## 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 website for the most current listing of exam objectives: http://www.microsoft.com/learning/en/us/Exam.aspx?ID=70-647.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Lesson</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Planning Network and Application Services (23 percent)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan for name resolution and IP addressing.</td>
<td>Chapter 1</td>
<td>Lesson 1, 2</td>
</tr>
<tr>
<td>Design for network access.</td>
<td>Chapter 5</td>
<td>Lesson 1, 2</td>
</tr>
<tr>
<td>Plan for application delivery.</td>
<td>Chapter 7</td>
<td>Lesson 2</td>
</tr>
<tr>
<td>Plan for Remote Desktop Services.</td>
<td>Chapter 7</td>
<td>Lesson 1</td>
</tr>
<tr>
<td><strong>Designing Core Identity and Access Management Components (25 percent)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design Active Directory forests and domains.</td>
<td>Chapter 2</td>
<td>Lesson 1</td>
</tr>
<tr>
<td>Design the Active Directory physical topology.</td>
<td>Chapter 2</td>
<td>Lesson 2</td>
</tr>
<tr>
<td>Design the Active Directory administrative model.</td>
<td>Chapter 4</td>
<td>Lesson 1</td>
</tr>
<tr>
<td>Design the enterprise-level group policy strategy.</td>
<td>Chapter 4</td>
<td>Lesson 2</td>
</tr>
<tr>
<td><strong>Designing Support Identity and Access Management Components (29 percent)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan for domain or forest migration, upgrade, and restructuring.</td>
<td>Chapter 3</td>
<td>Lesson 1</td>
</tr>
<tr>
<td>Design the branch office deployment.</td>
<td>Chapter 6</td>
<td>Lesson 1, 2</td>
</tr>
<tr>
<td>Design and implement public key infrastructure.</td>
<td>Chapter 10</td>
<td>Lesson 1, 2</td>
</tr>
<tr>
<td>Plan for interoperability.</td>
<td>Chapter 3</td>
<td>Lesson 2</td>
</tr>
<tr>
<td><strong>Designing for Business Continuity and Data Availability (23 percent)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan for business continuity.</td>
<td>Chapter 9</td>
<td>Lesson 3</td>
</tr>
<tr>
<td>Design for software updates and compliance management.</td>
<td>Chapter 11</td>
<td>Lesson 1, 2</td>
</tr>
<tr>
<td>Design the operating system virtualization strategy.</td>
<td>Chapter 8</td>
<td>Lesson 1, 2</td>
</tr>
<tr>
<td>Design for data management and data access.</td>
<td>Chapter 2, 4</td>
<td>Lesson 1, 1</td>
</tr>
</tbody>
</table>
This page intentionally left blank

David R. Miller
Paul Mancuso
John Policelli
Orin Thomas
Ian McLean
J.C. Mackin
with GrandMasters
I dedicate this, and each of my books, to my daughter, Veronica, and my son, Ross. With all my love, appreciation, and admiration.

—David R. Miller

I would like to dedicate my contribution to this book to my loving wife, Yaneth, and wonderfully musical son, Anthony. Thank you both for all of your love and support.

—Paul Mancuso

This book is dedicated to my beautiful wife, Maria. Your continued love and support means the world to me, and I wouldn’t be where I am today without you.

—John Policelli
This page intentionally left blank
# Contents at a Glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td></td>
<td>xv</td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td>Planning Name Resolution and Internet Protocol Addressing</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>Designing Active Directory Domain Services</td>
<td>75</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>Planning Migrations, Trusts, and Interoperability</td>
<td>137</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>Designing Active Directory Administration and Group Policy Strategy</td>
<td>165</td>
</tr>
<tr>
<td>CHAPTER 5</td>
<td>Designing a Network Access Strategy</td>
<td>213</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>Design a Branch Office Deployment</td>
<td>277</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>Designing Remote Desktop Services and Application Deployment</td>
<td>327</td>
</tr>
<tr>
<td>CHAPTER 8</td>
<td>Designing Virtualization</td>
<td>367</td>
</tr>
<tr>
<td>CHAPTER 9</td>
<td>Designing Solutions for Data Sharing, Data Security, and Business Continuity</td>
<td>403</td>
</tr>
<tr>
<td>CHAPTER 10</td>
<td>Planning and Designing a Public Key Infrastructure</td>
<td>451</td>
</tr>
<tr>
<td>CHAPTER 11</td>
<td>Designing Software Update Infrastructure and Managing Compliance</td>
<td>491</td>
</tr>
</tbody>
</table>

Answers 531

Glossary 567

Index 577
This page intentionally left blank
Contents

**Introduction**  
Lab Setup Instructions ............................................ xv  
Using the CD .............................................................. xvii  
Acknowledgments ....................................................... xx  
Support & Feedback ..................................................... xx  
Preparing for the Exam ............................................... xxii

**Chapter 1  Planning Name Resolution and Internet Protocol Addressing**  
Lesson 1: Planning Name Resolution ............................... 4  
  Planning Domain Name System Using Windows Server 2008 R2 5  
  Using New DNS Features and Enhancements ...................... 11  
  Planning a DNS Infrastructure ................................. 18  
Lesson 2: Planning Internet Protocol Addressing ............... 32  
  Analyzing the IPv6 Address Structure ......................... 33  
  Investigating the Advantages of IPv6 ......................... 42  
  Implementing IPv4-to-IPv6 Compatibility ....................... 44  
  Planning an IPv4-to-IPv6 Transition Strategy .................. 48  
  Using IPv6 Tools ..................................................... 50  
  Configuring Clients Through DHCPv6 ......................... 55  
  Planning an IPv6 Network .................................... 57

**Chapter 2  Designing Active Directory Domain Services**  
Lesson 1: Designing AD DS Forests and Domains ............... 77

---

What do you think of this book? We want to hear from you!  
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:  
[www.microsoft.com/learning/booksurvey/]
Designing the Forest Structure 77
Designing the Domain Structure 85
Designing Functional Levels 92
Designing the Schema 97
Designing Trusts to Optimize Intraforest Authentication 99

Lesson 2: Designing the AD DS Physical Topology 107
Designing the Site Structure 109
Designing Replication 112
Designing the Placement of Domain Controllers 117
Designing Printer Location Policies 121

Chapter 3 Planning Migrations, Trusts, and Interoperability 137
Lesson 1: Planning for Migration, Upgrade, and Restructuring 139
  Migration Paths 139
  Upgrading an Existing Domain to Windows Server 2008 R2 141
  Cross-Forest Authentication 143
Lesson 2: Planning for Interoperability 148
  Planning Active Directory Federation Services 148
  Planning for UNIX Interoperability 151

Chapter 4 Designing Active Directory Administration and Group Policy Strategy 165
Lesson 1: Designing the Active Directory Domain Services Administrative Model 168
  Delegating Active Directory Domain Services Administration 168
  Using Group Strategy to Delegate Management Tasks 172
  Planning to Audit AD DS and Group Policy Compliance 180
  Planning Organizational Structure 182
Lesson 2: Designing Enterprise-Level Group Policy Strategy 189
  Planning a Group Policy Hierarchy 190
  Controlling Device Installation 192
  Planning Authentication and Authorization 199
Chapter 5  Designing a Network Access Strategy  213
Lesson 1: Perimeter Networks and Remote Access Strategies .............. 216
  Designing the Perimeter Network  216
  Deploying Strategic Services in the Perimeter Network  223
  Designing a Remote Access Strategy  224
  Designing a RADIUS Solution for Remote Access  236
Lesson 2: Designing Network Access Policy and Server and
  Domain Isolation ........................................... 245
  Network Access Protection Overview  245
  Considerations for NAP Enforcement  252
  Planning NAP IPsec Enforcement  253
  Planning NAP VPN Enforcement  259
  Planning NAP 802.1x Enforcement  261
  Planning NAP DHCP Enforcement  265
  Domain and Server Isolation  267

Chapter 6  Design a Branch Office Deployment  277
Lesson 1: Branch Office Deployment .................................. 280
  Branch Office Services  280
  Branch Office Communications Considerations  295
Lesson 2: Branch Office Server Security  ............................. 301
  Overview of Security for the Branch Office  302
  Securing Windows Server 2008 in the Branch Office  303

Chapter 7  Designing Remote Desktop Services and Application Deployment  327
Lesson 1: Designing Remote Desktop Services  ...................... 329
  Planning a Remote Desktop Session Deployment  329
  Remote Desktop Licensing  331
  Deploying Applications Using Remote Desktop Web Access  337
  Planning the Deployment of Applications Using RemoteApp  338
  Planning RD Session Host Server Farms  340
  Planning the Migration to Remote Desktop Connection Broker  340
<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Designing Virtualization</th>
<th>367</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesson 1: Designing Operating System Virtualization</td>
<td>368</td>
<td></td>
</tr>
<tr>
<td>Planning for Hyper-V</td>
<td>370</td>
<td></td>
</tr>
<tr>
<td>Planning for Guest Operating Systems</td>
<td>371</td>
<td></td>
</tr>
<tr>
<td>Managing Virtualized Servers</td>
<td>377</td>
<td></td>
</tr>
<tr>
<td>Candidates for Virtualization</td>
<td>380</td>
<td></td>
</tr>
<tr>
<td>Planning for Server Consolidation</td>
<td>381</td>
<td></td>
</tr>
<tr>
<td>Lesson 2: Designing Application Virtualization</td>
<td>390</td>
<td></td>
</tr>
<tr>
<td>Microsoft Application Virtualization</td>
<td>390</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Designing Solutions for Data Sharing, Data Security, and Business Continuity</th>
<th>403</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesson 1: Planning for Data Sharing and Collaboration</td>
<td>405</td>
<td></td>
</tr>
<tr>
<td>Planning a DFS Deployment</td>
<td>405</td>
<td></td>
</tr>
<tr>
<td>DFS Namespaces Advanced Settings and Features</td>
<td>408</td>
<td></td>
</tr>
<tr>
<td>DFS Replication Advanced Settings and Features</td>
<td>410</td>
<td></td>
</tr>
<tr>
<td>Overview of the DFS Design Process</td>
<td>412</td>
<td></td>
</tr>
<tr>
<td>Planning a SharePoint Infrastructure</td>
<td>413</td>
<td></td>
</tr>
<tr>
<td>Lesson 2: Choosing Data Security Solutions</td>
<td>423</td>
<td></td>
</tr>
<tr>
<td>Protecting Volume Data with BitLocker</td>
<td>423</td>
<td></td>
</tr>
<tr>
<td>Choosing a BitLocker Authentication Mode</td>
<td>424</td>
<td></td>
</tr>
<tr>
<td>BitLocker Security Design Considerations</td>
<td>425</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10 Planning and Designing a Public Key Infrastructure 451
Lesson 1: Identifying PKI Requirements ........................................... 453
  Reviewing PKI Concepts 453
  Identifying PKI-Enabled Applications 454
  Identifying Certificate Requirements 456
  Reviewing the Company Security Policy 459
  Assessing Business Requirements 459
  Assessing External Requirements 460
  Assessing Active Directory Requirements 460
  Assessing Certificate Template Requirements 461
Lesson 2: Designing the CA Hierarchy ............................................. 464
  Planning the CA Infrastructure 464
Lesson 3: Creating a Certificate Management Plan ............................ 475
  Selecting a Certificate Enrollment Method 475
  Creating a CA Renewal Strategy 479
  Defining a Revocation Policy 479

Chapter 11 Designing Software Update Infrastructure and Managing Compliance 491
Lesson 1: Designing a Software Update Infrastructure ........................ 493
  Microsoft Update as a Software Update Solution 493
  Windows Server Update Services as a Software Update Solution 494
  System Center Essentials 2010 501
  System Center Configuration Manager 2007 504
Lesson 2: Managing Software Update Compliance ................. 513
  Microsoft Baseline Security Analyzer 513
  System Center Configuration Manager 2007 Compliance and Reporting 517
  Planning and Deploying Security Baselines 518

Answers 531

Glossary 567

Index 577

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our
books and learning resources for you. To participate in a brief online survey, please visit:
www.microsoft.com/learning/booksurvey/
Introduction

This training kit is designed for enterprise administrators who have several years’ experience managing the overall IT environment and architecture of medium to large organizations and who plan to take the Microsoft Certified Information Technology Professional (MCITP) 70-647 exam. As an enterprise administrator, you likely are responsible for translating business goals into technology decisions and designs and for developing mid-range and long-term strategies. You are responsible for making key decisions and recommendations about network infrastructure, directory services, identity management, security policies, business continuity, IT administrative structure, best practices, standards, and Service Level Agreements (SLAs). Your job role involves 20 percent operations, 60 percent engineering, and 20 percent support tasks. The Preparation Guide for Exam 70-647 is available at http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-647.

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

■ Plan network and application services.
■ Design core identity and access management components.
■ Design support identity and access management components.
■ Design for business continuity and data availability.

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

Lab Setup Instructions

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

■ One server running Windows Server 2008 R2 Enterprise configured as a domain controller.
■ One computer running Windows Vista (Enterprise, Business, or Ultimate). (Windows 7 Pro, Enterprise, or Ultimate may be used; however, dialogs may be slightly different than described or shown.)


All computers in these lab exercises must be connected to the same network. It is recommended 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, using virtual machines is recommended. To run computers as virtual machines within Windows, you can use Virtual PC 2007, Virtual Server 2005 R2, Hyper-V, or third-party

**Hardware Requirements**

You can complete almost all practice exercises in this book by using virtual machines rather than real server hardware. The minimum and recommended hardware requirements for Windows Server 2008 and Windows Server 2008 R2 are listed in the following tables:

**TABLE I-1** Windows Server 2008 Minimum Hardware Requirements

<table>
<thead>
<tr>
<th>HARDWARE COMPONENT</th>
<th>MINIMUM REQUIREMENTS</th>
<th>RECOMMENDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>1GHz (x86), 1.4GHz (x64)</td>
<td>2GHz or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>15 GB</td>
<td>40 GB</td>
</tr>
</tbody>
</table>

**TABLE I-2** Windows Server 2008 R2 Minimum Hardware Requirements

<table>
<thead>
<tr>
<th>HARDWARE COMPONENT</th>
<th>MINIMUM REQUIREMENTS</th>
<th>RECOMMENDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>1.4GHz (x64) or 1.3GHz (x64 Dual Core)</td>
<td>2GHz or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>32 GB</td>
<td>80 GB</td>
</tr>
</tbody>
</table>

If you intend to implement several virtual machines on the same computer (recommended), a higher specification will enhance your user experience. In particular, a computer with 4 GB of RAM and 100 GB of free disk space can host all the virtual machines specified for all the practice exercises in this book.

**Preparing the Computer Running Windows Server 2008 R2 Enterprise**

Detailed instructions for preparing for Windows Server 2008 R2 installation and installing and configuring the Windows Server 2008 R2 Enterprise domain controller are given in Chapter 1, “Planning Name Resolution and Internet Protocol Addressing.” The required server roles are added in the practice exercises in subsequent chapters.
Preparing the Computer Running Windows Vista or Windows 7

Perform the following steps to prepare your computer running Windows Vista or Windows 7 for the exercises in this training kit.

Check Operating System Version Requirements

In System Control Panel (found in the System And Maintenance category), verify that the operating system version is Windows Vista or Windows 7 (Enterprise, Business, Professional, or Ultimate). If necessary, choose the option to upgrade to one of these versions.

Name the Computer

In System Control Panel, specify the computer name as Melbourne.

Configure Networking

To configure networking, carry out the following tasks:

1. In Control Panel, click Set Up File Sharing.
2. In Network And Sharing Center, verify that the network is configured as a Private network and that File Sharing is enabled.
3. In Network And Sharing Center, click Manage Network Connections.
4. In Network Connections, open the properties of the Local Area Connection. Specify a static IPv4 address that is on the same subnet as the domain controller.

For example, the setup instructions for the domain controller specify an IPv4 address 10.0.0.11. If you use this address, you can configure the client computer with an IP address of 10.0.0.21. The subnet mask is 255.255.255.0, and the Domain Name System (DNS) address is the IPv4 address of the domain controller. You do not require a default gateway. You can choose other network addresses if you want to, provided that the client and server are on the same subnet.

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 Vista and Windows 7 by using electronic practice tests you customize to meet your needs from the pool of Lesson Review questions in this book, or you can practice for the 70-647 certification exam by using tests created from a pool of 200 realistic exam questions to ensure that you are prepared.
An eBook  An electronic version of this book is included for when you do not want to carry the printed book with you. The eBook is available in two formats: Portable Document Format (PDF), which can be viewed by using Adobe Acrobat or Adobe Reader, and XML Paper Specification (XPS).

How to Install the Practice Tests
To install the practice test software from the companion CD to your hard disk, do the following:

1. Insert the companion CD into your CD drive and accept the license agreement. A 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 alternative 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, click All Programs, and then select Microsoft Press Training Kit Exam Prep. A window appears that shows all the Microsoft Press training kit exam prep suites installed on your computer.

2. Double-click the lesson review or practice test you want to use.

   **NOTE** **LESSON REVIEWS VS. PRACTICE TESTS**

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 default settings, or you can customize the number of questions you want, how the practice test software works, the exam objectives
to which you want the questions to relate, 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 and Previous 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 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 you chose and the percentage of questions you got right 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.

- **Certification 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**  Creates an untimed test during which you can review the correct answers and the explanations after you answer each question.
- **Custom Mode**  Gives you full control over the test options so that you can customize them as you like.

In all modes, the user interface when you are taking the test is basically the same, but has 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 that 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 Programs And Features option in Windows Control Panel.
Acknowledgments

David Miller would like to acknowledge his coauthors, Paul Mancuso and John Policelli. Great job, guys. I am proud to be working with you. Thank you both.

All the authors would like to acknowledge and thank the talented teams from GrandMasters, LLC, and Microsoft Press for their tireless pursuit of accuracy, precision, and clarity. Thank you for your assistance, your support, and your skillful efforts.

Lastly, the authors would like to acknowledge and thank you, the reader, for your desire for self-improvement and your faith in us to produce a resource worthy of your time and consumption. We've done our best to make this book a powerful asset in your efforts to be a better IT professional. We hope you find it so. Thank you.

Support & Feedback

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

Errata

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=219405

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 mspininput@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’s keep the conversation going! We’re 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. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment 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 3

Planning Migrations, Trusts, and Interoperability

This chapter focuses on how to get Microsoft Windows Server 2008 R2 working with other technologies and other operating systems. In the first lesson, you learn which factors you need to consider when planning an organization’s move from an existing Active Directory directory service environment to one based on Windows Server 2008 R2 Active Directory Domain Services (AD DS). You will also learn what steps to consider when planning a trust relationship between one AD DS environment and another. The second lesson in this chapter focuses on the topic of interoperability, which includes ensuring that users of Windows-based and UNIX-based computers are able to work seamlessly together. This lesson also includes information about technologies by which you can migrate services and applications that traditionally run on UNIX-based computers only, so that they can be hosted on computers on which the Windows Server 2008 R2 operating system is installed.

Exam objectives in this chapter:
- Plan for domain or forest migration, upgrade, and restructuring.
- Plan for interoperability.

Lessons in this chapter:
- Lesson 1: Planning for Migration, Upgrade, and Restructuring 139
- Lesson 2: Planning for Interoperability 148
Before You Begin

To complete the lessons in this chapter, you must have installed a Windows Server 2008 R2 Enterprise domain controller named Glasgow as described in Chapter 1, “Planning Name Resolution and Internet Protocol Addressing.” No additional configuration is required for this chapter.

**REAL WORLD**

John Policelli

In the 10 years that I have been working with Active Directory, I have been involved in countless migrations and upgrades. Over these years, I have had the opportunity to see the evolution of Active Directory migrations. As one would expect, the migration processes have improved with the progression of the technology and the maturity of the product. I have also seen the complexity of migrations increase substantially over the years. Organizations have had to migrate and upgrade for fairly basic technical reasons, such as staying within support and leveraging new features, as new versions of the Windows Server operating system have been released. However, organizations in this day and age have important business drivers, such as mergers and acquisitions and increased pressure to consolidate, which often result in very complex migrations. I’ve come to realize that the most complex and difficult migrations are much more achievable through proper planning.
Lesson 1: Planning for Migration, Upgrade, and Restructuring

Although it is possible to add a member server running Windows Server 2008 R2 to an existing Microsoft Windows Server 2003 domain, at some point in your organization’s migration to Windows Server 2008 R2, you are going to want to upgrade your organization’s domain controllers. In this lesson, you learn which steps you need to take to move from a network environment that is dependent on a previous version of Microsoft Windows to a Windows Server 2008 R2 Active Directory–based network infrastructure.

After this lesson, you will be able to:
- Prepare the environment for Windows Server 2008 R2.
- Migrate objects.
- Plan domain consolidation.

Estimated lesson time: 40 minutes

Migration Paths

You can take one of three general paths to move from an existing AD DS environment to a Windows Server 2008 R2 AD DS environment. These paths are known as the domain upgrade, the domain restructure, and the upgrade-then-restructure. When planning which method to use, consider factors such as the amount of time the migration should take and the availability of new server hardware. An operating system upgrade is an ideal time to reassess your business requirements and compare these to your existing AD DS design, and potentially identify opportunities for increased efficiencies and cost savings.

Domain Upgrade Migration Path

The domain upgrade migration path involves upgrading the operating system of a domain controller running Windows Server 2003 or Windows Server 2008 to Windows Server 2008 R2 or installing Windows Server 2008 R2 domain controllers into a Windows 2000 Server or Windows Server 2003 domain. If you are planning to add Windows Server 2008 R2 domain controllers to a domain, you need to ensure that domains in your organization are at the Windows 2000 Native functional level or higher. Domains at the Windows 2000 mixed or Windows Server 2003 interim functional level do not support Windows Server 2008 R2 domain controllers. There is no direct upgrade path between Windows 2000 Server and Windows Server 2008 R2. Plan to use the domain upgrade migration path when you will not have access to a significant amount of new server hardware on which to install new deployments of Windows Server 2008 R2.
Domain Restructure Migration Path

The *domain restructure migration path* involves copying AD DS objects from the original domain or forest to the new Windows Server 2008 R2 domain or forest, using tools, such as the Active Directory Migration Tool, covered later in this lesson. After all objects are migrated, the domain controllers in the original domain or forest are decommissioned. The domain restructure migration path includes the following advantages:

- The original environment remains the same until the migration is completed. Users are not forced to the new environment until it is tested and ready.
- It enables the selective migration of objects. When you perform a domain upgrade, all objects are upgraded, including those that are redundant, inactive, and no longer necessary. Domain restructure migrations enable organizations to clean up their environments as they transition to the new technology.

The domain restructure migration requires you to have enough new server hardware to support both the original and destination environments concurrently. If the budget does not allow for new server hardware, the domain upgrade migration path is a more feasible alternative. Although it is possible to perform a domain restructure migration using virtualization, you should avoid this approach unless you are planning an AD DS deployment that primarily involves virtualized domain controllers.

Upgrade-Then-Restructure Migration Path

The upgrade-then-restructure migration path, also known as a two-phase migration, involves upgrading the original domain or forest and then migrating AD DS objects to a new Windows Server 2008 R2 domain or forest. This process essentially combines the domain upgrade and domain restructure approaches, enabling an organization to benefit immediately from a Windows Server 2008 R2 upgrade and then to transition to new Windows Server 2008 R2 domain controller hardware at some point in the future, with the added benefit of removing unnecessary AD DS objects through the selective migration process.

Active Directory Migration Tool

You can use the Active Directory Migration Tool v3.2 (ADMT v3.2) to migrate AD DS objects within a forest, referred to as an *intraforest migration*, or to migrate objects to another forest, referred to as an *interforest migration*. You can use the ADMT to migrate users, groups, managed service accounts, computers, and trusts. The ADMT has a simulation mode that enables administrators to evaluate the results of planned migrations prior to performing the actual migrations.

**MORE INFO  OBTAIN THE ACTIVE DIRECTORY MIGRATION TOOL**

Upgrading an Existing Domain to Windows Server 2008 R2

There are two basic strategies for transitioning from an existing domain to a Windows Server 2008 R2 AD DS domain. The first strategy is to introduce new Windows Server 2008 R2 domain controllers into the forest and then either to retire or upgrade existing Windows Server 2003 or Windows Server 2008 domain controllers. The second strategy is simply to perform an in-place upgrade of all existing Windows Server 2003 or Windows Server 2008 domain controllers. Both of these strategies are useful when pursuing the domain upgrade migration path.

Preparing the Environment

You need to perform several steps prior to adding a Windows Server 2008 R2 domain controller to an existing AD DS environment, even if you do not intend to change the current domain or forest functional level. These steps include ensuring that existing domain controllers in the environment have appropriate patches and service packs installed and that the AD DS schema has been appropriately prepared for the introduction of Windows Server 2008 R2 domain controllers.

If you are planning to add a Windows Server 2008 R2 domain controller to a domain that has active Windows 2000 Server domain controllers, which is possible when using the Windows 2000 Native domain and forest functional level, you must ensure that all Windows 2000 Server domain controllers have Service Pack 4 installed.

To prepare a forest for the installation of Windows Server 2008 R2 domain controllers, run the `adprep /forestprep` command on the schema master. To execute this command successfully, the user account must be a member of the Enterprise Admins, Schema Admins, and Domain Admins groups.

To prepare a forest for the installation of a read-only domain controller (RODC), run the `adprep /rodcprep` command on the schema master. This command needs to be run only once on the schema master and does not need to be run in each domain in the forest in which you intend to install Windows Server 2008 R2 RODCs. As is the case with `adprep /forestprep`, to execute this command successfully, the user account must be a member of the Enterprise Admins, Schema Admins, and Domain Admins groups.

After you have completed the forest-level preparation tasks, you must prepare each domain in the forest where you plan to install Windows Server 2008 R2 domain controllers. A user who is a member of that domain’s Domain Admins group must run the `adprep /domainprep /gpprep` domain preparation command on the domain controller that holds the infrastructure master role. After this command has been run, Windows Server 2008 R2 domain controllers can be introduced to that domain.
In-Place Domain Controller Upgrade

Upgrading each domain controller in the domain from Windows Server 2003 or Windows Server 2008 to Windows Server 2008 R2 works well within the limitations of the types of upgrades you can perform. The ability to perform in-place upgrades becomes slightly more complicated with Windows Server 2008 R2 because of the fact that Windows Server 2008 R2 only includes x64 support; there are no x86 editions of Windows Server 2008 R2. It is quite likely that you have existing domain controllers that have an x86 edition of Windows Server installed. Cross-architecture in-place upgrades, for example x86 to x64, are not supported. Additionally, in-place upgrades from computers that have operating systems prior to Windows Server 2003 SP2 are not supported.

EXAM TIP

For the 70-647 exam, ensure that you understand the upgrade paths from previous versions of Windows Server to Windows Server 2008 R2 because these affect the Active Directory Domain Services upgrade paths.

MORE INFO  WINDOWS SERVER 2008 R2 UPGRADEPATHS


Quick Check

1. On which domain controller should you perform the first forest preparation task?
2. Which of the Windows Server 2003 domain functional levels do not support the introduction of Windows Server 2008 R2 domain controllers?

Quick Check Answers

1. You must run `adprep /forestprep` on the domain controller hosting the schema master role.
Cross-Forest Authentication

The forest is the ultimate security boundary for AD DS. Organizations often have multiple AD DS forests or have partners with AD DS forests, for which the security boundary must be extended. Cross-forest authentication consists of enabling users in one forest to access resources in another forest. Cross-forest authentication is usually achieved by using forest trust relationships. Forest trust relationships are transitive; they allow users in any domain in one forest to access resources in any domain in another forest. In addition to forest trust relationships, external trusts can be used to provide cross-forest authentication. External trusts are created between domains in two separate forests and enable users in one domain to access resources in the other domain. Active Directory Federation Services (AD FS) also provides a method of granting access to forest resources; you will learn about this technology in Lesson 2, "Planning for Interoperability."

When planning a trust, you must consider the following factors:

- Whether a forest trust or external trust is required
- The direction of the trust
- The level of authentication that will be allowed through the trust
- Whether Security Identifier (SID) filtering should be implemented

Because trust relationships extend the AD DS security boundary, it is important to ensure that you grant only the minimum required access needed to meet business and technical requirements.

You can determine whether a forest trust or external trust is required by assessing the location of the users requiring access and the resources to which they require access. As previously mentioned, forest trusts are transitive. Therefore, if users from any domain in one forest require access to resources in any domain in another forest, then a forest trust is required. On the other hand, if users from a single domain in one forest require access to resources in a single domain in another forest, an external trust is better suited.

Once you’ve determined whether a forest trust or external trust is required, you must decide on the direction of trust. Forest trusts and external trusts can be one-way or two-way. A two-way trust is only required when users in each forest or domain need to access resources located in the other domain or forest. One-way trusts will suffice when bidirectional access is not required.

Trust relationships provide a pathway for all authentication requests between the forests or domains. By default, any user can authenticate over a trust relationship. However, selective authentication enables you to restrict which users can authenticate over a trust. Effectively, selective authentication can be used to limit the groups of users who are able to access resources across the trust and enables you to limit which computers in the trusting forest can be accessed across the trust. You can configure selective authentication when you first create the trust or alter the properties of an existing trust, as shown in Figure 3-1. If you choose not to implement selective authentication, plan to remove the Authenticated Users group from all sensitive resources in the trusting domain.
SID History is a feature that supports the migration of user and group accounts between domains and allows the user accounts to retain access to resources in their original domain. SID filtering prevents users from using SIDs stored in the SIDHistory attribute when accessing resources in a trusting forest. A new SID will be assigned to the account when it is moved to the new domain, and that new SID will not be assigned access to the resources that are yet to be migrated from the original domain. SID filtering can block the SIDHistory attribute across the forest trust, which ensures that accounts that have been migrated to a trusted forest no longer have access to resources in the original forest unless explicitly specified. When enabled, any SIDs from domains other than the trusted domain are ignored. For example, SID filtering is enabled by default on any trust created using a computer running Windows Server 2008 R2. Disable SID filtering only during the migration of user and group accounts from one forest to another. This allows access to resources during the migration process. After the migration is complete, plan to reenable SID filtering.

![Configuring selective authentication](image)

**FIGURE 3-1** Configuring selective authentication

**PRACTICE** Planning Forest Migration to Windows Server 2008 R2

Tailspin Toys has a 15-domain AD DS forest that contains a mix of domains running at the Windows 2000 Mixed, Windows Server 2003 Interim, and Windows Server 2003 functional levels. You are planning the transition of the Tailspin Toys environment so that the forest operates at the Windows Server 2008 R2 functional level.

The trafalgar.tailspintoys.internal, warragul.tailspintoys.internal, and bairnsdale.tailspintoys.internal domains are running at the Windows Server 2003 Interim level.
The yarragon.tailspintoys.internal, traralgon.tailspintoys.internal, and morwell.tailspintoys.internal domains contain only Windows 2000 Server domain controllers. The existing domain controller hardware in each of these domains will support Windows Server 2008 R2 domain controllers if they are running the Server Core installation. You want to deploy RODCs at several sites within these domains, and budget is available for one new Windows Server 2008 R2 domain controller, including hardware, for each of these domains.

**EXERCISE Plan the Migration of the Tailspin Toys Forest to Windows Server 2008**

In this exercise, you review the aforementioned business and technical requirements as part of planning a migration to Windows Server 2008 R2 AD DS at Tailspin Toys.

1. Which steps should you include in your plans with respect to the tailspintoys.internal root domain?
   - Join a Windows Server 2008 R2 member server to the domain.
   - Run `adprep /forestprep` on the schema master.
   - Run `adprep /rodcprep` on the schema master.
   
   This is because you must deploy RODCs in several domains in the forest.

2. Which steps should you include in your plans to transition the yarragon.tailspintoys.internal domain to the Windows Server 2008 R2 functional level?
   - Ensure that all Windows 2000 Server domain controllers have Service Pack 4 installed.
   - Ensure that `adprep /rodcprep` has been run on the schema master.
   - Join the Windows Server 2008 R2 member server to the domain.
   - Run `adprep /domainprep /gpprep` on the infrastructure master in the domain.
   - Promote the Windows Server 2008 R2 member server to domain controller. Seize all domain operations master roles for this domain controller.
   - Demote existing Windows 2000 Server domain controllers.
   - Upgrade the domain functional level to Windows Server 2008 R2.
   - Perform clean installations of Windows Server 2008 R2 Server Core on the hardware originally used by the Windows 2000 domain controllers.
   - Promote these computers running Windows Server 2008 R2 Server Core to domain controllers or RODCs as necessary.

**Lesson Summary**

- Run `adprep /forestprep` on the domain controller hosting the schema master role.
- To upgrade a domain in a forest that has been prepared using `adprep /forestprep`, run the `adprep /domainprep /gpprep` command on the domain controller that holds the infrastructure master role.
■ Selective authentication stops users from trusted domains from being treated automatically as members of the Authenticated Users group in the trusting domain.

■ SID filtering ensures that only SIDs from the trusted domain can be used when users attempt to access resources in the trusting domain. SID filtering is enabled by default on trusts created between Windows Server 2008 R2 domains. SID filtering is often disabled during cross-forest migration, allowing migrated user accounts access to resources in the source environment until the migration is complete.

■ You can use the Active Directory Migration Tool to migrate objects between domains and forests.

Lesson Review
You can use the following questions to test your knowledge of the information in Lesson 1, “Planning for Migration, Upgrade, and Restructuring.” 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. Assuming that the operations master roles are distributed across Windows Server 2003 domain controllers in the forest root domain so that no one domain controller hosts more than a single role, on which of the following computers should you run the adprep /forestprep command?
   
   A. Domain controller hosting the PDC emulator role  
   B. Domain controller hosting the schema master role  
   C. Domain controller hosting the RID master role  
   D. Domain controller hosting the infrastructure master role  
   E. Domain controller hosting the domain naming master role

2. You have upgraded the forest root domain so that it now has Windows Server 2008 R2 domain controllers. You now plan to upgrade a child domain in the same forest. Assuming that no domain controller in the forest hosts more than one flexible single master operations (FSMO) role, on which domain controller in the child domain should you run the adprep /domainprep /gpprep command?
   
   A. Domain controller hosting the PDC emulator role  
   B. Domain controller hosting the schema master role  
   C. Domain controller hosting the RID master role  
   D. Domain controller hosting the infrastructure master role  
   E. Domain controller hosting the domain naming master role
3. You are planning the migration of several thousand user accounts from the maffra.contoso.internal domain to the traralgon.fabrikam.internal domain. Each domain is in a separate AD DS forest. Each AD DS forest is configured to run at the Windows Server 2008 R2 functional level, and the forests share a two-way forest trust. During the migration, you want to ensure that migrated user accounts are able to access resources in both domains. Which of the following should you plan to do during the migration?

   A. Disable SID filtering.
   B. Enable SID filtering.
   C. Configure Selective Authentication.
   D. Configure name suffix routing.

4. You are planning a two-way forest trust between the Contoso and Fabrikam organizations. You want to ensure that only authorized users from each trusted forest have access to resources in the trusting forest. Many resources are available to authenticated users in each forest. These resources should not be available to users in the trusted forest unless explicitly allowed. Which of the following plans should you make?

   A. Implement selective authentication.
   B. Implement SID filtering.
   C. Implement user principal name (UPN) suffix routing.
   D. Implement forest-wide authentication.
Lesson 2: Planning for Interoperability

Organizations of all sizes are increasingly collaborating with partners and customers. Traditionally, this collaboration results in the need to manage multiple user accounts and groups, as well as the exchange of private information. The interoperability capabilities built into Microsoft’s Identity and Access solutions now enable organizations to securely collaborate with partners and vendors without users having to exchange private information. Moreover, it enables users to move seamlessly between applications across the enterprise and other organizations through consistent, persistent identity and credentials. This capability allows organizations to more securely establish and extend trust with partners and other external groups while reducing the complexity of managing multiple identities. Part of an enterprise administrator’s job is to make the user experience seamless. In this lesson, you will learn how you can use Windows Server 2008 R2 to enable disparate technologies to interoperate.

After this lesson, you will be able to:

- Determine the types of scenarios in which it is necessary to deploy AD FS 2.0.
- Determine which interoperability technology to deploy for UNIX-based computers, based on organizational needs.

Estimated lesson time: 40 minutes

Planning Active Directory Federation Services

AD FS allows organizations to more securely establish and extend trust with partners and other external groups while reducing the complexity of managing multiple identities. AD FS accomplishes this by securely sharing digital identity and entitlement rights across a set of preconfigured security boundaries. For example, AD FS enables you to configure a web application on your network to use a directory service on a trusted partner organization’s network for authentication. AD FS enables user accounts from one organization to access the applications of another organization while still enabling full administrative control to each organization’s IT departments. Rather than having to create a new account for a person when you need to grant access to a web application that you manage, you trust the partner organization’s directory service. Users from the partner organization can then authenticate to your organization’s web application using their own organization’s credentials.

Windows Server 2008 and Windows Server 2008 R2 include AD FS 1.1, which can be installed through Server Manager. Microsoft released AD FS 2.0 after Windows Server 2008 R2 was released. AD FS 2.0 is not integrated into the Windows Server 2008 R2 operating system or Service Pack 1 for Windows Server 2008 R2. AD FS 2.0 must be downloaded and installed separately. For information on downloading and installing the software, visit the following link: http://technet.microsoft.com/en-us/library/dd807096(WS.10).aspx.
AD FS 2.0 has the following features:

- An enterprise claims provider for claims-based applications
- A Federation Service for identity federation across domains
- Improved support for federation trusts
- An enhanced snap-in management console

An AD FS deployment can include the following components:

- **Federation Server** A computer running Windows Server 2008 or Windows Server 2008 R2 that has been configured using the AD FS 2.0 Federation Server Configuration Wizard to act in the federation server role. A federation server issues tokens and serves as part of a Federation Service.

- **Federation Server Proxy** A computer running Windows Server 2008 or Windows Server 2008 R2 that has been configured using the AD FS 2.0 Proxy Configuration Wizard to act in the federation server proxy role. A federation server proxy provides an additional layer of security to the Federation Service.

- **Claim** A statement that one subject makes about itself or another subject. For example, the statement can be about a name, identity, key, group, privilege, or capability. Claims have a provider that issues them, and they are given one or more values. They are also defined by a claim value type and, possibly, associated metadata.

- **Claim Rule** A rule that is created with a claim rule template or that is written using the claim rule language in AD FS 2.0 that defines how to generate, transform, pass through, or filter claims.

- **Attribute Store** A database or directory service that contains attributes about clients. These attributes can be used to issue claims about the clients. For example, AD FS 2.0 supports the use of either AD DS or Microsoft SQL Server as the attribute store for a claims provider.

- **Claims Provider** A Federation Service that issues claims for a particular transaction.

- **Relying Party** A Federation Service or application that consumes claims a particular transaction.

- **Certificate** The Federation Service in AD FS 2.0 uses certificates for issuing and receiving tokens, publishing federation metadata, or communicating through Secure Sockets Layer (SSL).

- **Endpoints** Endpoints provide access to the federation server functionality of AD FS 2.0, such as token issuance, and the publishing of federation metadata.

- **Information Card** Information cards, which a claims provider can issue, that represent a user's digital identity.
One of the most important aspects of designing AD FS 2.0 is selecting the appropriate AD FS 2.0 design. To do so, you must first identify your deployment goals. Typically, AD FS 2.0 deployment goals fall into one of the following three categories:

- Provide your Active Directory users access to your claims-aware applications and services
- Provide your Active Directory users access to the applications and services of other organizations
- Provide users in another organization access to your claims-aware applications and services

After you have identified your deployment goals, you can go ahead and map your deployment goals to an AD FS 2.0 design. AD FS 2.0 includes the following designs:

- Web Single Sign-On (SSO) design
- Federated Web SSO design

In the Web SSO design, users must authenticate only once to access multiple AD FS–secured applications or services. In this design, all users are external and no federation trust exists because there are no partner organizations. Typically, you deploy this design when you want to provide individual consumer or customer access to one or more AD FS 2.0–secured services or applications over the Internet. With the Web SSO design, an organization that typically hosts an AD FS–secured application or service in a perimeter network can maintain a separate store of customer accounts in the perimeter network, which makes it easier to isolate customer accounts from employee accounts.

The Federated Web SSO design involves secure communication that spans multiple firewalls, perimeter networks, and name-resolution servers, in addition to the entire Internet routing infrastructure. Typically, this design is used when two organizations agree to create a federation trust relationship to allow users in one organization (the account partner organization) to access web-based applications or services, which are secured by AD FS 2.0, in the other organization (the resource partner organization).

MORE INFO  MORE ON AD FS 2.0 DESIGN
To learn more about designing AD FS 2.0, consult the following link: http://technet.microsoft.com/en-us/library/adfs2-design-guide(WS.10).aspx.

✔️ Quick Check
1. What does the deployment of AD FS 2.0 enable you to accomplish?
2. Which role services are included with AD FS 2.0?
Planning for UNIX Interoperability

As an enterprise administrator, you are aware that many companies do not settle on a single company’s operating system solutions for the clients and servers. In some cases, your organization might choose an alternative solution because it meets a particular set of needs at a particular point in time; in other cases, you might inherit a diverse operating system environment when your company acquires a subsidiary. In either situation, it is your job as enterprise administrator to ensure that these diverse systems interoperate in a seamless manner. Windows Server 2008 R2 includes several features and role services that can assist in integrating UNIX-based operating systems in a Windows Server 2008 R2 infrastructure.

Identity Management

Identity Management for UNIX is a role service, available under the Active Directory Domain Services role, that enables you to integrate your Windows users in existing environments that host UNIX-based computers. You are most likely to deploy this feature in predominantly UNIX-based environments and where Windows users and computers running Windows must integrate in an existing UNIX-based infrastructure. Identity Management for UNIX is compatible with Internet Engineering Task Force (IETF) Request for Comments (RFC) 2307, “An Approach for Using LDAP as a Network Information Service.” A Lightweight Directory Access Protocol (LDAP) server resolves network password and Network Information Service (NIS) attribute requests. LDAP is a directory services protocol commonly used in UNIX environments in a way very similar to how AD DS is used on Windows networks.

Password Synchronization

The Password Synchronization component of Identity Management for UNIX simplifies the process of maintaining secure passwords in environments in which computers running UNIX and Windows are present and used by staff. When Password Synchronization is deployed, the user’s password on all UNIX computers in the environment will also be changed when a user changes his or her password in AD DS. Similarly, you can configure the Password
Synchronization component to change a password automatically in AD DS when a user’s UNIX password is changed. You configure the direction of password synchronization by setting the password synchronization properties as shown in Figure 3-2. Access the Password Synchronization Properties dialog box using the Microsoft Identity Management for UNIX console.

![Password Synchronization Properties](image)

**FIGURE 3-2** Configuring Password Synchronization Properties

Password Synchronization is supported between Windows Server 2008 R2 and the following UNIX-based operating systems:

- Hewlett Packard HP UX 11i v1
- IBM AIX version 5L 5.2 and 5L 5.3
- Novell SUSE Linux Enterprise Server 10
- Red Hat Enterprise Linux 4 Server
- Sun Microsystems Solaris 10 (SPARC architecture only)

You should deploy Password Synchronization on all domain controllers in a domain in which it is needed. Any newly deployed domain controllers in the domain should also have this feature installed. Microsoft also recommends that you demote a domain controller before removing Password Synchronization. Ensure that the password policies on the UNIX computers and within the Windows domain are similarly restrictive. Inconsistent password policies will result in a synchronization failure if a user is able to change a password on a less-restrictive system because the password will not be changed on the more-restrictive system due to the password policy. When configuring Password Synchronization, best practice is
to ensure that the passwords of sensitive accounts, such as those of administrators from both UNIX and Windows environments, are not replicated. By default, members of the local Windows Administrators and Domain Administrators groups are not replicated.

MORE INFO  MORE ON PASSWORD SYNCHRONIZATION

To learn more about Password Synchronization, consult the following TechNet document:

Subsystem for UNIX-Based Applications

Subsystem for UNIX-Based Applications (SUA) is a Windows Server 2008 R2 feature that enables enterprises to run UNIX-based applications on computers running Windows Server 2008 R2. SUA provides a UNIX-like environment, including shells, a set of scripting utilities, and a software development kit (SDK). SUA also provides support for case-sensitive file names, compilation tools, job control, and more than 300 popular UNIX utilities, commands, and shell scripts. You can install SUA as a Windows feature by using the Add Features Wizard.

A computer running Windows Server 2008 R2 that has the SUA feature installed enables two separate command-line environments: a UNIX environment and a Windows environment. Applications execute within a specific environment. A UNIX command executes within the UNIX environment, and a Windows command executes within the Windows environment. Although the environments are different, commands executing in these environments can manipulate files stored on Windows volumes normally. For example, you can use the UNIX-based grep command under SUA to search a text file stored on an NTFS volume.

UNIX applications that run on existing computers can be ported to run on Windows Server 2008 R2 under the SUA subsystem. This enables organizations to migrate existing applications that run on UNIX computers to Windows Server 2008 R2. SUA supports connectivity to Oracle and SQL Server databases by using the Oracle Call Interface (OCI) and Open Database Connectivity (ODBC) standards. SUA also includes support that enables developers to debug Portable Operating System Interface (POSIX) processes by using Microsoft Visual Studio. POSIX is a collection of standards that define the application programming interface (API) for software that is compatible with UNIX-based operating systems.

MORE INFO  MORE ON SUBSYSTEM FOR UNIX-BASED APPLICATIONS

Server for NIS

Server for NIS enables a Windows Server 2008 R2 domain controller to act as a master NIS server for one or more NIS domains. Server for NIS provides a single namespace for NIS and Windows domains that an enterprise administrator can manage by using a single set of tools. Server for NIS stores the following NIS map data in AD DS:

- Aliases
- Bootparams
- Ethers
- Hosts
- Group
- Netgroup
- Netid
- Netmasks
- Networks
- Passwd
- Protocols
- Rpc
- Services
- Pservers
- Shadow

It is possible to deploy Server for NIS on other domain controllers located in the same domain as the master NIS server. This enables these domain controllers to function as NIS subordinate servers, and NIS data is replicated through AD DS to the servers hosting the Server for NIS role. UNIX-based computers can also function as NIS subordinate servers because Server for NIS uses the same replication protocol to propagate NIS data to UNIX-based subordinates as a UNIX-based NIS master server does. When considering the deployment of Server for NIS in an integrated environment, remember that a computer running Windows Server 2008 R2 must hold the master NIS server role. A computer running Windows Server 2008 R2 cannot function as an NIS subordinate server to a UNIX-based NIS master.

When planning the migration from UNIX-based NIS servers to Windows-based NIS servers, your first task is to move the NIS maps to the new Windows Server 2008 R2 NIS server. After you do this, the computer running Windows Server 2008 R2 can function as an NIS master. It is possible to move multiple NIS domains to a single Windows Server 2008 R2 domain controller. Although you can configure Server for NIS to support multiple NIS domains concurrently, you can also merge the domains after they have been migrated to the Windows Server 2008 R2 domain controller running Server for NIS.
You are likely to plan the deployment of Server for NIS when you want to retire an existing NIS server infrastructure even though NIS clients are still present on your organizational network. Server for NIS enables you to consolidate your server infrastructure around the Windows Server 2008 R2 operating system while enabling UNIX-based NIS client computers to continue functioning normally on your organizational network.

When planning the deployment of Server for NIS, remember that this component is installed as a role service under the AD DS server role. Server for NIS can be installed only on a Windows Server 2008 R2 domain controller. You cannot deploy Server for NIS on a stand-alone computer running Windows Server 2008 R2 or on a member server running Windows Server 2008.

MORE INFO
MORE ON SERVER FOR NIS
To learn more about Server for NIS, consult the following TechNet link:

Services for Network File System

*Services for Network File System* (NFS) enables file sharing between Windows-based and UNIX-based computers. Plan to deploy Services for NFS if your environment contains a large number of UNIX-based client computers that need to access the same shared files as the Windows-based client computers on your organization's network. Figure 3-3 shows the NFS Advanced Sharing dialog box on a computer running Windows Server 2008 R2 configured with Services for NFS.

During the deployment of Services for NFS, you must configure AD DS lookup resolution for UNIX group ID and UNIX user ID (GID and UID). You do this by installing the Identity Management for UNIX Active Directory schema extension that is included in Windows Server 2008 R2. Lesson 1 of this chapter covered extending the schema in preparation for the deployment of the first Windows Server 2008 R2 domain controller in a domain. You can then configure identity mapping by configuring the properties of Services for NFS and specifying the domain in the forest in which Identity Management for UNIX has been installed. Figure 3-4 shows identity mapping configuration for Services for NFS.
Planning Migrations, Trusts, and Interoperability

Figure 3-3 Configuring an NFS share

Figure 3-4 Configuring NFS identity mapping

More Info  More on Services for NFS

To learn more about Services for NFS, consult the following TechNet document:

Practice  Planning for Interoperability

Wingtip Toys is a moderate-sized enterprise that has 15 branch offices located across the southeastern states of Australia. Wingtip Toys wants to move away from its existing network infrastructure that includes both Windows-based and UNIX-based computers to a more
homogeneous operating system environment. The company has a mixture of UNIX-based client and server computers at each branch office. UNIX-based client computers authenticate against the NIS service running on a UNIX server at each branch location. All existing UNIX-based client computers currently access shared files from UNIX servers. These shared files should be moved to a Windows-based platform. Previous attempts to achieve this have failed due to problems synchronizing user accounts and passwords between the disparate platforms. Because of budgetary constraints, management has asked that the UNIX servers at Wingtip Toys be decommissioned first, with a gradual transition from UNIX-based client computers to computers running Windows Vista over the next 24 months.

**EXERCISE**

**Plan the Interoperability Strategy for Phasing Out UNIX-Based Computers at Wingtip Toys**

In this exercise, you review the preceding business and technical requirements as part of a planned a migration from UNIX-based computers at Wingtip Toys.

1. What steps must you perform to ensure that the NIS master server is a computer running Windows Server 2008 R2 rather than a UNIX-based computer?
   - Install Server for NIS on a Windows Server 2008 R2 domain controller at each site.
   - Configure one Windows Server 2008 R2 domain controller as the master NIS server.
   - Migrate NIS maps to the new master NIS server.
   - Decommission existing NIS servers.

2. What steps must you perform to ensure that users who switch between Windows-based and UNIX-based client computers use the same passwords for their user accounts?
   - Install Password Synchronization.
   - Ensure that password policies are compatible.

3. What steps must you perform prior to decommissioning the UNIX-based file servers that UNIX-based client computers use?
   - Install Services for NFS on the file servers running Windows Server 2008 R2 that will replace the UNIX file servers.
   - Migrate files and permissions from the NFS shares on the UNIX-based computers to the NFS shares on the computers running Windows Server 2008 R2.
   - Decommission the UNIX file servers.

**Lesson Summary**

- Active Directory Federation Services (AD FS) 2.0 provides consistent, persistent identity and credentials that can flow between organizations, which helps reduce the need to manage multiple user accounts or group memberships.

- Services for Network File System (NFS) enables UNIX-based computers to access shared files hosted on a computer running Windows Server 2008 R2.
Subsystem for UNIX-Based Applications (SUA) enables POSIX-compliant applications to execute on a computer running Windows Server 2008 R2.


Password Synchronization enables user account passwords on UNIX-based computers and Windows-based computers to be synchronized. Password policies on both UNIX-based and Windows-based computers must be similar; otherwise, synchronization errors can occur.

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

1. In which of the following situations would you plan to deploy Active Directory Federation Services 2.0?
   A. You need to share files on a computer running Windows Server 2008 R2 to clients running UNIX-based operating systems.
   B. You need to synchronize user account passwords between computers running AD DS and UNIX-based computers.
   C. You need to run POSIX-compliant applications on a computer running Windows Server 2008 R2.
   D. You need to provide single sign on for a group of related web applications to users in a partner organization.

2. The organization that you work for wants your assistance in planning the deployment of a solution that will ensure that new employee data entered in the human resource Oracle 9i database is synchronized with your organization’s Windows Server 2008 AD DS and Exchange Server 2007 deployments. Which of the following solutions would you consider deploying to meet this need?
3. Your predominantly Windows-based organization has recently acquired a company that uses UNIX-based computers for all client and server computers. The recently acquired company has a significant amount of spare office space. A nearby branch office has older facilities, so there is a plan to redeploy staff from this older facility to the recently acquired company’s site. As part of this redeployment, it will be necessary to introduce computers running Windows Server 2008 R2 functioning as file servers. Which of the following Windows Server 2008 R2 role services or functions should you plan to deploy so that UNIX-based client computers will be able to access files hosted on a Windows Server 2008 R2 file server?

A. Subsystem for UNIX-Based Applications
B. Server for NIS
C. Services for NFS
D. Network Policy Server

4. You are putting the finishing touches on a plan to migrate several branch offices to Windows Server 2008 R2. Each branch office currently has an old UNIX-based computer that hosts several POSIX-compliant applications. You want to minimize the amount of hardware present at each branch office. Which of the following items should you include in your Windows Server 2008 R2 branch office migration plan? (Choose two. Each answer forms part of the solution.)

A. Deploy the Remote Desktop Services role.
B. Deploy the Hyper-V role.
C. Deploy the Subsystem for UNIX-Based Applications feature.
D. Deploy the Active Directory Federation Services role.
E. Migrate the applications from the UNIX-based computer to Windows Server 2008 R2.
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. This scenario sets up a real-world situation involving the topics of this chapter and asks you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- Run `adprep /forestprep` on the schema master and `adprep /domainprep /gpprep` on each domain’s infrastructure master.
- Limit the scope of trusts so that they meet the necessary requirements only. Do not create a two-way trust when a one-way trust is all that is required.
- Selective authentication enables administrators in a trusting forest or domain to allow limited access to specific users from a trusted forest or domain.
- AD FS 2.0 enables partner organizations to have single sign on for local web applications without configuring forest-based or domain-based trusts.
- Server for NIS enables a computer running Windows Server 2008 R2 to function as an NIS server for UNIX-based computers.
- Services for NFS enables a computer running Windows Server 2008 R2 to function as a file server for a UNIX-based computer.
- The Password Synchronization component enables account passwords for AD DS–based and UNIX-based computers to be the same.
- SUA enables POSIX-compliant applications to run on computers running Windows Server 2008 R2.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- Active Directory Federation Services (AD FS)
- Active Directory Migration Tool
- Attribute store
- Certificate
- Claim rule
Case Scenario

In the following case scenario, you apply what you have learned about restructuring and interoperability. You can find answers to these questions in the “Answers” section at the end of this book.

Case Scenario: Phasing Out a UNIX-Based Computer at Tailspin Toys

You are assisting Tailspin Toys to integrate the recently purchased Wingtip Toys company in its network infrastructure. The integration will proceed over time, with some tasks of higher priority to the management of Tailspin Toys than others. One high-priority task involves an aging UNIX-based computer at Wingtip Toys that hosts a POSIX-compliant payroll application. This is the only UNIX-based computer in either organization, and management would prefer not to replace the computer with another UNIX-based computer unless absolutely necessary. Wingtip Toys is using Lotus Notes 7.0, and Tailspin Toys uses Exchange Server 2007. The HR department at Tailspin Toys uses an SQL Server 2008–based database to manage employee data. The HR department at Tailspin Toys will now be responsible for managing all new and existing employee data for both organizations. Although the HR database will be managed centrally, each organization’s accounting teams will be kept separate, although they will use the existing Tailspin Toys financial web applications. One problem with this is that the Wingtip Toys accountants find the authentication process quite complicated, and
management hopes that you might offer some recommendations to make it simpler. With this information in mind, answer the following questions.

1. What plans could you make to simplify authentication to the Tailspin Toys accounting applications for Wingtip Toys staff?
2. What plans could you make to migrate the Wingtip Toys payroll application to Tailspin Toys?

Suggested Practices

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

Plan for Domain or Forest Migration, Upgrade, and Restructuring

Complete the following practice exercise.

- **Practice** Upgrade a Windows Server 2008 single-domain forest to Windows Server 2008 R2.
  - Using evaluation software, create a Windows Server 2008 single-domain forest.
  - Join a Windows Server 2008 R2 member server to this single-domain forest.
  - Use the `adprep` command to prepare the Windows Server 2008 single-domain forest.
  - Promote the Windows Server 2008 R2 member server to domain controller.
  - Transfer FSMO roles from the Windows Server 2008 domain controller to the Windows Server 2008 R2 domain controller.
  - Demote the Windows Server 2008 domain controller to member server.

Plan for Interoperability

Complete the following practice exercise.

- **Practice** Work with Services for NFS.
  - Install the Services for Network File System (NFS) role service on a computer running Windows Server 2008 R2.
  - Configure an NFS share that will be accessible to UNIX-based operating systems.
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 70-647 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.
This page intentionally left blank
Symbols and Numbers

3-leg firewalls, 220
6to4 technology, 50, 72
6to4cfg tool, 47
802.1x standard, 251, 261–265
80–20 rule, 57

A

A (host) records, 6, 9, 22
AAAA records
  about, 9, 72
  IPv6 addresses and, 18
  practice exercises, 28
access control lists (ACLs), 199, 263
access-based enumeration, 406, 410
Account Administrators, 174
Account Operators group, 173
Accounting Configuration Wizard, 241
ACLs (access control lists), 199, 263
Active Directory Certificate Services. See AD CS (Active Directory Certificate Services)
Active Directory Domain Services. See AD DS (Active Directory Domain Services)
Active Directory Domain Services Installation Wizard. See DCPro.exe utility
Active Directory Federation Services (AD FS), 143, 160
Active Directory integrated zone, 71
Active Directory Lightweight Directory Services (AD LDS), 78, 286, 483
Active Directory Migration Tool (ADMT), 140, 160
Active Directory Rights Management Services. See AD RMS (Active Directory Rights Management Services)
Active Directory Rights Management Services console, 428

Active Directory Users and Computers, 307
AD CS (Active Directory Certificate Services), 229, 452, 484
AD DS (Active Directory Domain Services)
  App-V support, 392
  auditing compliance, 180–181
  boundary networks and, 255
  delegating administration, 168–171
  designing domain controller placement, 117–121
  designing domain structure, 85–92
  designing forest structure, 77–84
  designing functional levels, 92–97
  designing printer location policies, 121–124
  designing replication, 112–116
  designing schema, 97–98
  designing site structure, 109–112
  designing trusts, 99–100
  DNS planning recommendations, 5
  identifying role of, 78–79
  integrating with DNS infrastructure, 24–25
  planning maintenance and recovery procedures, 434–438
  practice exercises, 125–130
  restartable, 437–438
  Server Core support, 286
  stopping at command line, 438
Windows Server integration, 5

AD FS (Active Directory Federation Services), 143, 148–150, 160
AD LDS (Active Directory Lightweight Directory Services), 78, 286, 483
AD RMS (Active Directory Rights Management Services)
  about, 428–429, 448
  applications supported, 431
  creating/viewing rights-protected information, 429–430
  smart card authentication and, 202
Windows SharePoint Services and, 416
Add Features Wizard

Add Features Wizard, 153
Address Resolution Protocol (ARP), 44
administration. See also data management; service management
auditing compliance, 180–181
branch office considerations, 280–281
delegating, 168–179
DNS, 9–10
planning organizational structure, 182–183
Administrator Role Separation
about, 282, 322
domain controllers and, 288–289
practice exercises, 298–299
ADMT (Active Directory Migration Tool), 140, 160
adprep command
/domainprep /gpprep switch, 98, 141
/forestprep switch, 98, 141
/rodcprep switch, 98, 141, 307
Advanced Encryption Standard (AES), 297
Advanced Firewall feature, 235
AES (Advanced Encryption Standard), 297
AFSDB (Andrew File System Database), 9
aggregatable global unicast addresses, 35–37
Agile VPN. See VPN Reconnect
Allowed list, 310
AMD NX (No eXecute), 371
AMD Virtualization (AMD-V) technology, 371
Andrew File System Database (AFSDB), 9
anycast addresses, 35, 41, 72
APIPA (automatic private IP addressing), 32, 37, 42
application deployment
Group Policy support, 352–354
practice exercises, 358–360
RD Session Host servers and, 330
RemoteApp support, 338–339
System Center Configuration Manager 2007, 356–358
System Center Essentials 2010, 354–355
TS Web Access, 337–338
application servers, 238
application virtualization, 390–395
Application Virtualization. See App-V (Application Virtualization)
apPLICATION-vmware, 219
Application-Specific Administrators, 175
App-V (Application Virtualization)
about, 330, 390–392
branch office deployments, 393–394
planning deployment, 392–393
App-V Client for Desktops, 393
App-V data store, 393
App-V Management Console, 393
App-V Management servers, 390, 392
App-V Management Web Service, 393
App-V Sequencer, 392
App-V Streaming Server, 393
ARP (Address Resolution Protocol), 44
ATM (Asynchronous Transfer Mode), 9, 39
attribute store, 149, 160
Audit Directory Service Access audit policy, 180
auditing
AD DS compliance, 180–181
Group Policy compliance, 180–181
replication compliance, 180
Authenticated list, 310
authentication
about, 199, 209
BitLocker modes, 424–425
boundary networks and, 255
case scenarios, 210
certificate, 233
cross-forest, 143–144
designing trusts to optimize, 99–100
DirectAccess, 230
EAP-TLS, 225, 228, 232, 454
EAP-TTLS, 454
intraforest, 99–100
IPsec, 12
Kerberos, 176, 199, 297
MS-CHAP, 228, 232
multifactor, 199
password, 200, 233
PEAP, 454
PEAP-MSCHAP, 232, 260
PEAP-TLS, 228, 232, 260
PKI considerations, 454–455
planning VPN enforcement, 260
RADIUS remote access solution, 239
restricted networks and, 255
RODC process, 310–311
security considerations, 232
smart card, 202–204, 455
supported, 232–233
authoritative restore, 436–437, 448
authoritative zones, 12
authorization
about, 199, 209
case scenarios, 210
Kerberos and, 199
multifactor, 199
RD Gateway, 344
autoconfiguring IPv6 addresses, 38, 42
automatic approval (software updates), 500
Automatic Approvals dialog box, 500
automatic private IP addressing (APIPA), 32, 37, 42
automatic site coverage, 312–313, 322
automatic tunneling, 49
autonomy
about, 169, 209
AD DS administration requirements, 169
data, 80, 84
forest design requirements, 80–81
service, 80, 84
stakeholders and, 172

B
back firewalls, 221
background zone loading, 14
Backup Operators group, 173–174, 201
backup procedures, 335, 370, 434–436
bandwidth throttling, 411
base CRLs, 480
baseboard management controller (BMC), 347
Best Practices Analyzer (AD CS), 484
BIND servers, 24–25, 72, 199
BitLocker
about, 317, 323, 448
additional information, 424–425
authentication modes, 424–425
performance issues, 424
protecting volume data, 423–424
virtual machines and, 373
BMC (baseboard management controller), 347
border networks, 217
boundary networks, 251, 255–256
branch office zones, 12
branch offices
about, 322
adding domain controllers, 287–295
App-V support, 393–394
BranchCache support, 297
communication considerations, 295–298
data confidentiality, 296–297
designing administration structure, 280–281
RADIUS remote access solution, 239
SCVMM support, 385
security considerations, 288, 302–318
Server Core considerations, 286
site link considerations, 296
typical components/services, 282–283
virtualization in, 294
VPN server deployment, 234
Windows Deployment Services, 283–287
BranchCache, 297, 323
broadcast traffic, 44
broken namespaces, 19
BuiltIn AD DS container, 173
business continuity
data security solutions, 423–431
data sharing and collaboration, 405–420
system recovery and availability planning, 434–444
Business Unit Administrators, 174

C
CA (certification authority)
boundary networks and, 255
defined, 454, 488
defining types and roles, 466–473
determining number required, 470–471
fault tolerance, 257
Health Registration Authority and, 256
internal versus third-party, 465–466
NAP IPsec enforcement, 257
offline, 469–470
practice exercises, 472–473
secure networks and, 255
tunneling protocols and, 227
virtualization considerations, 369
workgroup environment, 426
CA hierarchy, 464–471, 488
CA Web enrollment tool, 227
cache locking. See DNS Cache Locking
caching
credential, 289, 322
CRL, 481
CALs (client access licenses)
about, 330–331
license server activation, 333–334
license server deployment, 331–333
capacity planning

Remote Desktop Services, 333–335
TS, 335
capacity planning, 383
CDP (CRL distribution point), 454, 488
central sites, 505
centralized administration topology, 16
centralized replication topology, 16
certificate enrollment, 475–479, 488
certificate lifetime, 258, 457, 488
certificate practice statement (CPS), 454, 488
certificate renewal, 476, 479, 488
Certificate Renewal Wizard, 475
certificate repository, 454, 488
Certificate Request Wizard, 475, 477
certificate revocation, 479–484, 488
certificate revocation list. See CRL (certificate revocation list)
certificate templates, 459, 461, 488
certificate trust list, 488
certificate verification, 454, 488
certificates. See also digital certificates about, 149, 160
authenticating, 233
EFS support, 426
identifying requirements, 456–458
issuance policy, 488
preshared keys comparison, 227
rights account certificates, 202
Certificates MMC snap-in, 233
certification authority. See CA (certification authority)
child domains, 6, 22
child sites, 505
circuit-level firewalls, 219
claim rule, 149, 160
claims, 149, 161
claims provider, 149, 161
client access licenses. See CALs (client access licenses)
Client Certificate Mapping Authentication role service, 203
client-side targeting, 498
Clustered Shared Volumes (CSVs), 382
CNAME (canonical name) records, 9, 14, 26
code signing, 455
collaboration. See data sharing
collaboration sites, 415
colon-hexadecimal representation, 34
communication channels, 374
communication sites, 414
compatible IDs, 197
compliance
auditing AD DS, 180–181
auditing Group Policy, 180–181
auditing replication, 180
defined, 513
health policy, 249
restricted networks and, 254
software update, 513–521
System Center Configuration Manager, 517–518
WSUS reporting, 514–517
conditional forwarding, 7, 21, 72
cone NATs, 46
confidentiality, data, 296–297
Conflict and Deleted folder, 412
Coordinated Universal Time (UTC), 411
corporate namespaces, 19
CPS (certificate practice statement), 454, 488
credential caching, 289, 322
CRL (certificate revocation list)
defined, 480, 488
OCSP and, 223, 258
PKI support, 454
problems with, 480
CRL distribution point (CDP), 454, 488
CRL publication, 480, 482–483, 488
cross-certification, 460, 488
cross-file RDC, 411
cross-forest authentication, 143–144
cryptographic service provider, 458, 488
cryptography. See encryption
CSVs (Clustered Shared Volumes), 382

D

DACL (discretionary access control list), 477
data autonomy, 80, 84
data confidentiality, 296–297
Data Execution Prevention (DEP), 371
data isolation, 81, 84
data management
about, 169–170, 209
additional information, 175
data security solutions, 423–431
data sharing and collaboration, 405–420
delegating, 178
planning, 176–178
recommended roles, 174–175
system recovery and availability planning, 434–444
data recovery agent (DRA), 426
data security. See security considerations
data sharing
case scenarios, 448–449
DFS design process overview, 412
DFS Namespaces technology and, 408–410
DFS Replication technology, 410–412
planning DFS deployment, 405–407
planning SharePoint infrastructure, 413–419
practice exercises, 420
data storage. See storage considerations
Databaseless CA feature, 258
DCA (DirectAccess Connectivity Assistant), 28
DCOM (Distributed Component Object Model), 119, 478
DCPromo utility
/ADV switch, 309
/forceremoval switch, 438
/unattend switch, 291
about, 288
installing RODCs, 290
offline maintenance, 438
dedicated forest root domain, 90
Default Domain Controllers Policy, 180
defragmentation, offline, 437
delegated namespaces, 20
delegation of control
about, 209, 281, 322
AD DS administration, 168–171
Administrator Role Separation, 282, 298–299
benefits and principles, 169
case scenarios, 210
data management, 178
in centralized administration model, 171
in distributed administration model, 171
in mixed administration model, 171
management tasks and, 172–179
Delegation of Control Wizard, 182, 280
delegation records, 6
Deleting Domain Controller dialog box, 313
delta CRL, 480, 483, 488
demilitarized zone (DMZ), 303
Denied list, 310
DEP (Data Execution Prevention), 371
deployment. See also application deployment
App-V, 392–394
branch offices, 277–298
DFS, 405–407
DirectAccess, 28
Microsoft Office SharePoint Server, 419
RD license servers, 331–333, 336
Remote Desktop Session, 329–330
strategic services in perimeter networks, 223–224
virtual machines, 372–376
VPN server solution, 234–235
Web server services, 223–224
Windows SharePoint Services, 416
WSUS, 501
DES (3DES) encryption, 227, 297
device installation
controlling, 192–195
obtaining compatible IDs, 197
obtaining GUIDs, 198
obtaining hardware IDs, 196
Device Installation Restriction policies, 195
DFS (distributed file system)
about, 405, 448
additional information, 405
benefits of, 405
design process overview, 412
planning deployment, 405–407
read-only replicas, 316, 323
read-only replicated folders, 410
replication considerations, 293
DFS folder, 406, 448
DFS folder targets, 406, 409, 448
DFS namespace, 406, 448
DFS namespace root, 406, 448
DFS namespace servers, 406, 409, 448
DFS Namespaces technology
about, 407
access-based enumeration, 410
advanced settings and features, 408–410
domain-based namespace servers, 409
failover and failback, 409
namespace scalability mode, 410
read-only replicated folders, 410
referral ordering, 408
target priority, 409
DFS Referral, 408, 448
DFS Replication technology
about, 407, 448
advanced settings and features, 410–412
bandwidth throttling, 411
DFSR (distributed file system replication)

- Conflict and Deleted folder, 412
- cross-file RDC, 411
- disabled memberships, 412
- RDC, 411
- replication filters, 412
- replication schedule, 411
- staging folders, 412
- DFSR (distributed file system replication), 21
- DHCP (Dynamic Host Configuration Protocol)
  - boundary networks and, 255
  - domain controllers and, 293
  - integrating NAP, 59
  - NAP enforcement, 265–267
  - practice exercises, 64–66
  - Server Core support, 286
  - virtualization comparison, 368
  - Windows Server integration, 5
- DHCPv6
  - configuring clients, 55–57
  - practice exercises, 66–68
  - site-local addresses and, 37
  - Windows Server integration, 5
- differencing disks, 376
- digital certificates
  - defined, 453–454, 487
  - DNSSEC and, 12
  - identifying requirements, 456–458
  - license server activation, 333
  - practice exercises, 462
  - X.509, 296
- digital signatures
  - defined, 455, 488
  - DNSSEC and, 12
  - RD Connection Broker, 340
- DirectAccess, 28, 230–231, 297
- DirectAccess Connectivity Assistant (DCA), 28
- Directory Replication Services (DRS), 5
- Directory Services Restore Mode (DSRM), 436
- discontiguous namespaces, 19
- discretionary access control list (DACL), 477
- distributed administration model, 171
- Distributed Component Object Model (DCOM), 119, 478
- distributed file system. See DFS (distributed file system)
- distributed file system replication (DFSR), 21
- DMZ (demilitarized zone), 303
- DNS (Domain Name System)
  - administering, 9–10
  - boundary networks and, 255
  - case scenarios, 72
  - configuring, 5
  - DirectAccess support, 231
  - new features and enhancements, 11–18
  - planning, 5–10
  - planning infrastructure, 4, 18–26
  - practice exercises, 26–29
  - suggested practices, 73
  - troubleshooting problems, 55
  - virtualization comparison, 368
- DNS Administrators, 174
- DNS Cache Locking, 11, 13, 72
- DNS cache poisoning, 13
- DNS clients, 5, 21
- DNS Devolution, 12–13
- DNS forwarding, 7–8, 21
- DNS Manager MMC snap-in, 9
- DNS name resolution. See name resolution
- DNS namespaces. See namespaces
- DNS records, 9. See also specific record types
- DNS round robin, 337
- DNS Server service role
  - configuring, 5
  - new features and enhancements, 11–12
  - root hints and, 24
  - Server Core support, 286
- DNS servers
  - assigning IPv6 addresses, 55
  - conditional forwarders, 7
  - domain controllers and, 292
  - GlobalNames zone and, 15
  - root hints, 7
  - stub zones and, 6
  - virtual, 57
- DNS Socket Pool, 11, 13, 72
- DNS zones. See also specific zones
  - background loading, 14
  - configuring, 22–23
  - read-only, 289, 322
  - replicating, 8
  - RODCs and, 11
  - secure dynamic updates, 5, 23
  - transferring, 8, 71
dnsccmd tool, 10, 15, 18, 72
- DNSSEC (Domain Name System Security Extensions), 11–13, 72
determining number of domains required, 88
gathering requirements, 85–86
practice exercises, 102–103
RADIUS remote access solution, 239
restructuring, 140, 161, 281, 322
upgrading, 89–90, 139, 141–142, 161
dotted decimal notation, 34
DRA (data recovery agent), 426
DRS (Directory Replication Services), 5
DSRM (Directory Services Restore Mode), 436
dual stack, 48, 72
dual-stack nodes, 44, 48
Dynamic Host Configuration Protocol. See DHCP (Dynamic Host Configuration Protocol); DHCPv6
dynamic update protocol, 5, 23

E
EAP-TLS authentication, 225, 228, 232, 454
EAP-TTLS authentication, 454
edge firewalls, 220
EFS (Encrypting File System)
about, 317, 323, 448
additional information, 426
BranchCache data and, 298
PKI support, 455
planning for, 426–427
virtual machines and, 373
Embedded Rendezvous Point Flagging, 40
employee monitoring, 302
Encrypting File System. See EFS (Encrypting File System)
encryption. See also BitLocker; PKI (public key infrastructure)
AD RMS support, 429
AES, 297
cryptographic service provider, 458, 488
DES (3DES), 227, 297
EFS support, 426
network-level security, 42
payload, 43
endpoints, 149, 161
Enterprise Admins group
adding domain controllers, 287
adprep command and, 141
applying PSOs to, 201
branch office administration and, 281
security considerations, 167
enterprise CAs

enterprise CAs, 466–468, 488
enumeration, access-based, 406, 410
EUI–64 addresses, 36
Exchange Server, 293
explicit tunnels, 49
external CAs, 465–466
external networks, 375
external trust, 176

F

failover clusters
about, 293, 448
DFS Namespaces technology, 409
Hyper-V and, 370, 373
NLB comparison, 442
preparing hardware, 443–444
fault tolerance, 257, 293
Federated Web SSO design, 150
federation server, 149, 161
Federation Server Configuration Wizard, 149
federation server proxy, 149, 161
Fibre Channel, 373, 382
File Replication Service (FRS), 293
filtering
GPOs, 191
IP filters, 235
PPTP support, 226
replication filters, 412
SID, 144
Find Printers dialog box, 124
fine-grained password policies
about, 209
configuring, 200–202, 314–315
practice exercises, 204–207
FIPS 140-2 standard, 458, 488
firewalls
about, 267
branch offices, 303
host-based, 304
L2TP considerations, 227
perimeter networks, 217, 219–221
third-party products, 222
virtual machines and, 375
VPN server deployment and, 234

Forefront TMG (Threat Management Gateway) Server
NAP IPsec enforcement, 256
planning for, 220–222
RADIUS remote access solution, 238
Forest Configuration Operators, 174
forest functional levels, 95–97
forest root domain, 90–92
forest root domain controllers, 118
forest trusts
about, 175–176, 183–186
cross-forest authentication, 143–144
multifactor authorization, 199
practice exercises, 183–186
ForestDNSZones domain partition, 12
forests
case scenarios, 133
cross-forest authentication, 143–144
designing domain structure, 85–92
designing forest model, 82–84
designing structure, 77–84
determining number of forests required, 81
gathering requirements, 79–81
identifying role of AD DS, 78–79
intraforest authentication, 99–100
planning GlobalNames zones, 26
practice exercises, 101–102, 144–145
RADIUS remote access solution, 239
upgrading domains, 141

forwarders
about, 7–8, 71
conditional, 7, 21, 72
DNS, 7–8, 21
FP (Format Prefix), 36, 39
FQDN (fully qualified domain name), 13–14, 20, 26
FRS (File Replication Service), 293
FSMO roles, 438
full domain controllers, 289
full mesh replication topology, 16, 113
Full Volume Encryption Key (FVEK), 424
fully qualified domain name (FQDN), 13–14, 20, 26
functional levels
additional information, 92
domain, 93–95, 201, 407
forest, 95–97
practice exercises, 103–104
FVEK (Full Volume Encryption Key), 424
G

global catalog servers, 119, 121, 291
global catalogs, 289, 291
global groups, rights and permissions, 173
global unicast addresses
  about, 34–39, 72
  additional information, 37
  aggregatable, 35–37
  IPv4 equivalent, 35
global unique identifiers (GUIDs), 198
GlobalNames zone
  about, 4, 12, 71
  legacy support, 14
  planning, 25–26
glue records, 6, 22
GPOs (Group Policy objects)
  about, 209
  filtering, 191
  migration table usage, 179
  NRPT and, 12
  planning Group Policy hierarchy, 190
  precedence considerations, 190
  starter, 178–179, 210
grep command, 153
group IDs, 40
Group Policy
  about, 165, 209
  application deployment, 352–354
  auditing compliance, 180–181
  controlling device installation, 192–195
  distributing certificates, 233
  manipulating settings, 179, 193–195, 209
  planning authentication, 199–204
  planning authorization, 199–204
  planning for EFS, 426
  planning hierarchy, 190–191
Group Policy Management Console, 178–179
Group Policy Management Editor, 195
Group Policy Modeling node, 179
Group Policy objects. See GPOs (Group Policy objects)
guest operating systems
  additional information, 371
  installing, 376
  planning for, 371–372
  planning virtual machine deployment, 372–376
GUIDs (global unique identifiers), 198

H

hardware considerations
  failover clusters and, 443–444
  Hyper-V, 345
  IPv6 networks, 58
  virtualized servers, 378
hardware IDs, 196
hardware security module (HSM), 258
health certificate lifetime, 258
health policies
  compliance with, 249
  configuring NAP servers, 259, 261
  NPS templates and, 241
Health Registration Authority. See HRA (Health Registration Authority)
health state validation, 249
Help Desk Operators, 175
high availability
  failover clusters and, 441–444
  license servers, 336
  RADIUS infrastructures, 238–239
  virtual machines, 373
host computers, 370, 375
Host Credential Authorization Protocol, 294
host-based firewalls, 304
HRA (Health Registration Authority)
  about, 230
  boundary networks and, 256
  fault tolerance, 257
  NAP support, 253, 256–257
  RRAS support, 294
HSM (hardware security module), 258
HTTP (Hypertext Transfer Protocol), 297, 482
hub and spoke replication topology, 17, 112
hybrid replication topology, 114
Hypertext Transfer Protocol (HTTP), 297, 482
hyperthreading, 346, 373
Hyper-V
  about, 294
  advantages, 370
  considerations, 371
  hardware requirements, 345
  in branch offices, 294
  multisite clustering and, 293
  new features, 370
  SCVMM support, 382
Hyper-V management console

- storage considerations, 373
- Virtual Network Manager feature, 374
- Hyper-V management console, 372, 377
- Hyper-V server role, 380
- hypervisor, 370

I

- I8 format, 315
- IANA (Internet Assigned Numbers Authority), 36
- IAS (Internet Authentication Service), 236
- ICMP (Internet Control Message Protocol), 217
- ICMPv4 messages, 44
- ICMPv6 messages, 44, 53
- ID (interface identity), 36
- Identity Management for UNIX Active Directory schema extension, 155
- Identity Management for UNIX role service, 151–152, 155, 161
- IDS (intrusion detection system), 303–304
- IEEE (Institute of Electrical and Electronics Engineers), 36
- IEEE 802.1x standard, 251, 261–265, 454
- IETF (Internet Engineering Task Force), 151
- IFM (Install From Media), 309, 322
- IGMP (Internet Group Management Protocol), 294
- IIS (Internet Information Services), 223, 369
- InetOrgPerson objects, 201
- information cards, 149, 161
- Install From Media (IFM), 309, 322
- Integration Services, 372, 378
- Intel Virtualization Technology (Intel VT), 371
- Intel XD (eXecute Disable), 371
- interface IDs, 36, 51
- interforest migration, 140, 161
- internal CAs, 465–466
- internal networks, 217, 375
- Internet Assigned Numbers Authority (IANA), 36
- Internet Authentication Service (IAS), 236
- Internet Control Message Protocol (ICMP), 217
- Internet Engineering Task Force (IETF), 151
- Internet Group Management Protocol (IGMP), 294
- Internet Information Services (IIS), 223, 369
- Internet Protocol addressing. See IP addressing
- Internet Protocol Security. See IPSec
- Interetwork Packet Exchange (IPX), 35
- interoperability
  - AD FS considerations, 148–156

DNSSEC, 13
- practice exercises, 156–157
- UNIX considerations, 151–155
- Intersite Topology Generator (ISTG), 108
- intraforest authentication, 99–100
- intraforest migration, 140, 161
- intranets, 251
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
  - about, 47, 72
  - DirectAccess considerations, 231
  - transition strategies and, 50
- intrusion detection system (IDS), 303–304
- intrusion prevention system (IPS), 303–304
- IP addressing
  - configuring clients through DHCPv6, 55–57
  - IPv4-to-IPv6 compatibility, 44–47
  - IPv4-to-IPv6 transition strategy, 48–50
  - IPv6 address structure, 33–41
  - IPv6 advantages, 42–44
  - IPv6 tools, 50–55
  - planning, 32
  - planning IPv6 network, 57–61
  - virtual machines and, 375
- IP filters, 235
- IP Security Policies Management MMC snap-in, 54
- ipconfig tool
  - about, 10, 51
  - IPv6 support, 51, 53
  - showing link-local/site-local addresses, 38
- IP-HTTPS protocol, 231
- IPS (intrusion prevention system), 303–304
- IPSec (Internet Protocol Security)
  - authentication, 12
  - data confidentiality, 297
  - designing NAP enforcement, 254–256
  - encryption and, 42
  - moving from server/domain isolation to, 269–270
  - NAP enforcement considerations, 251, 253–254
  - PKI support, 257–259, 455
  - scaling NAP enforcement for large environments, 257
  - scaling NAP enforcement for small environments, 256
  - server/domain isolation comparison, 268–269
- IPSec Tunnel Mode, 225, 229, 297
- IPSec6 tool, 54
- IPv4 addresses, 33, 42, 44–47, 231
IPv4 headers, 43–44
IPv4-to-IPv6
  implementing compatibility, 44–47
  planning transition strategy, 48–50
IPv6
  additional information, 34
  advantages of, 42–44
  case scenarios, 73
  Embedded Rendezvous Point Flagging, 40
  planning an IPv6 network, 57–61
  practice exercises, 27, 61–68
  suggested practices, 74
  support considerations, 18
  tool usage, 50–55
  verifying connectivity, 52–53, 55
  web services access, 224
IPv6 addresses
  about, 33, 42
  additional information, 35
  analyzing structure, 33–41
  assigning, 55
  autoconfiguring, 38, 42
  IPv4-to-IPv6 compatibility, 44–47
  prefixes in, 34
  private, 37
  types of, 34
  Windows Server 2008 R2 support, 12
IPv6 headers, 43–44
IPv6 networks
  additional information, 61
  analyzing hardware requirements, 58
  documentation requirements, 60–61
  software and application requirements, 58–60
IPX addresses, 35, 39
ISA Server
  Network Access Quarantine Control and, 222
  RADIUS remote access solution, 238–239
  VPN server deployment and, 234
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
  about, 47, 72
  DirectAccess considerations, 231
  transition strategies and, 50
iSCSI SAN, 373, 375, 382
isolation
  about, 169, 210
  AD DS administration requirements, 169
  data, 81, 84
domain, 267–270
  forest design requirements, 80–81
  forest trusts and, 175
  server, 267–270
  service, 80, 84
  stakeholders and, 172
issuing CAs, 468–469, 488
ISTG (Intersite Topology Generator), 108
K
KCC (Knowledge Consistency Checker), 116
Kerberos protocol, 176, 199, 297
key pairs, 426
Knowledge Consistency Checker (KCC), 116
L
L2TP (Layer 2 Tunneling Protocol)
  about, 227–228
  data confidentiality, 296
  UDP ports for, 239
  VPN support, 455
latency, CRLs and, 480
LDAP (Lightweight Directory Access Protocol), 151, 289, 482
least privilege, principle of, 168–169, 210
legacy network adapters, 372, 375
legal considerations
  employee monitoring, 302
  for AD DS administration, 168
  for forest structure, 80
license servers. See RD license servers
licensing virtualized environments, 378
Lightweight Directory Access Protocol (LDAP), 151, 289, 482
limited connectivity for forest structure, 80
link-local addresses
  about, 35, 37, 72
  implementing connectivity via, 38
  showing, 38
Linux operating systems, 371
load balancing, 238–239, 340. See also NLB (Network Load Balancing)
Local Machine certificate store, 456
loopback addresses, 39, 72
MAC addresses

M

MAC addresses, 36, 41
maintenance procedures, 437–438
Manage Group Policy Links privilege, 281
management roles, 174
management stakeholders, 172–173
management tasks
  creating forest trusts, 176
deleagating, 172–173
  Group Policy Modeling, 179
management roles, 174
migration tables, 179
planning data management, 176–178
planning forest-level trusts, 175
planning trust type and direction, 175–176
starter GPO usage, 178–179
master NIS server role, 154–155
MBSA (Microsoft Baseline Security Manager), 513
memory settings, virtual machines, 373–374
Microsoft Application Virtualization. See App-V
  (Application Virtualization)
Microsoft Application Virtualization data store, 393
Microsoft Application Virtualization Management
  Console, 393
Microsoft Application Virtualization Management
  servers, 390, 392
Microsoft Application Virtualization Management Web
  Service, 393
Microsoft Application Virtualization Sequencer, 392
Microsoft Application Virtualization Streaming Server,
  393
Microsoft Baseline Security Manager (MBSA), 513
Microsoft Exchange Server, 293
Microsoft Hyper-V. See Hyper-V
Microsoft Identity Management for UNIX console, 151
Microsoft Office SharePoint Server
  assessing needs, 417–420
deploying, 419
  examples of solutions based on, 418–419
  Windows SharePoint Services comparison, 417–418
Microsoft SharePoint Foundation, 414
Microsoft SQL Server, 241, 293
Microsoft System File Checker, 305
Microsoft Update server, 493–494
migration paths, 139–140
migration planning
  cross-forest authentication, 143–144
migration paths, 139–140
practice exercises, 144–145
RD Connection Broker, 340–341
upgrading domains, 141–142
migration tables, 179
mixed administration model, 171
monitoring employees, 302
MS-CHAP authentication, 228, 232
multicast addresses, 35, 39–41, 72
multifactor authentication, 199
multifactor authorization, 199
multinetting technique, 34
multiple-sites model, 111
MX (Mail Exchanger) records, 9

N

NAC (Network Access Control), 245
name resolution
  DNS features and enhancements, 11–18
  GlobalNames zone and, 14
  planning, 4–10
  planning DNS infrastructure, 18–26
Name Resolution Policy Table (NRPT), 12, 231
namespace scalability mode, 410
namespaces
  conditional forwarding and, 21
  DFS, 406, 448
domain-based, 406, 409
  planning, 19–21
Server for NIS, 154
NAP (Network Access Protection)
  about, 245–249, 323
  case scenarios, 273–274
  common scenarios, 251
  enforcement considerations, 252
Health Registration Authority and, 256
  infrastructure overview, 249–251
  integrating DHCP, 59
  limited-access feature, 249
  moving from server/domain isolation to, 269–270
  NPS considerations, 236
  planning 802.1x enforcement, 261–265
  planning DHCP enforcement, 265–267
  planning IPsec enforcement, 251, 253–259
  planning VPN enforcement, 259–261
remote access connectivity, 233
security considerations, 318
NAP enforcement point, 250
NAP VPN enforcement point, 250
NAS (network attached storage), 373
NAT (Network Address Translation), 46, 72, 219
NAT editors, 226
ND (Neighbor Discovery), 37, 41
NDES (Network Device Enrollment Service), 456, 476
NetBEUI (NetBIOS Extended User Interface), 4
NetBIOS (Network Basic Input Output System), 3
NetBIOS Extended User Interface (NetBEUI), 4
NetBT, disabling, 14
netsh branchcache command, 298
netsh interface ipv6 add dnsserver command, 52
netsh interface ipv6 add route command, 55
netsh interface ipv6 delete destinationcache command, 52
netsh interface ipv6 delete route command, 55
netsh interface ipv6 set address command, 51
netsh interface ipv6 set interface command, 52
netsh interface ipv6 set route command, 55
netsh interface ipv6 show address command, 51
netsh interface ipv6 show destinationcache command, 52
netsh interface ipv6 show dnservers command, 10
netsh interface ipv6 show neighbors command, 51
netsh interface ipv6 show route command, 53–54
netstat tool, 10, 47, 51
netstat tool, 51, 54
Network Access Control (NAC), 245
Network Access Protection. See NAP (Network Access Protection)
Network Access Quarantine Control, 222, 249, 261
network access strategy
  deploying perimeter networks, 223–224
designing, 213
designing perimeter networks, 216–223
designing RADIUS solution, 236–241
designing remote access strategy, 224–235
network adapters, 375
Network Address Translation (NAT), 46, 72, 219
network attached storage (NAS), 373
Network Basic Input Output System (NetBIOS), 3
Network Device Enrollment Service (NDES), 456, 476
Network File System (NFS), 155, 161, 373
network interface cards (NICs), 44, 375
Network Load Balancing. See NLB (Network Load Balancing)
network location detection, 231
Network Policy Server (NPS), 59, 236
network-level security, 42
New Virtual Machine Wizard, 376
Next Secure (NSEC/NSEC3), 12
next-level aggregator (NLA), 36
NFS (Network File System), 155, 161, 373
NICs (network interface cards), 44, 375
NIS servers, 154–155, 161
NLA (next-level aggregator), 36
NLB (Network Load Balancing)
  about, 448
  best practices, 441
  failover cluster comparison, 442
  identifying applications for, 440–441
  Remote Desktop Web Access and, 337
  supporting high-usage servers, 439
  VPN considerations, 239
nodes
  dual-stack, 44, 48
  link-local addresses and, 37
  unicast addresses and, 35
nonauthoritative restore, 436, 448
nonuniform memory architecture (NUMA), 374
NOS directory, 78
NPS (Network Policy Server)
  DHCP support, 59
  Health Registration Authority and, 256
  RADIUS remote access solution and, 236
  RRAS support, 294
NRPT (Name Resolution Policy Table), 12, 231
NS (name server) records
  about, 9, 72
  glue records and, 22
  stub zones and, 5–6
NSAP addresses, 35, 39
NSEC/NSEC3 (Next Secure), 12
nslookup tool, 10, 72
ntdsutil utility
  about, 313, 323
  MetadataCleanup command, 313, 323, 438
  offline defragmentation, 437
  seizing FSMO roles, 438
NUMA (nonuniform memory architecture), 374
NX/XD, 346
Object Linking and Embedding (OLE)

O

Object Linking and Embedding (OLE), 390
OCI (Oracle Call Interface), 153
OCSP (Online Certificate Status Protocol)
  AD CS support, 452
  defined, 488
  perimeter network and, 223
  revocation policies and, 481–482
  SSL considerations, 223
ODBC (Open Database Connectivity), 153
offline CAs, 469
offline defragmentation, 437
OLE (Object Linking and Embedding), 390
Open Database Connectivity (ODBC), 153
Open Systems Interconnection (OSI), 39, 296, 375
operational considerations
  for AD DS administration, 168
  for forest structure, 79
operations masters, 120–121, 292, 438
Oracle Call Interface (OCI), 153
organizational forest model, 82
organizational structure
  AD DS administration requirements, 168
  forest structure requirements, 79
  planning, 182–183
organizational units. See OUs (organizational units)
OSI (Open Systems Interconnection), 39, 296, 375
OUs (organizational units)
  about, 210
  administrative authority and, 281
  applying Password Settings objects, 201
  planning Group Policy hierarchy, 190
  planning organizational structure, 182–183

P

P flag, 39
PAP (Password Authentication Protocol), 232
parent domains, stub zones and, 6
parent sites, 504
Password Authentication Protocol (PAP), 232
Password Replication Policy, 308, 310, 322
Password Settings container (PSC), 210
Password Settings objects. See PSOs (Password Settings objects)
Password Synchronization Properties dialog box, 151
passwords
  authentication considerations, 200, 233
  fine-grained policies, 200–202, 209, 314–315
  synchronizing, 151–152
pathping tool, 51, 53
PDC emulators, 120, 410
PEAP authentication, 454
PEAP-MSCHAP authentication, 232, 260
PEAP-TLS authentication, 228, 232, 260
Perform Group Policy Modeling Analysis permission, 179
perimeter networks
  about, 217, 303
  deploying strategic services in, 223–224
  designing, 216
  firewalls, 217, 219–221
  securing, 219–223
  types of architectures, 217–219
  VPN server deployment and, 234
permissions and rights. See also privileges
  security groups and, 173
  stakeholders, 172–173
personal firewalls, 304
personal identification number (PIN), 425
PIN (personal identification number), 425
ping tool, 51–52
ping6 tool, 51
PIPEDA legislation, 460
PKI (public key infrastructure)
  additional information, 454
  assessing AD requirements, 460
  assessing business requirements, 459
  assessing certificate template requirements, 461
  assessing external requirements, 460
  basic components, 454
  case scenarios, 489
  configuring NAP components, 258
  creating certificate management plan, 475–484
  defined, 453, 487
  designing CA hierarchy, 464–471
  DirectAccess requirements, 230
  identifying certificate requirements, 456–458
  IPsec enforcement support, 257–258
  practice exercises, 462, 472–473
  reviewing company security policy, 459
  structure overview, 258
PKI-enabled application/service, 453–455, 488
Point-to-Point Protocol (PPP), 228
Point-to-Point Tunneling Protocol. See PPTP (Point-to-Point Tunneling Protocol)
policy CAs, 468, 488
policy prototyping, 519
port rule affinity, 440
port-restricted cone NATs, 47
PPP (Point-to-Point Protocol), 228
PPTP (Point-to-Point Tunneling Protocol)
about, 225–227
data confidentiality, 296
TCP ports for, 239
VPN support, 455
preboot execution environment (PXE), 284, 375
preshared keys, 227
primary sites, 504
primary zone, 71
principle of least privilege, 168–169, 210
printer location policies, 121–124
private IP addresses, 37, 219
private key archival, 488
private keys, 453, 457, 487
privileges
about, 279, 322
Administrator Role Separation, 282
delegating, 280
processor settings (virtual machines), 373–374, 378
Properties dialog box, 180
Proxy Configuration Wizard, 149
proxy servers, 219
PSC (Password Settings container), 210
PSOs (Password Settings objects)
about, 210, 314–316
applying to OUs, 201–202
creating, 316
practice exercises, 204–207
PTR (Pointer) records, 9
public CAs, 460, 488
public key infrastructure. See PKI (public key infrastructure)
public keys
cryptography support, 426, 453
defined, 453, 487
zone signatures and, 12
pull replication, 16
push replication, 16
PXE (preboot execution environment), 284, 375

Q
QoS (Quality of Service), 43
qualified subordination, 460, 488
quorum disks, 444

R
R flag, 39
RACs (rights account certificates), 202
RADIUS (Remote Authentication Dial-In User Service)
about, 236
feature enhancements, 240
practice exercises, 241–242
remote access for branch office, 239
remote access for main office, 236–239
scaling authentication, 239
RADIUS client
authentication considerations, 239
designing main office solution, 236, 238–239
designing remote access solution, 236
scaling RADIUS authentication, 239
RADIUS proxy
authentication considerations, 239
designing branch office solution, 239
designing main office solution, 238–239
designing remote access solution, 236
scaling RADIUS authentication, 239
secure networks and, 255
RADIUS server
authentication considerations, 239
designing branch office solution, 239
designing main office solution, 238–239
designing remote access solution, 236
scaling RADIUS authentication, 239
RADIUS authentication
RADIUS client
RADIUS proxy
RADIUS server
RAPs (resource authorization policies), 344
RC4 cipher, 296
RD Connection Broker, 329, 340–341
RD Gateway role service, 223, 330, 342–344
RD license servers
activating, 333–334
backing up, 335
deploying, 331–333, 336
high availability, 336
restoring, 335
RD Licensing role service, 330–337
RD Session Host Configuration console, 332
Remote Desktop Session Host role service

RD Session Host role service, 329
RD Session Host servers/server farms, 329, 331–337, 340
RD Virtualization Host role service, 345–346, 363
RDC (Remote Desktop Client), 337, 411
RDC (Remote Differential Compression), 411
RDP (Remote Desktop Protocol), 339, 341
read-only DFS replicas, 316, 323
read-only DNS zones, 289, 322
read-only domain controllers. See RODCs (read-only domain controllers)
read-only zone, 71
realm trust, 176
Real-Time Streaming Protocol (RTSP), 392
Real-Time Streaming Protocol Secure (RTSPS), 392
recovery. See system recoverability
Recovery Environment (RE), 436
Red Hat operating system, 371
referral ordering, 408
regional domain controllers, 118
regional domain model, 87
registration authority, 453, 469, 488
relying party, 149, 161
remediation networks, 254–255
remote access
designing RADIUS solution, 236–241
designing secure VPN server deployment, 234–235
designing strategy, 224–235
designing VPN solution, 225–233
planning for VPN connections, 224–225
Remote Authentication Dial-In User Service. See RADIUS
(Remote Authentication Dial-In User Service)
Remote Desktop Client (RDC), 337, 411
Remote Desktop Connection Broker. See RD Connection Broker
Remote Desktop Connections, 329
Remote Desktop Gateway role service, 223, 330, 342–344
Remote Desktop Licensing role service, 330–337
Remote Desktop Protocol (RDP), 339, 341
Remote Desktop Services
about, 363
App-V support, 390
case scenario, 364
components supported, 329–330
licensing, 331–337
practice exercises, 348–349
secure communications, 344–345
Remote Desktop Services CALs, 333–335
Remote Desktop Session Host role service, 329
Remote Desktop Virtualization Host role service, 345–346, 363
Remote Differential Compression (RDC), 411
Remote Installation Services (RIS), 283
remote procedure call (RPC), 478
Remote Server Administration Tools (RSAT), 286
Remote Session Host servers. See RD Session Host servers/server farms
RemoteApp, 338–339
RemoteApp and Desktop Connection, 296, 330, 340
RemoteApp Manager, 339
RemoteFX
about, 330, 363
designing for content, 346–347
virtualization support, 371
replication
auditing compliance, 180
designing site link bridging, 116
designing site link properties, 115–116
designing site links, 114–115
designing topology, 112–114
DFS, 293, 407, 411–412, 448
DNS zones, 8
pull, 16
push, 16
RODC considerations, 312
WINS, 15–17
WINS-based, 16–17
Replication Management Administrators, 174
Replication Monitoring Operators, 174
reporting
System Center Configuration Manager, 517–518
System Center Essentials, 517
WSUS, 514–517
Requests for Comments (RFCs), 3, 12
resolvers, 21
Resource Administrators, 174
resource authorization policies (RAPs), 344
resource forest model, 83
resource records, 9. See also specific record types
restartable AD DS, 437–438
restore procedures. See also system recoverability
authoritative restore, 436–437, 448
nonauthoritative restore, 436, 448
planning for AD DS, 436–437
RD license servers, 335, 370
virtualization considerations, 370
restricted access forest model, 83
restricted cone NAT, 47
restricted networks, 254–255
Revealed list, 310, 323
reverse lookup zones, 18, 29, 71
RFC 1123, 19
RFC 2044, 19
RFC 2136, 5
RFC 2181, 19
RFC 2307, 151
RFC 2373, 35, 40–41
RFC 2374, 37
RFC 2893, 49
RFC 3007, 5
RFC 3041, 36
RFC 3053, 49
RFC 3056, 50
RFC 3280, 481
RFC 3306, 40
RFC 3879, 37
RFC 3956, 40
RFC 4057, 61
RFC 4191, 36
RFC 4193, 37
RFC 4213, 48
RFC 4214, 50
RFC 4380, 50
RFC 4941, 36
RFCs (Requests for Comments), 3, 12
rights account certificates (RACs), 202
rights and permissions. See also privileges
roles and, 174
security groups and, 173
stakeholders, 172–173
ring replication topology, 16
RIP (Routing Information Protocol), 294
RIS (Remote Installation Services), 283
RODC compatibility pack, 290, 313
RODC FAS (filtered attribute set), 289, 322
RODCs (read-only domain controllers)
about, 12, 210, 289–290, 305–306, 322
additional information, 11
authentication process, 310–311
boundary networks and, 255
compromise threats and, 313–314
determining placement, 119
disadvantages, 306
DNS Server role, 11
fault tolerance, 257
Health Registration Authority and, 256
installing, 307–310
NAP IPSec enforcement, 257
planning zone types, 22
read-only replicated folders, 410
replication considerations, 312
security considerations, 290
upgrading domains, 141
role sandboxing, 369
role-based security policy, 521–522
roles, management, 174
root CAs
best practices, 369
defined, 468, 488
designing, 464
secure network and, 255
root hints, 7, 24, 71
root scalability mode, 410
route aggregation, 43
route print command, 53–54
route tool, 51
Routing and Remote Access Services (RRAS), 56, 236,
293–294
Routing Information Protocol (RIP), 294
routing tables, TLAs and, 43
RPC (remote procedure call), 478
RRAS (Routing and Remote Access Services), 56, 236,
293–294
RSAT (Remote Server Administration Tools), 286
RTSP (Real-Time Streaming Protocol), 392
RTSPS (Real-Time Streaming Protocol Secure), 392
S
S/MIME (Secure/Multipurpose Internet Mail Extensions),
455
SAACL (system access control list), 180
SAM (Security Accounts Manager), 199
SAN (storage area network), 370, 373, 444
sandboxing, 369
SCEP protocol, 476
schema
designing modification process, 97–98
upgrading, 98
Schema Admins group, 141, 174, 201
screened subnets, 234, 238, 303
SCSI (Small Computer System Interface)

SCSI (Small Computer System Interface), 370
SCVMM (System Center Virtual Machine Manager)
   additional information, 386
   deploying virtual machines, 376
   deployment components, 383–385
   in branch offices, 385
   planning for server consolidation, 382–383
   portability support, 369
SCVMM Administrator console, 385
SCVMM agents, 384
SCVMM database, 384
SCVMM library server, 385
SCVMM self-service portal, 385
SCVMM servers, 384
Scwcmd tool, 520–521
sealing process, 488
secondary sites, 504
secondary zone, 71
Second-Level Address Translation (SLAT), 346
secure dynamic updates, 5, 23
secure networks, 251, 255–257
Secure Sockets Layer. See SSL (Secure Sockets Layer)
Secure Sockets Tunneling Protocol (SSTP), 228, 239, 297
Secure/Multipurpose Internet Mail Extensions (S/MIME),
455
Security Accounts Manager (SAM), 199
security baselines, 518–521
Security Configuration and Analysis Tool, 520
Security Configuration Wizard, 235, 518–519
security considerations
   AD DS objects, 181
   authentication protocols, 232
   BitLocker, 423–425
   branch offices, 288, 302–318
   case scenarios, 448–449
   certificates and, 457–458
   data confidentiality, 296–297
   data in storage, 316–317
   DNS Cache Locking, 13
   DNSSEC, 12
   domain design requirements, 85–86
   EFS, 426–427
   Forefront TMG Server, 220–222
   IPSec support, 12, 42
   NAP support, 318
   network-level, 42
   perimeter networks, 219–223
   reviewing company security policy, 459
   RO DCs and, 290
   Server Core, 285
   stakeholders and, 173
   TLS support, 344–345
   Security event log, 181
   Security Group Administrators, 175
security groups, 173, 201
security policy
   additional information, 521
   case scenarios, 529
   practice exercises, 522
   reviewing, 459
   role-based, 521–522
Security Policy Administrators, 174
security zones
   boundary networks, 251, 255
   restricted networks, 254–255
   secure networks, 251, 255–256
server consolidation
   case scenarios, 400
   planning for, 381
   SCVMM support, 382–385
   Virtual Server Migration Toolkit, 381
Server Core
   about, 284–286, 322
   domain controllers and, 290
   Hyper-V and, 370
Server for NIS, 154–155, 161
server hardening, 304–305, 323, 518
server isolation, 267–270
Server Operators group, 174
server-side targeting, 498
Service Administration Managers, 174
service autonomy, 80, 84
service isolation, 80, 84
service management
   about, 169–170, 210
   additional information, 174
   certificate considerations, 456
   PKI-enabled services, 453–455, 488
   recommended roles, 174
Services for Network File System, 155, 161
Session-Timeout RADIUS attribute, 263
Set Up a New Connection or Network Wizard, 229
SHA (System Health Agent), 254, 258
shadow groups, 201, 210
sharing data. See data sharing
Shiva Password Authentication Protocol (SPAP), 232
shortcut trusts
about, 99–100, 175
additional information, 100
practice exercises, 104
SHV (System Health Validator), 251, 259
SID filtering, 144
SID History feature, 144, 161
SIDHistory attribute, 144
signing process, 455–456, 488
Simple Mail Transfer Protocol (SMTP), 111, 220
single site model, 110
single-domain model, 86, 118
site link bridge, 116
site link properties, 115–116
site links
branch office considerations, 296
designing, 114–115
determining costs, 115
determining interval, 116
determining schedule, 116
site-level aggregator, 36
site-local unicast addresses, 35, 37–38
sites
automatic coverage, 312–313, 322
case scenarios, 134
designing site model, 110–112
gathering design requirements, 102–110
practice exercises, 126–127
slash notation, 34
SLAT (Second-Level Address Translation), 346
Small Computer System Interface (SCSI), 370
smart card authentication, 202–204, 455
SMP (symmetric multiprocessor), 370
SMTP (Simple Mail Transfer Protocol), 111, 220
snapshots, 377
SOA (Start of Authority) records, 5, 9, 71
software and application requirements, IPv6 networks, 58–60
software update points, 505
software updates
managing compliance, 513–521
MBSA tool, 513
Microsoft Update server solution, 493–494
planning automatic approvals, 500
System Center Configuration Manager support, 504–505
System Center Essentials support, 501–504
WSUS solution, 494–501
SoH (Statement of Health), 254
SoHRs (Statement of Health Responses), 254
solicited-node multicast addresses, 41
SPAP (Shiva Password Authentication Protocol), 232
special addresses, 35, 39
SQL Server
    Accounting Configuration Wizard and, 241
    fault tolerance and, 293
    SCVMM support, 382, 384
SQL Server Express, 384
SRV (Service Location) records
about, 9, 72, 312
GlobalNames zone and, 14, 26
SSL (Secure Sockets Layer)
    Federation Service and, 149
    OCSP considerations, 223
    PKI support, 455
    SCVMM considerations, 384
    smart card authentication, 202
    SSTP support, 297
SSoHR (System Statement of Health Response), 254
SSTP (Secure Sockets Tunneling Protocol)
about, 228
    NLB support, 239
    SSL support, 297
    VPN support, 455
staging folders, 412
stakeholders, management, 172–173
stand-alone CAs, 466–468, 488
starter GPOs, 178–179, 210
stateful inspection firewalls, 219
Statement of Health (SoH), 254
Statement of Health Responses (SoHRs), 254
storage area network (SAN), 370, 373, 444
storage considerations
document storage, 414
failover clusters and, 444
for virtual machines, 373
practice exercises, 431–432
security for data, 316–317
stub zones, 5–6, 71
SUA (Subsystem for UNIX-Based Applications), 153, 161
subject/end entity, 456, 468, 479, 488
subnet-router anycast addresses, 41
subordinate CAs, 468–469, 488
Subsystem for UNIX-Based Applications (SUA), 153, 161
Summary dialog box, 309
SUSE operating system, 371
symmetric cryptography, 426
symmetric multiprocessor (SMP), 370
synchronization, password, 151–152
system access control list (SACL), 180
System Center Configuration Manager
about, 364
compliance and reporting, 517–518
planning application deployment, 356–358
software update support, 504–505
System Center Essentials
about, 364
planning application deployment, 354–355
practice exercises, 509–510, 522–523
reporting support, 517
software update support, 501–504
System Center Operations Manager, 384
System Center Virtual Machine Manager. See SCVMM
(System Center Virtual Machine Manager)
System File Checker (SFC.exe), 305
System Health Agent (SHA), 254, 258
System Health Validator (SHV), 251, 259
system recoverability. See also restore procedures
failover clusters and high availability, 441–444
NLB supporting high-usage servers, 439–441
planning maintenance and recovery procedures, 434–438
seizing operations master roles, 438
System Statement of Health Response (SSoHR), 254

T

T flag, 39
TCP (Transmission Control Protocol), 43, 55, 239
TCP/IP (Transmission Control Protocol/Internet Protocol), 284
TCP/IPv6 Properties dialog box, 52
Telnet tool, 55
teredo technology, 45–46, 50, 72
Terminal Services Web Access, 337–338
third-party CAs, 465–466
Time-to-Live (TTL), 13
TLA (top-level aggregator), 36, 43
TLS (Transport Layer Security), 297, 344–345
TPM (Trusted Platform Module)
BitLocker support, 317, 423–424
with PIN, 425
with USB flash device, 424
tracert tool, 51, 53
translation planning, IPv4-to-IPv6, 48–50
Transmission Control Protocol (TCP), 43, 55, 239
Transmission Control Protocol/Internet Protocol (TCP/IP), 284
Transport Layer Security (TLS), 297, 344–345
Tripwire tool, 305
troubleshooting
connectivity problems, 51, 53–55
DNS problems, 55
URLs, 259
trust anchor, 12
trust relationships
certificate trust list, 488
designing, 99–100
forest, 143–144, 175–176
planning trust type and direction, 175–176
RADIUS authentication and, 239
Trusted Platform Module. See TPM (Trusted Platform Module)
TS CALs, 335
TS Web Access, 337–338
TTL (Time-to-Live), 13
tunnel brokers, 49
tunnels. See also specific tunneling protocols
6to4, 50
about, 49
automatic tunneling, 49
explicit, 49
two-phase migration, 140, 161

U

UDDI Services, 416
UDP (User Datagram Protocol), 43, 239, 297
UNC (Universal Naming Convention), 405
unicast addresses, 35–39, 72
unique-local unicast addresses, 35, 37–38, 72
universal groups, 173
Universal Naming Convention (UNC), 405
UNIX interoperability
identity management, 151–152
Server for NIS, 154–155, 161
Services for Network File System, 155, 161
SUA support, 153
unspecified addresses, 39, 72
updates. See software updates
upgrade-then-restructure migration path, 140, 161
upgrading
  domains, 89–90, 139, 141–142, 161
  schema, 98
URLs
  CRL publication and, 482
  troubleshooting, 259
USB flash devices, 424–425
User Datagram Protocol (UDP), 43
UTC (Coordinated Universal Time), 411

V
VDI (Virtual Desktop Infrastructure), 295
tenant-specific attributes (VSAs), 263
verifying
  certificates, 454, 488
  Group Policy settings, 179
  IPv6 connectivity, 52–53, 55
  zone signatures, 12
VHD file extension, 284
VHDs (virtual hard disks), 376
virtual adapters, 375
Virtual Desktop Infrastructure (VDI), 295
virtual DNS servers, 57
virtual hard disks (VHDs), 376
virtual local area networks (VLANS), 263, 374–376
Virtual Machine Manager. See SCVMM (System Center Virtual Machine Manager)
virtual machines. See VMs (virtual machines)
Virtual Network Manager feature, 374
virtual private network. See VPN (virtual private network)
Virtual Server Migration Toolkit, 381
virtual switches, 375
virtualization
  about, 368–370
  application, 390–395
  candidates for, 380–381
  in branch offices, 294
  licensing considerations, 378
  managing virtualized servers, 377–378
  planning for guest operating systems, 371–376
  planning for Hyper-V, 370–371
  planning for server consolidation, 381–385
  practice exercises, 394–396
  Virtualization Management console, 284
virtualized servers
  licensing considerations, 378
  managing, 377
  modifying hardware settings, 378
  practice exercises, 386–387
  snapshots, 377
VLANs (virtual local area networks), 263, 374–376
VMK (Volume Master Key), 424
VMMLibrary library share, 385
VMs (virtual machines)
  editing settings, 378
  guest operating systems and, 371
  Hyper-V and, 294, 370–371
  installing guest operating systems, 376
  licensing considerations, 378
  limiting processor usage, 378
  planning deployment, 372–376
  planning memory settings, 373–374
  planning network configuration, 374–376
  planning processor settings, 373–374
  planning virtual hard disks configuration, 376
  RemoteApp and Desktop Connection, 330
  RemoteFX and, 345
  storage considerations, 373
VMware ESX, 382
Volume Master Key (VMK), 424
volume shadow copy, 370
VPN (virtual private network)
  centralized access management, 235
  designing secure deployment, 234–235
  designing solution, 225–233
  load balancing and, 239
  NAP enforcement, 259–261
  PKI support, 455
  planning remote access connections, 224–225
  practice exercises, 242
  RADIUS remote access solution, 238–239
  RRAS support, 294
  SSTP support, 297
VPN Reconnect, 225, 229, 297
VSAs (vendor-specific attributes), 263

W
wbadmin tool, 435–436
WDDM drivers, 347
WDS (Windows Deployment Services)

WDS (Windows Deployment Services), 283–287, 372, 380
Web Enrollment Support pages, 476, 478
Web Server (IIS) server role, 203, 229, 286
Web server services, deploying, 223–224
Web Single Sign-On (SSO) design, 150
Windows Deployment Services (WDS), 283–287, 372, 380
Windows Firewall, 54, 235
Windows Internet Name Service. See WINS (Windows Internet Name Service)
Windows PowerShell, 382
Windows Recovery Environment (RE), 436
Windows Security Health Validator SHV, 259
Windows Server 2008 R2
  configuring DNS, 5
  installation options, 284–287
  IPv6 addresses, 12
  planning DNS, 5–10
  securing in branch offices, 303–318
Windows Server Backup, 435–436
Windows Server Update Services. See WSUS (Windows Server Update Services)
Windows Server Virtualization, 293–294
Windows SharePoint Services
  accessing needs, 413–416
  deployment options, 416
  downloading, 413
  Microsoft Office SharePoint Server comparison, 417–418
  reviewing features, 414–415
Windows System Resources Manager (WSRM), 416
WINS (Windows Internet Name Service)
  NAP support, 250
  NetBIOS considerations, 3
  planning replication for legacy support, 15–17
  support considerations, 14
  Windows Server integration, 5
WINS replication partners, 72
wireless access points, 238, 251
witness disk, 444
Workstation Administrators, 174
WSRM (Windows System Resources Manager), 416
WSUS (Windows Server Update Services)
  about, 294
  administration models, 496–497
  boundary networks and, 255
  case scenarios, 528
compliance reporting, 514–517
computer groups, 497–498
deployment hierarchies, 495
managing, 495
NAP infrastructure and, 250
planning automatic approvals, 500
planning deployment, 501
practice exercises, 505–508
software update support, 494–501
update policy settings, 499–500
Windows SharePoint Services and, 416
WSUS Administrators group, 495, 515
WSUS Reporters group, 495, 515
WSV servers, 293

X

X.509 standard, 296, 456, 487
XDDM drivers, 347
XPS (XML Paper Specification), 431

Z

zone signatures, 12
zone transfers, 8, 71
zone walking, 12
zones. See DNS zones
About the Authors

DAVID R. MILLER (PCI QSA, SME; MCT; MCITPro; MCSE Windows NT 4.0, Windows 2000, and Windows 2003: Security; CISSP; LPT; ECSA; CEH; CWNA; CCNA; CNE; Security+; A+; N+, etc.) is a consultant in the IT industry who specializes in compliance, security, and network engineering. David is an instructor, an author, and a technical editor of books, curricula, certification exams, and computer-based training videos. He regularly contributes as a Microsoft subject matter expert (SME) on product lines including Microsoft Windows Server 2003, Windows Server 2008 R2, Microsoft Exchange Server 2007, Windows 7, and Windows Vista. He is the lead author on this book, now in its second edition, and on the information systems security book titled Security Administrator Street Smarts for Sybex and Wiley Publishing, about to be released in its third edition. David has coauthored two books on Windows Vista for Que Publishing and another book on Exchange Server 2007 for Microsoft Press. In addition, David is working on two new titles for Microsoft Press and a new book for Pearson Education; all three new books are scheduled for publication in 2011.

PAUL MANCUSO (SME, CCSI, DCUCSS, DCNISS, CCNP, CCIP, CCNA, CCDA, VCP, VCAP-DCA, CTT+, CCISP, MCT, MCITP:EA) has offered consulting in the network services area for more than 21 years and has also provided authorized instruction for Cisco, VMware, and Microsoft for more than 18 years. Paul currently provides extensive training and consulting in data center design and support for Cisco, VMware, and Microsoft technologies. He earned a bachelor of science in zoology and pre-med from Ohio State University, deciding late in his studies to turn his attention toward business services, finance, marketing, and computers. His studies in these areas introduced him to the emerging field of local area networks (LANs), which later spearheaded a revolution in business processes. This early introduction to LANs prompted him to begin a career in network integration upon his graduation. It has become a passion ever since.

He has previously authored books on Windows Vista, Microsoft Exchange Server 2007, and Windows Server 2008. In addition to books, Paul has authored courseware for Microsoft and Cisco courses, and he is currently involved in authoring Cisco labs. Combining his real-world consulting and training experiences, Paul has come to understand the complexities involved in delivering network services in the data center that is rapidly evolving today. His enthusiasm for networking is evident in every lecture he gives and work he authors.
JOHN POLICELLI (MVP for Directory Services) is a solutions-focused IT consultant with Avanade Canada. John has more than a decade of success in architecture, security, strategic planning, and disaster recovery planning. He has designed and implemented dozens of complex directory service, collaboration, web, networking, and enterprise security solutions. John has spent many years focused on identity and access management and has provided thought leadership for some of the largest installations of Active Directory directory service in Canada. He has been involved as an author, technical reviewer, and SME for more than 75 training, certification, and technical white paper projects.

ORIN THOMAS, (MCITP, MCT, MVP) is an author, trainer, and frequent public speaker who has authored more than a dozen books for Microsoft Press. 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.

IAN MCLEAN (MCSE, MCITP, MCT) has more than 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. He currently provides technical support for a government organization and runs his own consultancy company. Ian has written 22 books in addition to many papers and technical articles. Books he has previously coauthored include MCITP Self-Paced Training Kit (Exam 70-444): Optimizing and Maintaining a Database Administration Solution Using Microsoft SQL Server 2005 and MCITP Self-Paced Training Kit (Exam 70-646): Windows Server Administration: Windows Server 2008 Administrator. When not writing, Ian annoys everyone by playing guitar very badly. However, he is forced to play instrumentals because his singing is even worse.

J.C. MACKIN (MCITP, MCTS, MCSE, MCDST, MCT) is a writer, editor, consultant, and trainer who has been working with Microsoft networks for more than a decade. Books he has previously authored or coauthored include MCSA/MCSE Self-Paced Training Kit (Exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, MCITP Self-Paced Training Kit (Exam 70-443): Designing a Database Server Infrastructure Using Microsoft SQL Server 2005, and MCITP Self-Paced Training Kit (Exam 70-622): Supporting and Troubleshooting Applications on a Windows Vista Client for Enterprise Support Technicians. He also holds a master’s degree in telecommunications and network management. When not working with computers, J.C. can be found with a panoramic camera photographing medieval villages in Italy or France.