforce Removal Of Remote Desktop Wallpaper policy, 205
  - Equal_Per_Session WSRM policy, 281
  - Equal_Per_User WSRM policy, 281
  - Group Policy Management Editor policy, 206
  - Group Policy Starter GPO Editor policy, 206
  - Password Replication, 111, 119–23, 125–26
  - Remote Desktop Connection Authorization Policies (RD-CAPS), 453
  - Remote Desktop Services (RDS), 276–77
  - Restrict Users To The Explicitly Permitted List Of Snap-Ins policy, 285
  - Set The Interval of Synchronization Retires for Servers Running Password Synchronization policy, 206
  - Set The Number of Synchronization Retires for Servers Running Password Synchronization policy, 206
  - Turn on Extensive Logging for Active Domain Services Domain Controllers Running Server for NIS policy, 207
  - Use RD Connection Broker Load Balancing policy, 207
  - Weighted_Remote_Session WSRM policy, 281

- Policies element, 196
- PolicyDefinitions element, 196
- PolicyNamespaces element, 196
- Port rules, NLB, 517–19
- Port-restricted cone NATs, 51
- Ports
  - DirectAccess, list of, 447
  - Fibre Channel host bus adapter (HBA), 497–98
  - managing, 312, 316
  - network printer, 303
  - Port 67, 19–21
  - TCP, 48, 61, 440, 443, 447, 453
  - User Datagram Protocol (UDP), 48, 50, 441, 447
- PowerShell
  - cmdlets, 116–17, 227, 344, 597
  - command-line tools, 231
  - delegation of authority using, 249–50
  - event logs, managing with, 245
  - modules, 116–17, 230
  - overview, 229–30
  - remote management using, 235–36
  - remote management using, practice exercise, 260
  - scripting, 231
  - Server Core support for, 7, 9
- PPP (Point-to-Point Protocol), 440
- PPTP (Point to Point Tunneling Protocol), 439–40
- Practice exercises
  - AAAA (quad-A) records, configuring, 100
  - account creation, auditing, 417–19
  - Active Directory Certificate Services (AD CS), deploying, 175–76
  - Active Directory Recycle Bin, enabling, 172
  - ADMX files central store, creating a, 215–17
  - delegation, resetting a, using a dsacls command, 261
  - DFS folders, creating, 503–4
  - DFS installation and configuration, 502
  - DFS Namespace (DFSN) configuring, 502
  - DHCP server configuration, 467
  - DNS and Member Servers, preparing for NLB clusters, 533
  - domain functional levels, raise, 170

- forest functional levels, raise, 171
- GPO report, generating, 218
- GPOs, creating and configuring, 217–18
- Group Policy Management Console (GPMC), installing, 214–15
- Group Policy settings, verifying, 219–20
- images, adding to WDS Server, 32–33
- IPv6, configuring, 98–99
- ISATAP routing, enabling, 100
- Namespace server, adding, 502
- Network Load Balancing (NLB) clusters, installing and configuring, 533–35
- Network Policy Server (NPS), configuring, 467–68
- Network Policy Server (NPS), installing, 467
- NLB clusters, configuring and verifying, 533–35
- NLB from NLB cluster, removing, 535
- offline share file settings, configuring, 504
- Online Responder, deploying, 176–79
- password policies, enabling, 172–74
- passwords, delegating management of, 260–61
- performance counters, adding and monitoring, 579–82
- performance monitoring properties, setting, 582–83
- Print and Document Services server role, adding, 359–62
- PSO, creating a, 172–74
- Quota, configuring, 367–69
- remote management using PowerShell, 260
- replication groups, creating, 503–4

Practice exercises, *continued*
- reverse lookup zones, configuring, 101–2
- Role Services, adding to the File Services server roll, 362–67
- security groups, creating, 419–22
- System Health Validators, configuring, 468–69
- user accounts, creating, 419–422
- WDS Server Role, preparing for installation, 30–32
- Windows Server Update Services (WSUS) installation, 423–28

Preboot Execution Environment (PXE)
- images in, adding, 24
- network cards, 13, 19
- response settings, 21–22

Presentation virtualization, 265

Print and Document Services, 301–3, 306
- adding, practice exercise, 359–62

Print devices, 302–3, 315

Print Management console, 304, 306–17

Print paths, 306

Print queues, 302, 306

Print rendering, 304, 307

Print Server role service, 301, 304, 308, 360, 529

Print servers
- adding, 308
- clustering, 303
- managing, 301
- migrating, 306–7
- permissions, individual, setting, 315–17
- properties, managing, 312–15
- remote, 308–9
- securing, 315–17

Print spooler service, 302, 307

Printer drivers, 302–3, 305–6

Printer pool, 302, 315

Printer Redirection Group Policy node, 276

Printer server management, 316

Printers
- access permissions for, 302, 315–17
- individual, 317
- installing, 307–8
- managing, 301–3, 308–17
- network, sharing, 303–4
- print devices and, 302
- publishing, 300, 303–4
- redirecting, 206, 276
- usage of, auditing, 302

Private addresses, 44–45

Private keys, 154–55

Private networks
- connecting to, 233–34
- virtual. *See* VPN (virtual private network)

Privilege use category, 389, 393

Privileges, administrative, delegation of, 251–52, 256

Process Explorer, 558–59, 565–68

Processes
- filtering, 563–64
- monitoring, 561–66
- opening and closing, 564–65
- priority of, changing, 560
- tracking, 382–83

Processes field, 560

Processor usage, tracking, 280

Product key, 13

Profiles Group Policy node, 276

Project planning, 67

Property pages, object, Active Directory Administrative Center, 115

Provision A Shared Folder Wizard, 323–24, 337, 350

Provision Storage Wizard, 326–327, 495

Proxy activation, 25

Proxy servers, 443, 449

PSO Precedence attribute, 129

PSOs. *See* Password Setting Objects (PSOs)

PTR (pointer record), 101–2

Public key infrastructure (PKI), 149, 151, 166–67

Publication, 286–87

Public-Key Cryptography Standards (PKCS) #10, 159

Pull partners, 84

Push partners, 84

PXE. *See* Preboot Execution Environment (PXE)

Q

Quality of Service (QoS), 48

Queries, 116, 551

Quorum models, failover cluster, 523–25

Quotas
- creating, 353–54
- editing, 354
- storage, 324
- templates for, creating, 353–54

R

RACTask, 554

RADIUS (Remote Authentication Dial-In User Service), 436, 438, 447–49

RAID (Redundant Array of Inexpensive Disks), 477, 494–95

RAM (random access memory), 560

RD. *See* Remote Desktop (RD)

RDP-TCP Properties, 272–76

RDS RemoteApp. *See* RemoteApp Manager tool

Read-only domain controllers (RODCs)
- accounts, creating, 120–21, 123–25
- branch office installation, 118–19, 123–25
- client updates, 119–20
- data recovery strategy, 130
- deployment of, 118–19

implementation, 118–23
installation, 112, 120–25, 130
passwords, 119
uses for, 110
Windows Server 2008 DNS Server support, 81
zone type selection, 92
Realm trusts, 140
Redirect Only the Default Client Printer policies, 206
Redirection, folder, 340–41
Redundancy, 475–77
Redundant Array of Inexpensive Disks (RAID), 477, 494–95
Referrals, 480
Registry Editor, 9
Relay agents, DHCP, 62
Releasing IPv4 and IPv6 configurations, 78
Reliability Monitor, 554, 556
Remediation servers, 463
Remote access
administration technologies, 232–36
monitoring, 449–50
Remote Access Service (RAS), 435–38, 453
Remote Desktop (RD), 232–36, 267–68
Remote Desktop Connection Authorization Policies (RD-CAPS), 453
Remote Desktop Connection Broker (RD Connection Broker), 207, 277–279, 529
Remote Desktop Gateway (RD Gateway)
configuration, 452–53
NAP enforcement, 279, 462–63
private networks, connecting to, 234
Remote Desktop Protocol (RDP), 267, 452–53
for Server Core remote connection, 7
shortcut, RemoteApp deployment, 289
Remote Desktop Resource Authorization Policies (RD-RAPS), 454
Remote Desktop Services (RDS), 4, 265. *See also* Terminal Services
deployment planning, 295–296
Group Policy settings in, 202–7, 276–77
installation and configuration, practice exercise, 295–296
licensing, 268–72
RD Connection Broker, 277
Remote Desktop Services Client Access License (RDS CAL), 268–72
Remote Desktop Session Host (RD Session Host) servers, 267–68
capacity, adding, 278
configuring, 272–74
connections, 272–73
encryption setting properties, 273–74
license server discovery scope, 269
load balancing, 278–79
monitoring, 280–81
Properties dialog box, 275
security settings, 272
security tab, 274
server properties, 275
software for, planning, 268
web access, 277
Remote Desktop Virtualization Host, 279
Remote Desktop Web Access (RD Web Access), 277, 289
Remote hosts, pinging, 58
Remote Procedure Call (RPC), 307
Remote Procedure Call Security_Generic Security Services (RPCSEC_GSS), 329
Remote Server Administration Tools (RSAT), 113, 188, 229–30, 306, 308
backups, 607
non-administrator server access, granting, 235–36
overview, 234
Remote Session Environment Group Policy node, 276
RemoteApp Manager tool
deployment, 288–89
installation and configuration, practice exercise, 295–96
remote start of unlisted programs, 202–4
Removable Storage Manager (RSM), 335–36
Renewal, certificate, 157–58
Renewing IPv4 and IPv6 configurations, 78
Replica mode, 405
Replication
AD DS, auditing, 131
DFS, 334, 482–85
filters, editing, 483–85
folder, 482–83
groups, 482–83, 503–4
linked-value, 137
push and pull, 84
scope, planning, 93
topology, 84–86, 484–85
zone, 71, 75–76
Reply attacks, 162
Report Viewer, 398–99, 423
Reporter accounts, 399
Reports
backup, 609
Data Collector Sets (DCSs), viewing, 547
Group Policy Management Console (GPMC), 210–11
Resultant Set of Policies (RSoP), 209–10
storage, 357
system diagnostics, generating, 551–52
Windows Server Update Services (WSUS), 412–13

Reserved address bits, 42
resmon command, 561
Resource allocation, 280–81
Resource and Performance Monitor, 552
Resource Manager, 558–59
Resource Monitor, 560–65
Resources
  authorization policies, 454
  sharing, 322–24
Resources element, 196
Response settings, PXE, 21–22
Restartable AD DS, 111
Restores
  authoritative, 618–22
  non-authoritative, 618. *See also* System state recovery
Restrict Users To The Explicitly Permitted List Of Snap-Ins policy, 285
Restricted-cone NATs, 51
Resultant Set of Policies (RSoP), 209
Retention, log, 237
Reverse lookup zones, 70
  configuring, 87–88
  configuring, practice exercise, 101–2
  creating, 77
Revocation, certificate, 154, 160–61
RFC 2373, 42
RFC 2893, 54
RFC 3053, 53
RFC 3056, 54
RFC 4123, 52
RFC 4214, 54
RFC 4380, 54
Ring replication topology, 85
Ring topology, 85
RODCs. *See* Read-only domain controllers (RODCs)
Role Based Access Control (RBAC), 256
Role services, recovering, 618–25
Roles, recovering, 618–25
Rollback
  forest functional levels, 133
  planning, 25–26
Root Certificate Authorities (CAs), 149, 151–52
Root hints, 93–94
Round-robin policy, load balancing policy, 499
Route aggregation, 48
route print command, 58, 60
Router advertisement messages, 44, 47
Router interfaces, 45, 58–59
Routers, 46, 48, 62
Routes
  existing, modifying, 60
  tracing, 59
Routing and Remote Access Service (RRAS), 62, 435–36
Routing table size, 48

S

Scalability, 137, 307, 345
Scanners, 301
Scavenging settings, 93
Scheduled backups, 598–1
Scheduled deployment, 23
Scheduled Tasks utility, 605–6
Scope
  address, 42
  DHCPv6, 61–62
  link-local address, 43
  site-local address, 44
Scope field, multicast, 46–47
Screening policies, file, 356–57
Scripting tools, 231
Search function, 330, 487
Search Handles box, 565
Secondary zones, 70, 75, 82, 92
Secure Socket Tunneling Protocol (SSTP), 440–41
Security. *See also* Access permissions
  auditing, 347
  checks and reviews, 384–86
  data snapshot, 130
  event logs, 237, 377–80, 391
  network, 47, 64–66
  new feature, 111
  password policies for. *See* Passwords
  policies, 376–77, 380–82, 384–90, 429–30
  print server, 315–17
  RD Session Host server tab, 274
  requirements, identifying, 376–77
  rules, configuring, 456
Security Assertion Markup Language (SAML), 142
Security Group Policy node, 276
Security groups
  creating, practice exercise, 419–22
  DirectAccess, 445
  global, 128–29
Security Identifier (SID) history, 135
Security settings
  delegation of authority using, 249–50
  RD Session Host server connection, 272
Segment hashes, 343
Selective Authentication, 141
Self-Monitoring Analysis and Reporting Technology (SMART), 205
Serially Attached Storage (SAS), 499
Server, content, 342
Server Core
  hardware requirements, 8
  installation, 7–10
  Servermanagercmd.exe on, using, 227
  upgrading issues, 14
  Wbadmin utility, installing, 603
  Windows Web Server 2008 R2 in, 6
Server For Network File System (NFS), 329, 336
Server for NIS (SNIS), 206–7
Server isolation, 457

Server Manager
- AD DS installation, 112–13, 122
- Best Practices Analyzer, 112
- certificate revocation lists (CRLs), 161
- console, 227
- Desktop Experience, 208
- GPMC installation, 188
- Group Policy management, 154, 157
- logon display, 205

Server Message Block protocol (SMB), 321–22, 345

Server role
- backing up, 606–7
- Print and Document Services, planning, 301–2

Server Share Check, 352

Servermanagercmd.exe command-line utility, 227–28

Servers
- Active Directory Domain Services (AD DS), 111–12
- administration tools, 227–32
- Dial-up remote access, 435
- DirectAccess, 444–46
- downstream, 401, 404–5, 413
- failover, implementing DHCP, 62–63
- file, 320–21, 345
- firewall protection, 456
- functional levels and, 133
- license, 270–72
- management technologies, 227–48
- NIS subordinate, 206
- RADIUS, 447
- recovering, 615–17, 622
- redundancy of, 476–77
- remediation, 463
- security for, 315–17, 376–77, 390–91

Server-side targeting, 406

Service Location (SRV) resource records, 83

Services Console, 561, 568–69

Services for Network File System (NFS), 324, 329–30, 336

services.msc command, 568

Session Time Limits Group Policy node, 277

Sessions, tracking, 280

Set The Interval of Synchronization Retires for Servers Running Password Synchronization policy, 206

Set The Map Update Interval for NIS Subordinate Servers, 206

Set The Number of Synchronization Retires for Servers Running Password Synchronization policy, 206

Setup event logs, 237

Shadow copies, 320, 337, 595

Shadow Copies of Shared Folders feature, 336–37, 593–95

Shadow groups, 128

Share and Storage Management, 321–28, 337, 485–86

Shared Folder MMC snap-in, 338, 347

Shared storage, 524

Sharepoint Foundation 2010, 488–90

Sharing
- content, folder and volume, 323
- files, 484
- network printers, 303–4

SHAs (System Health Agent), 343

Shiva Password Authentication Protocol (SPAP), 439

Shortcut trusts, 139

SHVs (System Health Validators), 459
- configuring, practice exercise, 468–69

Silos, 290

Simple Certificate Enrollment Protocol (SCEP), 165–66

Single filtering mode, 518

Single Instance Storage (SIS), 344

Single-host filtering mode, 518

Single-instance applications, 522

Single-sign-on (SSO) functionality, 142

Site IDs, 56

Site Level Aggregator (SLA), 42

Site redundancy, data availability through, 476

Site-local addresses, 44–45

Slash (/) notation, 41

SMART (Self-Monitoring Analysis and Reporting Technology), 205

Smart cards, 394, 438, 440

SMB (Server Message Block) protocol, 321–22, 350

Snap-ins, 228–29, 235

Snapshots
- data, 129–30
- shared folders, 337

SNIS (Server for NIS), 206–7

Soft quotas, 354

Software deployment. *See* Application deployment

Software requirements, IPv6 network, 64–66

Source tab, 544

Source-initiated log subscription, 573–74

Special addresses, 45

Special Administration Console (SAC), 232

SQL Server, 246, 451–52, 609

SSL certificates, 440–41, 453

SSTP (Secure Socket Tunneling Protocol), 440–41

Stability chart, 556

Stability index, 556

Stability, tracking, 554–56

Standalone Certificate Authority (CAs), 147–49

Stand-alone namespaces, 479

Standard primary zones, 70, 82, 92

Starter GPOs, 188–91
- backing up, 191
- configuring, 190
- creating, 189
- policy settings in, 192
- restoring, 191
- System, 188–89, 192
- using, case scenario, 222

Start-of-Authority (SOA) record, 93

Startup types, 568
Stateful address configuration, 44, 47, 61
Stateless address configuration, 44, 47, 61
Storage
  event log, 244
  forensic data, 384
  log file, 451–52
  provisioning, 326, 337, 495
  removable, 335–36
  shared, 524
  subsystem, 337
  Windows Server Update Services (WSUS), 410
Storage Area Networks (SANs), 509–10
Storage Explorer, 338–39, 499–500
Storage Manager for SANs
  Fibre Channel, 497
  File Services option, 321, 331
  installing, 327–28
  iSCSI, 497
  Logical Unit Number (LUN), 339, 496–97
Storage reports, 357
Stripe of mirrors, 477
Stub zones, 70, 73–74
Subnets, 43–45, 58
Subordinate Certificate Authorities (CAs), 149
SubscriptionManager, 577
Subscriptions, event log, 240–242, 391
  collector-initiated, 240–42, 573–76
  creating, 577–78
  details location, 569
  filters, 241
  source-initiated, 573–74, 576–77
Success audits, 377
Support structure, documenting requirements, 67
SupportedOn element, 196
Synchronization
  password, 206–7
  zone, 75–76
System, event logs, managing, 237
System Access Control List (SACL), 130
System category, 390
System Center Configuration Manager 2007 R 3, 414
System Center Data Protection Manager (DPM) 2010, 609–10
System Center Essentials 2010, 399, 414
System Center Operations Manager 2007 R2, 245–246, 380
System Center Operations Manager 2007 R3, 1
System Center Operations Manager 2010, 609
System Center Virtual Machine Manager 2008 R2, 246
System diagnostics data collector set, 546
System event logs, 237
System Health Agents (SHAs), 343, 459
System Health Validators (SHVs), 459
  configuring, practice exercise, 468–69
System Information, Process Explorer, 566–67
System modules, in RSAT tools, 230
System Monitor, 280
System partition, 495
System performance data collector set, 546
System recovery, operating vs. full server, 615
System Starter GPOs, 188–89, 192
System state backups, 597, 606–607
System state recovery
  performing, 617
  practice exercise, 634–37
System table fields, 560
SYSVOL folder, 135, 330, 620

T

Targeting, server-side, 406
Targets
  defined, 497
  priorities of, setting, 480
Task Manager, 558–61
Task Scheduler MMC snap-in, 554
Tasks
  alerts for, setting, 132
  attaching to events, 239–40, 571–72
  list of, for delegation, 251
  removing, 239
TCP connections, verifying, 61
TCP ports, 48, 61, 447
TCP/IPv6 graphical user interface (GUI), 52, 57
Telnet, 61, 236
Templates
  certificate, 147, 156–58
  for quotas, 353–56
Temporary folders Group Policy node, 277
Teredo, 40, 49–51, 54, 444
Terminal Services, 3–4, 202–4. *See also* Remote Desktop Services
Terminal Services Session Broker, 207
Threads field, 560
Time zone redirection policy, 204
Time-To-Live (TTL) values, 93
TMG (Forefront Threat Management Gateway), 457–59
Tombstone lifetime, 618
Tombstone reanimation, 117, 130, 623
Top Level Aggregator (TOP), 42
Topology
  global unicast, 43
  network, 338, 499
  replication, 84–86, 484–85
  WINS, 84–87
tracert-d command, 59

Tracking
processes, 382–83
processor usage, 280
sessions, 280
stability, 554–56
trends, 542, 549
Traffic management, 48, 456, 517–19
Transactions, defined, 528
Transfers, zone, 75–76
Transient (T) flag, 46
Transition strategies, IPv4-to-IPv6, 46–47, 52–54
Transmission Control Protocol (TCP) ports, 48, 61
Trends, tracking, 542, 549
Trojans. *See* Attacks, external
Troubleshooting
core processing, 211–12
Group Policy settings, 208–12
Trusted delegate, 252
Trusted Platform Module (TPM), 395
Trusts, 139–40. *See also* Forest trusts
TS Gateway. *See* Remote Desktop Gateway (RD Gateway)
TS Session Broker. *See* Terminal Services Session Broker
Tunnel brokers, 53
Tunneling
6to4, 54, 443–44, 447
automatic, 53
configured, 53
ISATAP, 54
Teredo, 54
Tunnels, 53
site-to-site, 441
VPN, 438, 440
Turn On Extensive Logging for Active Domain Services Domain Controllers Running Server for NIS policy, 207
Turn On Extensive Logging for Password Synchronization policy, 207
Two-stage installation, RODC, 120–25, 130

U

Unassigning LUNs, 495
Unicast addresses, 41–45
Unicast cluster operation mode, 515
Universal distribution groups, 135
UNIX environment
Kerberos authentication protocol in realm trust, 140
name resolution, 94
servers, printing to, 301
Services for Network File System, 329, 336
Unmapped UNIX User Access feature, 329, 336
Unspecified addresses, IPv6, 45
Up Time field, 560
Update certificates that use certificate templates policy, 158
Updates
automatic approval rules for, 410–11
certificate, 157
deploying, 398
dynamic, 72–73, 83, 93
intervals for, setting, 206
performance counter graph, 544
roaming client, 409
Upgrade process
compatibility checks for, 14–15
from Windows Server 2003, 13–15, 181
from Windows Server 2008, case scenario, 371
functional levels, practice exercise, 170–71
rollback, 25–26
Server Core, 14
Use RD Connection Broker Load Balancing policy, 207
User accounts
blocking, from delegation, 254
creating, practice exercise, 419–22
User Configuration settings
Administrative Templates settings, 190
disabling, 201
User Datagram Protocol (UDP) ports, 48, 50, 441, 447
User Logon Mode settings, 275, 278
User rights, 347
Users and Computers containers, 135

V

Validate A Configuration Wizard, 526
Validation
failover cluster, 526
system health, 459
VAMT (Volume Activation Management Tool), 25
VDS. *See* Virtual Disk Service (VDS)
Versioning, 488–90
Views, custom, 239, 391, 570
Violations, security policy, 377, 380–82
Virtual Disk Service (VDS), 326–27, 495–96
Virtual Hard Disk (VHD) files, 596
Virtual local area network (VLAN) identifiers, 62, 461
Virtual Machine, 529
Virtual private networks. *See* VPN (virtual private network)
Virtualization
Datacenter Edition, Windows Server 2008 R2, 5
platforms, backing up, 609
presentation, 265
upgrading issues, 14
Viruses. *See* Attacks, external
VLAN (virtual local area network) identifiers, 62, 461
Volume activation, 24
Volume Activation Management Tool (VAMT), 25
Volume management, 322–23

Volume Shadow Copy Service (VSS), 129, 602
Volume Snapshot driver, 337
Volumes
- managing, 322–23, 327, 334–35
- RAID (Redundant Array of Inexpensive Disks), creating, 477–78
- recovering, 615
- reverting, 337
- selecting, for indexing, 487
- shadow copies on, storing, 595
- viewing shared properties of, 324

VPN (virtual private network)
- authentication, 438–39
- Connection interface, 436–37
- DirectAccess comparison, 442–44
- NAP enforcement, 461–62
- protocols, 439–42
- Remote Access for, enabling, 436
- subnet connection, 233–34
- tunnels, 438, 440

VPN Reconnect, 441–42
VSS Copy Backup, 602
VSS Full Backup, 602

W

w.x.y.z (IPv4-compatible address), 49
WAIK (Windows Automated Installation), 17–18
Wait chains, viewing process, 565
Wbadmin command-line tool
- list of commands, 603–5
- restoring files and folders using, 625–26
- utility, 603

wbadmin commands, 596–97
Wbadmin.exe utility
- installation, 598
- volume and system state backup, practice exercise, 631–32

WDS. *See* Windows Deployment Services (WDS)
Web applications
- deployment, 285–86
- Sharepoint Foundation 2010, creating, 488–90

Web enrollment, certificate, 153, 159
Web proxy caching, 162
Web Services Federation (WS-Federation), 142
Web Services on Devices (WSD), 301, 307
WebDav (Web Distributed Authoring and Versioning), 286–87
Website configuration task, delegation of, 256–57
wecutil command, 575
Weighted path, load balancing policy, 499
Weighted_Remote_Session WSRM policy, 281
Wevtutil, 244–45
Wide area network (WAN) connections, 118–20, 341–43, 609
Windows 2008 DNS Server service, 75
Windows 7
- Administrative Template policy setting enhancements, 188
- ADMX files in, 194
- DirectAccess, connecting to, 443–44
- IKEv2 protocol, 441–42
- RD Session Host server connection, 272
- Remote Server Administration Tools (RSAT), 234
- System Health Validators in, configuring, 459
- Windows NT Backup Restore Utility, 335

Windows AIK tool, 17–18
Windows Automated Installation Kit (Windows AIK) tool, 17–18
Windows Complete PC Restore, 616
Windows Deployment Services (WDS), 7, 13, 19–22
- configuring and installing, practice exercise, 30–33
- images, 24, 32–33
- product activation, 24–25

Windows Deployment Services Configuration Wizard, 19
Windows Event Collector service, 573
Windows Firewall With Advanced Security snap-in, 59, 447, 456
Windows Installer Packages, 284, 289–90
Windows Internet Naming Service. *See* WINS (Windows Internet Naming Service)
Windows Management Instrumentation (WMI), 329
Windows Network Diagnostics, 572–73
Windows NT Backup Restore Utility, 335
Windows Preinstallation Environment (Windows PE), 13, 19
Windows Presentation Foundation (WPF), 305
Windows Process Activation Service, 175, 277
Windows Remote Management (WinRM), 7, 573–75
Windows Script Host scripts, 9
Windows Search Service, 330, 487
Windows Server 2003
- Teredo addresses, 49
- upgrading from, 13–15

Windows Server 2003 File Services, 330
Windows Server 2008
- Active Domain Directory Services (AD DS), 111
- cluster tools, 522–23
- configuring, 72–73
- differences between Windows Server 2008 R2 and, 3–4

- forest functional levels in, 135–36
- MPIO (Multipath I/O), 499
- namespace mode, 480
- PowerShell 2.0, adding to, 230
- Server Core in, 9
- server roles, adding and removing, 227
- Windows Server Backup, key enhancements, 596

Windows Server 2008 DNS
- compliance, 72
- new features of, 81
- planning, 71

Windows Server 2008 R2
- activation, 24–25
- Administrative Template policy setting enhancements, 188
- answer files, 17–19
- Datacenter Edition, 5–6, 12, 14
- differences between Windows Server 2008 and, 3–4
- editions, selecting appropriate, 4
- Enterprise Edition, 5, 10, 12, 14
- File Services enhancements, 332–45
- Foundation Edition, 4, 7–8
- FTP (File Transfer Protocol), 287–88
- Group Policy settings, new in, 202–7
- HPC Server, 7
- IKEv2 protocol, 441–42
- installation, 12–13
- Itanium-based systems, 6, 14
- new features, 4
- print enhancements, using, 304–7
- restoring, practice exercise, 632–34
- Server Core in, 9
- Standard Edition, 4–5
- storage, 494–500
- upgrading, 14
- versions, 4–7
- Windows NT Backup Restore Utility, 335
- Windows Server Backup, key enhancements, 596–98

Windows Server 2008 R2 DNS, 71–73

Windows Server Backup, 321, 331
- installation, 598–99
- manual backup, practice exercise, 628–31
- performance optimization, 602
- recovery operations, 613
- remote access using, 607–608
- restoring files and folders using, 625–26
- scheduled backups, configuring, 599–1
- unscheduled backups, 602
- Windows Server 2008 R2, key enhancements, 596–98
- Windows Server 2008, key enhancements, 595–96

Windows Server Update Services (WSUS)
- automatic approval rules, 410–11
- computer group properties, 406
- disconnected server deployment, 403
- multiple independent server deployment, 401
- multiple internally synchronized server deployment, 401–2
- overview, 398
- reports, 412–13
- scheduling, 407–9
- single server deployment, 400
- storage, 410

Windows Server Update Services (WSUS) SP2
- case scenario, 430
- features, 404
- installation, 398–400
- installation, practice exercise, 423–28
- local groups, 399

Windows Server Virtualization. *See* Hyper-V Dynamic Memory

Windows Storage Server 2008 R2, 344–45

Windows System Image Manager (Windows Sim) tool, 17–18

Windows System Resource Manager (WSRM), 280–81

Windows Update Agent (WUA), 404

Windows Vista
- ADMX files in, 194
- RD Session Host server connection, 272
- Remote Server Administration Tools (RSAT), 234
- System Health Validators in, configuring, 459

Windows Web Server 2008 R2, 6

Windows XP
- credential roaming policy, 155
- L2TP/IPsec protocol, 440
- NAP enforcement support, 460–61
- RD Session Host connection, 272–73
- Remote Desktop Protocol (RDP), 453
- Remote Desktop Web Access (RD Web Access), 277
- System Health Validators in, configuring, 459
- System Starter GPOs, 189
- Teredo addresses, 49
- WebDAV, 286
- Windows Search Service, 487
- XPS Document format, 305

Windows XP Professional, RSAT tools and, 234

WinRM (Windows Remote Management), 7, 573–75

winrm commands, 574–76

WINS (Windows Internet Naming Service)
- NetBIOS name resolution using, 70, 82–83
- replication topology, 83–87
- servers, 40, 529

Workgroup discovery scope, 269
Working patterns, documenting requirements, 67
Workload considerations, physical versus virtual deployment, 12
Worms. *See* Attacks, external

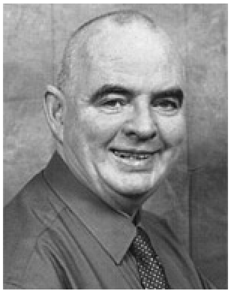
X

x64 processors, 3, 6, 12, 14, 24
x86 processors, 3, 13–14
XML declaration, 196
XPS (XML Paper Specification) document format, 304–5
XPSDrv printer drivers, 305

Z

Zero suppression, leading, 41
Zone data
  loading, 81–82
  storage of, 71
Zone ID, 58
Zone replication, 71, 75–76
Zone transfers, 71, 93
Zone types, 92
Zones
  forward lookup, 71, 92–93
  GlobalNames, 95–96
  integrated, 70, 92
  primary read-only, 81
  reverse lookup, 70, 77, 87–88
  reverse lookup, configuring, practice exercise, 101–2
  secondary, 70, 75, 82, 92
  standard primary, 70, 82, 92

About the Authors



IAN MCLEAN, MCSE, MCTS, MCITP, MCT, has over 40 years experience in industry, commerce, and education. He started his career as an electronics engineer before going into distance learning and then education as a university professor. Currently he runs his own consultancy company. Ian has written over 20 books plus many papers and technical articles. He has been working with Microsoft Server operating systems since 1997.

ORIN THOMAS, MCITP, MCT, MVP is an author, trainer and regular public speaker who has authored more than a dozen books for Microsoft Press. He holds the MCITP Server Administrator and Enterprise Administrator certifications. He is the convener of the Melbourne Security and Infrastructure Group and a Microsoft vTSP. His most recent books are on Windows 7 and Exchange Server 2010. You can follow him on Twitter @orinthomas.