

**Microsoft**

MCITP EXAM

**70-686**

# Windows® 7 Enterprise Desktop Administrator



Craig Zacker  
Orin Thomas

SELF-PACED

# Training Kit

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

Copyright © 2011 by Craig Zacker and Orin Thomas

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

Library of Congress Control Number: 2010933005

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at [www.microsoft.com/mspress](http://www.microsoft.com/mspress). Send comments to [tkinput@microsoft.com](mailto:tkinput@microsoft.com).

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

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

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

**Acquisitions Editor:** Martin DelRe

**Developmental Editor:** Maria Gargiulo

**Project Editor:** Rosemary Caperton

**Editorial Production:** Online Training Solutions, Inc.

**Technical Reviewer:** Kurt Meyer

**Cover:** Tom Draper Design

Body Part No. X17-13734

# Exam 70-686: Pro: Windows 7, Enterprise Desktop Administrator

OBJECTIVE	CHAPTER	LESSON
<b>1. PLANNING AND MANAGING A CLIENT LIFE CYCLE STRATEGY</b>		
1.1 Plan and manage client licensing and activation.	Chapter 2	Lesson 1
1.2 Plan and manage software updates.	Chapter 8	Lessons 1 and 2
1.3 Plan and manage a physical hardware and virtualization strategy.	Chapter 2	Lesson 2
<b>2. DESIGNING A STANDARD IMAGE</b>		
2.1 Design an image creation strategy.	Chapter 3	Lesson 1
2.2 Design a custom image.	Chapter 3	Lesson 2
2.3 Define an image update strategy.	Chapter 3	Lesson 2
<b>3. DESIGNING CLIENT CONFIGURATIONS</b>		
3.1 Design standard system settings.	Chapter 4	Lessons 1 and 2
3.2 Define client security standards.	Chapter 5	Lesson 1
3.3 Define Windows Internet Explorer settings.	Chapter 5	Lesson 2
<b>4. DESIGNING A WINDOWS 7 CLIENT DEPLOYMENT</b>		
4.1 Analyze the environment and choose appropriate deployment methods.	Chapter 6	Lessons 1 and 2
4.2 Design a lite-touch deployment strategy.	Chapter 7	Lesson 1
4.3 Design a zero-touch deployment strategy.	Chapter 7	Lesson 2
4.4 Design a user state migration strategy.	Chapter 2	Lesson 3
<b>5. DESIGNING APPLICATION PACKAGES FOR DEPLOYMENT</b>		
5.1 Design a delivery or deployment strategy.	Chapter 9 Chapter 10	Lesson 1 Lessons 1 and 2
5.2 Manage application compatibility.	Chapter 9	Lesson 2
<b>6. IDENTIFYING AND RESOLVING DEPLOYMENT AND CLIENT CONFIGURATION ISSUES</b>		
6.1 Identify and resolve Internet Explorer issues.	Chapter 11	Lesson 1
6.2 Identify and resolve Group Policy issues.	Chapter 11	Lesson 2
6.3 Identify and resolve networking issues.	Chapter 12	Lesson 1
6.4 Identify and resolve authentication and authorization issues.	Chapter 12	Lesson 2

**Exam Objectives** The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning Web site for the most current listing of exam objectives: <http://go.microsoft.com/fwlink/?LinkId=199933>.



# Contents at a Glance

<i>Introduction</i>	xix	
<b>CHAPTER 1</b>	<b>Preparing to Deploy Windows 7</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Designing a Client Life Cycle</b>	<b>41</b>
<b>CHAPTER 3</b>	<b>Creating and Managing System Images</b>	<b>75</b>
<b>CHAPTER 4</b>	<b>Configuring Clients</b>	<b>117</b>
<b>CHAPTER 5</b>	<b>Configuring Security and Internet Explorer</b>	<b>171</b>
<b>CHAPTER 6</b>	<b>Designing a Windows 7 Client Deployment Strategy</b>	<b>219</b>
<b>CHAPTER 7</b>	<b>Designing Lite-Touch and Zero-Touch Deployments</b>	<b>265</b>
<b>CHAPTER 8</b>	<b>Planning a Windows 7 Client Update Strategy</b>	<b>325</b>
<b>CHAPTER 9</b>	<b>Deploying Applications</b>	<b>355</b>
<b>CHAPTER 10</b>	<b>Using Application Deployment Tools</b>	<b>391</b>
<b>CHAPTER 11</b>	<b>Troubleshooting Internet Explorer and Group Policy Issues</b>	<b>431</b>
<b>CHAPTER 12</b>	<b>Troubleshooting Networking and Authentication-Authorization Issues</b>	<b>469</b>
<i>Answers</i>	505	
<i>Glossary</i>	539	
<i>Index</i>	545	
<i>About the Authors</i>	563	



# Contents

<b>Introduction</b>	<b>xix</b>
Hardware Requirements .....	xix
Software Requirements .....	xx
Using the Companion Media .....	xx
How to Install the Practice Tests	xxi
How to Use the Practice Tests	xxi
How to Uninstall the Practice Tests	xxiii
Microsoft Certified Professional Program .....	xxiii
Errata and Book Support.....	xxiii
We Want to Hear from You.....	xxiv
Stay in Touch .....	xxiv
 <b>Chapter 1 Preparing to Deploy Windows 7</b>	 <b>1</b>
Before You Begin.....	2
Lesson 1: Understanding the Windows 7 Deployment Life Cycle .....	3
Scaling the Deployment Process	3
Placing an MDT Deployment in the MOF Life Cycle	10
Lesson Summary	22
Lesson Review	22
Lesson 2: Gathering Upgrade Information.....	23
Compiling a Workstation Hardware Inventory	24
Creating Workstation Performance Benchmarks	31
Lesson Summary	35
Lesson Review	36

Chapter Review .....	37
Chapter Summary	37
Key Terms	37
Case Scenarios	38
Suggested Practices	39
Take a Practice Test	40
<b>Chapter 2 Designing a Client Life Cycle</b>	<b>41</b>
Before You Begin.....	42
Lesson 1: Designing and Managing a Licensing Strategy .....	43
Windows 7 Editions and Licensing	43
Windows Product Activation	44
Volume Licensing Activation Methods	45
Software Licensing Management Tool	50
Lesson Summary	50
Lesson Review	50
Lesson 2: Designing a Client Hardware Platform .....	52
Windows 7 Hardware Requirements	52
Windows 7 Editions	53
Windows 7 Virtualization	54
Virtualization Hosts	55
Boot from VHD	55
Lesson Summary	60
Lesson Review	60
Lesson 3: Migrating User Profiles.....	61
Understanding Migration Circumstances	62
User State Migration Tool	65
Lesson Summary	70
Lesson Review	70

Chapter Review .....	71
Chapter Summary	72
Key Terms	72
Case Scenarios	72
Suggested Practices	73
Take a Practice Test	74
<b>Chapter 3 Creating and Managing System Images</b>	<b>75</b>
Before You Begin.....	76
Lesson 1: Designing an Image Creation Strategy .....	77
Introducing Windows Imaging Files	77
Understanding the Image Creation Process	79
Building an Image Creation Laboratory	86
How Many Images Do I Need?	88
Understanding Image Types	90
Lesson Summary	97
Lesson Review	98
Lesson 2: Customizing and Updating Images .....	99
Customizing Images	100
Updating Images	101
Using Image Modification Tools	103
Testing Images	110
Lesson Summary	111
Lesson Review	112
Chapter Review .....	113
Chapter Summary	113
Key Terms	113
Case Scenarios	114
Suggested Practices	115
Take a Practice Test	116

<b>Chapter 4 Configuring Clients</b>	<b>117</b>
Before You Begin.....	117
Lesson 1: Designing a Client Configuration Strategy .....	118
Evaluating Business Requirements	119
Matching Configuration Settings to Requirements	119
Selecting a Configuration Method	120
Using Group Policy	121
Using Scripts	140
Lesson Summary	148
Lesson Review	149
Lesson 2: Creating a Client Baseline Configuration.....	150
Deploying a Baseline Configuration	150
Using GPO Accelerator	151
Configuring Windows Error Reporting	153
Creating Auditing Policies	155
Creating a Folder Redirection Policy	157
Designing a User Profile Strategy	159
Lesson Summary	165
Lesson Review	165
Chapter Review .....	166
Chapter Summary	166
Key Terms	167
Case Scenarios	167
Suggested Practices	168
Take a Practice Test	169

<b>Chapter 5 Configuring Security and Internet Explorer</b>	<b>171</b>
Before You Begin.....	172
Lesson 1: Configuring Client Security .....	172
Using Encryption	173
Creating Firewall Rules	179
Defining Account Policies	181
Defining User Account Control Policies	182
Configuring User Rights and Security Policies	183
Locking Down Services	185
Defining AppLocker Settings	185
Configuring Removable Drive Policies	187
Modifying Network Security Settings	189
Lesson Summary	194
Lesson Review	194
Lesson 2: Configuring Windows Internet Explorer .....	196
Internet Explorer Administration Kit	196
Windows Internet Explorer and Group Policy	199
Configuring Security Zones	199
Managing Cache Settings	202
Privacy Settings	203
Proxy Server Connections	207
Add-ons and Accelerators	208
Lesson Summary	214
Lesson Review	214
Chapter Review .....	216
Chapter Summary	216
Key Terms	216
Case Scenarios	217
Suggested Practices	218
Take a Practice Test	218

## **Chapter 6 Designing a Windows 7 Client Deployment Strategy 219**

Before You Begin.....	219
Lesson 1: Understanding the Windows 7 Deployment Process .....	220
Windows 7 Deployment Basics	221
Using Windows Deployment Services	225
Using Windows 7 Automated Installation Kit	230
Using Microsoft Deployment Toolkit 2010	235
Lesson Summary	246
Lesson Review	247
Lesson 2: Choosing a Deployment Method.....	248
Understanding Deployment Options	248
Understanding Deployment Scenarios	250
Evaluating the Infrastructure	253
Scaling the Client Deployment Process	256
Lesson Summary	259
Lesson Review	260
Chapter Review .....	261
Chapter Summary	261
Key Terms	262
Case Scenarios	262
Suggested Practices	263
Take a Practice Test	264

## **Chapter 7 Designing Lite-Touch and Zero-Touch Deployments 265**

Before You Begin.....	265
Lesson 1: Designing a Lite-Touch Deployment .....	266
Understanding Lite-Touch Deployment Requirements	267
Building Reference Computers	269
Deploying Images to Target Computers	269
Customizing Target Deployments	286
Lesson Summary	296
Lesson Review	297
Lesson 2: Designing a Zero-Touch Deployment .....	298
Using System Center Configuration Manager	298
Creating Task Sequences Using SCCM	300
Deploying ZTI Task Sequences to Target Computers	310
Lesson Summary	321
Lesson Review	321
Chapter Review .....	322
Chapter Summary	322
Key Terms	323
Case Scenarios	323
Suggested Practices	324
Take a Practice Test	324

<b>Chapter 8 Planning a Windows 7 Client Update Strategy</b>	<b>325</b>
Before You Begin.....	326
Lesson 1: Designing an Update Management Strategy.....	326
Understanding Updates	327
Update Deployment	328
Windows Server Update Services	330
Configuring an Update Testing Infrastructure	336
Verifying Update Deployment	336
Updating with System Center Configuration Manager	339
Lesson Summary	341
Lesson Review	341
Lesson 2: Deploying Updates to Clients.....	343
Managing Windows Update Clients	344
Configuring Update-Related Group Policy	345
Scheduling Deployment and Restart	347
Rolling Back Updates	348
Lesson Summary	350
Lesson Review	350
Chapter Review .....	352
Chapter Summary	352
Key Terms	352
Case Scenarios	353
Suggested Practices	354
Take a Practice Test	354

<b>Chapter 9 Deploying Applications</b>	<b>355</b>
Before You Begin.....	355
Lesson 1: Designing an Application Deployment Strategy .....	356
Selecting Applications	356
Deploying Applications	360
Lesson Summary	367
Lesson Review	368
Lesson 2: Managing Application Compatibility.....	369
Understanding Application Incompatibilities	369
Creating an Application Inventory	370
Detecting Incompatibilities	372
Evaluating Application Incompatibility Solutions	373
Using the Application Compatibility Toolkit	378
Lesson Summary	386
Lesson Review	386
Chapter Review .....	387
Chapter Summary	387
Key Terms	388
Case Scenarios	388
Suggested Practices	389
Take a Practice Test	389

## **Chapter 10 Using Application Deployment Tools** **391**

Before You Begin.....	391
Lesson 1: Deploying Applications Using Group Policy and SCCM 2007 .....	392
Deploying Applications Using Group Policy	393
Creating Software Installation Policies	397
Deploying Applications Using SCCM 2007	402
Lesson Summary	415
Lesson Review	416
Lesson 2: Deploying Applications Using RDS.....	416
Overview of RDS Deployment	417
Understanding RDS Deployment Options	418
Deploying RemoteApp Applications	418
Packaging RemoteApp Applications	420
Lesson Summary	425
Lesson Review	426
Chapter Review .....	427
Chapter Summary	427
Key Terms	427
Case Scenario	428
Suggested Practices	428
Take a Practice Test	429

<b>Chapter 11 Troubleshooting Internet Explorer and Group Policy Issues</b>	<b>431</b>
Before You Begin.....	431
Lesson 1: Troubleshooting Internet Explorer Issues .....	432
Understanding General Troubleshooting Procedures	432
Understanding Your Role in the Troubleshooting Process	434
Troubleshooting Web Site Access Issues	436
Troubleshooting Browser Performance Issues	444
Lesson Summary	450
Lesson Review	451
Lesson 2: Troubleshooting Group Policy Issues.....	452
Recognizing Group Policy Issues	452
Troubleshooting Group Policy Delivery	453
Lesson Summary	463
Lesson Review	464
Chapter Review .....	465
Chapter Summary	465
Key Terms	465
Case Scenarios	466
Suggested Practices	468
Take a Practice Test	468

<b>Chapter 12 Troubleshooting Networking and Authentication-Authorization Issues</b>	<b>469</b>
Before You Begin.....	469
Lesson 1: Troubleshooting Network Issues .....	470
Troubleshooting Wired Network Connections	470
Troubleshooting Wireless Network Connections	479
Troubleshooting Remote Network Connections	482
Lesson Summary	486
Lesson Review	487
Lesson 2: Troubleshooting Authentication and Authorization Issues . . .	488
Troubleshooting Logon Failures	488
Troubleshooting Authorization Failures	496
Lesson Summary	499
Lesson Review	500
Chapter Review .....	501
Chapter Summary	501
Key Terms	501
Case Scenarios	502
Suggested Practices	503
Take a Practice Test	503
Answers	505
Glossary	539
Index	545
About the Authors	563

---

**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/](http://www.microsoft.com/learning/booksurvey/)

# Introduction

---

This training kit is designed for Windows desktop administrators who want to update their current certification credentials to reflect their experience with Windows 7. As a desktop administrator, you have at least three years of experience installing, configuring, and administering clients in a medium to very large Windows network environment. You are likely responsible for deploying operating systems and applications, and should be familiar with the client administration capabilities of Windows Server 2008 R2 and the System Center suite of products. The Preparation Guide for Exam 70-686 is available at <http://www.microsoft.com/learning/en/us/exam.aspx?id=70-686>.

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

- Plan and manage a client life cycle strategy.
- Design a standard image.
- Design client configurations.
- Design a Windows 7 client deployment.
- Design application packages for deployment.
- Identify and resolve deployment and client configuration issues.

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

## Hardware Requirements

We recommend that you use a test workstation, test server, or staging server to complete the practice exercises in each lesson. However, it would be beneficial for you to have access to production-ready data in your organization. If you need to set up a workstation to complete the practices, the minimum system requirements follow:

- Personal computer with at least a 1-GHz 32-bit (x86) or 64-bit (x64) processor
- At least 1 GB of RAM (x86 systems) or 2 GB of RAM (x64 systems)
- At least a 40-GB hard disk
- DVD-ROM drive
- Super VGA (800 x 600) or higher resolution video adapter and monitor
- Keyboard and Microsoft mouse or compatible pointing device

For some chapters, your workstation must have access to an Active Directory Domain Services network. Chapter 10, "Using Application Deployment Tools," requires access to a computer running Windows Server 2008 R2.

## Software Requirements

The practices in each chapter have various software requirements, all consisting of products available as free downloads from the Microsoft Download Center at <http://www.microsoft.com/downloads/>. The following software is required to complete the practices.

- Microsoft Assessment And Planning Toolkit
- Microsoft Windows Automated Installation Kit for Windows 7
- Microsoft Deployment Toolkit 2010
- Microsoft Internet Explorer Administration Kit
- Microsoft Baseline Security Analyzer 2.2
- Microsoft SQL Server 2008 Express
- Microsoft Application Compatibility Toolkit

## Using the Companion Media

The companion media (CD/DVD) included with this training kit contains the following:

- **Practice tests** You can reinforce your understanding of how to configure Windows Vista 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 70-686 certification exam by using tests created from a pool of 200 realistic exam questions, which give you many practice exams to ensure that you are prepared.
- **An eBook** An electronic version (eBook) of this book is included for when you do not want to carry the printed book with you.

### **NOTE** DIGITAL CONTENT FOR DIGITAL BOOK READERS

If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion media. Visit <http://go.microsoft.com/fwlink/?LinkId=200181> to get your downloadable content. This content is always up to date and available to all readers.

## How to Install the Practice Tests

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

1. Insert the companion CD into your CD 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 for alternate installation instructions.

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

## How to Use the Practice Tests

To start the practice test software, follow these steps:

1. Click Start, 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**

Select the (70-686) Pro: Windows 7, Enterprise Desktop Administrator *lesson review* to use the questions from the “Lesson Review” sections of this book. Select the (70-686) Pro: Windows 7, Enterprise Desktop Administrator *practice test* to use a pool of 200 questions similar to those that appear on the 70-686 certification exam.

## Lesson Review Options

When you start a lesson review, the Custom Mode dialog box appears so that you can configure your test. You can click OK to accept the defaults, or you can customize the number of questions you want, how the practice-test software works, 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.

- **Article I** To take the test, answer the questions and use the Next and Previous buttons to move from question to question.
- **Article II** After you answer an individual question, if you want to see which answers are correct—along with an explanation of each correct answer—click Explanation.
- **Article III** 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, both overall and per objective. You can print a copy of your test, review your answers, or retake the test.

## Practice Test Options

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

- **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 test user interface is basically the same but with different options enabled or disabled depending on the mode. The main options are discussed in the previous section, “Lesson Review Options.”

When you review your answer to an individual practice test question, you see a “References” section 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 Program And Features option in Windows Control Panel.

## Microsoft Certified Professional Program

Microsoft certifications provide the best method for proving your command of current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies. Computer professionals who become Microsoft-certified are recognized as experts and are sought after industry-wide. Certification brings a variety of benefits to the individual and to employers and organizations.

### MORE INFO ALL THE MICROSOFT CERTIFICATIONS

For a full list of Microsoft certifications, go to [www.microsoft.com/learning/mcp/default.asp](http://www.microsoft.com/learning/mcp/default.asp).

## Errata and Book Support

We've made every effort to ensure the accuracy of this book and its companion content. If you do find an error, please report it on our Microsoft Press site at [Oreilly.com](http://Oreilly.com):

1. Go to <http://microsoftpress.oreilly.com>.
2. In the Search box, enter the book's ISBN or title.
3. Select your book from the search results.
4. On your book's catalog page, under the cover image, you'll see a list of links.
5. Click View/Submit Errata.

You'll find additional information and services for your book on its catalog page. If you need additional support, please e-mail Microsoft Press Book Support at [tkinput@microsoft.com](mailto:tkinput@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

**M**icrosoft 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 1

# Preparing to Deploy Windows 7

The smaller the enterprise, the less formal and complex its software deployment process tends to be. It is not unusual for a single team of administrators to be responsible for the conception, planning, and execution of an entire workstation deployment in a small to medium-size company. When the team consists of individuals who work together every day, collaboration and communication are relatively simple matters; the whole group can easily gather to report their progress to their managers.

Take, for example, the process of designing image files, as covered in Chapter 3, “Creating and Managing System Images.” For a small network, administrators can address easily issues such as how many images to create and of what type. Factors affecting these decisions, such as the number of client roles required, are manageable, and all of the people involved in the imaging process are likely to be available for consultation.

For a large enterprise, however, this same image creation process can be enormously complex. A company with thousands of users and dozens of offices around the world might require hundreds of image files that support a great many client roles, each in multiple languages. The team needed just to create and manage these image files could be far larger than the entire deployment team for a small company.

Lesson 1 of this chapter examines the entire Windows 7 deployment process, from planning to execution to retirement. Lesson 2 discusses how to gather the information you might need at the commencement of such a process.

### Exam objectives in this chapter:

This chapter provides a high-level overview of the Windows 7 workstation life cycle and describes how to gather the information you need to deploy and support Windows 7 in an enterprise environment. You might therefore say that Chapter 1 covers all of the 70-686 exam objectives in general and none of them in particular.

### Lessons in this chapter:

- Lesson 1: Understanding the Windows 7 Deployment Life Cycle **3**
- Lesson 2: Gathering Upgrade Information **23**

## Before You Begin

Although this training kit is dedicated largely to the process of deploying Windows 7, most of the tools involved in the deployment process can run on other operating systems as well. To install and run Microsoft Assessment And Planning (MAP) Toolkit 5.0, described in this chapter, you must have the following:

- A computer running Windows 7, Windows Vista, Windows XP SP2, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 R2, with all available updates installed.
- Microsoft .NET Framework 3.5 SP1.
- Microsoft Office Word 2007 or Word 2003 SP2.
- Microsoft Office Excel 2007 or Excel 2003 SP2.
- Microsoft Office PowerPoint 2007.
- Microsoft Office Primary Interop Assemblies for Word and Excel.



### REAL WORLD

Craig Zacker

**M**ass deployments of new operating systems or applications often have repercussions that haunt you long after all of the immediate technical problems are resolved. IT people are naturally inclined to dwell on the technical aspects of the deployment process; they might have to work hard to provide adequate consideration for its other aspects, such as approval by nontechnical managers, end-user training, and budgetary issues.

A company I once worked for decided to replace its existing e-mail client with a comprehensive groupware platform that, our new IT director insisted, would revolutionize the company's workflow and increase productivity across the board. The planning for the deployment, spearheaded by the director, was rushed, but the project proceeded on time and on budget. On the appointed morning, an army of IT staffers, with temporary reinforcements, flooded into the office, displacing users from their computers so that they could install the new application.

Unfortunately, the application deployment plan had omitted the real object of the exercise: to give the application's users a better work tool. With no training, no documentation, and virtually no help, everyone in the company had to muddle their way through learning to use a new e-mail client that was utterly different from any they had used before. Rather than increase productivity, the deployment slowed the work of many users for weeks. Before any palpable improvement was realized, the company had to pay for a series of expensive visits from several per diem consultants.

The project needed a much longer planning phase and a much wider base of advisors and contributors, including end-users and their supervisors. Additional time spent planning is rarely wasted and should include input from all concerned parties.

# Lesson 1: Understanding the Windows 7 Deployment Life Cycle

The bulk of this training kit is devoted to the process by which Windows 7 desktop administrators design a workstation deployment on an enterprise network. Subsequent chapters in this book discuss the processes by which administrators design and create image files, decide on a baseline client configuration, package applications, and select a deployment strategy. The primary tool for designing and implementing mass Windows 7 deployments is Microsoft Deployment Toolkit 2010. However, depending on the size and complexity of the network, the processes listed here can be but a small part of the overall deployment process.

**After this lesson, you will be able to:**

- Understand the phases involved in a large scale deployment of Windows 7 workstations.
- Review the life cycle of a Windows 7 workstation.

**Estimated lesson time: 90 minutes**

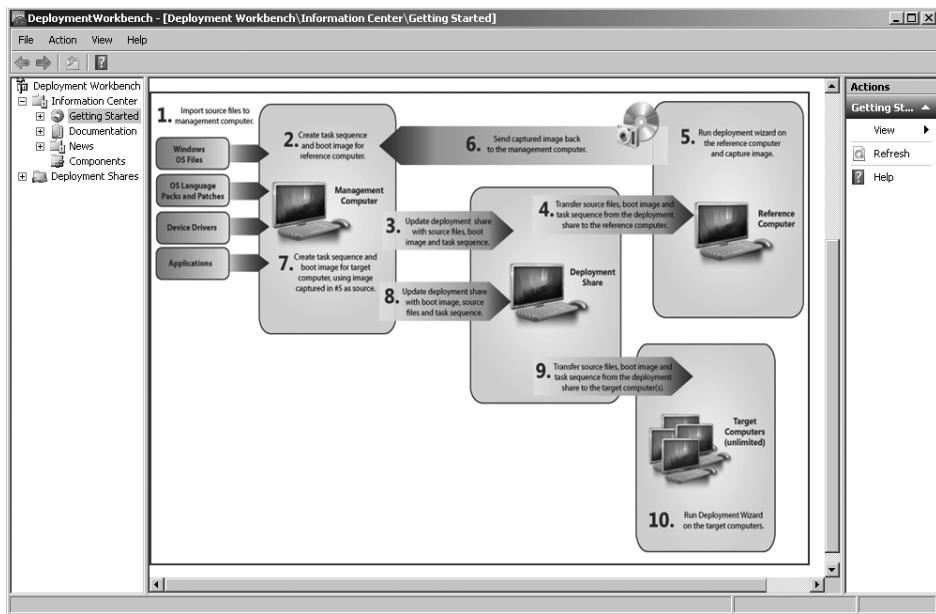
## Scaling the Deployment Process

How many people do we need for the image team? Should they be centrally located or distributed around the world? Who is going to evaluate the client roles required for each branch office? Where should we create and update the image files? These are just a few of the hundreds of questions that go beyond the scope of the imaging process as described in this training kit. What's more, in a large enterprise deployment, administrators must discuss, codify, and document the answers to these questions, not just handle them informally as the project proceeds, as is often possible in a smaller enterprise.

Image design and creation is just one part of a lengthy and complicated workstation deployment process. Windows 7 desktop administrators involved in a large-scale deployment must understand that they are part of a much larger and farther-reaching process than they might imagine. The deployment process begins long before they design and create their first image file and ends long after they complete the final workstation installations.

## Viewing the Highest Level

The tools and documentation included in Microsoft Deployment Toolkit (MDT) 2010 cover the basic tasks of the Windows 7 workstation deployment process. Deployment Workbench, the primary MDT 2010 tool, is shown in Figure 1-1. The deployment process includes such hands-on tasks as building a reference computer, capturing image files from it, and deploying those image files to the target workstations on the network. However, these tasks are just a subset of the entire enterprise deployment process.



**FIGURE 1-1** The Deployment Workbench tool from Microsoft Deployment Toolkit 2010

When Windows 7 desktop administrators take part in a large-scale workstation deployment, they are often required to devote themselves primarily to the technical details of the project, or possibly the details of one small part of the project. For this reason, they often lose sight of the big picture—the high-level conception, planning, and supervision that make a large IT project possible.

In previous MDT versions, including MDT 2008, the documentation supplied with the package included a “Planning Guide,” a series of job aids, and other documents that defined the place of the MDT deployment process within the bigger picture of an IT service life cycle. However, beginning with MDT 2008 Update 1, Microsoft removed this high-level documentation from the MDT package, in an effort to streamline what was already a document-heavy product.

This was a reasonable decision because the inclusion of the “Planning Guide” and other documents implied that every MDT deployment required a massive organizational effort, which is simply not the case. Therefore, instead of including this documentation in MDT 2010, Microsoft refers administrators to the original source for this high-level information: the Microsoft Operations Framework (MOF), the current version of which is MOF 4.0.

#### **MORE INFO COMPARING MOF VERSIONS**

For those familiar with the “Planning Guide” and other MOF-derived documents provided in MDT 2008, be aware that these documents are based on Microsoft Operations Framework 3.0. Compared to MOF 3.0, version 4.0 expands the scope of its guidance beyond operations to cover the entire IT service life cycle.

There are also substantial changes in the organization and nomenclature of the framework. For example, MOF 3.0 divides the IT service life cycle into four units that it calls quadrants, while MOF 4.0 defines three elements, known as phases. The “Microsoft Operations Framework Foundations” document (version 2.5, included as part of the MOF 4.0 IT Pro Quick Start Kit) includes a detailed discussion of the differences between MOF 3.0 and MOF 4.0, as well as a table that maps the 3.0 elements onto their 4.0 counterparts.

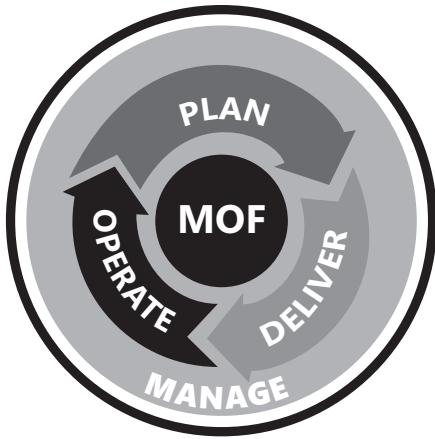
Microsoft also documents the MDT deployment process using the Microsoft Solutions Framework (MSF), a set of documents designed to guide the software development process, but which are also applicable to other IT projects, such as large-scale workstation deployments.

#### **MORE INFO DOWNLOADING MOF 4.0**

The core Microsoft Operations Framework 4.0 package, plus a number of updates and ancillary documents, is available free of charge from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyId=457ED61D-27B8-49D1-BACA-B175E8F54C0C&displaylang=en>.

## **Introducing the MOF**

The goal of MOF 4.0 is to define the entire life cycle of an IT service, beginning from the initial recognition of a need, proceeding through the planning, building, and deployment processes, and culminating in operation and finally retirement. The basic structure of the life cycle, as illustrated in Figure 1-2, consists of three distinct phases: Plan, Deliver, and Operate, all of which are figuratively surrounded by—and answerable to—a Manage layer.



**FIGURE 1-2** The phases of the MOF life cycle

The three phases are defined as follows:

- **Plan** The Plan phase refers not to specific IT service deployment plans but to a generalized understanding between the IT department and the business management elements of the organization. The object is for these two elements to reach an understanding about how IT services will support the business, how the reliability of IT services will be managed, ensured, and supervised, and what financial structure will support the organization's IT strategy.
- **Deliver** The Deliver phase encompasses the actual conception, planning, implementation, testing, and deployment of IT services. The MDT 2010 deployment process occurs primarily in the Deliver phase.
- **Operate** The Operate phase defines the procedures that ensure the stable operation, maintenance, and support of the deployed IT services. This phase also includes the eventual retirement of IT services at the end of their life cycles.

## Using Service Management Functions

These phases are described in a series of white papers called service management functions (SMFs), each of which defines processes and activities for a specific aspect of each phase, as well as the roles of the people who perform them. Table 1-1 lays out the SMFs for the Plan phase.

**TABLE 1-1** Service Management Functions for the MOF Plan Phase

SMF	PURPOSE
Business/IT Alignment	To recognize the needs of the organization and define a portfolio of IT services that address those needs
Reliability	To establish performance standards for IT services that meet the organization's requirements for service availability, continuity, capacity, and data integrity

SMF	PURPOSE
Policy	To define a set of policies for IT services that meet the organization's requirements in matters of security, privacy, and appropriate use
Financial Management	To estimate, optimize, and account for the costs involved in delivering IT services throughout their life cycles

Table 1-2 describes the SMFs for the Deliver phase.

**TABLE 1-2** Service Management Functions for the MOF Deliver Phase

SMF	PURPOSE
Envision	To conceptualize a solution to a particular need of the organization in the form of an IT service and define the scope and potential risks involved in implementing the project
Project Planning	To create a project plan that specifies the design and features of an IT service that addresses the stated needs of the organization and is agreeable to all stakeholders involved in the project
Build	To implement an actual solution that meets the specifications defined in the project plan and the expectations and requirements of all the stakeholders involved in the project
Stabilize	To fully test the solution, using laboratory or pilot deployments, and resolve any issues exposed by this testing so as to create a high-quality solution that fully meets the specifications defined in the project plan
Deploy	To implement the solution in a production environment in a manner that fully meets the expectations of all stakeholders in the project, as well as to smoothly transfer responsibility for the service from the project team to the operations and support personnel

#### **MORE INFO MOF AND THE MICROSOFT SOLUTIONS FRAMEWORK**

The SMFs of the Deliver phase, as well as the Operations SMF from the Operate phase, are largely derived from the Microsoft Solutions Framework (MSF) process model. MSF is a collection of documents that are primarily intended to govern database and application development projects but are adaptable to other large scale IT projects as well, such as workstation deployments. Unlike MOF, the MSF documents do not attempt to cover the entire life cycle of an IT service, just the tasks involved in envisioning, planning, developing, stabilizing, and deploying the application or service. For more information on MSF and to download the component documents, see <http://www.microsoft.com/downloads/details.aspx?familyid=A71AC896-1D28-45A4-880C-8B0CC8265C63&displaylang=en>.

Table 1-3 describes the SMFs for the Operate phase.

**TABLE 1-3** Service Management Functions for the MOF Operate Phase

SMF	PURPOSE
Operations	To define the procedures needed to operate IT services while minimizing down time and maximizing efficiency
Service Monitoring and Control	To observe the ongoing health of IT services, anticipate potential problems, and take proactive steps to minimize the impact of those problems should they occur
Customer Service	To provide efficient and positive assistance to users of IT services, and address all complaints and other issues raised by those users
Problem Management	To predict potential problems and devise problem resolution procedures that generate workarounds and permanent solutions

The SMFs in Table 1-2 represent a sequence of procedures for a project in the Deliver phase. In the Plan and Operate phases, however, the processes defined in the various SMFs can in many cases occur simultaneously.

The Manage layer, which applies equally to all of the MOF life cycle phases, is designed to create a decision making, risk management, and change management infrastructure that is consistent throughout the life cycle of an IT service. The Manage layer too has its own SMFs, as listed in Table 1-4.

**TABLE 1-4** Service Management Functions for the MOF Manage Layer

SMF	PURPOSE
Governance, Risk, and Compliance	To establish policies that delegate authority, accountability, and responsibility for the outcome of IT projects, assess the likelihood and possible impacts of actions taken or not taken, and ensure that everyone involved in a project is aware of and adheres to the policies and regulations resulting from senior management decisions
Change and Configuration	To manage project and service changes in a predictable and repeatable manner, while minimizing the risks inherent in those changes
Team	To define the roles of all team members involved in an IT service life cycle, including their responsibilities and accountabilities, and assign those roles to specific individuals

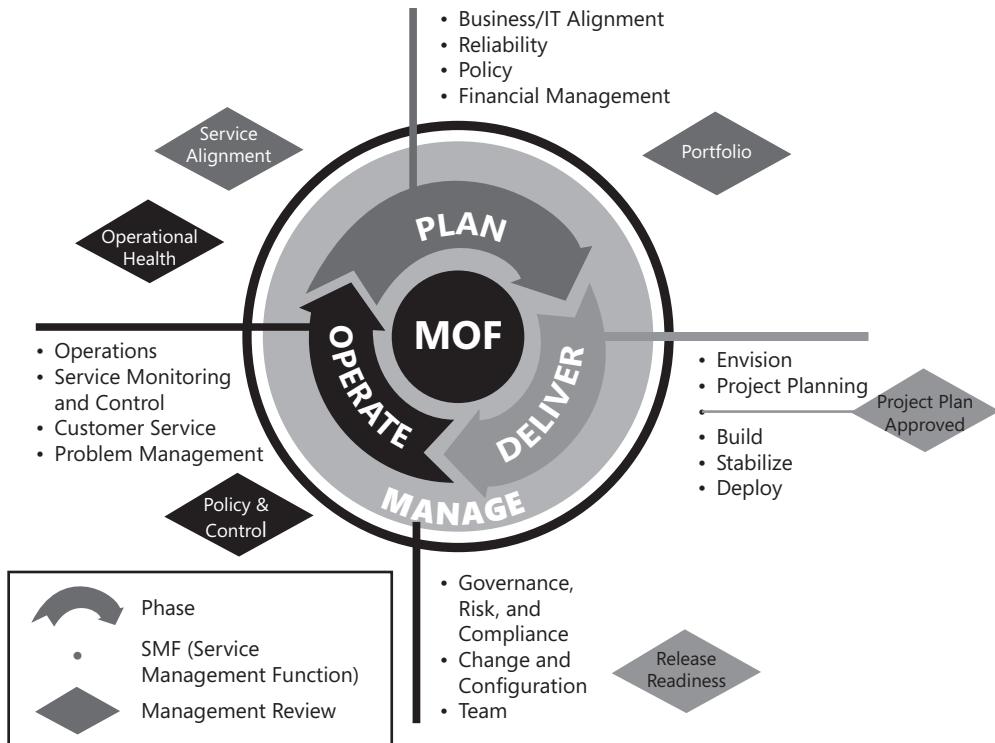
## Management Reviews

Finally, the MOF life cycle model includes milestones in the form of periodic management reviews that evaluate the current state of the project and signal its readiness to move forward. These management reviews, and the phases with which they are associated, are listed in Table 1-5.

**TABLE 1-5** Management Reviews in the MOF Life Cycle

MANAGEMENT REVIEW	PHASE	PURPOSE
Service Alignment	Plan	To evaluate a recognized need as having the potential to become a new project and, if it is approved, initiate the process of gathering information from management and stakeholders
Portfolio	Plan	To evaluate the proposal for a new project and, if it is approved, form a team, draft an initial project charter, and signal the Deliver phase to commence
Project Plan Approved	Deliver	To evaluate a completed project plan and, if it is approved, signal the commencement of the Build stage
Release Readiness	Deliver	To evaluate the results of the Stabilize process, confirm the satisfactory completion of all laboratory testing and pilot deployments, verify that the team has addressed all issues arising during those processes, and signal the readiness for the Deploy process to begin
Operational Health	Operate	To evaluate the current health of projects in the Operate phase and, if necessary, modify the procedures established during that phase
Policy and Control	Manage	To evaluate the current state of a service relative to the policies established during the Governance, Risk, and Compliance process and, if necessary, initiate changes to the compliance mechanisms currently in place or to the policies themselves

The phases of the MOF life cycle, along with their component SMFs and management reviews, are shown in Figure 1-3.



**FIGURE 1-3** The phases of the MOF life cycle, with SMFs and management reviews

## Placing an MDT Deployment in the MOF Life Cycle

The following scenario portrays the entire life cycle of a Windows 7 workstation deployment in terms of the SMFs in the Microsoft Operations Framework, from the realization of a need through deployment, and all the way to the ultimate retirement of the computers, sometime in the future. An organization undertaking a large-scale Windows 7 workstation deployment often has company-wide and IT-specific management policies already in place. This scenario at times assumes the existence of these policies.

### **NOTE UNDERSTAND THE SMF SEQUENCE**

As mentioned earlier, the Manage layer of the MOF life cycle applies equally to the Plan, Deliver, and Operate phases, and its SMFs can appear (and reappear) almost anywhere in the life cycle. In much the same way, the management reviews occur at various times during the three phases.

## Realizing the Need

A. Datum Corporation is opening a new Genetic Research division, for which they have leased an entire new office building. The new division must be operational by July 1 of the next year. The process of outfitting the new division with everything they need is a huge undertaking, involving virtually every one of the company's existing departments. The IT division is responsible for satisfying the highly specific and specialized computing requirements of the new personnel, one specification of which is the deployment of new workstations.

## Management Review: Service Alignment

Largely a formality in this case, because the formation of the new division is already approved and the new personnel must have computers and other equipment, the company management officially recognizes the need for a workstation deployment, along with a variety of other IT projects related to the rollout of the new division. The process of gathering the information needed to begin the project from stakeholders, managers, and other personnel can begin.

## The Plan Phase

The SMFs in the Plan phase, shown in Figure 1-4, encompass all of the currently operative IT services and are therefore already in use. The following sections describe how the meetings and practices generated by those SMFs apply to the workstation deployment.

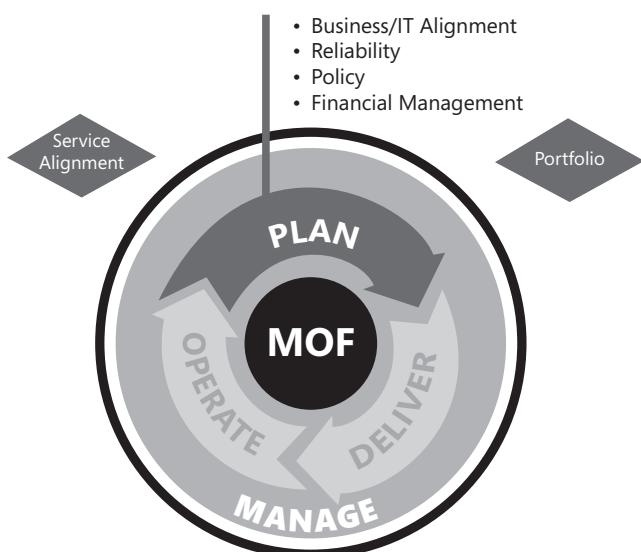


FIGURE 1-4 The Plan phase of the MOF life cycle

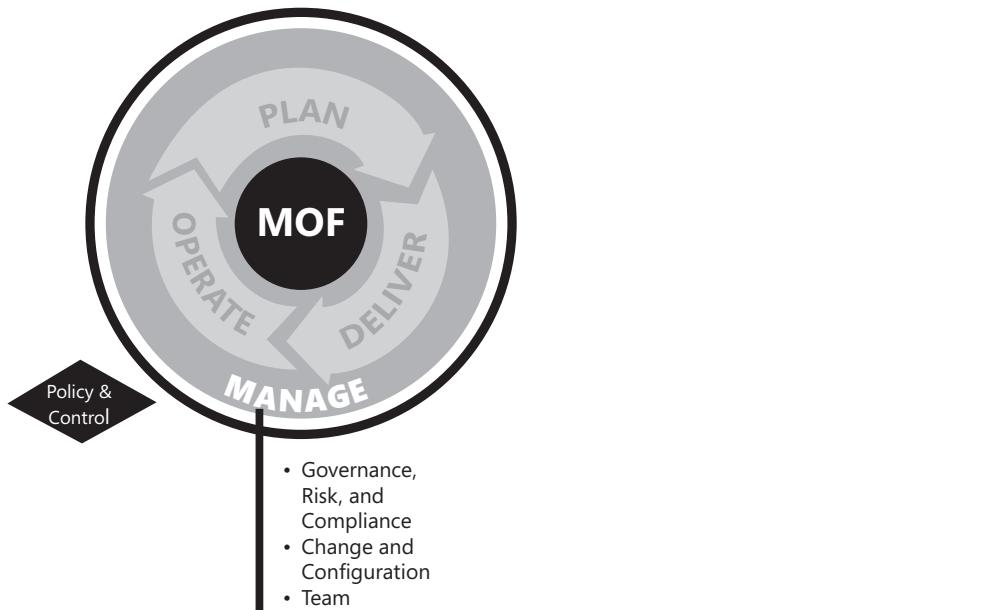
## GOVERNANCE-RISK-COMPLIANCE

The vice president responsible for the creation of the new division meets with the new director of Genetic Research and the IT director, to discuss the extension of existing company governance, risk, and compliance (GRC) policies to encompass the new division and the upcoming IT projects needed to support that division. Eventually, as the directors fill positions and form teams in their divisions, additional managers and supervisors attend the GRC meetings as well.

During these meetings, the vice president and the directors do the following:

- Establish a chain of command and define the responsibilities and accountabilities of all personnel in supervisory positions, whether permanently or for the life of a specific project.
- Discuss the possible consequences of failure to adhere to the policies and requirements defined by management, both in terms of project failures and personal culpability, as well as methods for minimizing the risk of such failures.
- Impress upon all supervisory personnel the need for compliance with established policies throughout the enterprise.

GRC meetings, which actually constitute part of the Manage level, as shown in Figure 1-5, continue at regular intervals throughout the life of the project.



**FIGURE 1-5** The Manage level of the MOF life cycle

## POLICY

The company already has policies in place that govern the nondisclosure of company information, the privacy of employees' personal information, and appropriate use of company computing facilities. However, the Genetic Research division will do classified work for government agencies, which increases both the need for high security and the consequences of noncompliance.

The vice president meets with the director of security and a government security consultant to discuss the specialized policies that they need to prevent secret information from leaking, both within and outside the company. In later meetings, the IT director is involved to discuss the technical feasibility of some of the requirements. Among many other considerations, the conferees decide that the new workstations must all have encrypted local storage and biometric authentication capability.

These meetings produce a new policy addendum for the Genetic Research division and a list of technical security requirements for the IT rollout, including the encryption and authentication mechanisms for the new workstations.

## RELIABILITY

The IT division already has policies and technologies in place to ensure high availability of data and services, so the IT director meets with the Genetic Research director and a government consultant to discuss whether the existing measures are sufficient for the new division. They all approve the existing high availability technologies; the conferees agree to use the same reliability plan as the rest of the enterprise.

## BUSINESS/IT ALIGNMENT

The directors of Genetic Research and IT, along with various managers and representatives from both divisions, meet to discuss, among other things, the workstation requirements for the new division. The Genetic Research scientists will use many specialized software products and also require computers that can work with microscopes and other scientific hardware devices. The result is a service map that defines both the workstation requirements already established by the company managers for existing users and the new division's various types of users. The service map for the workstation deployment consists of the following sections:

- **Customers** Lists the categories of users who require workstations
- **Hardware** Lists the basic hardware requirements for the workstations
- **Applications** Lists the types of applications that will run on the workstations
- **Settings** Lists specialized configuration settings that the workstations will need
- **Services** List the internal and external services that the workstation will access

These are highly general specifications, intended to provide only the most basic estimation of the requirements.

## CHANGE AND CONFIGURATION

The service map for the Genetic Research workstations is substantially different from that for the typical A. Datum user workstation. For this reason, the documents that the IT director submits to the financial and management teams include a Request For Change (RFC), which lists the reasons why these workstations differ from the company standard and why they cost more.

## FINANCIAL MANAGEMENT

IT people meet with the financial team and, using a previous workstation deployment as a guide, create a budget model that reflects cost changes since the earlier project and the special requirements of the Genetic Research division users.

## MANAGEMENT REVIEW: PORTFOLIO

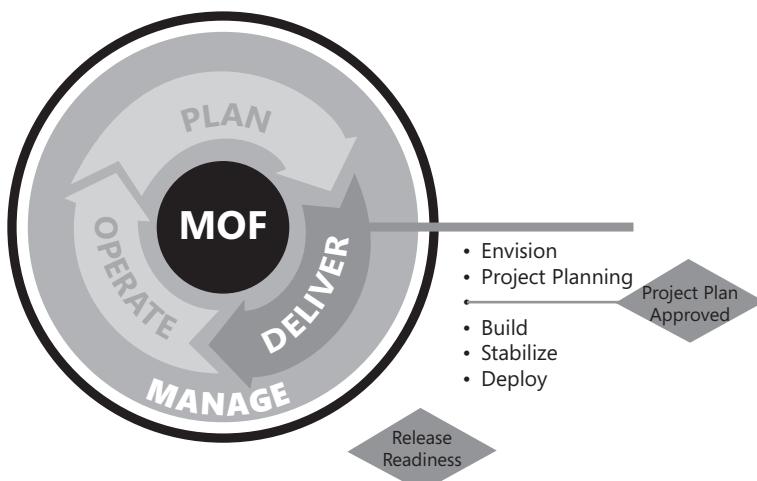
The IT director assembles the various documents defining the criteria for the workstation deployment and into a project proposal. The management team decides that the proposed project meets the company's business and financial requirements, as well as those of the prospective customers—the Genetic Research division—and approves the proposal, allowing the project to proceed to the Deliver phase.

## TEAM

The IT director, in cooperation with the rest of the management team and the Genetic Research director, creates a roster for the team that will manage the workstation deployment project. The roster defines the duties and responsibilities of the various team members. The managers then select individuals to fill the roles and hand the workstation deployment project off to the new team.

## The Deliver Phase

After the project enters the Deliver phase, as shown in Figure 1-6, the tasks defined in the SMFs correspond to the basic stages of the deployment process, as defined in MDT 2010.



**FIGURE 1-6** The Deliver phase of the MOF life cycle

## **ENVISIONING THE GOALS**

The process of envisioning the goals of the workstation deployment project actually began during the Plan phase, with the stipulations documented during the Policy, Reliability, and Business/IT Alignment meetings. However, these stipulations were basic premises: high-level observations that enabled the management team to create a project proposal. The Envision SMF calls for a more detailed analysis of the business requirements that the new workstations for the Genetic Research division must satisfy.

For this particular workstation deployment project, the envisioning process produces a list of user types in the new division and an inventory of the tasks that users of each type are required to perform using their workstations. With this information, the IT personnel on the project team can begin to determine the exact hardware and software requirements for each workstation. This information goes into a vision/scope document that defines in detail the overall goals of the project.

During the envisioning process, the project management team begins defining the roles for the project delivery team—the individuals who will be responsible for planning, building, testing, and deploying the new workstations. Each of these tasks of the Deliver phase requires its own team; each of these is a subgroup of the overall project delivery team. Although it is not necessary to name all members of the team at this point, the project managers install the core team members. These include the individuals who will lead each of the subgroups and other people who begin to work immediately on the planning process and the construction of the test laboratory.

## **PROJECT PLANNING**

With the vision/scope document in hand, the project delivery team can begin to plot the entire deployment process in detail. Their goals are to decide what to build, how to build it, and who will build it.

As part of their process, the team performs the following tasks:

- Evaluate hardware and software products and technologies
- Create a functional specification for the new workstations
- Define the individual processes involved in the remaining stages of the Deliver phase
- Designate subordinate groups to create individual process plans
- Create a master schedule for the remaining stages of the Deliver phase
- Combine the individual process plans into a master project plan for management review

For this deployment, many of the requirements established during the Plan phase and the Envision process are highly specific. The users in the Genetic Research division require specialized hardware and software tools, and building their workstations is primarily a matter of creating an efficient and workable environment for those tools. The product evaluation process consists largely of evaluating the system requirements for the tools that various types of users require and outfitting the workstations with appropriate components to accommodate them.

For the functional specification, the team evaluates the business requirements established during the Plan phase, as well as the requirements of the various types of users they must support. With this information, they design three separate workstation hardware/software configurations. For each configuration, the functional specification provides a complete and detailed description of the workstation's hardware, software, and configuration settings. This functional specification is the key document that guides the rest of the Deliver phase; it tells the Build team what to build, the Stabilize team what to test, and the Deploy team what to deploy.

#### **IMPORTANT FUNCTIONAL SPECIFICATIONS AND VERSION CONTROL**

After all of the stakeholders in the project approve the functional specification, the management accepts the document and places it under version control. The functional specification will probably require changes before the deployment is complete, but the version control mechanism tracks all of the changes made to the document and requires stakeholder approval before it allows anyone to make changes.

With the functional specification completed, the managers of the planning team assign teams to create detailed plans for the following elements of the Deliver phase:

- **Imaging** This plan specifies how many images the team will create, how they will create them, and how the operations team will manage them in the future.
- **Applications** This plan indicates the applications that the workstations will run and how to deploy them.
- **Configuration** This plan specifies the configuration settings that the team will deploy on the workstations, both for the operating system and for applications.
- **Testing** This plan sets a testing regimen for the workstations, which includes building a laboratory and executing pilot deployments.
- **Deployment** This plan describes how the team will deploy the images to the workstations and ready them for use.

After the planning subgroups complete their individual plans, the project delivery team assembles them into a single master plan and draws up a master schedule that accounts for all of the remaining tasks in the Deliver phase.

#### **MANAGEMENT REVIEW: PROJECT PLAN APPROVED**

The project delivery team submits the functional specification, the master plan, and the master schedule to the management team for review. After the management team approves these documents, the Build stage of the Deliver phase can begin.

#### **BUILD**

In the Build stage, the various delivery teams use all of the planning completed this far to realize a physical product and prepare it for final deployment. The IT management places the order for the new workstation computers immediately after the approval of the project plan.

The vendor is able to supply the computers with the exact hardware listed in the functional specification, so the build teams are responsible only for installing and configuring the operating system and the applications on each computer.

During the Build process, the teams created during the Project Planning stage might work together or separately. For example, the configuration and applications teams initially work together to create a viable workstation environment, according to the requirements stated in the master plan. This process must be near to completion before the imaging team can start creating and working with the actual images they eventually deploy. However, the imaging team members are also busy evaluating and selecting the tools they will use to create the images during the deployment, as well as the tools that the support personnel will use to maintain the workstations during the Operate phase of the life cycle.

Meanwhile, the testing team is preparing the laboratory environment that is required for the Stabilize phase. In a workstation deployment such as this, the lab computers also function as the reference computers for the creation of the actual deployment images, so the lab must duplicate the production workstation environment precisely. The testing team is also busy planning two pilot deployments, which involves the selection of appropriate users and the development of reporting and documentation procedures.

Documentation is a major concern throughout the Build stage, as it will be during the Stabilize and Deploy stages. To adequately support the workstations later, during the Operate phase, a complete documentation of the build process is required, as is a full record of the three final workstation configurations.

## STABILIZE

The Build stage culminates in the creation of images that are nearly ready for deployment on the workstations, and the design of the process the team will use for the actual production deployment. But a team must first test both of these elements, in the lab and then in a pilot deployment. The testing team begins designing and constructing the laboratory during Project Planning stage, to be sure they have the necessary infrastructure to develop and create the workstation image files and to duplicate as closely as possible the actual working environment of the new workstations.

The IT division sets up a workroom that is equipped with the same network infrastructure used throughout the company, including its own servers, which they can isolate from the rest of the network for testing purposes. The testing team installs several of the new workstations intended for the Genetic Research division in this room. Because of the special requirements documented in the plan, the testers also take delivery of some of the scanning and microscopy equipment that the new users require. To help install, configure, and test the scientific equipment, the manufacturers have sent two technicians to A. Datum; the suppliers' technicians will function as adjuncts to the testing team.

The Build and the Stabilize stages of the Deliver phase are not sequential; many of their activities occur simultaneously, and it often seems that the two teams are actually functioning as one. As the builders generate interim versions of their image files, the testers deploy them in the lab and begin documenting issues for consideration in future builds.

After the two teams have generated images that are feature complete, the testing team performs pilot deployments to evaluate them further. Because the actual Genetic Research division is not operational yet, standard pilot deployments in the live environment are not possible. Therefore, the team plans two pilot deployments that they hope will simulate the live environment as closely as possible. The first uses a selected group of users in other divisions, and concentrates on testing general business requirements, such as security mechanisms. The second pilot deployment uses a group of Genetic Research division new hires, who the company is bringing in before the division launch especially for this testing. This pilot concentrates on the specialized scientific applications and hardware that require experienced users.

Both pilot deployments emulate real-world use in an attempt to expose any flaws in the plan or its implementation. The building and testing teams work together to assess, triage, and debug any problems that arise. During this stage, it might be necessary to revise the functional specification, the master plan, or the master schedule. If this is the case, all of the project's stakeholders must approve these revisions before they are adopted.

#### **MANAGEMENT REVIEW: RELEASE READINESS**

At the conclusion of the Stabilize process, the management team reviews all of the documentation generated during the testing and debugging processes. When team members conclude that the workstation environments are stable and meet all of the requirements set down in the master plan, they sign off on the build, signaling that the Deploy stage can begin.

#### **DEPLOY**

The deployment process has been carefully plotted during the Project Planning stage, and it has been tested during the Stabilize stage. Now, the live production deployment can begin with the installation of the workstations and other required hardware in the new site for the Genetic Research division. Other IT teams have already completed their own projects, to provide the division with the network infrastructure and other resources it will need to operate.

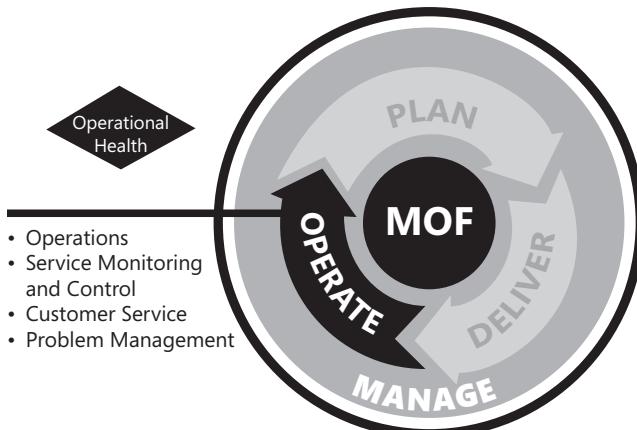
A hardware installation team first unpacks and assembles the new computers on site, testing them for basic functionality. The hardware order included spares, so the team can immediately swap out any computers that are nonfunctional on arrival.

With the hardware in place, the deployment team can begin the process of installing the completed image files on the workstations. Although the Stabilize process is formally ended, testing continues during the deployment because there are always variables that cannot be duplicated in the lab. Most of the issues that arise during the deployment likely concern the specialized scientific equipment, and it is prudent for the manufacturers to send technicians to the site. To take advantage of the technicians' presence, several of the operations team members participate in the sessions as well because they will likely have to service the equipment later.

The Deploy stage concludes with the installation of all of the planned workstations, fulfillment of all planned requirements, and the satisfaction of all stakeholders involved, including management, IT, and end users. The life cycle now proceeds from the Deliver phase to the Operate phase, with responsibility for the workstations passing to the operations teams.

## The Operate Phase

The completion of the workstation deployments signals the beginning of the life cycle's Operate phase, as shown in Figure 1-7. The Operate phase is the culmination of the two phases that preceded it. The Plan phase was concerned with what workstations to build, and the Deliver phase with the process of building them. The Operate phase is all about keeping the workstations running smoothly after they are built.



**FIGURE 1-7** The Operate phase of the MOF life cycle

Responsibility for the workstations now passes to the operate teams, many members of which are individuals who participated in the Deploy phase. The SMFs for the Operate phase all occur concurrently, with each one defining tasks and services that the workstations will use at various times throughout their operational lives.

### OPERATIONS

The initial part of the Operations stage is devoted to acceptance testing, the process by which the Operate team evaluates the work of the Deliver team and declares the workstations ready to pass into their care. This process is largely a formality, because many of the IT workers are members of both teams, and the two teams have already been working together in any case.

The remainder of the Operations stage is devoted to defining the regular maintenance tasks that will keep the workstations running smoothly. In many respects, the maintenance for the Genetic Research workstations is no different from that for the other computers at A. Datum, and the team was able to use the existing operational work instructions with only a few modifications.

These instructions describe the periodic maintenance tasks for the workstations, such as backups, drive defragmentations, and software updates, as well as contingency plans for unforeseen events, such as virus infections, drive failures, and other disasters.

The management team has decided that the specialized scientific equipment falls outside the purview of the IT operations team. The IT team will service issues related to the equipment interface, but the Genetic Research division will provide its own support for the devices themselves, and deal with the manufacturers directly, when necessary.

## **SERVICE MONITORING AND CONTROL**

Service Monitoring and Control covers the process by which the IT division tracks the ongoing performance of the Genetic Research workstations and takes action when conditions warrant it. The IT staff already has performance monitoring, security auditing, and antivirus policies in place for the existing network, and they extend these policies to include the Genetic Research division as well.

Because of the classified work the new division will be performing, however, these policies will require some modifications, and the management team establishes a new operational security team specifically for this purpose. This team is responsible for extending these policies as needed and seeing to it that the government security requirements for the Genetic Research division's work—which change frequently—are always met.

## **MANAGEMENT REVIEW: POLICY AND CONTROL**

Beginning several months after the launch of the Genetic Research division, and each quarter thereafter, the management team meets to evaluate how well the workstations are complying with the policies and requirements defined during the Plan phase. Toward this end, the IT director provides the conferees with performance summaries, auditing reports, and a list of policy violations that have occurred. The vice president of Genetic Research supplies a list of changes to the government security requirements that are due to go into effect during the next quarter.

None of the policy violations that occurred were severe, and none of the other records point to any major policy compliance problems. The IT directory takes receipt of the new security requirements and calls a meeting of the policy team to discuss modifications to the Genetic Research workstation configurations.

## **CUSTOMER SERVICE**

In this project, the “customers” are the users of the workstations in the Genetic Research division. The Customer Service process defines the interface between these users and the IT division, which is the standard help desk provided to all of A. Datum’s computer users. The process by which the help desk personnel work with the Genetic Research users will be largely the same as for the other users in the company. The operations team updates the help desk technical support database with the functional specification for the Genetic Research workstations, as well as documentation for the specialized hardware and applications they use and the troubleshooting records generated during the Stabilize phase.

## **PROBLEM MANAGEMENT**

The Problem Management service deals with issues that are beyond the scope of the help desk resources defined in the Customer Service process. These are typically problems that go beyond user error and transient service outages, reflecting instead incidents that cause a significant reduction or interruption of workstation performance.

Although the MOF classifies Problem Management as part of the Operation phase, the skills and procedures it requires are equally applicable to the Plan and Deliver phases. In fact, at A. Datum, most of the same individuals who handled complex problems during the earlier phases are now doing so as part of the Operate team. When the help desk personnel escalate an issue, the problem management team becomes responsible for performing an independent investigation, researching the problem, and developing a workaround or a resolution—whether proactive or reactive.

As with all other stages in the life cycle, documentation is a key part of the problem management process, so that in the future, others can benefit from the team's experiences.

#### **MANAGEMENT REVIEW: OPERATIONAL HEALTH**

Every quarter, the IT director holds an operational health review with the IT division managers and the heads of the company's other divisions. The purpose of the meeting is to assess customer satisfaction with all of the services the IT division provides. It is this meeting that decides when a change to an IT service is needed, such as an upgrade to an application, modified configuration settings, or a hardware replacement.

Three years after the launch of the Genetic Research division, the director of that division expresses the dissatisfaction of her users with the performance of their workstations. Several of their applications have been upgraded several times, and their system requirements have increased. Discussion then begins regarding the possibility of retiring the existing workstations and replacing them with new, upgraded models, thus signaling the imminent end of one IT service life cycle and the beginning of another.

#### **PRACTICE    Leading a Workstation Build Team**

---

In this practice, you take on a supervisory role in one stage of a workstation deployment project and use SMFs from Microsoft Operations Framework 4.0 to assemble your team and plan your course of action.

#### **EXERCISE 1   Assembling a Stabilization Team**

Wingtip Toys is expanding their sales operation and plans to open a new call center, which requires 100 new Windows 7 workstations. At the latest deployment project planning session, the IT director placed you in charge of the stabilization team responsible for testing the new workstations prior to their deployment on the production network. To help you organize and lead the workstation stabilization effort, the IT director suggests that you read the Stabilize SMF from Microsoft Operations Framework 4.0. This document is available online at <http://technet.microsoft.com/en-us/library/cc543320.aspx>.

The call center users have a limited set of tasks that they are required to perform, so their workstations are relatively simple. All of their database entry screens are exposed through Microsoft Internet Explorer, and the users do not require Microsoft Office or any other outside applications. To keep the users focused, the functional specification for the workstations calls for a limited interface, locking the users out of the Windows 7 features they do not need.

As the leader of the stabilization team, you function as Solution Manager and Program Manager, responsible for designing, scheduling, and overseeing the entire workstation testing process. The IT director is allowing you to recruit six additional persons for your team, who can come from the IT division or any other department in the company.

To complete this exercise, create a roster of your proposed team members by using the Stabilize SMF for guidance. Your roster should specify the departments your team members come from, the skills they need, their roles, and their responsibilities during the stabilization effort.

### **EXERCISE 2 Planning the Stabilization Process**

The stabilization effort begins as soon as the build team delivers their first feature-complete workstation configuration. To complete this exercise, create a high-level outline listing the basic steps of your proposed testing process and the team members involved in each step, beginning with your team's receipt of the initial workstation build and culminating in the release readiness management review. The stabilization process should include both lab testing and at least one pilot deployment, as described in the Stabilize SMF.

## **Lesson Summary**

- The goal of Microsoft Operations Framework 4.0 is to define the entire life cycle of an IT service, beginning from the initial recognition of a need, proceeding through the planning, building, and deployment processes, and culminating in operation and finally retirement.
- MOF 4.0 divides the life cycle of an IT service into three phases: Plan, Deliver, and Operate, all of which are surrounded by a Manage level.
- The MOF 4.0 phases consist of a series of white papers called service management functions (SMFs), each of which defines processes and activities for a specific aspect of each phase, and the roles of the people who perform them.
- The MOF 4.0 life cycle model includes milestones in the form of periodic management reviews that evaluate the current state of the project and signal its readiness to move forward.

## **Lesson Review**

You can use the following questions to test your knowledge of the information in Lesson 1, "Understanding the Windows 7 Deployment Life Cycle." The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE ANSWERS**

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

1. Which of the phases in the MOF 4.0 life cycle contains stages that run sequentially, and not concurrently?

  - A. The Plan phase
  - B. The Deliver phase
  - C. The Operate phase
  - D. The Manage Level
2. Which of the following SMFs is concerned primarily with security, privacy, and appropriate use?

  - A. Governance, Risk, and Compliance
  - B. Business/IT Alignment
  - C. Policy
  - D. Change and Configuration
3. The majority of the tasks involved in a Microsoft Deployment Toolkit 2010 deployment project occur during which phase of the MOF 4.0 life cycle?

  - A. The Plan phase
  - B. The Deliver phase
  - C. The Operate phase
  - D. The Manage level

## Lesson 2: Gathering Upgrade Information

---

Deploying Windows 7 on a fleet of brand new workstations is a complex undertaking, to be sure, but the process is complicated further when you are deploying Windows 7 on an existing group of hundreds or even thousands of workstations in an enterprise network environment. Before you can even begin to plan the deployment project, you must gather information about the existing computers so that you can determine what preliminary steps are necessary before they can run Windows 7.

For such a project to be worth the investment, the benefits of the new operating system must exceed—or at least balance—the outlay. Before even beginning to study the benefits versus outlay equation, an organization must know exactly what the outlay is. Decision makers must assess what they currently have in terms of hardware, software, and performance, and compare it with what they need. Some of the questions that are likely to arise at this time include the following:

- Do the existing workstations have the hardware required to run the new operating system?
- Will the new operating system improve performance, and if so, how much?

In Lesson 1, you might have noticed that issues like these first come up in the Plan phase, quite early in the MOF 4.0 life cycle. Some of the earliest tasks for an IT department in a Windows 7 deployment are feasibility studies, as discussed in the following sections.

**After this lesson, you will be able to:**

- List the various tools you can use to compile a hardware inventory for your workstations.
- Create a workstation performance baseline using Performance Monitor.

**Estimated lesson time: 60 minutes**

## Compiling a Workstation Hardware Inventory

When you consider these basic questions—what hardware does the new software require? and do our workstations meet those requirements?—you are likely to find the first question is easy because the Windows 7 system requirements are readily available on the Microsoft Web site. But the second can pose a problem.

In the IT manager's idea of a perfect world, all of the organization's workstations are identical: the same model computer with the same hardware inside, a single operating system, and application configuration throughout the enterprise. Of course, most of these managers know that this is a dream that very seldom comes true.

Companies rarely buy all of their workstations at once. They typically buy computers in lots from large vendors or manufacturers. Even if they buy from the same vendor every time, models and supply situations change so quickly that the computers they purchase today are likely to have substantially different components than those they bought only a few months ago.

IT managers also must consider the practices of maintenance and support. When a workstation hard disk fails, an IT person might replace it with a different model the team happens to have on hand. When a department adopts a new application, workstations might need installations of extra memory to support it. The designers in the Marketing department might require high-end graphics adapters in their workstations. The result is a fleet of workstations with widely varying hardware and software configurations. A dedicated and disciplined IT staff might keep careful records of these modifications, but in a busy department, the documentation often is deferred, delayed, or forgotten altogether.



## REAL WORLD

Craig Zacker

Some organizations run a “tight ship,” as far as IT considerations are concerned, maintaining rigorous control over workstation configurations and preventing users from installing or modifying any software or hardware themselves. Other organizations are considerably more casual. I once worked in the technical support department for a small, but rapidly growing, software company full of inveterate tinkerers.

Our computer cases were always open, and we were constantly swapping out hard drives and memory sticks, installing beta software, and reconfiguring the operating system. Any hardware or software inventory the IT department attempted to compile would be outdated only a few hours after its completion.

This experimental atmosphere fostered an excellent learning environment for the technical support staff, but it also led to chaos when the IT department wanted to deploy a database application to track technical support incidents. The IT staffers who arrived to install the application found half the workstations in various stages of disassembly, and most of the others unready in other ways to support the new software.

This fiasco forced the management team to supply the technical support staff with new production workstations that we were forbidden to modify in any way. The moral of this story is that if your organization has highly skilled computer users who take care of their own workstation support, the everyday burden on the IT staff might be reduced, but large projects such as operating system upgrades might be considerably more complicated.

Organizations considering a Windows 7 deployment might need to perform a detailed inventory of the hardware in each existing workstation. A hardware inventory should include the following information for each computer:

- Processor type and speed
- System memory
- Number and capacities of hard disks
- Amount of free hard disk space
- Graphic adapter type

The ways to discover this information are discussed in the following sections. Which one you choose depends on how many workstations you have to inventory, how much you can afford to spend, and what other uses you might make of the inventory tool.

## Using the Manual Method

The simplest method for gathering workstation inventory information is, of course, to look at each computer. You can open each computer case and look inside, but even then, it can be hard to locate the information you need. Components are often not clearly marked on the outside, and many computers pack them in so tightly that you would have to disassemble them to find out, for example, the capacities of the hard disks. And even if you can determine the disk capacities in this way, you have no way of knowing how much free space there is on the disks without starting the computer and manually checking free space as well.

This method is far too complicated if you have more than two or three workstations to inventory. What you need is some sort of tool that produces a report listing the hardware inside the computer.

## Using System Information

All of the Windows operating systems have an application called System Information, which can display extensive information about the hardware and software configuration of the local computer or another computer on the network. System Information can provide all of the essential inventory information listed earlier, and a great deal more. You can save the reported information to a System Information file with an .nfo extension, for later access, or to a text file.

In Windows 7, Windows Vista, and Windows XP, System Information is accessible from the Start menu, in the All Programs\Accessories\System Tools\ folder. Launching the program displays a system summary for the local computer, as shown in Figure 1-8. This page includes processor and memory information.

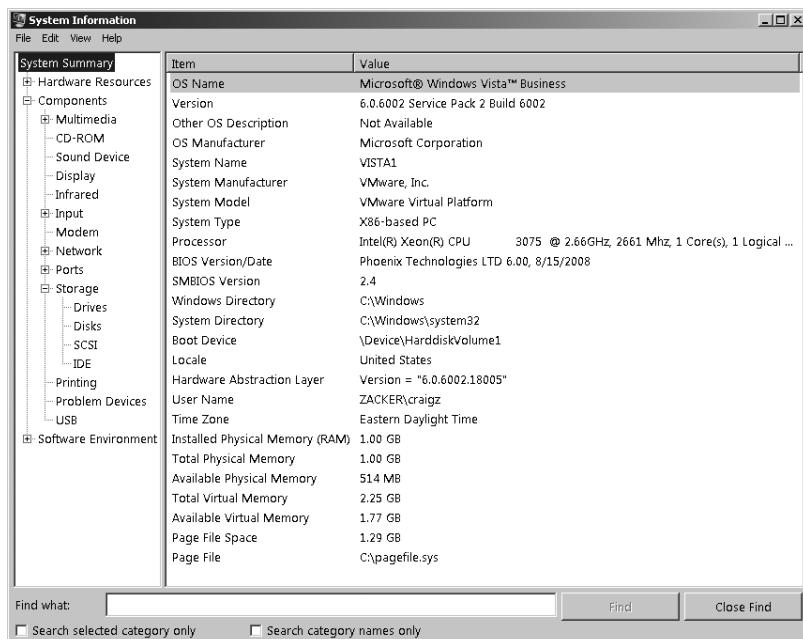
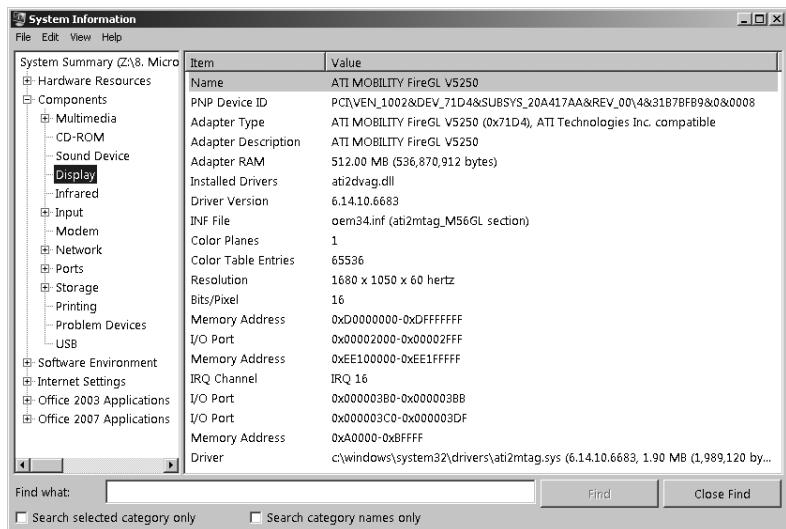


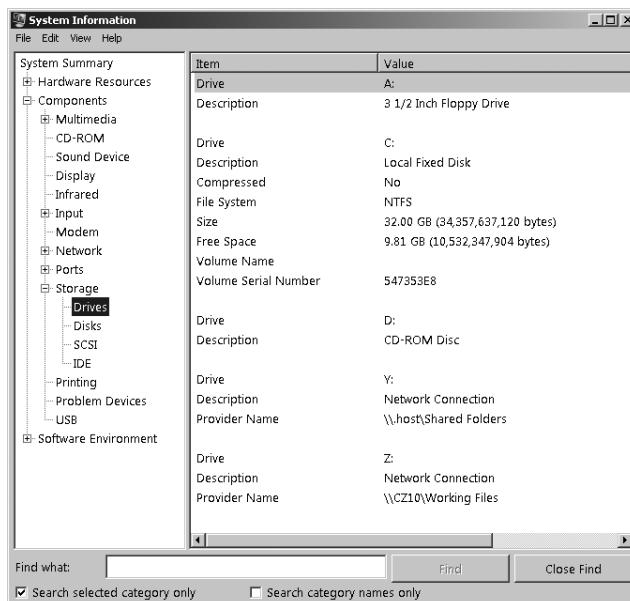
FIGURE 1-8 The System Summary page in System Information

The Components\Display\ page, shown in Figure 1-9, contains information about the graphics adapter.



**FIGURE 1-9** The Components\Display\ page in System Information

The Storage\Drives\ page, shown in Figure 1-10, lists the hard disks in the system, their capacities, and the amount of free space available. Selecting View\Remote Computer\ enables you to connect to another system on the network and view its system information as well.



**FIGURE 1-10** The Storage\Drives\ page in System Information

Although the System Information program provides the inventory information an IT technician needs to determine whether a workstation meets the system requirements for Windows 7, the process of gathering and analyzing the information is slow, and for a large network, all but unmanageable. The only way to store the workstation hardware inventory information in one central location would be to create a repository yourself, manually, using a spreadsheet or similar program. The administrators of a medium or large enterprise network need a tool that can gather hardware information from all of the computers on the network into a single interface.

## Using Microsoft System Center Configuration Manager

Microsoft System Center Configuration Manager (SCCM) 2007 is a network management application that, among many other capabilities, can perform an inventory of the hardware and software in all of the computers on your network and store the information in a centralized database for later analysis. SCCM can also manage software updates, distribute software packages, remotely administer network computers, and deploy operating systems. In fact, the Zero Touch Installation (ZTI) deployment process defined in Microsoft Deployment Toolkit 2010 requires an SCCM infrastructure. For more information on using System Center Configuration Manager 2007 to deploy Windows 7, see Chapter 6, “Designing a Windows 7 Client Deployment Strategy.”

SCCM is an excellent tool for creating a hardware inventory, but it is not a product that you are likely to use solely for that purpose. First, it’s an expensive product, requiring you to purchase licenses for each server and client on your network. Second, installing, configuring, and deploying SCCM requires a separate database server and the installation of client agents on each workstation.

For assessing the current hardware configuration of your workstations, with an eye toward a Windows 7 deployment, SCCM is almost overkill. The SCCM Hardware Inventory Client Agent queries Windows Management Instrumentation (WMI) on the workstation, enabling it to collect information on over 1,500 hardware properties and report it to the SCCM site server.

Assuming that you have SCCM fully installed, enabling the Hardware Inventory Client Agent on your workstations causes them to transmit inventory information to the site server at regular intervals. You can then view the information by using Resource Explorer in the SCCM 2007 Administrator Console.

## Using the Microsoft Assessment And Planning Toolkit 5.0

For an enterprise that has not invested in SCCM, you can choose other, simpler, options for automating the process of compiling a hardware inventory. There are many third-party products that can compile a workstation inventory, but the Microsoft Assessment And Planning (MAP) Toolkit 5.0 is particularly well suited to this task.

### NOTE DOWNLOADING MAP TOOLKIT 5.0

The MAP Toolkit 5.0 is available from the Microsoft Download Center at  
<http://www.microsoft.com/downloads/details.aspx?familyid=67240B76-3148-4E49-943D-4D9EA7F77730>.

One of the biggest advantages of the MAP Toolkit is that it does not require you to install an agent or other client program on the computers you want to inventory. After you install the program on a Windows server or workstation, it can scan the network and, by using Active Directory Domain Services, IP addresses, or network broadcast messages, locate other computers and query them for information about their hardware and software configurations, as shown in Figure 1-11.

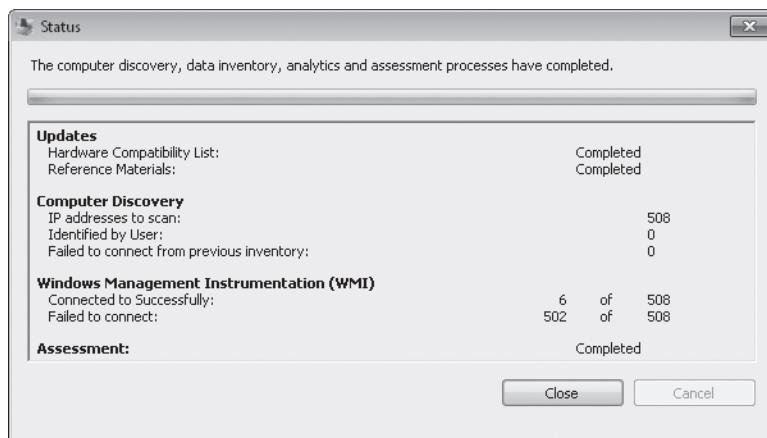
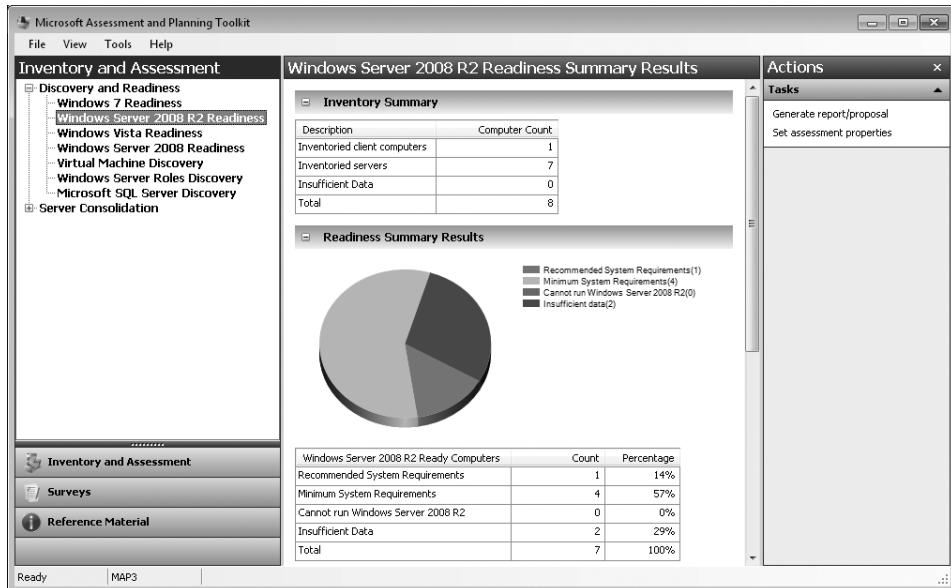


FIGURE 1-11 The Status display produced by MAP Toolkit 5.0 as it scans the network

### EXAM TIP

The MAP Toolkit is not a full-featured network management tool, as SCCM 2007 is. Instead, it is specifically designed to assess the readiness of workstations and servers for the installation of Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008. The program is relatively easy to install and use, and it's free.

Like SCCM, the MAP Toolkit stores its inventory information in a Microsoft SQL Server database, but unlike SCCM, it can use the free SQL Server 2005 Express Edition, which it downloads and installs automatically during the setup process. The toolkit is scenario-based, enabling you to specify how you want to use the inventory data. After the program completes its client scan, it displays its results in the Microsoft Assessment And Planning Toolkit console, as shown in Figure 1-12.



**FIGURE 1-12** Readiness summary results, as displayed in the Microsoft Assessment And Planning Toolkit console

Because it is designed specifically for Windows deployment scenarios, MAP Toolkit also enables you to generate boilerplate reports and proposals, into which the program inserts the inventory information it has gathered from the clients. A hardware assessment report generated by the toolkit takes the form of an Excel spreadsheet containing the raw inventory results, as shown in Figure 1-13.

Computer Name	Computer Model	Active Network Adapter	Number of Processors	CPU	System Memory (MB)	Video Card	Video Card Memory (MB)	Disk Drive
cz1.zacker.local	ProLiant ML330 G3	BCM5703 Gigabit Ethernet (Server Local Area Connection)	2	Intel(R) Xeon(TM) CPU 2.40GHz, 32 bit	3584	RAGE XL PCI Family (Microsoft Corporation)	8	FANTOM WD10EACS-00ZJB0 USB Device Maxtor 6 Y080LD SCSI Disk Device
cz10.zacker.local	ProLiant ML350	3Com 3C996B Gigabit Server NIC (Local Area Connection 2)	1	Intel(R) Pentium(R) III processor, 32 bit	1024	RAGE XL PCI Family (Microsoft Corporation)	4	COMPAQ BD01873A4 SCSI Disk Device
cz4.zacker.local	ProLiant ML110 G5	VMware Virtual Ethernet Adapter for VMnet8 (VMware Network Adapter VMnet8) VMware Virtual	1	Intel(R) Xeon(R) CPU 3075 @ 2.66GHz, 64 bit	8192	Standard VGA Graphics Adapter	7	GB0160CAABV
ServerA.example.local	VMware Virtual Platform	Intel(R) PRO/1000 MT Network Connection (Local Area Connection)	1	Intel(R) Xeon(R) CPU 3075 @ 2.66GHz, 64 bit	1024	VMware SVGA II	N/A	VMware, VMware Virtual S SCSI Disk Device VMware,

**FIGURE 1-13** A hardware assessment report generated by the MAP Toolkit 5.0



### Quick Check

- As a tool for collecting hardware inventory information from the computers on your network, what are the two primary advantages of the MAP Toolkit 5.0?

### Quick Check Answer

- The MAP Toolkit 5.0 requires no agents on the client computers, and it's free.

## Creating Workstation Performance Benchmarks

Workstation performance is another issue to consider when proposing a Windows 7 deployment. System administrators always hope that software upgrades result in performance improvements, but that is not always the case. For example, a computer running Windows XP might have sufficient system memory to run well, but after installing Windows 7 on that same computer, the amount of memory might be barely adequate.

Generalized performance levels can be difficult to quantify, but if you are going to perform any kind of comparison, you must establish a performance-level baseline on your workstations before you do any test or pilot deployments. There are many third-party benchmarking tools available, or you can use the Performance Monitor tool provided with all versions of Windows. For network performance benchmarking, you can use a third-party product or download the Microsoft protocol analyzer tool, Network Monitor.

#### **NOTE DOWNLOADING NETWORK MONITOR**

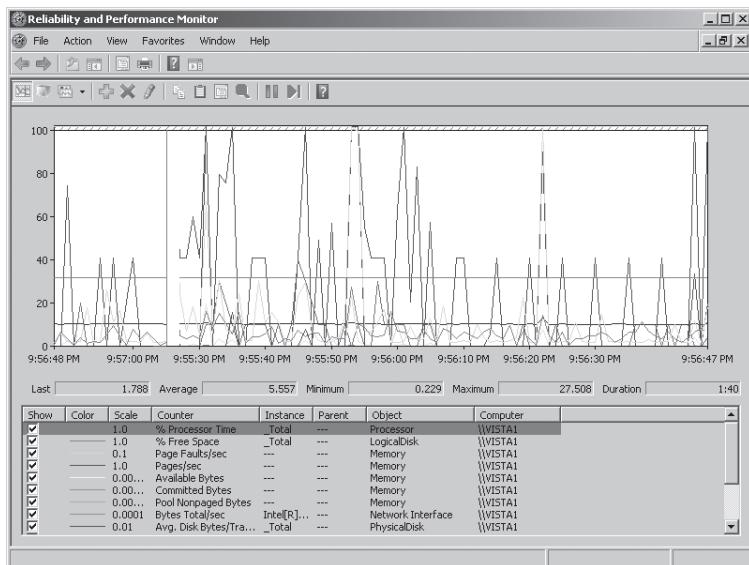
Microsoft Network Monitor is available from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=983b941d-06cb-4658-b7f6-3088333d062f>.

To establish a performance baseline for a test workstation running Windows Vista by using Reliability And Performance Monitor, you could create a data collector set that samples the following performance counters for an extended period of time, as shown in Figure 1-14:

- Processor (\_Total): % Processor time
- Processor (\_Total): Interrupts/sec
- System: Processor Queue Length
- Server Work Queues (0): Queue Length
- Memory: Page Faults/Sec
- Memory: Pages/Sec
- Memory: Available Bytes
- Memory: Committed Bytes
- Memory: Pool Nonpaged Bytes
- PhysicalDisk (\_Total): Disk Bytes/sec
- PhysicalDisk (\_Total): Avg. Disk Bytes/Transfer
- PhysicalDisk (\_Total): Current Disk Queue Length
- PhysicalDisk (\_Total): % Disk Time
- LogicalDisk (\_Total): % Free Space
- Network Interface (All Instances): Bytes Total/sec
- Network Interface (All Instances): Output Queue Length
- Server: Bytes Total/Sec

#### **NOTE UNDERSTANDING PERFORMANCE COUNTER NOTATION**

For each of the performance counters listed, the first term (before the colon) is the name of the performance object in which the counter is located. The second term (after the colon) is the name of the counter itself. A value in parentheses appearing after the performance object name (immediately before the colon) is the instance of the counter.



**FIGURE 1-14** Baseline performance counter readings in Windows Vista

After installing Windows 7 on the workstation, you can then evaluate the computer's performance by creating the same data collector set and comparing the results with the baseline you created earlier.

Benchmarking tools do not necessarily provide absolute measurements that are verifiably accurate. However, they are usually consistent in their measurements. Whatever tools you elect to use when establishing your performance benchmarks, make sure you use the same ones in the same manner for all of your subsequent measurements.

#### MORE INFO USING PERFORMANCE MONITOR

For more detailed information on using Performance Monitor, see Chapter 13, "Monitoring and Performance," in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7* by Ian McLean and Orin Thomas (Microsoft Press, 2009).

## PRACTICE Using the Microsoft Assessment And Planning Toolkit 5.0

---

The Microsoft Assessment And Planning Toolkit 5.0 package is a single executable that checks for a program's prerequisites before installing the software and, if necessary, downloads and installs SQL Server Express.

### EXERCISE 1 Installing the MAP Toolkit

Microsoft provides the MAP Toolkit 5.0 free of charge, from the Microsoft Downloads Center.

1. Open a browser window and, in the address box, type the following URL and press Enter:  
**<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730>**. The Microsoft Assessment And Planning Toolkit download page appears.
2. Click the Download button for the Microsoft\_Assessment\_and\_Planning\_Toolkit\_Setup.exe file and save the file to a folder on your local drive.
3. Open Windows Explorer, then locate and run the file you downloaded. The Microsoft Assessment And Planning Toolkit Setup Wizard appears.
4. If any of the prerequisites that the toolkit requires are missing, a Prerequisites Not Found page appears. Click the links for the missing prerequisites for more information or to download them. The installation will not proceed until the computer meets all of the prerequisites.
5. After meeting the prerequisites, restart the installation process, and then accept the terms of the license agreement and the default installation folder location.
6. On the SQL Server Express page, specify whether you want the program to download SQL Server Express or install from previously downloaded files.
7. Accept the terms of the SQL Server Express license agreement and complete the installation.

### EXERCISE 2 Compiling an Inventory

To use the MAP Toolkit 5.0, you select one of the scenarios provided with the package.

1. From the Start menu, open the Microsoft Assessment And Planning Toolkit. The Microsoft Assessment And Planning Toolkit console appears and displays a Create Or Select A Database To Use dialog box.
2. Specify a name for the database, and click OK.
3. Click the link for the Inventory And Assessment Wizard. The wizard appears, displaying the Computer Discovery Methods page.

4. Clear all of the check boxes except Scan An IP Address Range, and click Next. The Scan An IP Address Range page appears.
5. Specify the Starting Address and Ending Address values for the range of addresses you want to scan, and click Next. The WMI Credentials page appears.
6. Click New Account and, in the Inventory Account dialog box, specify the credentials for the account the wizard will use to connect to the computers on your network. Then click Save. You can create as many additional accounts as needed; the wizard will try each one in turn for each computer. Then click Next. The Summary page appears.
7. Click Finish. The Status dialog box appears, updating as the wizard connects to the computers it finds on the network.
8. Click Close, and then in the Microsoft Assessment And Planning Toolkit console, in the scope (left) pane, expand the Discover And Readiness node and select Windows 7 Readiness. The results of the inventory appear in the detail (right) pane.

## Lesson Summary

- Before IT staff can begin to compare the benefits of a Windows 7 deployment with the outlay required, they must assess what they currently have, and compare it with what they need, in terms of hardware, software, and performance.
- The most basic questions regarding any software installation are these: what hardware does the new software require and do our workstations meet those requirements?
- Organizations considering a Windows 7 deployment might need to perform a detailed inventory of the hardware in each existing workstation. A hardware inventory should include, for each computer: processor type and speed, amount of system memory, number and capacities of hard disks, amount of free hard disk space, and the graphic adapter type.
- To inventory workstation hardware, you can examine each computer manually, use the System Information tool, purchase System Center Configuration Manager 2007, or download the Microsoft Assessment And Planning Toolkit 5.0.
- If you are going to perform any kind of performance comparison on your workstations, you must establish a performance-level baseline on your workstations before you do any test or pilot deployments. Many third-party benchmarking tools are available, or you can use the Performance Monitor tool provided with all versions of Windows.

## Lesson Review

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

### **NOTE ANSWERS**

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

- 1.** Which of the following hardware inventory tools is available as a free download from Microsoft?
  - A.** Performance Monitor
  - B.** Microsoft Assessment And Planning Toolkit 4.0
  - C.** System Center Configuration Manager 2007
  - D.** System Information
- 2.** Which of the following is NOT a valid reason to use the Microsoft Assessment And Planning Toolkit 5.0 to create a hardware inventory, rather than System Center Configuration Manager 2007?
  - A.** The MAP Toolkit does not require client agents.
  - B.** The MAP Toolkit is free.
  - C.** The MAP Toolkit can use SQL Server 2005 Express Edition.
  - D.** The MAP Toolkit can perform ZTI deployments.
- 3.** Which of the following hardware specifications is necessary to determine whether a workstation is capable of running Windows? (Choose all that apply.)
  - A.** Amount of system memory
  - B.** Number and type of network adapters
  - C.** Amount of free hard disk space
  - D.** Processor type and speed

## Chapter Review

---

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

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

## Chapter Summary

- The operating system deployment tasks that fall to a Windows 7 desktop administrator can actually be part of a much larger project life cycle that involves management and policy makers through the organization. The Microsoft Operations Framework 4.0 specifies the phases of this life cycle and defines each one by using a series of white papers called service management functions (SMFs).
- Deploying Windows 7 on a fleet of existing workstations is considerably more complicated than on new hardware. Before you can begin to plan the deployment project, you must gather information about the existing computers so that you can determine what preliminary steps are necessary before they can run Windows 7.

## 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.

- Microsoft Assessment And Planning (MAP) Toolkit 5.0
- Microsoft Deployment Toolkit (MDT) 2010
- Microsoft Operations Framework (MOF) 4.0
- Microsoft Solutions Framework (MSF)
- Microsoft System Center Configuration Manager (SCCM) 2007
- Service management functions (SMFs)

## Case Scenarios

In the following case scenarios, you will apply what you've learned about the Windows 7 deployment process. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Making a Windows 7 Deployment Decision

Bob is the IT manager for a company with a single office and 150 workstations. Approximately 100 of the workstations are several years old and are running Windows XP. The remaining 50 were purchased less than a year ago and are running Windows Vista. With the release of Windows 7, Bob is trying to determine whether it is worthwhile to upgrade the operating system workstations. If he decides to proceed, he will have to create a project proposal and present it to the company management team.

Using the Microsoft Assessment And Planning Toolkit 5.0, Bob performs a hardware inventory of his workstations and generates a Windows 7 readiness report. The report states that all of the workstations are capable of running Windows 7. However, Bob is still concerned about performance levels after the upgrade because many of his users run resource-intensive graphics applications.

Bob is considering each of the following courses of action as the next step in his Windows 7 deployment project. For each option, specify reasons why Bob should or should not take that course of action.

1. Purchase and install Microsoft Systems Center Configuration Manager 2007 so that he can perform a more detailed hardware inventory.
2. Propose installing Windows 7 on all 150 workstations as they are currently configured.
3. Propose installing additional memory in the Windows XP workstations and then upgrading all 150 workstations to Windows 7.
4. Conduct performance baseline benchmarks on one Windows XP and one Windows Vista workstation, then upgrade both to Windows 7 and repeat the performance testing.

### Case Scenario 2: Preparing for Windows 7 Deployment

Carol is the manager of the Windows 7 Deliver Team in her company's IT department, and this team is preparing to deploy Windows 7 on the company's entire fleet of 500 user workstations. Laboratory testing of the workstation builds has been completed. According to the MOF and MSF procedures they are using to guide the project, should Carol complete each of the following tasks before she begins the actual deployment on the production workstations? Why or why not?

1. Hand off control of the project to the Operate team.
2. Perform one or more pilot deployments.
3. Submit the build and testing reports for a release readiness review by the management team.

## Suggested Practices

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

### Using the IT Pro Quick Start Kit

The base Microsoft Operations Framework 4.0 package consists of 23 documents totaling nearly 600 pages. Although these documents contain a lot of valuable information, students' intent on preparing for the 70-686 exam can probably make better use of their time than by reading that package. Fortunately, Microsoft has also published the IT Pro Quick Start Kit, which contains a collection of presentations, graphics, podcasts, and relatively brief documents that provide a basic overview of Microsoft Operations Framework 4.0. In this practice, you download the IT Pro Quick Start Kit and examine its contents.

- **Practice 1** Download the IT Pro Quick Start Kit from the Microsoft Operations Framework page on their TechNet site at <http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx> and save it to a new folder on your local drive.
- **Practice 2** Extract the files from the IT Pro Quick Start Kit and double-click the START HERE.pptx file. When PowerPoint launches and loads the file, press F5 to start the presentation. View the Get Started: MOF Overview Presentation and listen to the MOF 4.0 Overview Podcast.

### Benchmarking a Performance Baseline

In this practice, you create a performance-level baseline on a lab computer running Windows Vista, and then repeat the performance benchmark test after installing Windows 7 on the same computer.

- **Practice 1** On a lab computer running Windows Vista, use the Performance Monitor tool in Reliability And Performance Monitor to create a data collector set that captures a 30-minute data sample for the performance counters listed in Lesson 2. When you have captured the data sample, copy it to a removable drive or a network share on another computer.
- **Practice 2** Install Windows 7 on the same lab computer, and then use Performance Monitor to create an identical data collector set as before, using the same performance counters. Compare the results from the Windows Vista benchmark to those from the Windows 7 benchmark and decide whether the computer's hardware configuration is sufficient to support a permanent Windows 7 installation.

## 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 70-686 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.

# Designing a Client Life Cycle

When you are designing a client life cycle, you should ensure that your plan reduces the amount of time you have to spend maintaining parts of that life cycle. Your aims can include reducing the amount of time you spend managing operating system activation, configuring the operating system so that the installation is easily transferrable to another computer, and minimizing the amount of time it takes to move data from an older computer to its replacement.

Although it is not a problem to enter a unique product key when you perform a traditional installation of Windows 7 on a small number of computers, a simple operation that takes a minute or so becomes problematic when you have to perform the same operation on several thousand. Microsoft offers enterprise customers an alternative way of ensuring that their computers are properly licensed without consuming an inordinate amount of time. The name for this method is volume activation. You will learn about volume activation in the first lesson of this chapter.

A new feature of Windows 7 is the ability to deploy the operating system directly to a VHD file and boot that VHD file on physical hardware. Installing Windows 7 on a bootable VHD allows an installation to be easily migrated to new hardware. When configured in this manner, migration to new hardware is as simple as transferring the VHD container in which Windows 7 has been installed to the new physical or virtual host.

Although the promise of VHD deployments suggest that in the future it will be relatively simple to migrate users from their old computers to their new computers, most of the users coming to a new Windows 7 installation will be coming from computers running the Windows XP or Windows Vista operating systems. The User State Migration Tool offers administrators the ability to automate the process of user data migration, vastly speeding the process of transitioning users from these older computers to new computers that run Windows 7.

## Exam objectives in this chapter:

- Plan and manage client licensing and activation.
- Plan and manage a physical hardware and virtualization strategy.
- Design a user state migration strategy.

## Lessons in this chapter:

- Lesson 1: Designing and Managing a Licensing Strategy **43**
- Lesson 2: Designing a Client Hardware Platform **52**
- Lesson 3: Migrating User Profiles **61**

## Before You Begin

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

- Installed the Windows 7 operating system on a stand-alone client PC named WKSTN1, as described in the introduction.
- Downloaded and installed the Windows Automated Installation Kit (Windows AIK).

### **MORE INFO DOWNLOAD WINDOWS AIK**

You can obtain the Windows Automated Installation Kit from the following location on TechNet: [http://technet.microsoft.com/en-us/library/dd349343\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd349343(WS.10).aspx).



### **REAL WORLD**

Orin Thomas

Enterprise desktop administrators have the same enthusiasm for operating system licensing that the average five year old has for a tetanus shot. The only thing that excites enterprise desktop administrators less than operating system licensing is the thought of going through a licensing audit to ensure that all of the client computers at your organization are properly licensed. A few years ago, I had to manage the client operating system licenses for a number of postgraduate computer labs at a local university. Each semester we would reimage the computers because the students tended to be brutal with them, and it was easier to wipe-and-replace than it was to figure out the creative ways they had managed to compromise the original installation. Keeping track of keys during this process was a nightmare, and we always feared that some of the machines would not be properly activated when it was time for the new semester's classes to start. When I first heard about Key Management Services, I thought how useful it would have been in managing those computer labs. Rather than worrying about reactivating those computers each time I did a deployment, I would have been able to sit back and let the KMS service handle it.

# Lesson 1: Designing and Managing a Licensing Strategy

The licensing strategy that you choose depends on the circumstances of your Windows 7 deployment. When you are determining which strategy to pursue, you must take into account factors such as client connectivity to the Microsoft activation servers on the Internet, the number of clients that you need to activate, and the editions of Windows 7 that you have chosen to deploy. In this lesson, you learn about the licensing and activation options that are available to volume licensing customers and how these differ from the licensing and activation options available to normal retail customers.

## After this lesson, you will be able to:

- Understand different Windows 7 licensing options.
- Deploy Key Management Services.
- Utilize Multiple Activation Keys.
- Describe licensing options for virtual clients.

**Estimated lesson time: 40 minutes**

## Windows 7 Editions and Licensing

Windows 7 uses three types of license: the OEM license, the retail license, and the volume license. OEM licenses are tied to a specific hardware vendor. This license type is used with computers that are sold with Windows 7 already installed by the vendor, such as those you might purchase from your local computer retailer. The product keys associated with an OEM license do not allow you to transfer the license to a computer made by a different vendor. Computers that have OEM licenses undergo activation prior to being deployed to customers.

Retail keys are provided when you buy a retail copy of Windows 7. You can use the Home Premium, Professional, and Ultimate editions of Windows 7 with retail keys. Because a retail key is used only for a single computer, this type is not used with zero touch or lite touch automated volume deployments.

Volume License keys are made available to organizations that have a volume licensing agreement with Microsoft. Volume licenses include the Open, Select, and Enterprise agreement types. You can use volume license keys only with computers running the Windows 7 Professional and Enterprise operating systems. You can use a mixture of retail, volume license, and OEM keys in an organizational environment.

### MORE INFO VOLUME LICENSING

To find out more about volume licensing, consult the following reference on the Microsoft Web site: <http://www.microsoft.com/licensing/default.aspx>.

## Windows Product Activation

Each computer that runs the Windows 7 operating system installed in your organization must undergo Windows Product Activation (WPA). Microsoft uses WPA to ensure that it is possible to use the Windows 7 operating system on a computer only when the computer has a license. Windows 7 must undergo the WPA process within 30 days of the completed installation. You can extend this 30-day period to a total of 120 days by using the *slmgr.vbs –rearm* command. Each use of this command extends the activation period for 30 days. You can use this command to extend the activation period only three times. After the grace period expires, the WPA process must successfully occur or Windows enters reduced functionality mode.

WPA relies on two specific identifiers and a third identifier that Windows generates based on the previous two identifiers. These identifiers have the following properties:

- **Hardware ID** This identifier is generated using information about computer hardware configuration. This ID is unique and changes if the hardware configuration of the computer changes.
- **Product ID** 25-character key. This is either a retail key or a Multiple Activation Key. Unless Key Management Services is in use, this key must be input on the computer running the Windows 7 operating system. You can deploy keys through the unattended installation process. You learn about Key Management Services and deploying keys in an unattended installation later in this lesson.
- **Installation ID** Windows 7 generates this ID using the Hardware ID and Product ID. You forward the installation ID to Microsoft when you perform an activation using the telephone.

During the online WPA process, the computer forwards the Product and Hardware IDs to Microsoft activation servers. If the activation check determines that the Product ID has not exceeded its allowed number of activations, the activation servers record the Hardware ID and Product ID, the number of recorded activations for the Product ID is incremented, and the activation servers forward an activation code to the client.

Microsoft allows you to reinstall and reactivate Windows 7 on the same computer once without incrementing the number of recorded activations. Substantially altering the computer's hardware configuration also triggers reactivation. This can cause problems if a prior event has triggered a reactivation: you might need to contact Microsoft if a single computer goes through several rapid hardware configuration changes that prompt multiple reactivations.

### MORE INFO WINDOWS ACTIVATION TECHNOLOGIES

To learn more about Windows Activation Technologies, consult the following document on TechNet: <http://technet.microsoft.com/en-us/library/dd979803.aspx>.

# Volume Licensing Activation Methods

You can choose from two methods for performing volume licensing activation: Multiple Activation Keys (MAK keys) or Key Management Services. In the real world, one method is more appropriate for some situations but in other situations, the choice is a matter of personal preference. You often need to choose a volume activation method prior to deploying client computers running the Windows 7 operating system. In the next few pages, you learn about the solutions that you can implement and the types of situations in which you would choose one volume licensing activation method over another.

## MORE INFO VOLUME ACTIVATION OPERATIONS GUIDE

For more information about the techniques that you can use to activate volume licenses, consult the Volume Activation Operations Guide at the following address:  
<http://technet.microsoft.com/en-us/library/dd772270.aspx>.

## Multiple Activation Keys

MAK keys are special keys that allow an organization to perform multiple activations using a single key. MAK keys are similar to retail keys except that instead of allowing a single activation, they allow multiple activations from different computers to occur up to the limit defined by the particular key. The number of activations that a MAK key allows depends on the number you purchase when you obtain the key. You cannot recover an activation on a MAK key after you have consumed it. For example, if an organization uses a MAK key and replaces one computer running Windows 7 activated using a MAK key with another computer, the replacement computer consumes a new activation of the MAK key. In some scenarios, this circumstance makes KMS a preferred solution to MAK key activation.

As a single key is used, you can add MAK keys images when deploying them centrally. When using the Sysprep utility to prepare an image, you add a MAK key to an image during the Specialize configuration pass. When performing a traditional installation, you can enter MAK keys in the same way that you would enter a retail key. The main issue that requires consideration when using a MAK key is how you will perform activation.

You can activate a MAK key in one of two ways:

- **MAK Independent Activation** Similar to normal retail activation in that it requires that each computer independently activate. You can activate the key automatically over the Internet or use the telephone to call the licensing clearinghouse. MAK Independent Activation is a good option for locations in which you do not have sufficient numbers of clients to make KMS or MAK Proxy Activation viable. For example, if you plan to deploy five clients on an isolated network, it is simpler for you to perform MAK Independent Activation over the telephone than it is to configure MAK Proxy Activation for such a small number of clients.

- **MAK Proxy Activation** Allows administrators to configure activation of multiple independent clients using a single connection to Microsoft. MAK Proxy Activation is suitable for isolated networks that do not meet the KMS client threshold but have sufficient numbers of clients to make independent activation more time consuming than configuring proxy activation. For example, consider MAK Proxy Activation for an isolated network of 23 clients for the Windows 7 Enterprise operating system. Performing 23 separate telephone activations would take more time than configuring proxy activation. To use MAK Proxy Activation, you need to configure the Volume Activation Management Tool (VAMT). You learn about the VAMT in the next section.

#### **MORE INFO MAK KEYS AND VOLUME DEPLOYMENTS**

To learn more about entering product keys when preparing volume deployments, consult the following TechNet document: [http://technet.microsoft.com/en-us/library/dd744266\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744266(WS.10).aspx).

## **Volume Activation Management Tool**

The Volume Activation Management Tool (VAMT) allows you to collect activation requests from multiple computers and then forward those requests to Microsoft all at one time. After the VAMT receives the activation confirmation identifiers from Microsoft, it can distribute those IDs back to the computers that originally requested activation. The term for this process is MAK Proxy Activation, described previously.

The VAMT stores activation confirmation identifiers in a database called a collection. Because these identifiers are stored locally, you can perform operating system reactivation without being required to initiate a new connection between the computer hosting the VAMT and Microsoft. This allows organizations to reimagine computers without the concern of consuming an additional activation on an existing MAK key. You can use the Volume Activation Management Tool to transition client computers between MAK and KMS volume activation if necessary.

To use MAK Proxy Activation, perform the following general steps:

1. Install the VAMT on a computer on the isolated network and the VAMT on a computer that is located on a network connected to the Internet. For the purposes of this explanation, the computer on the isolated network is VAMT-Isolated and the computer on the connected network is VAMT-Connected.
2. Create a computer group named Isolated Computers on VAMT-Isolated. Use the VAMT discovery process to discover the identity of the computers on the isolated network.

3. Add the MAK key to the VAMT on computer VAMT-Isolated. Right-click the Isolated Computers group on VAMT-Isolated and then choose the MAK Proxy Activate option. Make sure of the following:

  - The Get Confirmation ID From Microsoft check box is not enabled.
  - The Apply Confirmation ID And Activate check box is not enabled.
4. When VAMT finishes assigning the MAK keys on the isolated network, save the collection file on VAMT-Isolated, and then transfer and import the collection file to the VAMT-Connected computer. This action populates the VAMT on VAMT-Connected with the Isolated Computers group.
5. On the VAMT-Connected computer, right-click the Isolated Computers group and then choose MAK Proxy Activate. Make sure of the following:

  - The Get Confirmation ID From Microsoft check box is selected.
  - The Install MAK (Overwrite Existing) check box is not selected.
  - The Apply Confirmation ID And Activate check box is not selected.
6. VAMT on VAMT-Connected now interacts with the Microsoft servers and procures confirmation identifiers.
7. After the confirmation IDs have been obtained from the Microsoft servers, export the collection with a new name. Transfer this file to the VAMT-Isolated computer and import the file.
8. After you import the file, save the file in a secure location such as a removable flash device placed in a safe. This allows you to perform reactivation if it is necessary to reimagine hosts on the isolated network.
9. On VAMT-Isolated, select the Isolated Computers group and choose MAK Proxy Activate. Make sure of the following:

  - The Apply Confirmation ID And Activate check box is selected.
  - The Get Confirmation ID From Microsoft check box is not selected.
  - The Install MAK (Overwrite Existing) check box is not selected.
10. VAMT assigns the confirmation identifiers to computers on the isolated network, activating them.

You can configure VAMT clients on an Active Directory computer account, a stand-alone workgroup membership, a fully qualified domain name, or an IP address, as shown in Figure 2-1. The tool also allows you to see the current licensing state of clients on your network, allowing you to determine whether your organization is compliant with the number of purchased licenses.

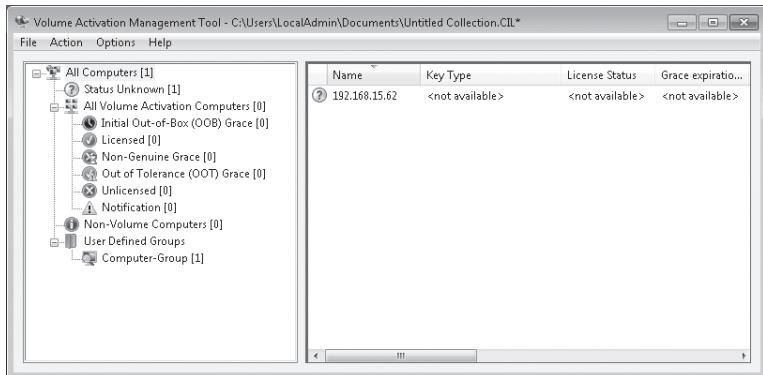


FIGURE 2-1 Volume Activation Management Tool

You can also use the VAMT to activate a large number of computers that are located on a network connected to the Internet. The name for this process is MAK Independent Activation. When you perform MAK Independent Activation, the VAMT installs the MAK key on a group of selected computers and then prompts those computers to undergo the activation process on Microsoft activation servers.

#### MORE INFO MAK PROXY ACTIVATION

To learn more about MAK Proxy Activation, consult the following TechNet document:

<http://technet.microsoft.com/en-us/library/dd981010.aspx>.



#### Quick Check

- What tool do you use to perform MAK Proxy Activation?

#### Quick Check Answer

- Volume Activation Management Tool

## Key Management Service

Key Management Service (KMS) allows you to place an activation server on the local area network. Rather than activate on the Microsoft activation servers on the Internet, clients activate on the KMS server on the LAN. Clients locate KMS servers using DNS. Because KMS provides activation servers, you should not expose a KMS server to hosts on the Internet by allowing direct access from the Internet. You can also configure clients to use a specific KMS server by using the VAMT. Computers running the Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2003 operating system can function as KMS servers. When you configure a computer running Windows Server 2008 R2 as a KMS server,

you can activate both server and client operating systems. When you configure a computer running the Windows 7 operating system as a KMS server, it is able to activate only computers running Windows client operating systems.

A certain number of clients must contact a KMS server before the KMS activation can occur. This number is the KMS activation threshold. Clients activating on the KMS server can be running in a traditional hardware deployment or as virtual hosts. The KMS activation threshold differs between clients and servers and is as follows:

- The KMS client threshold is 25 Windows clients.
- The KMS server threshold is five servers.

When a new client or server contacts the KMS server, the server increments the activation count by one. Clients do not activate until the activation count reaches the threshold value. Clients contact the KMS server every two hours until the activation threshold is reached or the activation grace period expires. After the activation count on the KMS server exceeds 5, any servers that contact or have contacted the KMS server successfully activate. After the activation count on the KMS server exceeds a value of 25, clients that contact or have contacted the server successfully activate.

To configure a host to function as a KMS server, perform the following steps:

1. Install the KMS key on the computer that will function as the KMS server. This computer can be running the Windows 7 operating system, although this means that it is able to activate only Windows client operating systems and is unable to activate Windows server operating systems.
2. Activate the computer that you installed the KMS key on with Microsoft over the Internet or by using the telephone. After activation is complete, the computer functions as a KMS server.

Each KMS key can be installed on up to six computers that will function as KMS servers. Each KMS server can be reactivated up to nine times with Microsoft, should it be necessary. If your organization needs more than six KMS servers, you must contact a Microsoft Licensing representative to enable additional activations for the organization's KMS key. For example, if your organization has 12 separate sites covered by a single Volume Licensing agreement and a KMS server is to be placed at each site, you need to enable additional activations for the organization's KMS key.

After a KMS client has been activated, it tries to reconnect with the KMS server every 7 days but must reconnect with the KMS server at least once every 180 days. If the client is unable to reconnect with the KMS server in 180 days, it enters a reduced functionality mode. Each time a KMS client successfully connects with a KMS server, the 180-day activation countdown timer is reset.

#### MORE INFO KMS ACTIVATION WEBCAST

To learn more about KMS activation, view the following webcast on the Microsoft Web site: <http://technet.microsoft.com/en-us/library/dd936199.aspx>.

## Software Licensing Management Tool

The software licensing management tool is a command-line utility that you can use to manually manage licensing. The tool uses the slmgr.vbs script. Unlike VAMT, which you must obtain and install manually, slmgr.vbs is included in a default installation of the Windows 7 operating system. The slmgr.vbs script is usually run locally from an elevated command prompt. You can also use it to manage licensing on computers configured for remote management. You can configure the slmgr.vbs command to perform the following tasks:

- Install and remove product keys from hosts.
- Display current host licensing information including current license expiration date.
- Force a host to undergo the activation process.
- Configure a client to use a KMS server and specify the address of the KMS server.
- Extend the evaluation period by 30 days up to three times.



### **EXAM TIP**

Know which editions of Windows 7 can be used with volume licensing. Know the situations in which you can use a KMS server. Know which licensing scenarios require a host to have Internet access.

## Lesson Summary

- MAK keys and KMS can be used only with editions of Windows 7 that support volume licensing. Only the Windows 7 Professional and Enterprise editions support this type of licensing.
- A KMS server requires 25 clients before it can function. A client must check in with the KMS server every 180 days.
- You can use the VAMT to perform MAK proxy activation.
- You add the MAK key to an operating system image using Sysprep during the configuration pass.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. You need to deploy the Windows 7 operating system to 10 computers that are located on a network isolated from the Internet. These computers have been custom-built using hardware purchased from different vendors. These 10 computers are the only hosts on this network. These computers have the Windows 7 Enterprise operating system installed. Which of the following components should you deploy in your solution?

  - A.** Retail key
  - B.** MAK key
  - C.** OEM key
  - D.** KMS server
2. Your organization has an isolated network with one computer running the Windows Server 2008 R2 operating system. This server is configured as a KMS server and uses KMS for activation. How many clients running the Windows 7 Enterprise edition operating system must you add to this isolated network before clients can successfully activate using the KMS server?

  - A.** 4
  - B.** 9
  - C.** 24
  - D.** 29
3. Which of the following methods can you use to activate 15 clients using a MAK when they are on a network isolated from the Internet? (Choose all that apply; each answer forms a complete solution.)

  - A.** MAK Independent Activation
  - B.** MAK Proxy Activation
  - C.** KMS
  - D.** Telephone activation
4. You are using Sysprep to prepare a Windows 7 Enterprise image for deployment. During which Sysprep configuration pass do you add the MAK key?

  - A.** auditUser
  - B.** Generalize
  - C.** Specialize
  - D.** auditSystem
5. Which of the following editions of Windows 7 support volume licensing? (Choose all that apply; each answer forms a complete solution.)

  - A.** Enterprise
  - B.** Ultimate
  - C.** Professional
  - D.** Home Premium

## Lesson 2: Designing a Client Hardware Platform

You must ensure that Windows 7 is deployed on hardware that meets the minimum hardware requirements. Although it is unusual today to find new hardware that would not meet the Windows 7 requirements, you might encounter problems when you attempt to install Windows 7 on older computers that had previous operating systems installed, such as Windows XP.

**After this lesson, you will be able to:**

- Understand hardware requirements.
- Choose an edition of Windows 7 for deployment.
- Determine when to choose physical or virtual deployments.

**Estimated lesson time: 40 minutes**

### Windows 7 Hardware Requirements

Make sure you deploy Windows 7 only to hardware platforms that meet the minimum requirements. Windows 7 has the following minimum hardware requirements:

- 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) of RAM (x86) or 2 GB of RAM (x64)
- 16 GB of hard disk space (x86) or 20 GB (x64)
- DirectX 9 graphics card with WDDM 1.0 or higher graphics adapter driver

The primary limitation of the x86 versions of Windows 7 is that they do not support more than 4 GB of RAM. You can install the x86 version of Windows 7 on a computer that has more than this amount of RAM, but only 4 GB is usable by the operating system. Some editions support more RAM than other editions.

The Starter edition of Windows 7 supports a maximum of 2 GB of RAM. The x64 version of Windows 7 Home Basic x64 supports a maximum of 8 GB of RAM. The x64 Home Premium edition supports a maximum of 16 GB of RAM. The x64 Professional, Enterprise, and Ultimate editions support up to 192 GB of RAM.

#### **MORE INFO PHYSICAL MEMORY LIMITS**

To find out more about memory limitations in Windows 7, consult the following MSDN article: [http://msdn.microsoft.com/en-us/library/aa366778\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa366778(VS.85).aspx).

Although the x86 version of Windows 7 can be installed on computers that have x64 compatible processors, you cannot install an x64 version of Windows 7 on a computer with an x86 processor. Different editions of Windows 7 support different numbers of physical processors, although each edition of Windows 7 supports an unlimited number of cores on that processor. For example, all editions of Windows 7 support quad-core CPUs. Windows 7 supports either one or two physical processors. The editions and the number of processors that they support are as follows:

- **1 Physical Processor** The Starter and Home Basic.
- **2 Physical Processors** The Home Premium, Professional, Ultimate, and Enterprise editions of Windows 7 support a maximum of two physical processors.

#### **MORE INFO WINDOWS 7 SYSTEM REQUIREMENTS**

To learn more about the Windows 7 system requirements, consult the following document:  
<http://windows.microsoft.com/systemrequirements>.

## Windows 7 Editions

Because the 70-686 exam is primarily concerned with issues related to the deployment and management of Windows 7 in enterprise environments, the exam concentrates on those editions of Windows 7 that are most likely to be present in those environments. Only three editions of Windows 7 can be joined to an Active Directory Domain Services domain and are likely to be managed by enterprise administrators on an organizational network. These are the Professional, Ultimate, and Enterprise editions of Windows 7. Although these editions all share the same basic features, such as the ability to join domains and be subject to Group Policy, these editions differ from one another in the following ways:

- **Windows 7 Professional** This edition of Windows 7 supports Encrypting File System and Remote Desktop Host. You can use either a retail product key or an enterprise licensing key with this edition of Windows 7.
- **Windows 7 Ultimate** This edition of Windows 7 supports enterprise features such as Domain Join, EFS, Remote Desktop Host, AppLocker, DirectAccess, BitLocker Drive Encryption, BranchCache, and Boot from VHD. You can use Windows 7 Ultimate only with a retail product key.
- **Windows 7 Enterprise** This edition of Windows 7 has support for identical features to the Ultimate edition. The difference between Enterprise and Ultimate is that Enterprise supports only volume licensing and cannot be used with a retail key. The Enterprise edition also includes four licenses for virtualized clients.

### Quick Check

- Which edition of Windows 7 would you choose if you needed to use a retail license key and the BranchCache feature on a computer hardware platform that had 8 GB of RAM?

### Quick Check Answer

- You would choose the x64 version of Windows 7 Ultimate. Windows 7 Ultimate supports use with a retail license key and can also access the BranchCache feature. Only x64 versions of Windows 7 support computer hardware that has more than 4 GB of RAM.

## Windows 7 Virtualization

Only certain editions of Windows 7 can be installed as virtual guests. For example, you can install the Professional, Ultimate, and Enterprise editions of Windows 7 as virtual guests on servers running Hyper-V; you cannot deploy the Starter and Home Premium editions in this manner. The x86 and x64 versions of Windows 7 can be run as virtual clients, although the x64 versions of Windows 7 can be run only as virtual clients in virtualization solutions that support this processor architecture. You learn more about virtualization solutions later in this chapter.

Running Windows 7 Professional or Ultimate virtually consumes a license activation. Windows 7 Enterprise edition works differently from the other two editions in that this edition includes four virtual licenses as a part of its licensing terms. This means that if you deploy a computer running Windows 7 Enterprise and you install virtualization software, you are licensed to run four virtual instances of Windows 7 on that computer. This can be very useful for developers whose testing practices might compromise the operating system environment in a way that requires a clean install. The extra virtual licenses included in the Enterprise edition means that you can provision a virtual machine that you run tests on without consuming an extra operating system license.

#### **MORE INFO SUPPORTED VIRTUAL GUESTS**

To find out more about which operating systems are supported as virtual guests on Hyper-V, consult the following TechNet document: [http://technet.microsoft.com/en-us/library/cc794868\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc794868(WS.10).aspx).

## Virtualization Hosts

Microsoft ships several products that can host virtual guests running the Windows 7 operating system. Software that hosts virtual guests can run on both client and server operating systems. You can also deploy the Windows 7 operating system as a virtual client on virtualization host products that are available from third-party vendors. These are the virtualization host products available from Microsoft:

- **Virtual PC 2007** Runs on previous Windows client operating systems. Virtual PC 2007 supports only x86 versions of Windows 7.
- **Windows Virtual PC** Can be installed on Windows 7. Windows Virtual PC is limited to running x86 versions of Windows 7.
- **Virtual Server 2005 R2** Can host x86 and x64 versions of Windows 7. Virtual Server 2005 R2 can be run on Windows Server 2003, Windows Server 2008, and the Windows XP operating systems.
- **Hyper-V** A role service that you can run only on x64 versions of Windows Server 2008. Hyper-V is the platform most commonly used to host virtual machines on networks in which third-party virtualization host solutions have not been deployed.

Because Hyper-V functions only on x64 versions of Windows Server 2008 and Windows Server 2008 R2, Hyper-V can be reliably used to deploy all versions of the Windows 7 operating system. On Windows Server 2008 R2, you can install the Remote Desktop Virtualization Host role service. This service allows users to connect to a Remote Desktop Server that also holds the Hyper-V role, allowing users to connect to virtual machines hosted on the Hyper-V server.

### MORE INFO REMOTE DESKTOP VIRTUALIZATION HOST

To learn more about Remote Desktop Virtualization Host, consult the following page on TechNet: <http://technet.microsoft.com/en-us/library/dd759170.aspx>.

## Boot from VHD

The Enterprise and Ultimate editions of Windows 7, as well as all editions of Windows Server 2008 R2, can be configured to boot from a virtual hard disk file (VHD). The VHD file is stored on the hard disk as a normal file, and the deployed operating system is contained within this file. In essence, the VHD file serves as a container located on the hard disk. The benefit of deploying an operating system to a container is that the container can be moved to another platform if you need to move it. For example, to transfer a fully deployed computer from one host to another, boot using the Windows PE environment and copy the VHD file to a new location. The only step required to prepare the new location is to edit the boot configuration file to point to the operating system on the VHD. You perform the task of boot environment configuration in the practice exercise at the end of this lesson.

Another benefit of deploying to VHD rather than consuming an entire disk partition with an installation of Windows 7 is that it simplifies the process of deploying Windows 7 in a multiple operating system boot configuration. For example, you could configure two VHD files, one of which is configured and optimized to run one set of applications, and another that you have configured and optimized to run a separate set of applications.

You can create VHD files using the Diskpart.exe utility and through the Create And Attach Virtual Hard Disk dialog box available from the Disk Management Console. This dialog box is shown in Figure 2-2. When you create a VHD on a hard disk that you intend to use as the host for an operating system, you choose between dynamically expanding and fixed-size disk types. A dynamically expanding virtual hard disk increases size as needed until it consumes the volume that hosts it. Dynamically expanding virtual hard disks become increasingly fragmented over time. Fixed-size disks use a fixed amount of space and are less likely to become fragmented, which increases overall performance. The drawback to fixed-size disks is that you cannot expand them if the need arises. It is also possible to use Diskpart.exe to configure a boot from VHD on differencing disks. Differencing disks allow you to discard changes to the operating system at a later time.

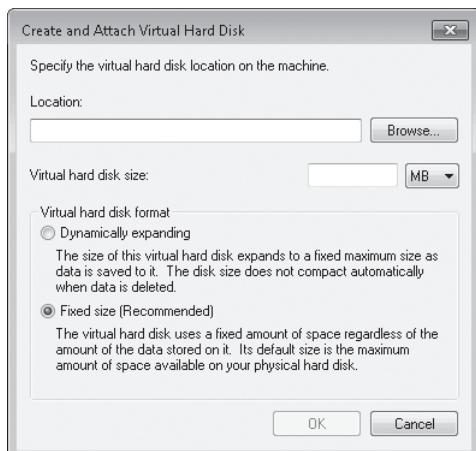


FIGURE 2-2 Creating and attaching VHD

You can deploy an operating system to an existing VHD file using the traditional installation method or by mounting the VHD file and using the ImageX.exe utility to apply an image to the VHD file. You use this second method in the practice exercise at the end of this lesson. You can also obtain a utility that converts files in Windows Imaging Format (WIM) directly to VHD files, although Microsoft does not directly support this method.

#### **MORE INFO WIM TO VHD CONVERTER**

To learn more about the WIM to VHD converter, consult the following page on MSDN:  
<http://code.msdn.microsoft.com/wim2vhd>.

You can deploy fully prepared VHD files from Windows Deployment Services running on computers with the Windows Server 2008 R2 operating system. This allows VHD files to be deployed directly to hard disk drives through a multicast transmission.

A native VHD boot has the following limitations:

- Can be used only for Enterprise and Ultimate editions of Windows 7 and Windows Server 2008 R2.
- A maximum of 512 VHD files can be attached concurrently.
- Operating system hibernation is not supported, although sleep mode is supported.
- VHD files cannot be nested.
- BitLocker cannot be used to encrypt the host volume used for native VHD boot. BitLocker cannot be used on volumes hosted inside a VHD.
- The parent volume of the VHD cannot be configured as a dynamic disk.
- The attached VHD volume cannot be configured as a dynamic disk.

#### **MORE INFO** **BOOT FROM VHD**

To learn more about configuring Windows 7 to boot from VHD, consult the following document on TechNet: [http://technet.microsoft.com/en-us/library/dd799282\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd799282(WS.10).aspx).



#### **EXAM TIP**

Remember which editions of Windows 7 can use the boot from VHD functionality. Remember which edition of Windows 7 includes four virtual licenses.

### **PRACTICE** **Preparing Boot from VHD**

You can install the Windows 7 operating system so that it boots from a VHD file that is installed on physical hardware. This method has a benefit of making the operating system more portable.

#### **EXERCISE 1** **Preparing for and Installing a VHD Boot**

In this exercise, you prepare a computer for a VHD installation of Windows 7. Only the Enterprise and Ultimate editions of Windows 7 allow you to perform an installation to a VHD file on physical hardware. To perform this practice, ensure that your computer running Windows 7 has at least 20 GB of free hard disk space. You need to have access to ImageX.exe, which is part of the Windows AIK tools, to complete this practice.

1. Log on to computer WKSTN1.
2. Open an elevated command prompt and copy the file Install.wim, which is located in the sources directory of the Windows 7 installation media to the directory c:\wim-store. Also, copy the ImageX.exe utility from the Windows AIK directory to the c:\wim-store folder.
3. Start diskpart by entering the command **diskpart**.

- At the diskpart prompt, type **list disk** to list the current disks on the computer.
- At the diskpart prompt, type **create vdisk file=c:\win7vhd.vhd maximum=20000 type=fixed**.
- At the diskpart prompt, type **select vdisk file=c:\win7vhd.vhd**.
- At the diskpart prompt, type **attach vdisk**, which attaches the selected disk.
- At the diskpart prompt, type **list disk** to verify that the disk has been created. On your screen, you should see something like the text shown in Figure 2-3.

```

Administrator: Command Prompt - diskpart
Microsoft DiskPart version 6.1.7600

DISK      - Shift the focus to a disk. For example, SELECT DISK.
PARTITION - Shift the focus to a partition. For example, SELECT PARTITION.
VOLUME   - Shift the focus to a volume. For example, SELECT VOLUME.
UDISK    - Shift the focus to a virtual disk. For example, SELECT UDISK.

DISKPART> select vdisk file=c:\win7vhd.vhd
DiskPart successfully selected the virtual disk file.

DISKPART> attach vdisk
100 percent completed
DiskPart successfully attached the virtual disk file.

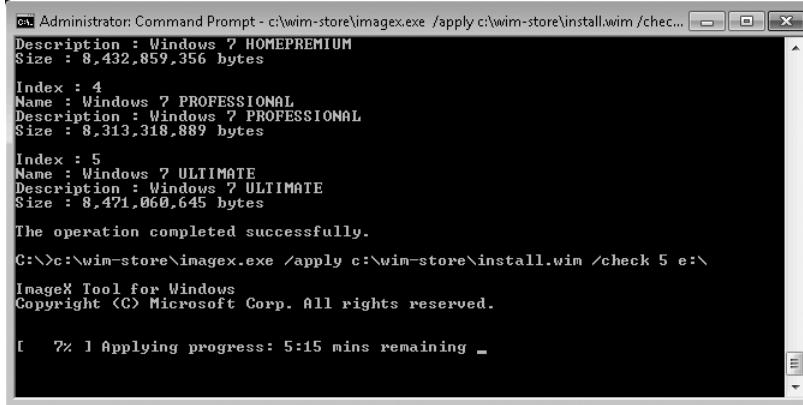
DISKPART> list disk
Disk ###  Status     Size     Free     Dyn  Gpt
* Disk 0  Online    126 GB   0 B
* Disk 1  Online     19 GB   19 GB

DISKPART>

```

**FIGURE 2-3** Verifying VHD

- Select the disk that you created using the **select disk X** command where X is the identifier of the newly created virtual hard disk.
- Issue the **create partition primary** command to create a partition on the selected virtual hard disk.
- Issue the **select partition 1** command to select the partition, and then issue the **active** command to mark the partition as active.
- Issue the command **format fs=ntfs quick**. When this command completes execution, issue the command **assign**. A pop-up window that details the drive letter assigned to the VHD file is displayed. Close this dialog box, and then in the command prompt, type **exit** to leave the diskpart utility.
- Use the command **dism.exe /get-wiminfo /wimfile:c:\wim-store\install.wim** to determine the index assigned to the Windows 7 Ultimate or Windows 7 Enterprise operating system file image.
- Use the command **c:\wim-store\imagex.exe /apply c:\wim-store\install.wim /check X e:\** where e:\ is the volume address label that was assigned to the VHD file when you used diskpart in step 12, and X is the index number of the operating system you discovered in step 13, as shown in Figure 2-4.



```
Administrator: Command Prompt - c:\wim-store\imagex.exe /apply c:\wim-store\install.wim /check 5 e:\
Description : Windows 7 HOMEPREMIUM
Size : 8,432,859,356 bytes

Index : 4
Name : Windows 7 PROFESSIONAL
Description : Windows 7 PROFESSIONAL
Size : 8,313,318,889 bytes

Index : 5
Name : Windows 7 ULTIMATE
Description : Windows 7 ULTIMATE
Size : 8,471,060,645 bytes

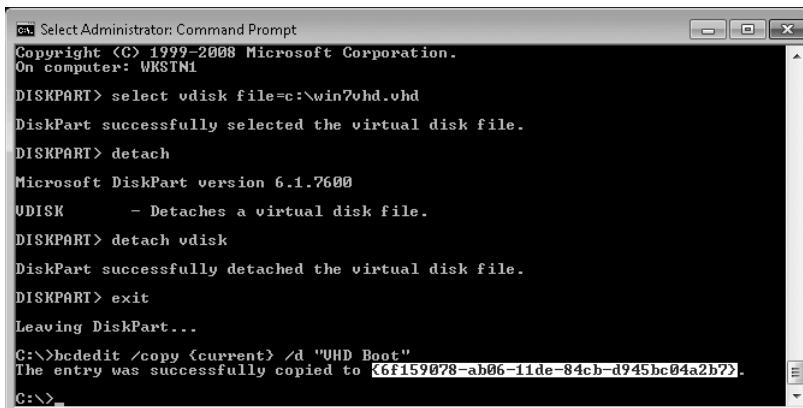
The operation completed successfully.

C:>c:\wim-store\imagex.exe /apply c:\wim-store\install.wim /check 5 e:\
ImageX Tool for Windows
Copyright <C> Microsoft Corp. All rights reserved.

[ 7% Applying progress: 5:15 mins remaining ]
```

FIGURE 2-4 Applying the image to the VHD

15. Enter the command **diskpart** to start the diskpart utility.
16. Enter the command **select vdisk file=c:\win7vhd.vhd**, and when this command completes, enter the command **detach vdisk**. This detaches the virtual disk from the drive where you applied it. Type **exit** to leave the diskpart utility.
17. Create a copy of the current boot loader entry by entering the command **bcdedit /copy {current} /d "VHD Boot"**. Make a note of the GUID that is generated, as highlighted in Figure 2-5. You should use the command prompt's ability to mark and copy text to copy this to the buffer.



```
Administrator: Command Prompt
Copyright <C> 1999-2008 Microsoft Corporation.
On computer: WKSTN1

DISKPART> select vdisk file=c:\win7vhd.vhd
DiskPart successfully selected the virtual disk file.

DISKPART> detach
UDISK      - Detaches a virtual disk file.

DISKPART> detach vdisk
DiskPart successfully detached the virtual disk file.

DISKPART> exit
Leaving DiskPart...
C:>bcdedit /copy {current} /d "VHD Boot"
The entry was successfully copied to {6f159078-ab06-11de-84cb-d945bc04a2b7}.
C:>_
```

FIGURE 2-5 GUID of the new boot entry

18. Enter the command **bcdedit /set {6f159079-ab06-11de-84cb-d945bc04a2b7} device vhd=[c:]\\win7vhd.vhd** where {6f159079-ab06-11de-84cb-d945bc04a2b7} is the unique GUID assigned on your computer.

19. Enter the command **`bcdedit /set {6f159079-ab06-11de-84cb-d945bc04a2b7} osdevice vhd=[c:]\win7vhd.vhd`** where {6f159079-ab06-11de-84cb-d945bc04a2b7} is the unique GUID assigned on your computer. This command differs from the one in step 18 in that you use the *osdevice* parameter instead of the *device* parameter.
20. Enter the command **`bcdedit /set {6f159079-ab06-11de-84cb-d945bc04a2b7} detecthal on`**.
21. Type **`bcdedit /set {6f159079-ab06-11de-84cb-d945bc04a2b7} description "Boot from VHD"`**.
22. You can now reboot into the operating system deployed to the VHD file.

## Lesson Summary

- Windows 7 Professional supports domain join and volume licensing, but does not support the boot from VHD, BranchCache, AppLocker, or DirectAccess features.
- X86 versions of Windows 7 can be installed on x64 hardware, but x64 versions of Windows 7 cannot be installed on x86 hardware.
- X86 versions of Windows 7 can address a maximum of 4 GB of RAM.
- Only the Enterprise and Ultimate editions of Windows 7 support the boot from VHD.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, “Designing a Client Hardware Platform.” The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE** ANSWERS

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

1. Which of the following editions allow you to use KMS activation and can be installed to a VHD file during a physical deployment?
  - A. Windows 7 Home Premium
  - B. Windows 7 Enterprise
  - C. Windows 7 Ultimate
  - D. Windows 7 Professional

2. What is the maximum number of instances of Windows 7 Enterprise that you can host virtually on a computer running Windows 7 Enterprise without having to purchase additional operating system licenses?

  - A. 2
  - B. 3
  - C. 4
  - D. 5
3. Your organization has recently purchased 15 computers that have 16 GB of RAM. You want to deploy these computers to a branch office location. Because they are located in a branch office, you want to take advantage of the DirectAccess feature. Which of the following versions and editions of Windows 7 should you acquire for these computers while also attempting to minimize licensing costs?

  - A. The x64 version of Windows 7 Enterprise
  - B. The x86 version of Windows 7 Enterprise
  - C. The x64 version of Windows 7 Professional
  - D. The x86 version of Windows 7 Professional
4. You want to allocate 8 GB of memory to a virtual instance of Windows 7 Enterprise edition. Which of the following virtualization hosts support this configuration?  
(Choose all that apply; each answer forms a complete solution.)

  - A. Hyper-V
  - B. Virtual PC 2007
  - C. Virtual Server 2005 R2
  - D. Windows Virtual PC

## Lesson 3: Migrating User Profiles

---

From a user's perspective, a successful migration to Windows 7 means that all of the data that the user relied upon on her old computer is present and available on her new computer. When you have to move only a few users to new computers, you can take time and care to ensure that every bit of data and setting that was present on the previous computer is available to users on their new systems. When you need to move user profile data on several thousand computers, you do not have the time to provide this personal attention to detail. In this lesson, you learn how to automate the collection and migration of important user data. This ensures that that you can move large numbers of users to computers running the Windows 7 operating system, while ensuring that all the files and settings that the users needed from their old systems remain available.

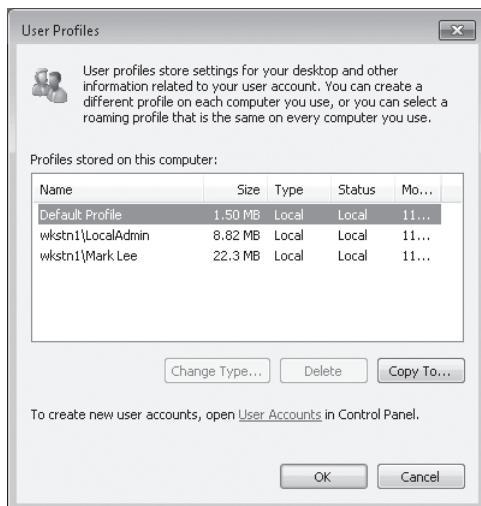
**After this lesson, you will be able to:**

- Determine which data and settings to preserve.
- Choose between local and remote storage.
- Secure migrated data.
- Decide between wipe-and-load or side-by-side migration.

**Estimated lesson time: 40 minutes**

## Understanding Migration Circumstances

Unless your organization uses roaming user profiles, the computer that a person uses probably has important data stored locally. Migrating users from the Windows XP or Windows Vista operating systems to Windows 7, or even migrating them from one computer running Windows 7 to another, means that you must get all important data from one local computer to the next. You can view user profile data by opening the System item within Control Panel and then opening the User Profiles area of the Advanced tab, as shown in Figure 2-6. You can use this tool to copy user profile data to another location, but you cannot use this tool to import user profile data.



**FIGURE 2-6** User profile data

#### **MORE INFO ROAMING USER PROFILES**

To learn more about how to implement Roaming User Profiles in your organization, consult the following TechNet reference: [http://technet.microsoft.com/en-us/library/cc784961\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784961(WS.10).aspx).

#### **MORE INFO CUSTOMIZING USER PROFILES**

To learn more about customizing user profiles in Windows 7, consult the following reference on the Microsoft Web site: <http://support.microsoft.com/kb/973289>.

When you are considering the migration of a large number of users from one platform to another, you must address the following factors:

- Choosing what type of migration you will perform. Will you be migrating users to new computers, a task known as PC replacement, or will you be upgrading their current computers, a task known as a PC refresh?
- Choosing where migrated data will be stored during the migration. If you are moving a large number of users, you may need to use a network migration store. This can cause problems if you are not careful about cataloging the location of each migrated user profile store.
- Choosing an appropriate migration tool. In small migrations, you may choose to use Windows Easy Transfer, a tool built into the Windows 7 operating system. In larger migrations, you are more likely to choose the User State Migration Tool, a tool available as a free download from Microsoft.

If you are moving users of a small number of computers, you should consider using Windows Easy Transfer rather than other tools. Windows Easy Transfer is a utility built into the Windows 7 operating system that allows you to move user profile data from one location to another. The tool is wizard driven, which simplifies use and allows migration of the most common user profile components. You can use Windows Easy Transfer to migrate user profile data from computers running the Windows XP, Windows Vista, and Windows 7 operating system to computers running the Windows 7 operating system. The drawback of Windows Easy Transfer is that you cannot automate the utility, which makes migrating user profile data for a large number of computers prohibitively time consuming.

#### **MORE INFO WINDOWS EASY TRANSFER**

To learn more about the Windows Easy Transfer, consult the following Web page:  
<http://www.microsoft.com/windows/windows-vista/features/easy-transfer.aspx>.

## Choosing a Migration Type

The nature of your task influences the migration type you ought to choose. Depending on whether you are migrating user profile data because you are replacing an existing computer's operating system or because you are moving a user from one computer to another, one type is more suitable than another. These are the two basic types of migration:

- **Wipe-and-load migration** This is appropriate when the current hardware can support a new operating system. Sometimes people refer to this as a PC Refresh scenario. For example, you are deploying the Windows 7 operating system to a group of users whose computers are presently running the Windows XP operating system. In most cases with a wipe-and-load migration, you move user data, format the hard disk drive, and then perform a clean installation of the new operating system, importing the new data after the clean installation completes. You can use the local hard disk as a migration store in a wipe-and-load migration. You can keep the data on the computer during the migration or use a remote store, such as a network location or a removable storage device.
- **Side-by-side migration** This is appropriate when you are replacing the user's current computer with a new computer. People also refer to this type of migration as a PC Replacement scenario. For this type, you need to use an intermediate store for the migrated data that is accessible to both the current and replacement computer. This intermediate store might be a network location or could be a removable storage device.

You can perform an upgrade only when users already have Windows Vista installed on their original computer. Upgrades are possible only across versions of the operating system that support the same processor architecture. For example, you can upgrade an x86 version of Windows Vista to an x86 version of Windows 7, but you cannot upgrade an x86 version of Windows Vista to an x64 version of Windows 7. To transition from an x86 to an x64 edition requires that you perform a migration rather than an upgrade.

### MORE INFO COMMON MIGRATION SCENARIOS

To learn more about common migration scenarios, consult the following article on TechNet:

[http://technet.microsoft.com/en-us/library/dd560802\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560802(WS.10).aspx).



### Quick Check

- What type of migration do you perform when you are replacing people's computers running Windows Vista with computers that will run the Windows 7 operating system?

### Quick Check Answer

- You perform a side-by-side migration when you are replacing a person's computer running Windows Vista with a computer running the Windows 7 operating system.

## User State Migration Tool

The User State Migration Tool (USMT) is a command-line utility that you can use to automate the task of migrating user profiles in wipe-and-replace and side-by-side migrations. USMT is a part of the Windows AIK and is designed to be used in highly automated migration scenarios. USMT migrations occur in two phases: in collecting profile data from the source computer using Scanstate.exe and in importing profile data to the destination computer using Loadstate.exe. In PC Refresh scenarios, the source computer and the destination computer are the same machine.

USMT allows you to capture user accounts, user files and folders (including NTFS permissions), operating system settings, and application settings. You can use USMT to migrate profile data to destination computers running Windows 7 from source computers running the Windows XP, Windows Vista, and Windows 7 operating systems. You cannot use USMT to migrate settings for mapped network drives, local printers, device drivers, local user account passwords, shared folder permissions, and Internet connection sharing settings.

### MORE INFO USER STATE MIGRATION TOOL

To learn more about the User State Migration Tool, consult the following TechNet document:  
[http://technet.microsoft.com/en-us/library/dd560801\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560801(WS.10).aspx).

## Configuring USMT Migration Settings

If you use USMT with basic options, it moves the most common application settings as well as data from folders most commonly used to store documents. Although this selection works in most cases, many organizations use unique local storage configurations and deploy unusual applications. You can configure USMT to migrate data stored from these unique locations and unusual applications by configuring an appropriate XML-formatted configuration files. Here are the XML-formatted configuration files that you can use with USMT:

- **MigUser.xml** This file contains rules about user profiles and user data. The default settings for this file move all data in My Documents, My Video, My Music, My Pictures, desktop files, Start Menu, Quick Launch settings, Favorites, Shared Documents, Shared Video, Shared Music, Shared desktop files, Shared Pictures, Shared Start menu, and Shared Favorites. This file also contains rules to ensure that all the following file types are migrated from fixed volumes: .qdf, .qsd, .qel, .qph, .doc, .dot, .rtf, .mcw, .wps, .scd, .wri, .wpd, .xl\*, .csv, .iqy, .dqy, .oqy, .rqy, .wk\*, .wq1, .slk, .dif, .ppt\*, .pps\*, .pot\*, .sh3, .ch3, .pre, .ppa, .txt, .pst, .one\*, .mpp, .vsd, .vl\*, .or6, .accdb, .mdb, .pub, .xla, .xlb, and .xls. The asterisk (\*) represents zero or more characters.
- **MigDocs.xml** This file contains information about the location of user documents. Use this file if local user documents are stored in nonstandard locations.

- **MigApp.xml** This file contains rules about migrating application settings. These include Accessibility settings, dial-up connections, Favorites, folder options, fonts, group membership, Open Database Connectivity (ODBC) settings, Microsoft Office Outlook Express mailbox files, mouse and keyboard settings, phone and modem options, Remote Access Service (RAS) connection phone book files, regional options, remote access, screen-saver settings, taskbar settings, and wallpaper settings.
- **Config.xml** This file is used to exclude features from the migration. You can create and modify Config.xml using Scanstate.exe with the /genconfig option.

In some situations, there may be files or application settings that are not migrated when you configure the XML files listed in the preceding paragraphs. In these instances, you must create a custom XML file. You can also use custom XML files to reroute folders, specific file types, or specific files. Rerouting is the process by which you move all files of one type that may have been stored in separate places on the source computer to a specific, final location on the destination computer.

#### **MORE INFO CREATING CUSTOM XML FILES**

To learn more about creating custom XML files, consult the following document on TechNet:  
[http://technet.microsoft.com/en-us/library/dd560773\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560773(WS.10).aspx).

## **ScanState**

Scanstate.exe runs on the source computer. If you are running Scanstate.exe from within Windows on computers that have either the Windows Vista or Windows 7 operating system, you must do so from an elevated command prompt. If you are running Scanstate.exe on a computer running the Windows XP operating system, you must be logged on with an account that is a member of the local administrators group.

You can use Scanstate.exe to perform an offline migration of data. An offline migration occurs when you run Scanstate.exe from the Windows PE environment, rather than from a client Windows operating system environment. The benefit of performing an offline migration is that it occurs more quickly than when you perform an online migration. You can configure a special bootable Windows PE image that performs an automatic offline migration. You can also deploy this image using Windows Deployment Services, which allows you to perform automatic offline migrations on a computer from a PXE boot. Although you can use Scanstate.exe in offline mode, you cannot use Loadstate.exe in this manner. You must always run Loadstate.exe from within the Windows client operating system environment.

#### **MORE INFO OFFLINE MIGRATIONS**

To learn more about performing offline migrations using Scanstate.exe, consult the following TechNet Web page: [http://technet.microsoft.com/en-us/library/dd560758\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560758(WS.10).aspx).

Scanstate.exe is a command-line utility. When using Scanstate.exe, you must specify the location in which the migration store will be hosted. The following command creates an encrypted migration store named store123 on the file share named Migration on the file server named Fileserver and uses the files MigApp.xml and MigUser.xml. You encrypt the store using the key mykey:

```
Scanstate \\fileserver\Migration\store123 /i:MigApp.xml /i:MigUsr.xml /o /encrypt /key:"mykey"
```

#### **MORE INFO SCANSTATE**

To learn more about how to use the Scanstate.exe command-line utility, consult the following TechNet document: [http://technet.microsoft.com/en-us/library/dd560781\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560781(WS.10).aspx).

## **LoadState**

You run the Loadstate.exe utility from an elevated command prompt on the destination computer. You should install all applications that were on the source computer on the destination computer prior to running Loadstate.exe. If you install applications on the destination computer after running Loadstate.exe, individual application settings might be overwritten by the new installation.

You need to use the same custom XML files when using the Loadstate.exe utility to restore data if you used custom XML files during the Scanstate.exe process. For example, to load data from the store123 store that you created in the example earlier in this chapter, you would use this command:

```
Loadstate \\fileserver\Migration\store123 /i:MigApp.xml /i:MigUsr.xml /decrypt /key:"mykey"
```

#### **MORE INFO LOADSTATE**

To learn more about how to use the Loadstate.exe command-line utility, consult the following TechNet document: [http://technet.microsoft.com/en-us/library/dd560804\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560804(WS.10).aspx).

## **Selecting a Migration Store**

When you have determined exactly what files and settings you need to migrate from the source computer to the destination computer, you need to determine which type of migration store you will use. Although you can use a removable storage device as a migration store, most administrators do not use this option when they are moving a large number of user profiles. This store type requires the technician performing the migration to attach and detach the device as a part of the migration process. This level of manual intervention can significantly lengthen the migration process when you are dealing with several thousand computers. If you choose to use

a network share as a migration store host, you need to consider the amount of storage space required and the possible impact on network bandwidth of transferring a substantial amount of user profile data to and from the network share as the migration progresses. USMT supports three general migration store types:

- **Uncompressed** This type holds data in a hierarchy of folders that mirror the user profile data that is being transferred. Uncompressed migration stores create a duplicate of the migrated data in a separate location on the original volume, on an attached volume, or on a remote location such as a network share. You can navigate the folder hierarchy using Windows Explorer or the command line. Uncompressed migration stores are not encrypted when created by the Scanstate.exe utility, and they lack the security of other migration store types. When you are moving multiple computers by using uncompressed migration stores on a shared network folder, you need to ensure that each migration store is written to a separate folder location on the store.
- **Compressed** This type writes all migration data to a single compressed file. You can encrypt this file. You can extract the data located in this file using the Loadstate.exe utility. When you move data for multiple computers by using compressed migration stores, ensure that the resulting migration store has a unique name that allows you to tie it back to the computer that you migrated from.
- **Hard-link** You can use hard-link migration stores only in wipe-and-load migrations. The hard-link migration store allows files to be stored on the local computer while the old operating system is removed entirely and a new operating system is installed. Hard-link migrations do not create a duplicate of the migrated profile data and use less space than an uncompressed or compressed migration store. You cannot use a hard-link migration store when you are using a network share as a storage location.

You should consider the security of uncompressed and compressed migration stores that are located on shared network folders. If the security of user profile data is a concern during a migration, you should use a compressed migration store with encryption. This method minimizes the risk that unauthorized third parties are able to access user profile data during the migration process. You configure an encrypted migration store in the practice exercise at the end of this lesson.

## Estimating Storage Requirements

You can use Scanstate.exe to determine the amount of space required for each storage type on a computer given a specific set of migration rules. This can be useful when you are planning a migration and you do not know how much data actually has to be stored. The migration report is written in XML format. You can open the report for review using Windows Internet Explorer, as shown in Figure 2-7.

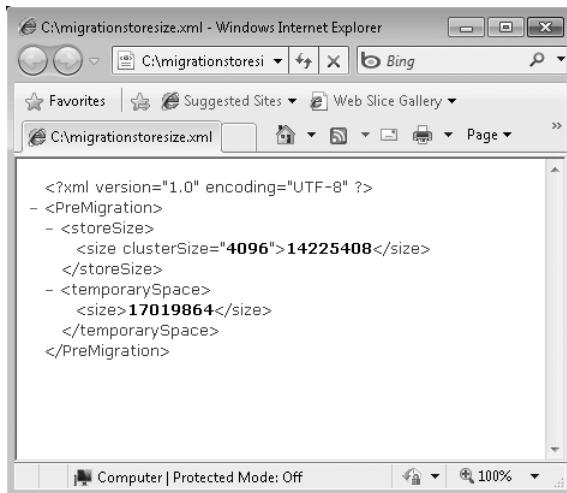


FIGURE 2-7 Migration store report

You run the following command to generate an estimate of the migration store size:

```
Scanstate.exe c:\migrationstore /o /p:"C:\migrationstoresize.xml"
```

## PRACTICE Using USMT

USMT allows you to automate the process of migrating user profile data. In this set of practice exercises, you perform several steps that you would perform with USMT when preparing to migrate profile data. These include creating an estimate of the size of the migration store, creating a custom XML file that has the location of any nonstandard document directories and then creating an encrypted migration store.

### EXERCISE 1 Creating an Estimate of the Migration Store Type

Prior to performing this practice exercise, ensure that the Windows Automated Installation Kit is already installed on WKSTN1. To complete this exercise, follow these steps:

1. Log on to computer wkstn1 with the Mark Lee user account.
2. Create the directories c:\mig-store, c:\mig-reports, and c:\usmt.
3. Depending on whether your Windows 7 installation is x86 or x64, copy the contents of the c:\Program Files\Windows AIK\Tools\USMT\x86 or c:\Program Files\Windows AIK\Tools\USMT\amd64 directories to the c:\usmt directory.
4. Run the following command to generate an estimate of the migration store size:

```
C:\USMT\scanstate.exe c:\mig-reports /p:"c:\mig-reports\MigrationStoreSize.xml"
```

5. Use Internet Explorer to open the file c:\mig-reports\MigrationStoreSize.xml.
6. Run the following command to create an encrypted store:  

```
C:\usmt\scanstate c:\mig-store /encrypt /key:"Pa$$w0rd"
```
7. Verify that the migration store has been created in the c:\mig-store directory.

## Lesson Summary

- The User State Migration Tool can be automated to migrate profile data.
- The process of replacing the operating system on a computer is known as a PC Refresh scenario or as a wipe-and-load migration. You can use a hard-link migration store during this type of migration if you want to minimize the use of disk space.
- The process of replacing an old computer with a new computer is called a PC Replacement scenario or side-by-side migration. You cannot use a hard-link migration store for this type of migration.
- Scanstate.exe is run on the source computer. Loadstate.exe is run on the destination computer.
- USMT uses XML configuration files such as MigUser.xml, MigApp.xml, and MigDocs.xml to control which data is migrated from the source computer to the destination computer.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 3, "Migrating User Profiles." 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. Your organization has just purchased 400 new computers and you need to move user data from 400 existing installations in a side-by-side migration. These computers run a mix of Windows 2000 Professional, Windows XP Professional, Windows Vista, and the Windows 7 operating systems. You want to extract data from as many computers as possible by performing an offline migration with the User State Migration Tool. Which of these operating systems support this type of migration? (Choose all that apply; each answer forms a complete solution.)
  - A. Windows 7
  - B. Windows XP Professional
  - C. Windows Vista
  - D. Windows 2000 Professional

2. Which of the following XML files do you modify to specify information about a custom user documents folder when you use the User State Migration Tool?
  - A. MigApp.xml
  - B. Config.xml
  - C. MigUser.xml
  - D. MigDocs.xml
3. Which of the following migration store types support encryption when you use Scanstate.exe?
  - A. Hard-link migration
  - B. Uncompressed Remote Store
  - C. Compressed Remote Store
  - D. Uncompressed Local Store
4. Which of the following migration store types should you use when you have to perform a wipe-and-load migration on a large number of computers, you want to ensure that no data is transferred from the computers, and that a minimum amount of disk space is used?
  - A. Compressed remote store
  - B. Uncompressed local store
  - C. Hard-link migration store
  - D. Compressed local store

## Chapter Review

---

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

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

## Chapter Summary

- Volume activation allows organizations with large operating system deployments to use multiple activation keys and key management services servers to simplify the process of activating computers.
- x86 versions of Windows 7 support a maximum of 4 GB of RAM.
- Windows 7 Enterprise and Ultimate editions support boot from VHD.
- You can use the User State Migration Tool to automate the user profile migration process through XML configuration files.

## 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.

- Activation
- Hard-link
- KMS
- MAK

## Case Scenarios

In the following case scenarios, you apply what you've learned about subjects of this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Branch Office and Head Office Activation

Your organization has a volume license agreement with Microsoft. You will be deploying Windows 7 to 200 clients at your organization's head office. You will be deploying between 15 and 20 clients on isolated networks at 11 separate branch offices. You want to minimize the amount of administrative effort required. With these facts in mind, answer the following questions:

1. Which editions of Windows 7 can you deploy at Contoso as a part of your volume license agreement with Microsoft?
2. Which activation solution should you use at your head office site?
3. Which activation solution should you use for the clients located on isolated branch office networks?

### Case Scenario 2: Migrating Users to Virtual Machines

Your organization has a large number of people using computers that have the Windows XP Professional operating system. Rather than migrate all these users to new computers running the Windows 7 Enterprise operating system, you have decided to migrate users to Windows 7 virtual machines hosted on a server running Hyper-V. During the migration, you want to ensure

that user profile data is stored on a network share as a single encrypted file. You should be able to create this file with the User State Migration Tool and not use any additional utilities. You want to apply AppLocker policies to secure application execution on the virtual machines. You also want to use KMS to activate the virtual machines. With these facts in mind, answer the following questions:

1. Which edition of Windows 7 should you choose to be hosted on the Hyper-V server?
2. What type of migration should you use to move data off computers running Windows XP Professional so that it can be imported into virtual machines running Windows 7?
3. What is the name of the command-line utility you should use to import data from the encrypted migration store to the Windows 7 virtual machines?

## Suggested Practices

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

### Plan and Manage Client Licensing and Activation

You should complete this practice if your computer is connected to the Internet.

- **Practice 1** Download and install the Volume Activation Management Tool.
- **Practice 2** Use the Volume Activation Management Tool to scan a group of computers by IP address range.

### Plan and Manage a Physical Hardware and Virtualization Strategy

Perform this exercise if your computer is connected to the Internet and you have access to a computer running Windows 7 Enterprise or Ultimate on physical hardware.

- **Practice 1** Download and install Windows Virtual PC on a computer running Windows 7 Enterprise or Ultimate on physical hardware.
- **Practice 2** Install a virtualized copy of Windows 7 under Windows Virtual PC. Make note of which versions of Windows 7 you can install under Windows Virtual PC.

### Design a User State Migration Strategy

Perform these practices if you have downloaded the Windows Automated Installation Kit and have access to a separate computer.

- **Practice 1** Use the Scanstate.exe utility to create a custom XML file that includes documents located in nonstandard directories.
- **Practice 2** Use the Loadstate.exe utility to import migration data generated in the practice exercise at the end of Lesson 3 on to a second computer running the Windows 7 operating system.

## 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 70-686 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.

# Creating and Managing System Images

System images are the heart of the Windows 7 workstation deployment process. Whether you are aware of it or not, all Windows 7 installations use a system image as the source for the operating system files. When designing a mass Windows 7 deployment, desktop administrators typically generate their own system images, modifying them as needed throughout their life cycle. The process of creating and managing system images, like all elements of a deployment, is one that requires careful planning and a good strategy. Lesson 1 examines the benefits of file-based images and various strategies for creating them. Lesson 2 discusses how to modify offline images after you have created them.

## Exam objectives in this chapter:

- Design an image creation strategy.
- Design a custom image.
- Define an image update strategy.

## Lessons in this chapter:

- Lesson 1: Designing an Image Creation Strategy **77**
- Lesson 2: Customizing and Updating Images **99**

## Before You Begin

Although this training kit is dedicated largely to the process of deploying Windows 7, most of the tools involved in the deployment process can run on other operating systems as well.

To install and run Windows 7 Automated Installation Kit and Microsoft Deployment Toolkit 2010, as described in this chapter, you must have the following:

- A computer running Windows 7 or Windows Server 2008 R2.
- A DVD-ROM burner and appropriate disk burning software.
- A blank DVD-ROM.
- A Windows 7 installation DVD.
- A device driver of any kind, packaged with a Windows Information (.inf) file.



### REAL WORLD

Craig Zacker

Image files have been around for many years, but until relatively recently, all image files were sector-based. A sector-based image contains an exact copy of every bit on the source disk, without consideration for the disk's file system or directory structure. Microsoft and other software developers still use sector-based images (such as .iso files) to distribute operating systems and applications in downloadable form, but you can't easily edit a sector-based image, and when you deploy one onto another hard disk, it overwrites all existing data.

System administrators have long used sector-based images for their own purposes, primarily for disaster recovery applications that enable them to create an exact copy of a computer's hard disk, but also for workstation deployments. However, deploying multiple workstations by using a single sector-based disk image presents several problems, including the need for a uniform hardware configuration and the need to supply each computer with a unique security ID (SID) at some point during the process.

File-based images, such as those that Microsoft now uses for its operating system deployment technologies, address these problems and many others. Because they are modular, you can use a single file-based image to deploy workstations with various applications and language packs. Because they are editable, you can update file-based images with the latest drivers and updates as needed. However, in a large-scale deployment environment, you often need to create and manage dozens—or even hundreds—of image files, and this requires careful strategizing.

## Lesson 1: Designing an Image Creation Strategy

Microsoft supplies Windows 7 desktop administrators with a great many tools to facilitate mass workstation deployments, including the Windows 7 Automated Installation Kit (Windows AIK) and Microsoft Deployment Toolkit (MDT) 2010, as well as extensive documentation to govern the workstation deployment process, such as Microsoft Operations Framework (MOF) 4.0. What these tools cannot provide, however, is a plan for creating image files that is precisely suited to the needs of a particular business and its users. That is something that administrators have to devise for themselves.

To devise a workstation image creation strategy, desktop administrators must understand the properties of image files, as well as the tools and procedures for creating them. However, image creation is not solely a technical process. Administrators must also recognize the needs of the workstation users and the overall economy of the deployment process in terms of storage space, network bandwidth, installation time and effort, and ongoing maintenance and support.

**After this lesson, you will be able to:**

- List the advantages of file-based images.
- Understand the image creation process.
- Design an image creation strategy.
- Understand the properties of thick, thin, and hybrid images.

**Estimated lesson time: 120 minutes**

## Introducing Windows Imaging Files

Beginning with Windows Vista, Microsoft started supplying its operating systems as file-based images in a format called Windows Imaging. Windows Imaging files have a .wim extension and, compared with sector-based images, have some decided advantages, including the following:

- **Single file** A Windows Imaging file is actually a database that can contain all of the installation files for a Windows 7 deployment. When you are performing a workstation installation over the network, transferring a single large Windows Imaging file is inherently more efficient than transferring the hundreds of installation files it contains because the Server Message Blocks (SMB) protocol does not have to open and close each of the transferred files individually.
- **File-based** The smallest data storage unit in a Windows Imaging file is the file, not the sector. This means that Windows Imaging files are independent of the formatted partition on a target disk, unlike sector-based images. To deploy a Windows Imaging file, you must create low-level structures, such as partitions and volumes, on the target disk. Microsoft supplies a command-line tool called Diskpart.exe, which Microsoft deployment systems use to create and format volumes on a disk before they write the contents of a Windows Imaging file to them.

- **Hardware independent** Because they are file-based, Windows Imaging files do not reflect the hardware from which they were created, nor do they impose any hardware restrictions on the target disk, other than sufficient storage space to hold the files contained in the image.
- **Nondestructive** Because Windows Imaging files are independent of low-level disk structures, you can apply an image to an existing volume without wiping the disk clean of its existing data beforehand. Deploying an operating system image to a system disk behaves no differently from individual file copying: new files are added and existing files are overwritten.
- **Multiple images** A single Windows Imaging file can contain multiple images, enabling you to save space and deploy various operating system versions or workstation configurations with a single .wim file. For example, the Install.wim file on a Windows Server 2008 R2 installation disk typically contains images of all four editions of the operating system: Standard, Enterprise, Datacenter, and Web, in both full and server core versions. However, the Windows Imaging file itself is only about two and a half gigabytes (GB) in size, far smaller than the eight individual sets of installation files would be.
- **Compressed** Because they are file-based, Windows Imaging files contain only the actual files on the source medium; they do not contain empty space. Many sector-based imaging formats copy all of the sectors on the source disk, whether they contain any useful data or not. Windows Imaging files also use standard data compression technologies to minimize the size of the file.
- **Single-instance storage** Windows Imaging files store their directory information separately from the files themselves. This enables Windows Imaging to store a single copy of a file and use it for any one of multiple images in that file. Thus, if you have a Windows Imaging file that already contains the Windows 7 Professional installation files, adding Windows 7 Ultimate increases the image only by the size of the files unique to the Ultimate edition. Single-instance storage therefore reduces both the size of the Windows Imaging file and the amount of bandwidth consumed when systems transmit it over the network.
- **Partial captures** When you are capturing an image from a computer's disk, you can choose to exclude specific files, such as memory paging files, which take up space and add no benefit.
- **Spannable** Windows Imaging files can be split into multiple parts, a technique called spanning, which enables administrators to burn them onto multiple CD-ROMs or create smaller files for downloading. The individual parts of a spanned Windows Imaging file have a .swm extension.
- **Bootable** You can create Windows Imaging files that contain a bootable version of the Windows Preinstallation Environment (Windows PE).
- **Mountable** Using ImageX.exe or DISM.exe, you can mount a Windows Imaging file as a volume on any Windows computer, enabling you to view, extract, or update its contents.

- **Editable** Sector-based image files can be edited only at the sector level, irrespective of the files the image contains. Although you can theoretically update a sector-based disk image, the process is extremely complicated, and the most minute error can render the image unusable. However, editing Windows Imaging files, because they are file-based, is a relatively simple matter, enabling administrators to apply the latest operating system updates to existing images, or add applications, language packs, or other software packages.

## Understanding the Image Creation Process

The process of creating a Windows Imaging file consists essentially of taking a snapshot of an existing workstation, often called the reference computer, using a program like ImageX.exe. The program reads the files and configuration settings on the workstation, packages them into a Windows Imaging file, and saves the file to a specified location. Therefore, in its simplest form, the process of creating the image files you will use for the deployment of production workstations consists of the following two steps:

1. Install Windows 7 on a reference computer.
2. Capture an image of the reference computer installation.

As you might imagine, however, the process is often considerably more complicated, especially when you have to deploy a large number of workstations.

In a large enterprise, you are likely to require a number of different workstation configurations—possibly a large number of them. The primary function of deployment tools such as the Windows 7 AIK and MDT 2010 is to prevent administrators from having to perform lengthy and complicated installation and configuration procedures on each workstation. Therefore, an efficient enterprise imaging strategy should enable you to create image files that deploy complete workstation environments with little or no interaction on the client side. The images should contain all of the applications, settings, and other components the workstations need, in addition to the basic operating system.

Here are some of the ways in which the workstations in a large enterprise can differ:

- **Applications** You might have a standard application package that you want to deploy on all of your workstations, such as Microsoft Office 2007, but you are also likely to have users with specific application needs.
- **Hardware** Users requiring specialized hardware might require device drivers, or even full-blown applications, to support that hardware. For example, a workstation with a flatbed scanner requires drivers for the scanner, as well as graphics software that enables the user to operate the scanner.
- **Configuration settings** Different users in the enterprise might require different configuration settings for several reasons. For example, users working with sensitive data might need increased security. In other cases, you might want to deploy some workstations with a highly restrictive, locked-down configuration, while leaving others relatively open.

- **Languages** A corporation with offices in different countries might require workstations supporting various languages. In Windows 7, Microsoft has modularized language support so that instead of requiring multiple versions of the operating system to support different languages, you can use the one core version and install various language packs.
- **Editions** Depending on the licensing strategy your organization uses, you might have to deploy different Windows 7 editions on your workstations. Some computers might need Windows 7 Ultimate, while others can run Windows 7 Professional.

You can design an image-creation strategy using various combinations of the deployment tools that Microsoft provides, depending on how many workstations you have to install, how many image files you have to create, and how much you want to automate the process. Three of the most common methods for creating deployment images, in order of increasing complexity, are described in the following sections.

This chapter is concerned solely with the creation, customization, and management of Windows Imaging files, not with the process of deploying them on target workstations. For more information on the deployment process, see Chapter 6, “Designing a Windows 7 Client Deployment Strategy” and Chapter 7, “Designing Lite-Touch and Zero-Touch Deployments.”

## Manually Creating Images

Working manually, you can perform an individual installation of Windows 7 on a reference computer by using a standard installation DVD; configure it with the applications, features, and settings you want; and then start the reference computer with a Windows PE boot disk and run the ImageX.exe utility from the command line to create a Windows Imaging file.

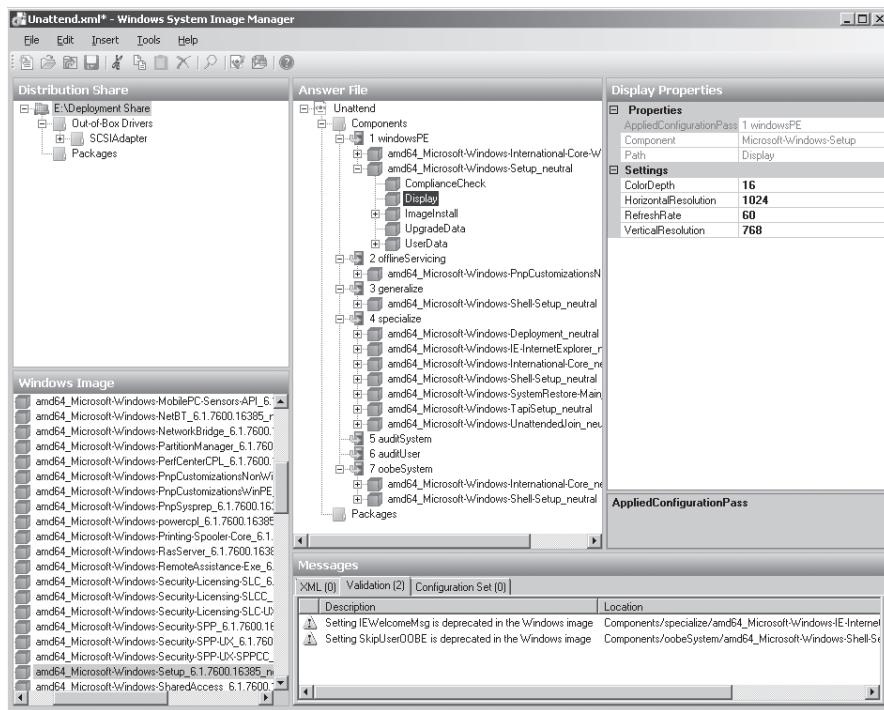
Windows PE and ImageX.exe are both supplied as part of the Windows AIK package. This is a relatively low-tech solution, one that requires the administrator to manually keep track of all the requirements for each workstation configuration. For all but the smallest workstation deployment projects, one of the following two solutions is nearly always preferable.

## Creating Images with the Windows 7 AIK

The ImageX.exe utility that enables you to capture a workstation configuration as a Windows Imaging file is supplied with the Windows 7 Automated Installation Kit. However, the Windows AIK also includes other tools that you can use to automate the image creation process to a greater degree. Although you can vary the procedure in several different ways, the following steps define a basic Windows 7 AIK image creation method:

1. **Create an answer file** An answer file is an XML script file (called Unattend.xml or Autounattend.xml by default) that contains all of the settings that the Windows 7 Setup program uses when installing the operating system. The basic answer file settings specify options such as the location of the Windows 7 image you want to install and how the setup program should partition the workstation’s hard disk. However, you can also use an answer file to configure the Windows 7 environment by supplying values for display settings and many other options, or by adding device drivers and software packages containing updates, service packs, or language packs to the installation.

To create an answer file, you use the Windows System Image Manager (SIM) utility, as shown in Figure 3-1. Windows SIM enables you to define values for all of the configurable settings available in Windows 7, as well as to specify the phase of the installation process in which the setup program should apply each setting.



**FIGURE 3-1** Windows System Image Manager

#### MORE INFO EDITING ANSWER FILES

Prior versions of Windows used plain text answer files (such as `Unattend.txt`), which administrators could easily modify using any text editor. The XML-based answer files that Windows 7 now uses are still text-based, and therefore manually editable, but the format is now complex enough that Microsoft recommends using Windows SIM for all answer file modifications. For complete documentation of the answer file settings available in the Windows SIM interface, see the Windows Automated Installation Kit User's Guide, which is distributed as part of the Windows AIK package.

2. **Install the reference computer** Using a Windows 7 installation DVD, start the reference computer and supply it with the answer file you created on another medium, such as a flash drive. The answer file provides responses to all of the prompts generated by the Windows 7 setup program, enabling the installation to proceed unattended.

- 3. Run Sysprep.exe** After you have installed and configured the reference computer, prepare it for imaging by running the Sysprep.exe utility (installed by default in the \Windows\System32\Sysprep folder) with the */generalize* and */oobe* parameters. The */generalize* parameter removes the computer-specific and user-specific settings from the installation, so you can deploy a single image of the reference computer on multiple target computers. For example, each Windows computer must have a unique security ID (SID). Sysprep removes the reference computer's SID so that it is not duplicated on all of your production workstations. Each target workstation generates its own unique SID when the installation starts. The */oobe* parameter configures the computer to boot to the Windows Welcome screen the next time the computer starts, providing the end user with the appropriate introductory interface.
- 4. Create a bootable Windows PE disk** To create an image of the reference computer, you must boot the system from another disk. The Windows 7 AIK includes a script called Copype.cmd that creates a Windows PE build directory in a folder you specify. After creating this directory and copying the ImageX.exe program into it, use the Oscdimg.exe utility to generate a sector-based image (with an .iso extension) of the Windows PE boot disk. You can then burn this image to a CD-ROM or DVD-ROM.
- 5. Create an image with ImageX.exe** Start the reference computer with the Windows PE disc you created and use the ImageX.exe utility to create an image file in the Windows Imaging format. You can configure ImageX.exe to write the image file to another disk in the computer or to a network share.

#### **MORE INFO USING WINDOWS 7 AUTOMATED INSTALLATION KIT**

For more information on the individual procedures for installing and using the tools in the Windows 7 AIK, see Chapter 2, "Configuring System Images," in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7*.

## **Creating Images with MDT 2010**

For large enterprises that require many different workstation configurations, MDT 2010 provides a more efficient platform for creating and deploying multiple Windows Imaging files. The Deployment Workbench application supplied with MDT 2010 provides a central interface both for the creation of reference computer images and for the deployment of those images to the target workstations.

In MDT, the image creation process consists of the following basic steps:

- 1. Create a build computer** This is the computer on which you install MDT 2010, and which hosts all of the software that will go into the Windows Imaging files, as well as the image files themselves.
- 2. Create a deployment share** Using the Deployment Workbench application included in MDT 2010, you create a deployment share, as shown in Figure 3-2, from which the reference computer and the target workstations can access the software and image files they need. You can create the deployment share on a local disk, a network share, or a stand-alone Distributed File System (DFS) namespace. You should not create the deployment share on a domain-based DFS namespace, however, because Windows PE cannot access them.

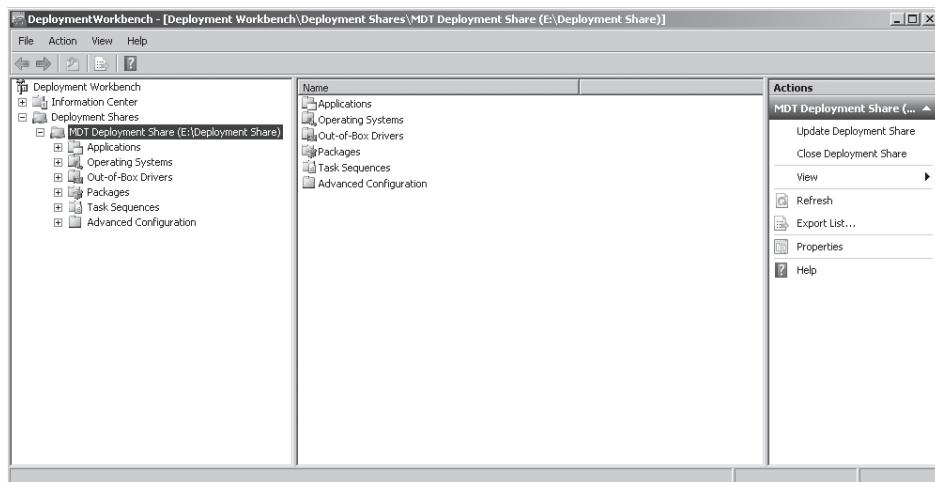
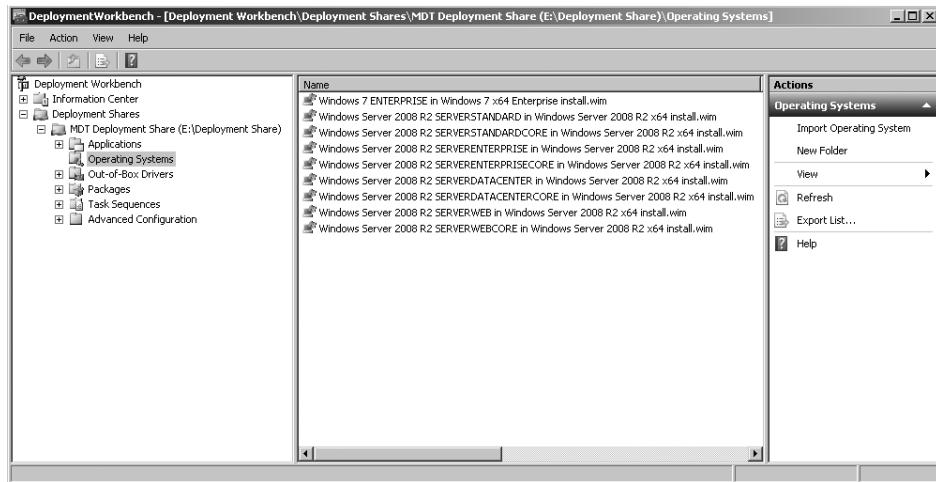


FIGURE 3-2 A deployment share in MDT 2010 Deployment Workbench

#### NOTE NEW TO MDT 2010

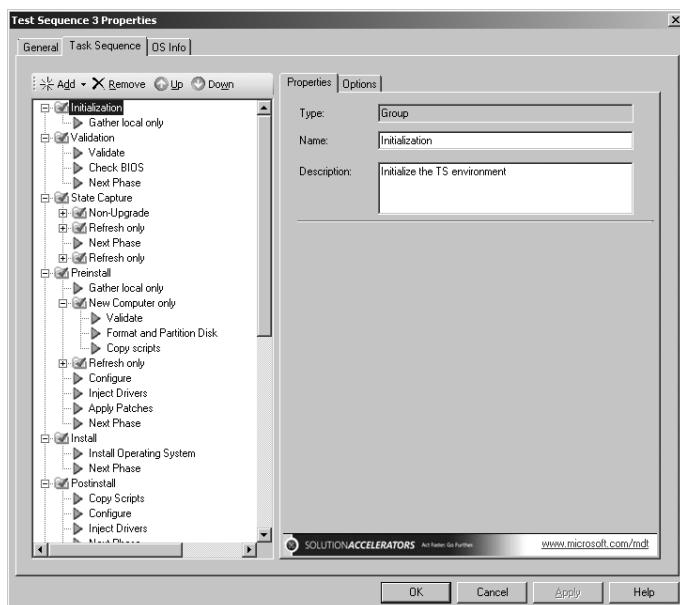
The deployment share in MDT 2010 is a consolidation that replaces the distribution share and the deployment point from MDT 2008.

- 3. Populate the deployment share** Again using Deployment Workbench, you add the operating system versions you want to deploy to the deployment share, as shown in Figure 3-3, as well as all of the other software you want to install on your workstations, including applications, device drivers, language packs, and updates.



**FIGURE 3-3** Operating systems added to a deployment share

4. **Create a task sequence** A task sequence defines the order in which the various steps of a workstation deployment occur. At this stage in the process, you use the interface shown in Figure 3-4 to create a task sequence that installs Windows 7 and all of the other required software components you have added to the deployment share on the reference computer. The task sequence can then capture an image of the installed reference computer, package it as a Windows Imaging file, and save it back to the deployment share.



**FIGURE 3-4** The task sequence editing interface in Deployment Workbench

#### MORE INFO TASK SEQUENCES AND ANSWER FILES

MDT 2010 uses answer files, just as a Windows 7 AIK image deployment does, but it does so invisibly. When you create or edit a task sequence in Deployment Workbench, the program automatically generates an answer file containing the settings that apply to the Windows 7 operating system installation.

5. **Update the deployment share** When you update the deployment share, as shown in Figure 3-5, the Deployment Workbench application packages the software you have provided and creates a Windows PE boot image that you use to start the reference computer and initiate the installation process.

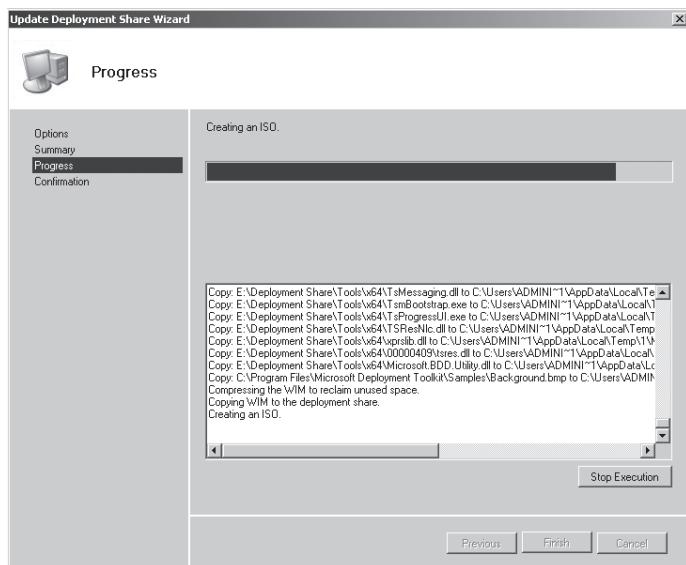
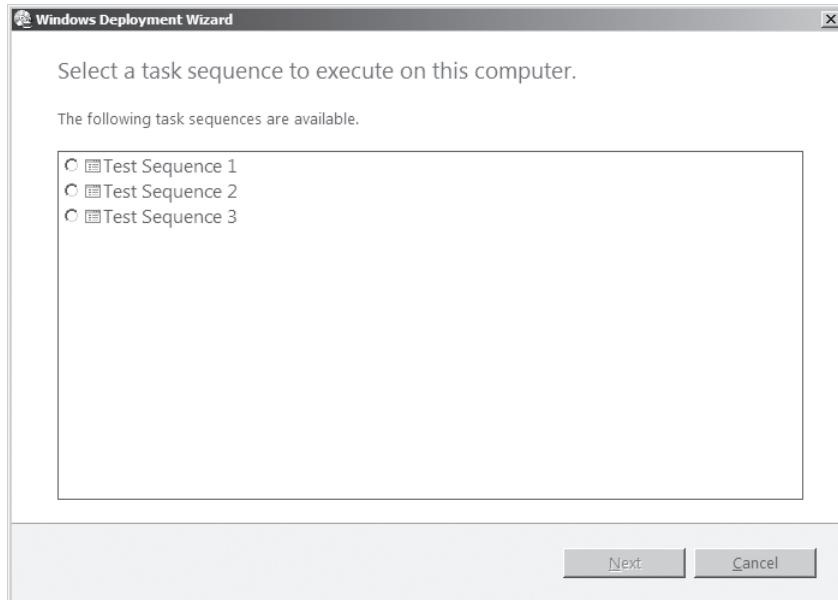


FIGURE 3-5 The Update Deployment Share Wizard

6. **Deploy the boot image to the reference computer** To start the reference computer, you must provide it with the boot image that Deployment Workbench created. You can do this by burning the boot image to a removable medium, such as a DVD-ROM or flash drive, or you can deploy the image by using Windows Deployment Services (WDS).
7. **Run Windows Deployment Wizard on the reference computer** When you start the reference computer by using the boot image, the Windows Deployment Wizard appears, as shown in Figure 3-6, in which you provide credentials for the deployment share, select the task sequence you want to run, and provide the other information required prior to initiating the deployment process.



**FIGURE 3-6** Selecting a task sequence in the Windows Deployment Wizard

- 8. Add the custom image file to the deployment share** After the wizard has completed the deployment to the reference computer, captured an image of the workstation configuration, and saved it to the build computer, you must add that image to the deployment share by using Deployment Workbench before you can use it to install the target workstations on your production network.

#### MORE INFO USING MICROSOFT DEPLOYMENT TOOLKIT 2010

For more information on the individual procedures for installing, configuring, and using MDT 2010, see Chapter 3, “Deploying System Images,” in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7*.

## Building an Image Creation Laboratory

Although the physical process of creating Windows Imaging files is not terribly complicated, the design aspects can be, particularly when it comes to creating task sequences and answer files. As you can see from the interfaces provided in the Windows SIM and Deployment Workbench programs, answer files and task sequences can both support a huge number of options and settings. Administrators also have to concern themselves with the order in which workstations perform the tasks and with the configuration passes in which the setup program applies the answer file settings.

To implement a large-scale image creation strategy, you need a laboratory in which you can experiment with your task sequences and test them in an environment that simulates—or at least resembles—your actual production network. Although it is certainly possible to

construct individual team labs, many organizations dedicate a single lab facility to an entire workstation deployment project, with the various teams sharing space and equipment.

As discussed in Chapter 1, “Preparing to Deploy Windows 7,” the design and the construction of the deployment lab should begin early in the Deliver phase of the workstation life cycle, preferably during the Envision stage. This is because the Deliver team might need the lab facilities to determine whether it is economically feasible to deploy Windows 7 on existing workstations.

The design of the lab will almost certainly be uniquely suited to the organization’s requirements, but to accommodate the image creation, testing, and management processes, it should contain the elements described in the following sections.

## Network

The deployment lab should have an isolated network of its own, preferably using the same local area network (LAN) technologies as the production network. Because Windows Imaging files can be quite large, a wired network running at a speed of at least 100 megabits per second (Mbps) is recommended. If you are planning to deploy image files to workstations at other sites, you might want to consider simulating (or duplicating) the approximate speed of any slower wide area networking (WAN) links involved.

## Computers

Depending on the method you choose for creating images, your lab may require any or all of the following types of computers:

- **Build server** If you plan to use MDT 2010 to create your image files, you need a computer to function as your build server. This is the computer on which you will install MDT 2010 and create your deployment share. The build server can actually be a workstation running Windows 7, Windows Vista, or Windows XP SP2; or a server running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 SP1. The computer should have a large amount of free disk space for the deployment share, preferably on a physical disk separate from the system disk. The amount of space the build server needs depends on the number of images you must create, but 50 GB should be the minimum. The server should also have access to backup equipment, to protect against accidental loss of the deployment share.
- **Reference computer(s)** You require at least one workstation to function as a reference computer, essentially the template from which you will create your Windows Imaging files. If your deployment project involves multiple workstation hardware configurations, you might want to use several reference computers, or modify the hardware configuration of one as needed.
- **Test workstation(s)** Although the deployment process requires its own testing and stabilization regimen, the image creation facilities in the lab must include target workstations on which you can test the functionality of your final images. To provide an accurate simulation, the test workstations should be as identical to your actual production workstations as possible.

## Software

In addition to Windows 7 itself, the image creation lab should include the distribution files for all of the software components your workstations need, including device drivers, updates, service packs, language packs, and all applications. In addition, individual applications might also require their own updates and service packs.

## Infrastructure

In addition to the computers and the network hardware, your image creation network might require any or all of the following services:

- **Domain controller** If you are deploying workstations in an Active Directory Domain Services (AD DS) environment, you should have a domain controller on your lab network as well, although the lab domain should be completely separate from the production domains. You should not use the domain controller as your build server, however.
- **Domain Name System (DNS)** AD DS requires a DNS server to function, so you must have the DNS Server role installed on your domain controller or on another lab network server.
- **Dynamic Host Configuration Protocol (DHCP)** Although you can, using a task sequence or an answer file, configure a workstation with a static IP address during installation, having a DHCP server on the lab network simplifies the workstation configuration process and eliminates one possible source of communication problems during testing.
- **Windows Deployment Services (WDS)** WDS enables bare metal workstations equipped with preboot execution environment (PXE) network adapters to boot from an image supplied by a server on the network, rather than from a local boot device. Although not required, WDS is—for testing purposes, and even for the production deployment—much more convenient than burning Windows PE boot disks and hand carrying them to the workstations.

### MORE INFO USING WINDOWS DEPLOYMENT SERVICES

For more information on installing and configuring Windows Deployment Services, see Chapter 3, “Deploying System Images,” in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7*.

## How Many Images Do I Need?

As mentioned earlier in this chapter, the overall goal of a workstation deployment project is to be able to install and configure client computers with little or no administrative interaction on the workstation itself. The goal of the image creation process, however, is to achieve this primary goal with as few images as is practical. Each image you create for your workstations represents an expenditure of resources, including development and testing time, storage space, network bandwidth, and maintenance effort.

You could create a separate image for each one of your workstations, complete with all applications and user settings, but the process of creating, organizing, storing, and maintaining all of the images for a large enterprise deployment would be monumental. At the other extreme, you could create a single image and use it for all of your workstations.

For some deployment projects, this might actually be practical. If, for example, you were deploying hundreds of identical Windows 7 computers for a large call center, one image could suffice. However, in most cases, a large Windows 7 deployment project requires a number of different workstation configurations, and your image creation strategy should specify how many images you need to support them.

## Defining Core and Supplemental Applications

By the time you begin planning your image creation strategy, you should have functional specifications for your workstations in place. These specifications should include elements such as business requirements, hardware requirements, application requirements, language requirements, and functional roles for the workstation users. Based on this information, you should be able to devise a series of workstation configurations—that is, combinations of hardware, software, and system settings—that satisfy all of the stated requirements.

In many cases, the functional specifications call for a series of core applications on every workstation. This group might include a productivity suite, such as Microsoft Office 2007; security applications, such as antivirus software; and possibly line-of-business applications, such as a client for a company database. Supplemental applications are those that you do not have to install on every workstation. These can include applications that only certain users require, or applications that the organization has licensed for a limited number of users.

In addition to the applications, you might have to deploy device drivers for specialized hardware only installed in certain workstations, additional language packs for users that require them, and updates for the operating system and the applications. Workstations are likely to include various combinations of these software components, and there are various ways in which you can realize them in your image creation strategy.

## Organizing Images

One way of planning and organizing your images is to base them on specific workstation roles. For example, if your organization has administrative assistants in every department, all of whom have similar job descriptions, you might be able to design a single workstation configuration for that role and create an image that provides all of the tools an administrative assistant needs.

However, if workstation requirements in your organization tend to vary more by department, it might be preferable to design one workstation configuration for users in Sales, another for Quality Control, and so forth. Of course, if the requirements demand it, it might be necessary to create more than one image for each role, or for each department. You might even consider combining the two, when necessary, and creating role images for each department.

## Localizing Images

Starting with Windows Vista, Microsoft began making its operating systems language-neutral, meaning that instead of releasing different operating system versions for each language, Microsoft placed all of the language-specific code in separate modules called language packs. To add support for a language to a Windows 7 installation, you simply have to install the correct language pack.

For some multinational organizations, localizing role-specific or departmental images might be as easy as installing an extra language pack. It is up to administrators to decide whether this modification alone is worth creating and maintaining a separate image file. However, if users in other countries working in specific roles or departments have their own unique requirements, administrators might be forced to create separate images for them.

## Understanding Image Types

After you know the elements you need to install and configure on the workstations, the next question is when you are going to install and configure them; this is the heart of the image creation strategy. When you use tools such as the Windows 7 AIK and MDT 2010 to deploy workstations, you always install the core operating system components, but the installation of other software elements during the actual image deployment is optional. You can choose to incorporate these components into your images or install them afterward. The strategy you choose dictates whether you will be creating thick images, thin images, or hybrid images, as described in the following sections.

### Using Thick Images

As mentioned earlier, you can add an application to your MDT 2010 deployment share, install it on your reference computer, and thereby incorporate it into the image file that you deploy to your workstations. When you deploy the image, the target workstation receives the application along with the operating system. The same is true for other software components, including device drivers, updates, and language packs: you can incorporate them all into your images and deploy them along with the operating system.

A system image that includes all of the applications, drivers, updates, and language packs that a workstation needs is called a thick image. Creating thick images for your workstations has several advantages, including the following:

- **Quick development** Incorporating applications and other software components into image files is a relatively simple process that requires little or no custom scripting. This streamlines both the image creation and image testing processes.
- **Simple installation** Because everything the workstation needs is contained in a single image, the deployment process is relatively simple and relatively fast.

- **Heightened security** When you incorporate applications and other software components into an image file, they are available to the workstation immediately upon the installation of the image. In the case of security updates and anti-malware applications, this strategy minimizes the vulnerability of the workstation to attack because there is virtually no period during which the operating system is unprotected. For deployments with stringent security requirements, this can be an important consideration.
- **Self-contained** The deployment process requires no specialized network management infrastructure other than the components provided in the Windows 7 AIK and MDT 2010.

There are also disadvantages to using thick images, such as the following:

- **More images** Using thick images means that you must create, test, and deploy a separate image for each of your workstation configurations. This can substantially lengthen the Develop phase of a workstation deployment project.
- **Larger size** Because thick images include applications and other software components, they are larger in size than thin or hybrid images. Depending on how many and what types of applications you plan to deploy, they can be very much larger. This means that the images require more time to create, more disk space to store, and more network bandwidth during the actual deployment process.
- **Increased maintenance** Thick image files require more maintenance, both because there are more of them and because there are more software components in them. Every time you want to update the operating system, an application, or any other software component, you must modify or recreate every image file that contains that component.

## Using Thin Images

A thin image contains the operating system, but fewer applications or other software components, if any at all. Instead of deploying the applications, updates, device drivers, and language packs with the operating system, administrators deploy them afterward, typically using a software distribution product, such as Systems Center Configuration Manager (SCCM) 2007.

The advantages of creating thin images are as follows:

- **Fewer images** Because thin images are more generic, administrators do not have to create as many of them as they would if using thick images. In some cases, an entire deployment project might require only one image file, containing nothing but the operating system.
- **Smaller size** Because thin images contain the operating system and little else, they are smaller than thick images and therefore require less creation time, less storage space, and less bandwidth during the deployment process. You can also reduce bandwidth utilization during the deployment by using Background Intelligent Transfer Service (BITS) to avoid flooding the network.
- **Simpler maintenance** Thin images require less maintenance, or, if administrators choose to apply all updates after the image deployment, no maintenance at all.

The disadvantages of using thin images consist of the following:

- **More complex installation** Although the thin images themselves are smaller, the deployment's development and testing process can be substantially more complicated because of the scripting that might be required to install the applications and other software components after the image is applied.
- **Requires software distribution infrastructure** Because thin images have a minimal amount of software in the image file, the deployment needs another software distribution mechanism to provide the workstations with the remaining applications, updates, drivers, and language packs. Many organizations use SCCM 2007 for this purpose.
- **Increased security vulnerability** If the thin image does not include security updates and malware protection, the workstation is vulnerable until it receives these components by other means.



### REAL WORLD

Craig Zacker

**W**hen you encounter two theoretical definitions that describe opposite extremes, you can be reasonably sure that in the real world, actual practice falls somewhere between the two. The Microsoft thick image and thin image definitions are, of course, two such extremes, with one including all of the additional software a workstation requires and the other including none of it. In my experience, I've never seen an enterprise deployment project that used either one in its strict definition.

Most workstation deployments that I've seen and participated in include at least some of the workstation's core software requirements in the deployment image file. At the very least, the image includes the operating system's latest service pack and/or critical updates, and in some cases antivirus and other core applications. In no case have I encountered an administrator who thought it worthwhile to create thick images containing all of the supplemental applications that each workstation requires, nor have I ever seen a thin image deployment that used images containing nothing but the operating system. This isn't to say that they don't happen, however, just that I've never seen them.

## Using Hybrid Images

Hybrid images are similar to thick images in that they install all of the applications and other software components the workstation needs, but like thin images, they do not include all of those other components as part of the image file. Instead, they access the additional components from a share on the network. As a result, hybrid images share most of the same advantages of thin images. These are some of the advantages of hybrid images:

- **Smaller size** Hybrid images, like thin images, are relatively small because they do not contain all of the software components the workstation ultimately needs.
- **Less bandwidth** Hybrid images are smaller than thick images, and therefore use less network bandwidth during the actual image download. The workstations still have to download the remaining software components from the network share, but they do so over a longer period of time, lessening the impact on the network.
- **Simpler maintenance** Like thin images, hybrid images require less maintenance than thick images because they have fewer internal components to maintain.
- **Does not require software distribution infrastructure** Although they do have all of the required software components in the image file, hybrid images still install those components during the image deployment, and therefore do not require an external software distribution mechanism such as SCCM 2007.

Most of the disadvantages of using hybrid images are the same as those for the thin images as well, although to a lesser degree. The disadvantages are as follows:

- **Longest installation time** Of the three image types, hybrid images typically take the longest to install, which can be a matter of concern in large-scale deployments.
- **More complex installation** As with thin images, hybrid images can require some scripting to achieve a complete deployment, but their scripting is typically not as complex as that required by thin images.
- **Increased security vulnerability** Like thin images, hybrid images are usually subject to a period of vulnerability between the operating system installation and the installation of security components.

## PRACTICE Creating a Deployment Share

Using Microsoft Deployment Toolkit 2010, you can configure a system to function as a build computer for automated workstation deployments.

### EXERCISE 1 Downloading and Installing the Windows 7 AIK

Microsoft Deployment Toolkit 2010 requires that you install the Windows 7 AIK. Microsoft provides the Windows 7 AIK free of charge from the Microsoft Downloads Center.

1. Open a browser window and, in the address box, type the following URL and press Enter:  
**<http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en>**. The Windows Automated Installation Kit (AIK) for Windows 7 download page appears.
2. Click the Download button and save the KB3AIK\_EN.iso file to a folder on your local drive.
3. Burn the KB3AIK\_EN.iso file to a DVD-ROM and insert the disc into the computer's DVD drive. The Welcome To Windows Automated Installation Kit window appears, as shown in Figure 3-7.

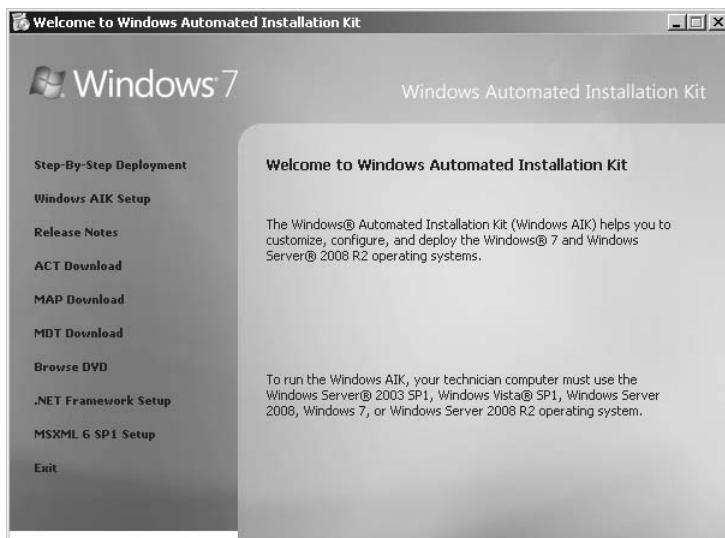


FIGURE 3-7 The Welcome To Windows Automated Installation Kit window

4. Click Windows AIK Setup. The Windows Automated Installation Kit Setup Wizard appears.
5. Complete the wizard, agreeing to the license terms and using the default settings.
6. Click Close to complete the installation process.
7. Close the Welcome To Windows Automated Installation Kit window.

## **EXERCISE 2** Downloading and Installing MDT 2010

Microsoft provides MDT 2010 free of charge, from the Microsoft Download Center.

1. Open a browser window and, in the address box, type the following URL and press Enter:  
**<http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en>**. The Microsoft Deployment Toolkit (MDT) 2010 download page appears.
2. Click the Download button for the MicrosoftDeploymentToolkit2010\_x64.msi or MicrosoftDeploymentToolkit2010\_x86.msi file, depending on the platform of the computer you are using, and save the file to a folder on your local drive.
3. Open Windows Explorer, then locate and run the file you downloaded. The Microsoft Deployment Toolkit 2010 Setup Wizard appears, as shown in Figure 3-8.



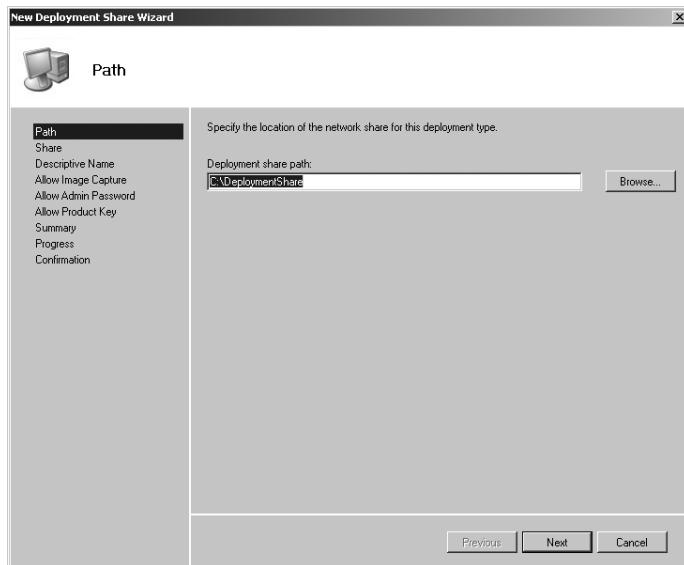
**FIGURE 3-8** The Microsoft Deployment Toolkit 2010 Setup Wizard

4. Complete the wizard, agreeing to the license terms and using the default settings.
5. Click Finish to complete the MDT 2010 setup.

## **EXERCISE 3** Creating a Deployment Share

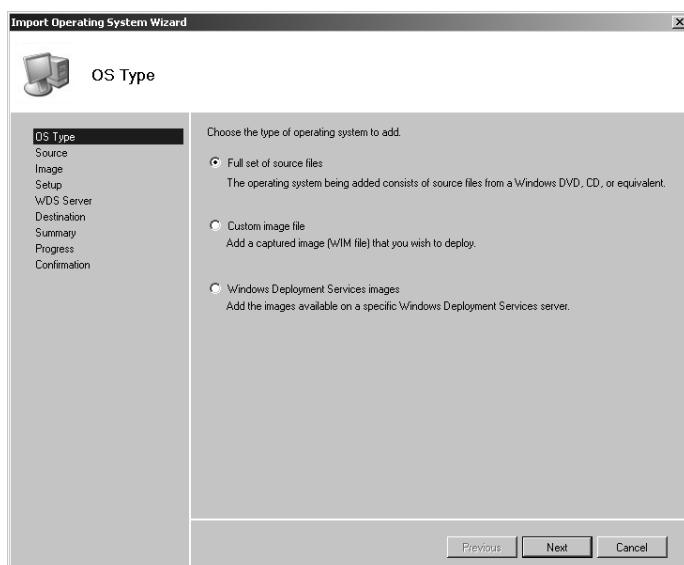
Before you can deploy image files by using MDT 2010, you must create a deployment share and populate it with images.

1. From the Start menu, open the Deployment Workbench under the Microsoft Deployment Toolkit program group. The Deployment Workbench window appears.
2. In the scope (left) pane, double-click Deployment Workbench, then right-click Deployment Shares and, from the context menu, select New Deployment Share. The New Deployment Share Wizard appears, displaying the Path page, as shown in Figure 3-9.



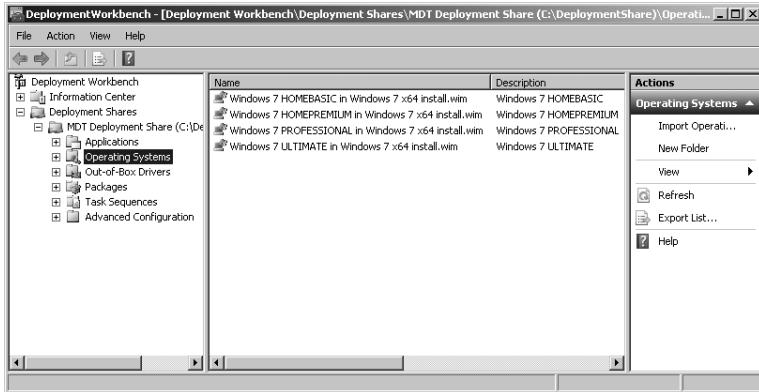
**FIGURE 3-9** The Path page in the New Deployment Share Wizard

3. Click Next seven times to accept the default wizard settings. The wizard creates the deployment share and the Confirmation page appears.
4. Click Finish. The new share appears under Deployment Shares.
5. Expand the MDT Deployment Share node, right-click Operating Systems and, from the context menu, select Import Operating System. The Import Operating System Wizard appears, displaying the OS Type page, as shown in Figure 3-10.



**FIGURE 3-10** The OS Type page in the New Deployment Share Wizard

- Click Next to accept the default OS Type value. The Source page appears.
- Insert the Windows 7 installation DVD into the computer's disc drive. Then click Browse, select the root of the DVD-ROM drive, and click Next. The Destination page appears.
- Click Next to accept the default Destination Directory Name setting. The Summary page appears.
- Click Next to begin importing the operating system image file from the Windows 7 installation disk.
- When the importation process is completed, click Finish. The imported images appear in the Deployment Workbench, as shown in Figure 3-11.



**FIGURE 3-11** Operating system images added to a deployment share

## Lesson Summary

- Windows Imaging files are file-based images, with a .wim extension, which can contain multiple operating system images. Compared with sector-based images, Windows Imaging files are hardware independent, nondestructive, compressed, spannable, bootable, mountable, and editable.
- Large-scale deployment environments require careful strategizing because you often need to create and manage dozens—or even hundreds—of image files. To devise a workstation image creation strategy, desktop administrators must understand the properties of image files, as well as the tools and procedures for creating them.
- An efficient enterprise imaging strategy should enable you to create image files that deploy complete workstation environments with little or no interaction on the client side.
- For large enterprises that require many different workstation configurations, MDT 2010 provides an efficient platform for creating and deploying multiple Windows Imaging files.
- To implement a large-scale image creation strategy, you need a laboratory in which you can experiment with your task sequences and test them in an environment that simulates—or at least resembles—your actual production network.

- A system image that includes all of the applications, drivers, updates, and language packs that a workstation needs is called a thick image.
- A thin image is a system image that contains the operating system, but fewer applications or other software components, if any at all. Instead of deploying the applications, updates, device drivers, and language packs with the operating system, administrators deploy them afterward.
- Hybrid images are similar to thick images in that they install all of the applications and other software components the workstation will need, but like thin images, they do not include all of those other components as part of the image file. Instead, they access the additional components from a share on the network.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Designing an Image Creation Strategy." 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. Microsoft helps Windows 7 desktop administrators design and create Windows Imaging files with two primary support packages: the Windows 7 AIK and MDT 2010. Which of the following tools is not included as part of the Windows 7 AIK?
  - A. Deployment Workbench
  - B. Windows System Image Manager (SIM)
  - C. Sysprep.exe
  - D. ImageX.exe
2. Which of the following lists the three most common methods for creating operating system images, in order of increasing complexity?
  - A. Manual image creation, Microsoft Deployment Toolkit 2010, Windows 7 Automated Installation Kit
  - B. Microsoft Deployment Toolkit 2010, Windows 7 Automated Installation Kit, Manual image creation
  - C. Windows 7 Automated Installation Kit, Manual image creation, Microsoft Deployment Toolkit 2010
  - D. Manual image creation, Windows 7 Automated Installation Kit, Microsoft Deployment Toolkit 2010

3. Which of the following is not a step in a typical Windows 7 AIK image creation process?
  - A. Create an Unattend.xml or Autounattend.xml file.
  - B. Start the reference computer and supply it with the answer file to enable the operating system installation to proceed unattended.
  - C. Prepare the reference computer for imaging by running the Oscdimg.exe utility.
  - D. Start the reference computer with a Windows PE disk and use the ImageX.exe utility to capture a Windows Imaging file.
4. When you are creating a deployment share using the Deployment Workbench application included in MDT 2010, which of the following can you not use as a location for the share?
  - A. A stand-alone DFS namespace
  - B. A domain-based DFS namespace
  - C. A local disk
  - D. A network share
5. Which of the following types of computer is not a required component in a Windows 7 AIK or MDT 2010 workstation image creation lab?
  - A. A domain controller
  - B. A build computer
  - C. A reference computer
  - D. A test workstation

## Lesson 2: Customizing and Updating Images

---

The basic image creation process described in Lesson 1 of this chapter, in which you install and configure a reference computer and then capture an image of that computer for later deployment, is essentially a method of customizing a workstation image. Without this process, you would have to install the core operating system image on each workstation and update it from there, which is exactly what you are doing when you perform a manual installation by inserting a Windows 7 installation DVD into a new computer. By adding applications, updates, device drivers, language packs, and configuration settings to the core operating system, you are taking a generic image and bringing it closer to the functional specification you defined for the workstation. In this lesson, you learn about how to modify images directly, by editing them in place.

**After this lesson, you will be able to:**

- Understand the circumstances under which you might want to update custom image files.
- Understand how to customize images by adding files.
- Select a tool or technique for modifying image files.

**Estimated lesson time: 90 minutes**

## Customizing Images

The reference computer image creation process assumes that administrators have a relatively complex workstation configuration that they want to deploy to a large number of computers. However, this is not always the case. If you have only minor changes to make to the core operating system image, such as applying a few updates or a language pack, it might be easier to modify an image directly while it is offline, rather than deploy it on a reference computer and capture an entirely new image.

Every Windows 7 installation disk includes a Windows Imaging file called `Install.wim`, located in the `Sources` folder, which contains the core images for one or more editions of the operating system. After copying this file to a read/write medium, such as a hard disk, you can use the `ImageX.exe` or Deployment Image Servicing and Management (`DISM.exe`) utility from the Windows 7 AIK to do any or all of the following:

- Add packaged applications
- Add packaged updates
- Add device drivers
- Add language packs
- Enable or disable operating system features
- Append a volume image to a workstation image
- Combine multiple images in a single Windows Imaging file

For more information on using `DISM.exe` to modify offline images, see “Using Deployment Image Servicing and Management,” later in this lesson.

It is up to the individual administrator to decide at what point capturing a new reference computer image becomes preferable to manually customizing an image file. After you have customized an offline image file, you can install it on your target workstations using any of the standard deployment methods.

## Updating Images

Administrators who have already chosen to capture new images from a reference computer installation can still update those image files after creating them. Depending on the size and complexity of your deployment project, you might choose to install your reference computer manually, or use the tools provided in the Windows 7 AIK or MDT 2010. Whichever method you choose, you are essentially configuring a workstation the way you want it and taking a snapshot of it for later use. The image file is your snapshot, which you can copy to any number of other computers as needed.

Of course, workstations are not static; they change over time, and it might become necessary to modify your image files to reflect those changes. As with the initial image creation process, there are several different tools and techniques you can use to do this.

### Why Modify Your Images?

Workstations change, just as people do, and snapshots—your image files—can eventually go out of date. You can choose from several ways to update image files, but first you might question why you should bother. After all, you can, and probably do, update your workstations on a regular basis. Automatic Updates, Windows Server Update Services (WSUS) and System Center Configuration Manager (SCCM) 2007 are all Microsoft products that enable administrators to automate the deployment of operating system updates. With these mechanisms available, why then should you have to update your workstation images?

Security is one reason. Microsoft regularly releases critical updates that address operating system security issues. As time passes and your images are less current, your original workstation configurations could become increasingly vulnerable to attack. When you deploy new workstations, up to a full day might pass before they receive updates from WSUS or SCCM, and intruders might be able to take advantage of this gap in protection.

The update process can also become increasingly long and complex over time. Microsoft releases dozens of operating system updates each year, some of which have their own interdependencies. As your images grow older, they might eventually require literally hundreds of updates, some of which must be installed before the system can install others. It might be days after the initial deployment before WSUS or SCCM brings a new workstation fully up to date.

Finally, your organization's requirements for the workstations might change over time, requiring you to add and remove applications or change configuration settings. If, for example, your organization decides to substitute one application for another, it would become necessary for you to uninstall the old application on each new workstation you deploy and then install the new one. This is not only inconvenient for the administrator, it could also have a negative effect on workstation performance if the old application leaves files, registry settings, or other artifacts of itself behind.

For any of these reasons, you might prefer to modify your workstation images, rather than reconfigure the workstations themselves after deployment.

## Recreating Images

When a snapshot is out of date, you can always shoot another one, and the same is true of your workstation image files. If, after your initial deployment project is completed, you want to modify your base workstation configuration, you can always reconfigure the reference computer and create another image—take another snapshot.

To do this, you can go back to your original reference computer deployment and modify the task sequence or answer file you used to install the reference computer in the first place. Then, you must reinstall the reference computer and capture a new image of it. Of course, this assumes that you still have your original build computer and reference computer(s) in place, waiting to be updated. If you have multiple workstation images to recapture, this method assumes that you are willing to redeploy each of your reference computers and recapture an image of each one. In essence, you would be repeating your entire image creation process over again.

If modifying the original task sequences or answer files seems impractical, you can always consider updating your reference computers manually, or by using standard tools such as WSUS and SCCM, mentioned earlier, and then reimaging them. This strategy would address the problem of applying multiple security updates, as described earlier, but might not be the best solution for uninstalling applications. After all, if uninstalling an old application leaves artifacts behind on the reference computer, you would just be replicating those artifacts in your new image file.

This method too assumes that you still have your reference computers sitting around, waiting to serve as models for your revised image snapshots, and that you are prepared to create and store new versions of every image you created in the first place.

## Modifying the Image Deployment

One possible way to avoid having to recapture new images is to modify the deployment process for your existing images. By modifying the answer files or task sequences you use to deploy your images to your target workstations (not the ones you use to deploy your reference computers), you can install software packages and updates or reconfigure operating system settings almost immediately after the installation of the operating system. This approach reduces the time during which the workstation is vulnerable to attack because of missing updates.

For more information on working with task sequences and answer files, see Chapter 7, "Designing Lite-Touch and Zero-Touch Deployments."

## Modifying Existing Image Files

When faced with changing workstation requirements, you can always recapture new image files or modify the process by which you deploy your existing image files, but you can also modify offline image files themselves. Working with an existing image file is no different from customizing the base image file supplied on a Windows 7 distribution disk. You can use DISM.exe to perform any of the tasks listed earlier, as described later in this lesson.

#### **MORE INFO MODIFYING OFFLINE AND ONLINE IMAGES**

An offline image file is one that is stored on a disk and not currently in use. ImageX.exe and DISM.exe enable you to modify offline images in a variety of ways: by adding and removing files, modifying operating system configuration settings, and appending volume images, for example. An online image is one that is currently in use—that is, the image of the operating system that is active and running on the computer. ImageX.exe and DISM.exe can display information about online images, but the modifications you can make while the image is online are relatively limited.

Assuming that you have properly prepared your reference computer by running the Sysprep.exe tool before capturing your images, you do not need to prepare them again after modifying them with ImageX.exe or DISM.exe. You can proceed to deploy the modified image files in the normal manner.

### **Image Versioning**

When you update your image files manually, you are obliged to keep track of those updates manually as well. If you maintain a large number of workstation images, and update them regularly, it's easy to lose track of which hotfixes you've applied, which configuration settings you've changed, and which drivers you've upgraded. As a result, version control is a critical part of any image update strategy, particularly if you update your images on a regular basis. For a relatively low-tech version control mechanism, you can combine a filenames scheme with a spreadsheet listing the modifications you have applied.

## **Using Image Modification Tools**

You can manually modify offline images using either the DISM.exe or ImageX.exe utility, both of which are included in the Windows 7 AIK. DISM.exe is also included with Windows 7 itself, so you can modify the Install.wim image file included on all Windows 7 installation disks without downloading the Windows 7 AIK. Although the two programs are functionally similar and can perform many of the same image modification tasks, each one has its own syntax, and their commands are not interchangeable.

ImageX.exe has been around since Microsoft first developed the Windows Imaging file format for use with Windows Vista. The Windows 7 AIK uses ImageX.exe to capture workstation images and save them as Windows Imaging files. Because it utilizes the various tools in Windows AIK, MDT 2010 also relies on ImageX.exe to capture images.

Deployment Image Servicing and Management (DISM.exe) is a new program, first released in Windows 7 and the Windows 7 AIK, which replaces the Windows Vista Package Manager (Pkgmgr.exe), PEImg.exe, and Intcfg.exe tools. Although you cannot capture images with DISM.exe, as you can with ImageX.exe, you can modify them in much the same way.

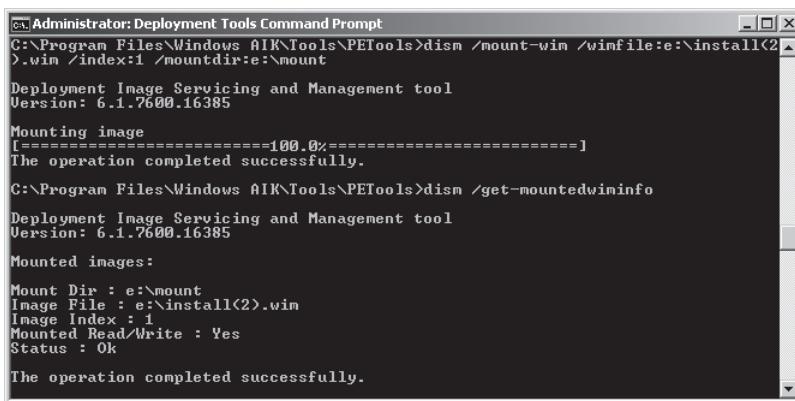


#### EXAM TIP

Although experienced Windows AIK users might be more comfortable using the familiar ImageX.exe syntax on the job, you should be familiar with the functionality of the DISM.exe tool for the 70-686 exam. Microsoft certification exams tend to emphasize the latest tools over the existing ones, even if the older tools have recently been updated to new versions, as is the case with ImageX.exe.

## Mounting Images

Before you can modify an offline image by using either DISM.exe or ImageX.exe, you must mount the image to a folder on a local drive, as shown in Figure 3-12. Mounting an image extracts the component files from the Windows Imaging file and writes them to a folder. If the Windows Imaging file contains multiple operating system images, you must specify the one you want to mount.



```
C:\Administrator: Deployment Tools Command Prompt
C:\Program Files\Windows AIK\Tools\PETools>dism /mount-wim /wimfile:e:\install<2>.wim /index:1 /mountdir:e:\mount
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385

Mounting image
[=====100.0%=====]
The operation completed successfully.

C:\Program Files\Windows AIK\Tools\PETools>dism /get-mountedwiminfo
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385

Mounted images:

Mount Dir : e:\mount
Image File : e:\install<2>.wim
Image Index : 1
Mounted Read/Write : Yes
Status : Ok

The operation completed successfully.
```

FIGURE 3-12 Mounting an image file with DISM.exe

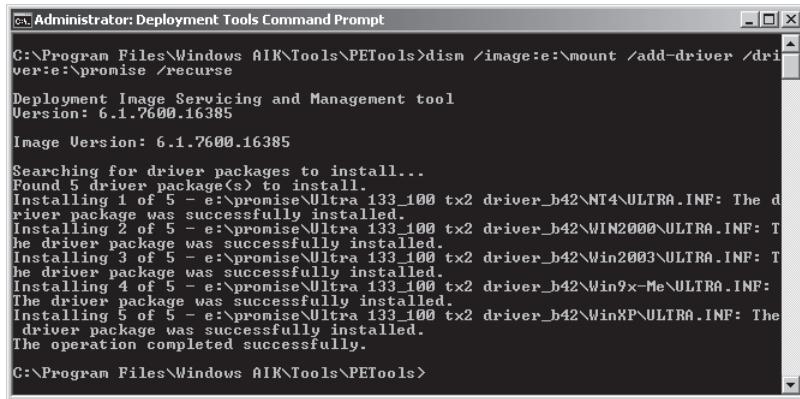
As you apply modifications, you are working on the mounted image. When you are finished, you must unmount the image, which saves the changes you made back to the Windows Imaging file.

#### MORE INFO DISM.EXE AND IMAGEX.EXE SYNTAX

For detailed information on the syntax for modifying image files by using DISM.exe and ImageX.exe, see Chapter 3, “Deploying System Images,” in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7 or the Windows Automated Installation Kit User’s Guide*.

## Adding Device Drivers to Image Files

Adding device drivers is one of the most common modifications administrators can make to offline image files, and using DISM.exe, the process is simple. In earlier versions of the Windows AIK, you had to create an answer file that pointed to the drivers and then use Package manager to apply the answer file to an image mounted using ImageX.exe. With DISM.exe, a single command installs drivers to a mounted image, as shown in Figure 3-13.



```
C:\Administrator: Deployment Tools Command Prompt
C:\Program Files\Windows AIK\Tools\PETools>dism /image:e:\mount /add-driver /driv
er:e:\promise /recurse
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image Version: 6.1.7600.16385
Searching for driver packages to install...
Found 5 driver package(s) to install.
Installing 1 of 5 - e:\promise\Ultra_133_100_tx2\driver_b42\NT4\ULTRA.INF: The d
river package was successfully installed.
Installing 2 of 5 - e:\promise\Ultra_133_100_tx2\driver_b42\WIN2000\ULTRA.INF: T
he driver package was successfully installed.
Installing 3 of 5 - e:\promise\Ultra_133_100_tx2\driver_b42\Win2003\ULTRA.INF: T
he driver package was successfully installed.
Installing 4 of 5 - e:\promise\Ultra_133_100_tx2\driver_b42\Win9x-Me\ULTRA.INF:
The driver package was successfully installed.
Installing 5 of 5 - e:\promise\Ultra_133_100_tx2\driver_b42\WinXP\ULTRA.INF: The
driver package was successfully installed.
The operation completed successfully.

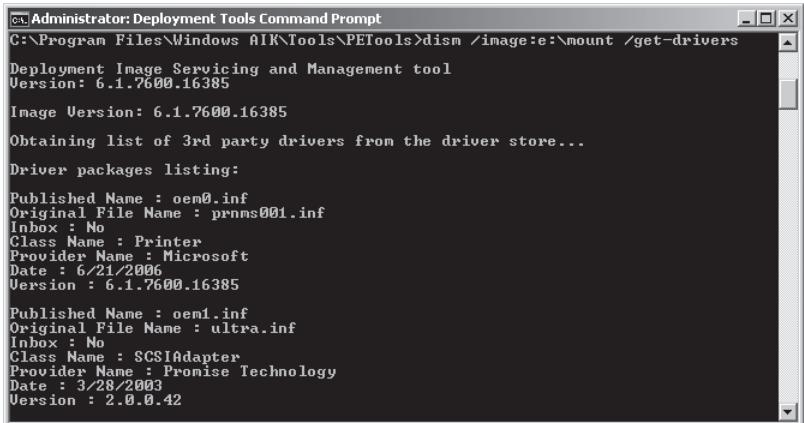
C:\Program Files\Windows AIK\Tools\PETools>
```

FIGURE 3-13 Installing a driver with DISM.exe

### **IMPORTANT** INSTALLING PACKAGED DRIVERS

With DISM.exe, you can use the */Add-Driver* parameter to install only drivers that have a Windows Information file with an .inf extension. You cannot install drivers packaged as Microsoft System Installer (.msi) files or as executable (.exe) files in this manner. You can configure an answer file or a task sequence to install drivers in this form, however.

When DISM.exe installs drivers, it renames them using the file names oem1.inf, oem2.inf, and so on. To remove a driver you have previously installed, you must refer to it on the command line by its new name. To determine the name of the specific driver you want to remove, you can run DISM.exe with the */Get-DriverInfo* parameter, as shown in Figure 3-14. This is a common practice in many DISM.exe image modification procedures. As a result, the program has several of these “Get” parameters that enable you to display information about the currently mounted image.



```
Administrator: Deployment Tools Command Prompt
C:\Program Files\Windows AIK\Tools\PETools>dism /image:e:\mount /get-drivers
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image Version: 6.1.7600.16385
Obtaining list of 3rd party drivers from the driver store...
Driver packages listing:
Published Name : oem0.inf
Original File Name : prnns001.inf
Inbox : No
Class Name : Printer
Provider Name : Microsoft
Date : 6/21/2006
Version : 6.1.7600.16385

Published Name : oem1.inf
Original File Name : ultra.inf
Inbox : No
Class Name : SCSIAdapter
Provider Name : Promise Technology
Date : 3/28/2003
Version : 2.0.0.42
```

FIGURE 3-14 Displaying driver information with DISM.exe

#### **NOTE DISPLAYING ONLINE IMAGE INFORMATION**

As a general rule, you cannot use DISM.exe to add or remove drivers and other software packages from an online image, but you can display information about the current online image by using */Get-DriverInfo* and other similar parameters.



#### **Quick Check**

- DISM.exe has command-line parameters that enable you to view information about Windows Installer applications in the image, but it does not have an */Add-App* parameter. What method can you use to add a new application to an offline image file?

#### **Quick Check Answer**

- The only way to install an application to an offline image file is to add the appropriate commands to an answer file and then apply the answer file to the image by using DISM.exe.

## **Applying Operating System Updates to Image Files**

The process of installing hotfixes, language packs, service packs, and other operating system updates to an offline (or online) image is roughly the same as that of installing drivers. You specify the location of a package file on the command line, and DISM.exe adds it to the image, as shown in Figure 3-15. You can use DISM.exe only to install updates that are packaged as cabinet (.cab) files or Windows Update Stand-alone Installer (.msu) files. As with drivers, you cannot install .msi or .exe files to an offline image from the DISM.exe command line.



```
C:\Administrator: Deployment Tools Command Prompt
C:\Program Files\Windows AIK\Tools\PETools>dism /image:e:\mount /add-package /packagepath:c:\users\windows6.1-kb973540-x64-RC.msu
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image Version: 6.1.7600.16385
Processing 1 of 1 - Adding package c:\users\windows6.1-kb973540-x64-RC.msu
The operation completed successfully.
C:\Program Files\Windows AIK\Tools\PETools>_
```

FIGURE 3-15 Installing a package with DISM.exe

If you specify multiple packages in a single command, DISM.exe installs them in the order you specify them. By default, DISM.exe checks each package you attempt to add to an image, to make sure that it is applicable. The program will not, for example, allow you to add a Windows Server 2008 update to a Windows 7 image. You can override this behavior by running the command with the */IgnoreCheck* parameter.

You can also remove .cab packages you have previously installed to an offline image by using DISM.exe, but after you have installed an .msu package, you cannot remove it from the image by using DISM.exe.

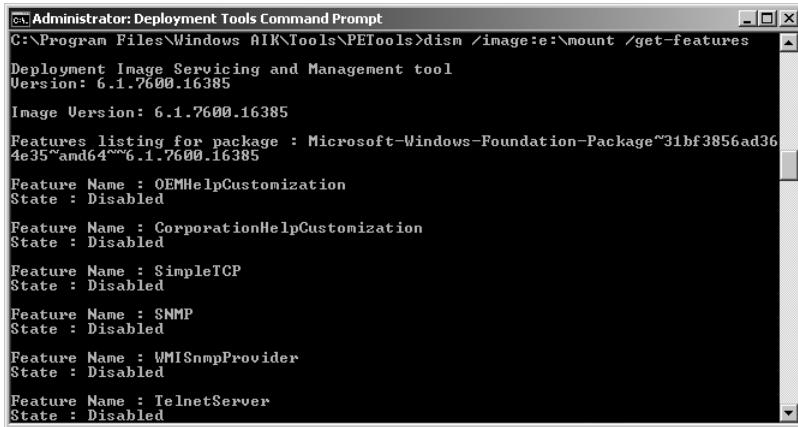
#### NOTE OBTAINING PACKAGES

Most of the update packages that are available from the Microsoft Download Center take the form of executables, with an .exe extension, or sector-based disk images, with an .iso or .img extension. You cannot add these files to an offline image in those forms, but most of them contain .cab or .msu packages inside the archive.

For example, service packs with .exe extensions are actually self-extracting archives. When you execute the file with the */x* parameter from a command prompt, the self-extraction program writes the contents, including a .cab file containing the actual service pack, to a folder you specify. For an .iso or .img disk image, you can either burn the image file to a DVD-ROM or CD-ROM and copy the .cab or .msu files from the disk or you can mount the image file to a drive letter using a third-party utility.

## Configuring Operating System Features

In addition to installing and removing software components, DISM.exe also allows you to enable and disable certain operating system features, whether they are found in a package or in the operating system itself. The `/Get-Features` parameter displays a list of the features in an image, as shown in Figure 3-16, or in a specific package file. Using the feature names specified by this parameter, you can specify the features in the image or package that you want to enable or disable.



```
C:\Administrator: Deployment Tools Command Prompt
C:\Program Files\Windows AIK\Tools\PETools>dism /image:e:\mount /get-features
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image Version: 6.1.7600.16385
Features listing for package : Microsoft-Windows-Foundation-Package~31bf3856ad36
4e35~amd64~~6.1.7600.16385
Feature Name : OEMHelpCustomization
State : Disabled
Feature Name : CorporationHelpCustomization
State : Disabled
Feature Name : SimpleTCP
State : Disabled
Feature Name : SNMP
State : Disabled
Feature Name : WMIISnmpProvider
State : Disabled
Feature Name : TelnetServer
State : Disabled
```

FIGURE 3-16 Listing image features with DISM.exe

## Changing the Interface Language

The need to support multiple languages can complicate the image creation and management process greatly. Depending on your organization's workstation requirements, you might have to create and maintain separate configurations for users in various countries. However, in many cases, administrators can use the same configurations, simply changing the language as needed. DISM.exe enables you to manage these language requirements offline, so you can capture a single image for each workstation configuration, and then make copies that use different interface languages.

To modify the interface language of an offline image, you must first install the appropriate language pack and then activate the language by modifying the operating system's international settings. When referencing languages on the DISM.exe command line, you must use the standard Microsoft language abbreviations, such as *fr-FR* for French, *en-EN* for English, *de-DE* for German (*Deutsch*), and so forth.

Microsoft typically supplies language packs in groups, which it packages as sector-based disk image files. Each disk contains the .cab files for a number of languages. After burning the image to a disk or mounting it to a drive, you can select the .cab files you need and install them to your offline image by using DISM.exe in the usual manner.

#### **BEST PRACTICES ORGANIZING LOCALIZED IMAGES**

Some administrators prefer to install all of the language packs they need to an image, and then make a copy in which they activate each separate language. Others make copies of the image first, apply only one language pack to each copy, and then activate that language.

## Applying Answer File Settings

Packages that have dependencies can pose problems when you attempt to apply them to offline images. Even if you specify the packages in the correct order on the command line, or add them using separate DISM.exe commands, you cannot be certain that, when the image goes live, the system will fully install one package before it installs other packages that depend on it. For this reason, when you have multiple packages to install that are dependent on each other, Microsoft recommends that you create an answer file that installs the packages and apply that answer file to the offline image by using DISM.exe.

To create an answer file for this purpose, you use Windows System Image Manager in the usual way, adding elements to the offlineServicing configuration pass. When you apply an answer file to an image by using DISM.exe, the program reads the settings in the offlineServicing configuration pass only. However, because the program could process settings in other configuration passes, Microsoft recommends that you create an answer file specifically for this purpose with no settings in any configuration passes other than offlineServicing.

## Committing and Unmounting Images

When you mount an image to a folder by using ImageX.exe or DISM.exe, the program actually copies the files stored in the Windows Imaging file to the folder you specify. When you execute additional commands to modify the image, you are working with the copy; the original Windows Imaging file is unchanged. After you have made all of your modifications, you must commit your changes, essentially rewriting the Windows Imaging file with the modified contents of the mount folder.

#### **CAUTION AVOIDING COMMITMENT**

Administrators who modify offline image files suffer a rite of passage at least once: After making extensive modifications to an image, the administrator proceeds to deploy the Windows Imaging file, having forgotten to commit the changes first. If you always remember that you have to commit before you unmount or deploy, you can avoid this standard pitfall.

## Testing Images

Testing is an essential part of the image creation process, and the same is true of images that you have modified offline. Whatever testing regimen you have created for your initial workstation deployment, you should test each time you modify one of your images.

### PRACTICE Using Deployment Image Servicing and Management

---

Deployment Image Servicing and Management (DISM.exe) takes the place of several utilities in previous versions of Windows AIK, consolidating their diverse functions into one program.

#### EXERCISE 1 Mounting an Image

Before you can work with an image by using DISM.exe, you must mount it to a folder.

1. At the computer on which you installed the Windows 7 AIK, insert your Windows 7 installation DVD (canceling autoplay, if necessary) and using Windows Explorer, create a folder called Image in the C:\Users folder and copy the Install.wim file from the Sources folder on the DVD to C:\Users\image.
2. Using Windows Explorer, create an empty folder called Mount in your C:\Users folder.
3. On the Start menu, open the Windows AIK program group, right-click Deployment Tools Command Prompt and, from the context menu, select Run As Administrator.
4. In the Administrator: Deployment Tools Command Prompt window, type the following command all on one line to mount the image and press Enter:

```
dism /mount-wim /wimfile:c:\users\image\install.wim /index:1 /mountdir:c:\users\mount
```

5. When the mounting process is completed, type the following command to display information about the mounted image and press Enter:

```
dism /get-mountedwiminfo
```

Leave the Administrator: Deployment Tools Command Prompt window open for the next exercise.

#### EXERCISE 2 Installing a Device Driver to an Offline Image

After you have mounted an image, you can modify it by installing device drivers and other software packages.

1. In Windows Explorer, create a folder called C:\Users\Drivers and copy your device driver files to that folder.
2. In the Administrator: Deployment Tools Command Prompt window, type the following command and press Enter:

```
dism /image:c:\users\mount /add-driver /driver:c:\users\drivers /recurse
```

- When the driver installation process is completed, type the following command to display information about the drivers installed to the image, including the oem#.inf names the program assigns to them:

```
dism /image:c:\users\mount /get-drivers
```

Leave the Administrator: Deployment Tools Command Prompt window open for the next exercise.

### **EXERCISE 3 Enabling and Disabling Windows 7 Features**

Using DISM.exe, you can modify the state of windows features in an offline image.

- In the Administrator: Deployment Tools Command Prompt window, type the following command to display the status of the features in the image and the names you must use to manipulate them, and press Enter:

```
dism /image:c:\users\mount /get-features
```

- Type the following command to disable the Solitaire feature in the image, and press Enter:

```
dism /image:c:\users\mount /disable-feature /featurename:Solitaire
```

- Type the following command to enable the Telnet Server feature in the image, and press Enter:

```
dism /image:c:\users\mount /enable-feature /featurename:TelnetServer
```

Leave the Administrator: Deployment Tools Command Prompt window open for the next exercise.

### **EXERCISE 4 Committing and Dismounting an Image**

To save the changes you made to the image, you must commit and then unmount the image.

- In the Administrator: Deployment Tools Command Prompt window, type the following command to commit the changes you made to the Windows Imaging file and unmount the image. Then press Enter:

```
dism /unmount-wim /mountdir:c:\users\mount /commit
```

- Close the Administrator: Deployment Tools Command Prompt window.

## **Lesson Summary**

- Administrators who have only minor changes to make to a core operating system image, such as applying a few updates or a language pack, might find it easier to modify an image directly while it is offline, rather than deploy it on a reference computer and capture an entirely new image.

- As time passes and your workstation images are increasingly out of date, your original workstation configurations could become increasingly vulnerable to attack. For this reason, you might find it better to update your images while they are offline, rather than update the workstations after deployment.
- You can manually modify offline images by using either the DISM.exe or ImageX.exe utility, both of which are included in the Windows 7 AIK. Although the two programs are functionally similar and can perform many of the same image modification tasks, each one has its own syntax, and their commands are not interchangeable.
- To modify an offline image, you must first mount it in a folder. After you have made your changes, you must commit them to the Windows Imaging file and then unmount the image.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. Which of the following package file types are you unable to add to an offline image by using DISM.exe?
  - .cab
  - .msi
  - .inf
  - .msu
2. Which of the following modifications can you make to an online image by using DISM.exe? (Choose all that apply.)
  - Add a device driver.
  - Add a language pack cabinet file.
  - Disable an operating system feature.
  - Reset the default user interface language.
3. Which of the following modifications can you NOT make to an offline image file by using DISM.exe?
  - Install a device driver required to boot the workstation.
  - Disable the Solitaire application.
  - Remove a Windows Update Stand-alone Installer (.msu) package you previously installed.
  - Install an application by using an answer file.

## Chapter Review

---

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

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

## Chapter Summary

- The Windows 7 Automated Installation Kit (AIK) and Microsoft Deployment Toolkit (MDT) 2010 provide administrators with the tools and documentation they need to devise an efficient strategy for creating Windows 7 workstation image files.
- Tools such as ImageX.exe and DISM.exe enable desktop administrators to modify workstation image files by adding and removing software components, as well as enabling and disabling operating system features, which can be a viable alternative to reconfiguring and recapturing reference computers.

## 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.

- build computer
- Deployment Image Servicing and Management (DISM.exe)
- file-based image
- hybrid image
- ImageX.exe
- language pack
- offline image
- online image
- reference computer
- sector-based image
- target computer
- thick image

- thin image
- Windows 7 Automated Installation Kit (AIK)
- Windows Imaging
- Windows Preinstallation Environment (Windows PE)
- Windows System Image Manager (SIM)

## Case Scenarios

In the following case scenarios, you will apply what you've learned about subjects of this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Capturing an Image Using ImageX.exe

Ralph is a new hire in the IT department, and his manager has assigned him the task of deploying 10 new computers as Windows 7 workstations for the Order Entry department. Although he has never used the Windows AIK tools before, Ralph decides that creating an image of one computer and deploying it to the other nine would be faster and easier than performing 10 separate manual installations.

After unpacking and assembling the first computer, Ralph inserts the Windows 7 DVD his manager gave him and installs the operating system. Then he installs Microsoft Office 2007, an antivirus program, and the company's custom order entry application. After that, Ralph installs the Windows 7 AIK on the computer and, after glancing briefly at the documentation, runs ImageX.exe to capture an image. However, ImageX.exe terminates almost immediately after starting and displays an error message that says "The process cannot access the file because it is being used by another process."

What went wrong, and what does Ralph have to do to successfully capture an image of the computer?

### Case Scenario 2: Modifying the User Interface Language

Harold is an IT engineer for a company that has recently expanded its operation from the United States into Canada. He has been assigned the task of preparing 25 Windows 7 workstations for deployment in the company's new office in Montreal. Harold has already ordered the new computers, using the company's standard workstation hardware configuration, and had them delivered to the Montreal office.

Harold has completed several workstation deployment projects before, and he already has Windows Imaging files that contain the standard configurations his company uses for its workstations. After investigating the requirements for the new office, Harold has decided that he can use the images he already has. The only problem is that the new users speak French and expect the user interface on their computers to be in French as well, while his Windows 7 images support only English.

To simplify the deployment process, Harold wants to modify his existing workstation images to use a French user interface now, offline, while he is still at the company's headquarters, using the DISM.exe program. He will then transfer the images to a server at the new office over the Internet and deploy the images to the computers there.

The process of modifying each image requires several steps. From the list below, choose the steps that Harold must perform on each image to convert it to the French user interface and list the steps in the proper order.

- a. Create an answer file containing the commands needed to activate the French user interface.
- b. Reset the default user interface language.
- c. Enable the French feature in the language pack.
- d. Commit the changes you have made to the image.
- e. Unmount the image.
- f. Apply the answer file to the image.
- g. Clean up the resources left by the mounted image.
- h. Mount the image to a folder.
- i. Add the French language pack to the image.
- j. Create an answer file containing the commands needed to install the language pack.

## Suggested Practices

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

### Design an Image Creation Strategy 1

In this practice, you work on implementing a Windows AIK-based image creation strategy by creating an answer file with Windows System Image Manager.

- **Practice 1** Open Windows System Image Manager, create a new answer file, and practice adding settings to the various configuration passes.
- **Practice 2** Validate the answer file to ensure that all of the settings you added are configured correctly.

### Design an Image Creation Strategy 2

In this practice, you use Deployment Workbench to create and edit a task sequence, as part of implementing an MDT 2010-based image creation strategy.

- **Practice 1** Open Deployment Workbench and create a new task sequence.
- **Practice 2** Open the Properties dialog box for the task sequence you created, click the Task Sequence tab, and practice configuring settings for the various stages of the sequence.

## 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 70-686 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.

# Configuring Clients

Windows 7 contains a multitude of configuration settings that control all aspects of the operating system's behavior. In an enterprise network environment, administrators treat these settings as they do most other workstation management chores: by creating standard configurations and deploying them to groups of workstations. This chapter and the next one are dedicated to the selection of appropriate configuration settings for your workstations and the various methods you can use to distribute those settings. Lesson 1 discusses the methods you can use to deploy configuration settings, and Lesson 2 describes some of the standard settings you might want to use for all of your workstations.

## Exam objectives in this chapter:

- Design standard system settings.

## Lessons in this chapter:

- Lesson 1: Designing a Client Configuration Strategy **118**
- Lesson 2: Creating a Client Baseline Configuration **150**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- A computer running Windows 7 that is joined to an Active Directory Domain Services domain
- Internet access



## REAL WORLD

Craig Zacker

Standardizing workstation configurations for an enterprise network requires not only prior planning, but also strict discipline. Desktop administrators often spend a good deal of their time putting out fires, and they naturally want to use the most expedient solution available. In some cases, this means configuring (or reconfiguring) operating system settings on an individual workstation to address a specific issue.

The problem with changing settings on an individual workstation is that you complicate the situation for anyone working on that computer in the future. The primary advantage of creating standard workstation configurations is that administrators know what to expect when they are troubleshooting a problem. A standard configuration has a predictable set of applications, settings, and other parameters, which makes the task of diagnosing the cause of a problem easier. When someone modifies the configuration of an individual workstation, a change that fixes one problem might easily cause another, and the person who has to troubleshoot future problems is faced with a multitude of additional variables.

When a workstation experiences a problem that is not hardware-related, other workstations of the same configuration could easily suffer the same problem. When administrators discover a configuration setting that resolves the problem, they should have a policy in place to deploy that setting to all similar workstations and add it to the standard configuration. This might complicate the process of addressing the immediate problem, but by maintaining workstation consistency across the enterprise, administrators simplify the troubleshooting process for future problems.

## Lesson 1: Designing a Client Configuration Strategy

Designing Windows 7 workstation configurations for an enterprise deployment is not just a matter of selecting hardware, applications, and other software components. Administrators also have to consider the many operating system configuration settings that workstations might need and the various methods available for configuring those settings. This lesson discusses the process of devising standardized workstation configurations and the methods for deploying them on an enterprise network.

**After this lesson, you will be able to:**

- Select a method for deploying configuration settings to Windows 7 workstations.
- Understand the process of creating and deploying Group Policy objects.
- Understand the differences between startup/shutdown scripts and logon/logoff scripts.

**Estimated lesson time: 120 minutes**

## Evaluating Business Requirements

As with nearly every aspect of the workstation deployment process, you should derive the configuration settings you apply to your Windows 7 client computers from your original business requirements. As part of your deployment planning process, you should have documented both the needs of the workstation users and the needs of your managers. For example, the management team might dictate security requirements, while user needs might call for drive mappings to network shares and other policies.

An enterprise workstation deployment typically has a baseline configuration that applies to all of the computers. This configuration might consist of standard applications, but typically also includes configuration settings that control features such as error reporting, auditing, and user profiles. Other configuration requirements for your workstations are likely to be security-related. In addition to protecting the computers from outside intrusion, you usually need to provide protection against accidental data loss as well.

## Matching Configuration Settings to Requirements

With a list of workstation requirements in hand, IT personnel have to determine how they will satisfy those requirements on their Windows 7 workstations. This process is essentially a comparison of what the organization needs the workstations to do, and what Windows 7 is capable of doing.

If your IT personnel are familiar with the Windows 7 capabilities involved in the definition of the workstation requirements, the process of matching workstation requirements to configuration settings should be relatively simple. By indicating what the operating system can and cannot do, IT input can steer the process of defining requirements in the right direction. If the planners defined the workstation requirements without sufficient IT guidance, you might have requirements that Windows 7 cannot satisfy internally, and you might have to seek out third-party solutions.

As with the image creation process discussed in Chapter 3, “Creating and Managing System Images,” you are likely to want to apply certain configuration settings to all of your workstations, forming what is essentially a baseline configuration. For more information on creating a baseline configuration, see Lesson 2, “Creating a Client Baseline Configuration,” later in this chapter. You are also likely to have other, differing requirements for various groups of workstations in your enterprise. You might therefore have some different configuration settings for each of the workstation images you maintain.

Defining the configuration settings for your workstations is as complex and important a task as selecting hardware components and applications. The process should begin early in the Plan phase of the deployment project and be subject to the same planning, testing, and deployment procedures.

## Selecting a Configuration Method

After determining what configuration settings you have to deploy to your workstations, you must consider how to deploy them. Sitting down at every Windows 7 computer and manually configuring the settings you want to apply is obviously a tedious and impractical solution, even for a small number of workstations. Fortunately, you can choose from a number of tools to deploy configuration settings to a large number of workstations. These are the primary tools desktop administrators typically use for this purpose:

- **Group Policy** Active Directory Domain Services (AD DS) objects, containing configuration settings, which administrators can apply to users or computers and can associate with domains, sites, or organizational units (OUs)
- **Logon/logoff scripts** Script files that execute when a user logs on
- **Startup/shutdown scripts** Script files that execute when the system starts and that apply to all users

Group Policy, familiar to even the most junior administrators, is by far the most common—and the most powerful—workstation configuration tool available. By setting values for configuration settings in Group Policy objects (GPOs) and associating the GPOs with AD DS objects, you can deploy the settings to your entire enterprise or to selected groups of computers. Windows 7 now supports more than 2,500 settings that you can configure using Group Policy, including a large number of preference settings that formerly were configurable only by using scripts.

Those who prefer working with scripts can configure settings on multiple Windows 7 workstations using startup/shutdown scripts and/or logon and logoff scripts. These are scripts that launch whenever a workstation starts and shuts down or when a user logs on and logs off, respectively. The primary difference between the two is that logon/logoff scripts run under the account with which the user logged on, while startup/shutdown scripts use the credentials of the computer object and have System privileges on the local computer. This makes it possible for startup/shutdown scripts to access the entire local file system and the registry, while logon/logoff scripts are relatively limited in the types of tasks they can perform.

Startup/shutdown scripts and logon/logoff scripts both support multiple script languages. You can write scripts using batch or command files, Windows PowerShell commands, or any scripting language supported by the Windows Script Host (WSH), including Microsoft JScript and Microsoft Visual Basic Scripting Edition (VBScript) by default.

For most enterprise deployments in an AD DS environment, Group Policy is the preferred method for deploying configuration settings. This is particularly true now that Group Policy supports preferences. However, the expanded role of Windows PowerShell in Windows 7 and Windows Server 2008 R2 has increased the potential power of startup/shutdown and logon/logoff scripts as well. The following sections discuss how to deploy configuration settings using each of these methods.

## Using Group Policy

Group Policy enables you to package configuration settings for Windows 7 and other operating systems and deploy them to all or part of an enterprise network, based on the AD DS infrastructure. Using Group Policy, you can deploy baseline configuration settings to all of the computers in the enterprise, and also deploy settings specific to individual workstation configurations.

### Creating GPOs

Group Policy objects are individualized entities that can contain policy settings and preference settings that apply to computers or to users. Although you can create local GPOs on individual workstations, the real power of Group Policy is as an enterprise configuration tool, enabled through AD DS. By default, an AD DS domain has two GPOs, as follows:

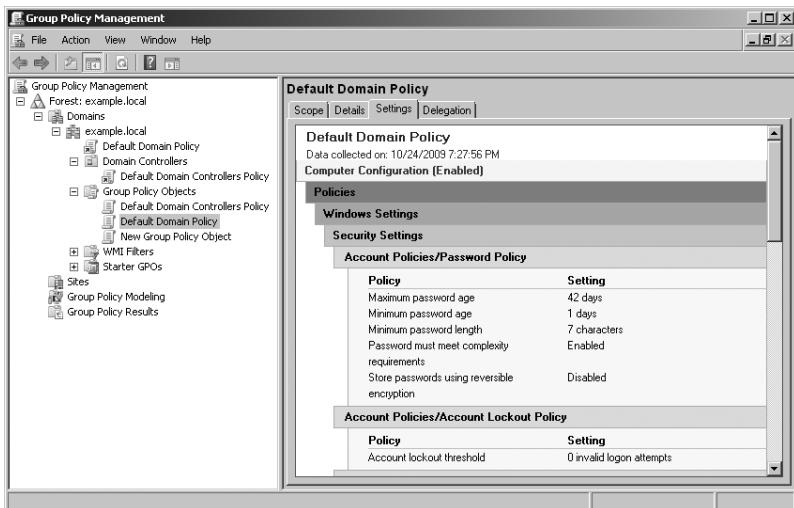
- **Default Domain Policy** Contains settings that apply to all of the computers and users in the domain
- **Default Domain Controllers Policy** Contains settings that apply to all of the domain controllers in the domain

#### BEST PRACTICES CREATING CUSTOM GPOS

You can modify the two default GPOs to add your own settings, but the recommended practice is to create new GPOs for your custom settings and leave the two default GPOs intact.

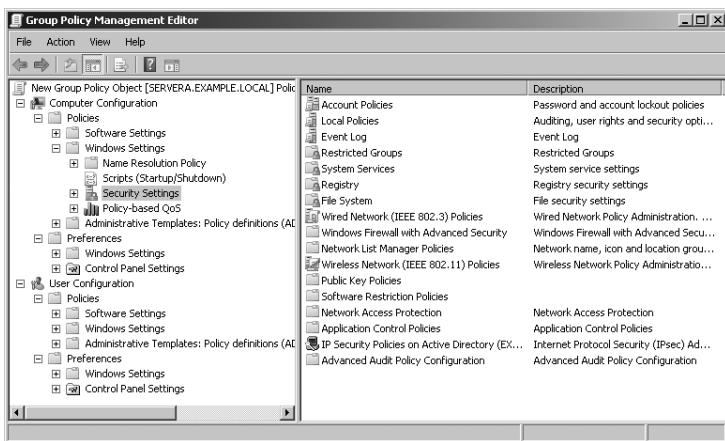
### USING GPMC

To create and manage your own GPOs, most administrators use the Group Policy Management Console (GPMC), as shown in Figure 4-1. GPMC is a graphical tool that provides an overview of all Group Policy information for an AD DS forest.



**FIGURE 4-1** Group Policy Management Console

GPMC also provides access to the Group Policy Management Editor (GPME), as shown in Figure 4-2, the tool you use to actually work with GPOs and their component settings.



**FIGURE 4-2** Group Policy Management Editor

GPMC is supplied as a feature in Windows Server 2008 R2 and with all other Windows Server versions since 2003. The feature is installed by default on AD DS domain controllers. To use the GPMC on a member server, you must add the Group Policy Management feature by using the Server Manager console, as shown in Figure 4-3.

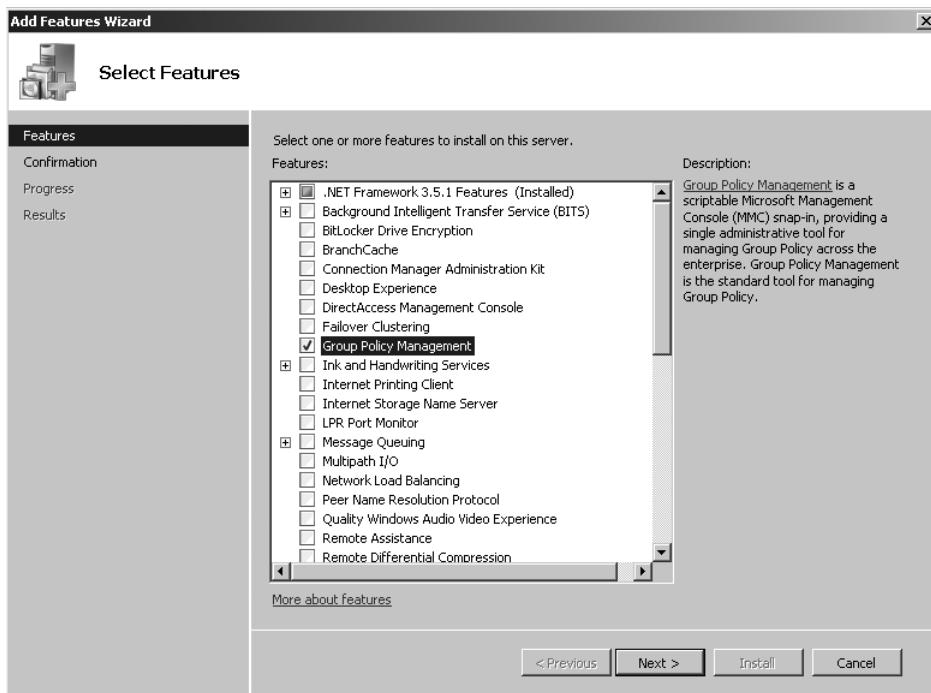
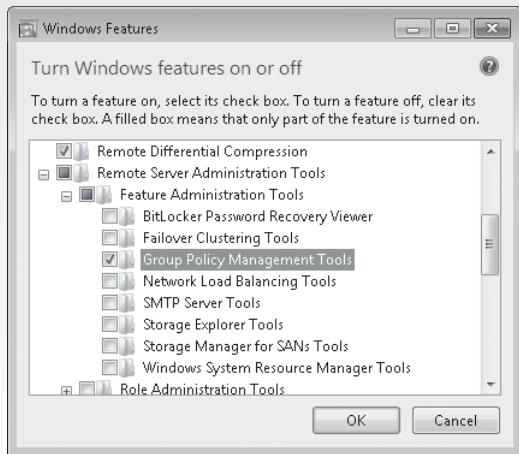


FIGURE 4-3 Adding the Group Policy Management feature in Windows Server 2008 R2

#### **NOTE** MANAGING GROUP POLICY FROM WINDOWS 7

Windows 7 includes a Local Group Policy Editor snap-in for Microsoft Management Console, which you can use to manage local Group Policy settings, but this snap-in cannot manage GPOs for AD DS. To manage AD DS Group Policy on a Windows 7 workstation, you must download and install the Remote Server Administration Tools for Windows 7 package from the Microsoft Download Center at <http://go.microsoft.com/fwlink/?LinkId=130862>. Then, you must turn the Group Policy Management Tools feature on by selecting Turn Windows Features On Or Off in the Programs And Features control panel, as shown in Figure 4-4.

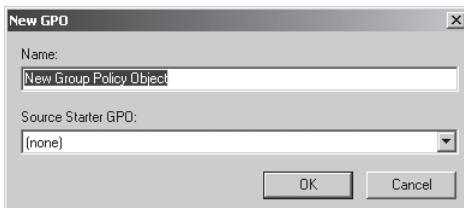


**FIGURE 4-4** Turning on Group Policy Management Tools in Windows 7

After you turn on the group Policy Management Tools feature, a Group Policy Management shortcut appears in the Administrative Tools program group.

To create a new GPO using GPMC, use the following procedure:

1. Click Start, click Administrative Tools, and then click Group Policy Management. The Group Policy Management Console appears.
2. Expand the Domains node and the node for your domain.
3. Right-click the Group Policy Objects container and, from the context menu, select New. The New GPO dialog box appears, as shown in Figure 4-5.
4. In the Name text box, type a name for the GPO and, if you want, select a Source Starter GPO from which to create the new GPO. Then, click OK. The new GPO appears in the Contents list.



**FIGURE 4-5** The New GPO dialog box

After you create the GPO, you can open it in Group Policy Management Editor and configure its settings.

#### USING GROUP POLICY CMDLETS

In Windows Server 2008 R2 and Windows 7, you can also create and manage GPOs from a command line by using a new set of Group Policy cmdlets for Windows PowerShell. Because these cmdlets rely on the GPMC application programming interfaces (APIs), you must have GPMC installed on the computer where you plan to run them. You must also import the GroupPolicy PowerShell module before you can access any of the 25 new cmdlets, using the following command from an elevated Windows PowerShell prompt:

```
import-module GroupPolicy
```

---

#### EXAM TIP

The increased emphasis Microsoft places on Windows PowerShell and its new capabilities in Windows 7 and Windows Server 2008 R2 is reflected in the 70-686 exam. Individuals taking the exam should be familiar with the new Group Policy cmdlets and with the procedure for importing the GroupPolicy module into a Windows PowerShell session.

---

#### COMPUTER CONFIGURATION OR USER CONFIGURATION

When you edit a GPO—or create a new one—in Group Policy Management Editor, you see two top-level nodes: Computer Configuration and User Configuration. As the names imply, when you associate a GPO with an AD DS object, the Computer Configuration settings in the GPO apply to computer objects and the User Configuration settings apply to user objects. In practice, when a Windows 7 workstation receives the settings in the GPO, it applies the Computer Configuration settings as Windows starts, and the User Configuration settings when a user logs on to the AD DS domain.

Each of the two nodes contains different settings, which depend on the nature of the operating system elements they are designed to configure. Most of the security settings in Windows 7, for example, fall under the Computer Configuration node. This makes perfect sense, because you want a computer to be secure as soon as it starts, not later when a user logs on. On the other hand, Folder Redirection settings (which are based on user or group identities) are located in the User Configuration node.

As far as the process of designing Windows 7 workstation configurations is concerned, administrators cannot choose between using the Computer Configuration and User Configuration nodes. If you want to configure a specific Windows 7 setting, it appears in GPOs under one of the nodes, but not both. Subordinate structures in the two nodes resemble one another—both contain Security Settings containers, for example—but the settings themselves that you find in the containers are different.

So although administrators do not have to choose between Computer Configuration and User Configuration settings when realizing their workstation requirements in GPOs, they do have to be concerned about how this distinction affects the GPO deployment process. Depending on the design of your organization's AD DS domain hierarchy, you might need to create separate GPOs for Computer Configuration and User Configuration settings. For more information on the GPO deployment process, see "Deploying GPOs," later in this lesson.

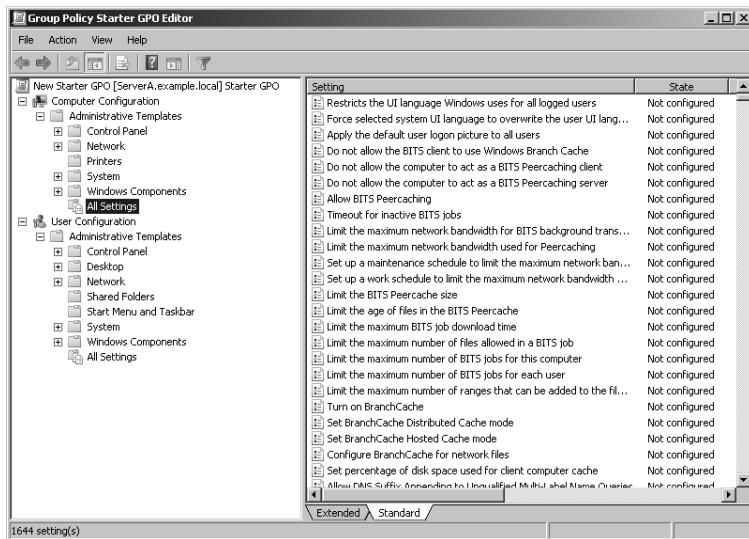
#### POLICIES AND PREFERENCES

Beneath the Computer Configuration and User Configuration nodes, you find two second-level headings: Policies and Preferences. The Policies nodes contain the Group Policy settings that have been present since Active Directory directory service was first introduced. Microsoft first added the Preferences nodes in Windows Server 2008 and Windows Vista. Group Policy preferences include settings that were previously configurable only by using scripts, such as drive mappings and printer connections.

In contrast, Preferences do not permanently lock down settings so that users cannot change them. Preferences enable administrators to deploy settings without enforcing them. With the introduction of Preferences, administrators can now deploy a complete workstation configuration using GPOs, which allow them to avoid scripting entirely.

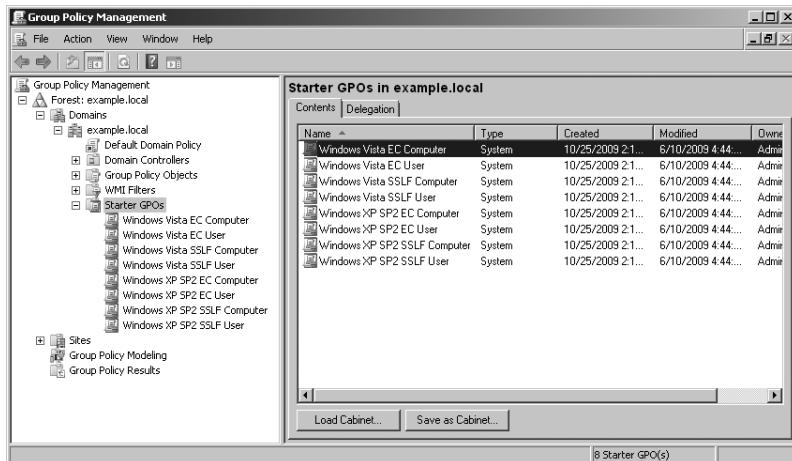
#### USING STARTER GPOS

Also new in Windows Server 2008 and Windows Vista are starter GPOs, which you can use to create your own custom GPOs. Starter GPOs are special Group Policy objects that contain only Administrative Templates settings, as shown in Figure 4-6. When you create a new GPO from a starter GPO, the new GPO automatically receives all of the settings in the starter GPO. You can therefore create a starter GPO containing baseline settings and use it to create individual GPOs containing settings for specific workstation configurations.



**FIGURE 4-6** The Group Policy Starter GPO Editor console

The GPMC implementations for Windows 7 and Windows Server 2008 R2 include eight preconfigured starter GPOs, as shown in Figure 4-7, four for Windows Vista (which you can also apply to Windows 7 workstations) and four for Windows XP R2.



**FIGURE 4-7** Starter GPOs in Group Policy Management console

These starter GPOs contain Computer Configuration and User Configuration settings for two preconfigured workstation environments: Enterprise Client (EC) and Specialized Security Limited Functionality (SSLF), as defined in the Windows 7 Security Guide. The EC environment is a standard configuration for AD DS-based networks, while SSLF is a highly restrictive environment that provides additional security by limiting user access to operating system functions.

#### **MORE INFO DOWNLOADING THE WINDOWS 7 SECURITY GUIDE**

The Windows 7 Security Guide is part of the Security Compliance Management Toolkit for Windows 7, available from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e&displaylang=en>.

#### **CREATING MONOLITHIC VS. FUNCTIONAL GPOS**

When you create your own GPOs for your workstation configurations, you can choose from two basic approaches: monolithic or functional. A monolithic GPO is one that contains all of the settings a workstation needs, including Computer Configuration and User Configuration settings, Policies and Preferences settings, and Administrative Templates settings. As with the thick images discussed in Chapter 3, monolithic images are easier to manage because everything is in one place. However, in a complex administration environment, monolithic GPOs could cause problems because you cannot delegate administration of specific parts of a GPO.

Functional GPOs, by contrast, are more numerous, contain relatively few settings, and are dedicated to a specific area or type of setting. For example, you might consider creating separate GPOs for your Computer Configuration and User Configuration settings. In the same way, you can separate Policies and Preferences settings. Administrators typically create divisions like these to accommodate an AD DS design. For example, if your domain hierarchy separates computer objects and user objects into separate organizational units, it makes sense to assign a GPO containing Computer Configuration settings to one OU and a User Configuration GPO to another.

Administrative delegation is another reason for creating functional GPOs. By placing all of your security-related settings in a separate GPO, for example, you can delegate responsibility for it to a security administrator.

As with image files, the more functional GPOs you create, the more difficult it is to manage them all. The ultimate solution, in which each configuration setting has its own individual GPO, is in almost every case not practical, but some administrators do create large numbers of GPOs containing only a few settings each. When you create functional GPOs, it is often necessary to link multiple GPOs to a single AD DS object, which complicates the deployment process and can result in performance problems.

#### **SELECTING A FUNCTIONAL GPO DESIGN STRATEGY**

If you elect to create functional GPOs, there are several design strategies you might consider when deciding just how many GPOs to create and how you should divide your settings among them. Some of these design strategies are as follows:

- A layer-based design uses the structure of the AD DS hierarchy to distribute configuration settings among multiple GPOs. By linking GPOs to OUs at each level of the hierarchy and then configuring each GPO with only the settings that all of the users and computers in that particular OU need, you facilitate Group Policy maintenance and administrative delegation.

- A role-based design requires that you create GPOs that contain the settings a user needs to perform a single, relatively limited task and then assign those GPOs to OUs in various combinations as needed. In this method, the AD DS hierarchy does not typically correspond to the GPO design strategy, so you must use security filtering to ensure that each computer and user receives only the GPOs it needs.
- A type-based design strategy distributes settings into GPOs according to their genres, such as security GPOs, script GPOs, folder redirection GPOs, and so forth. This facilitates delegation and management, but can result in a large number of GPOs.

### GROUP POLICY PERFORMANCE ISSUES

The other big issue with monolithic and functional GPOs is how they affect workstation performance, and unfortunately, this is not a simple comparison. The process by which workstations locate and access GPOs on domain controllers and then apply the GPOs is quite complicated and includes multiple exchanges with the domain controller and local processes that variously affect overall performance. For example, the process by which the workstation compiles a list of the GPOs it needs to apply is relatively quick, while the client-side extension (CSE) processing that the workstation must perform on each GPO can be quite lengthy. So even though more obvious factors, such as the size and number of the GPOs a workstation must apply, certainly affect performance, you must consider many other variables in addition, including the following:

- **Link speed** The speed of the link between the workstation and the domain controller affects how long it takes to download GPOs, but there are other considerations as well. Group Policy processing begins with a slow link detection process, during which Windows 7 uses the Network Location Awareness (NLA) protocol to measure the link speed. If the workstation determines that it is connected using a slow link, it does not execute some of the most resource-intensive CSE processes, including Software Installation and Folder Redirection.
- **Change frequency** As part of Group Policy processing, the workstation determines whether the GPOs—or other factors, such as group membership—have changed since it last processed them. If a GPO is unchanged, no processing occurs for that GPO. So if you plan to make frequent changes to your settings, functional GPOs are preferable because they minimize the amount of CSE processing that occurs. A minor change to a monolithic GPO forces the workstation to repeat the CSE processing sequence for all of its settings.
- **Foreground vs. background processing** Foreground Group Policy processing occurs when a workstation restarts and when a user logs on; background processing occurs at regular intervals, to refresh the GPOs while the workstation is running. As with slow link speed processing, background processing excludes the Software Installation and Folder Redirection CSEs as well as other processes that can adversely affect performance.

- **Asynchronous vs. synchronous processing** By default, workstations use asynchronous Group Policy processing, which enables users to access their desktops faster by using background instead of foreground processing during logon. This speeds up the logon process, but because the system uses background processing, it defers the application of foreground-only policies such as Software Installation and Folder Redirection policies until the next logon.

#### NOTE USING SYNCHRONOUS PROCESSING

To modify the default asynchronous processing behavior of your workstations, you can enable the Always Wait For The Network At Computer Startup And Logon policy, found in the Computer Configuration\Policies\Administrative Templates\System\Logon folder of any GPO. This forces computers to use synchronous processing, which slows the logon process but applies all foreground-only policies in one pass.

Unfortunately, it is difficult to estimate or predict Group Policy performance; the only reliable way to measure the efficiency of your GPO design strategy is to monitor the processing empirically. To do this, you can examine the Group Policy operational log in the Event Viewer console, as shown in Figure 4-8. This log contains events corresponding to each phase of GPO processing, with time stamps that you can use to compare processing times for various types of GPOs.

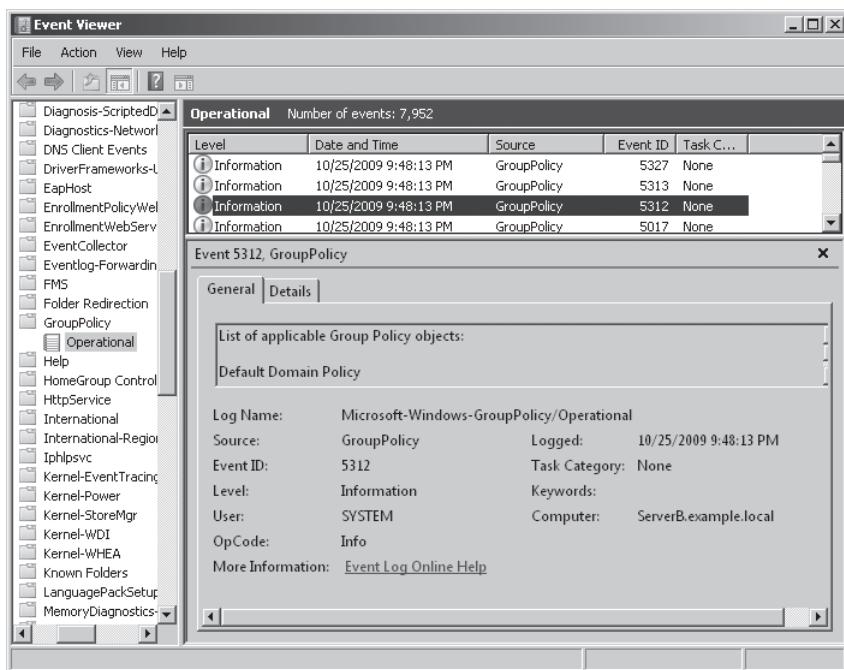


FIGURE 4-8 The Group Policy operational log in the Event Viewer console

## Deploying GPOs

To deploy GPOs, you link them to AD DS container objects, such as domains, sites, and organizational units. A link is simply an association between the Group Policy object and the container object. When you link a GPO to a container, all of the objects in that container receive the settings in the GPO.

The default settings created by an AD DS domain controller are in a GPO called Default Domain Policy, which the domain controller links to the AD DS domain object, as shown in Figure 4-9. As a result, the settings in that GPO flow downward all through the domain hierarchy. In the same way, a GPO called Default Domain Controllers Policy is linked to an OU called Domain Controllers, which contains the computer objects for the network's domain controllers.

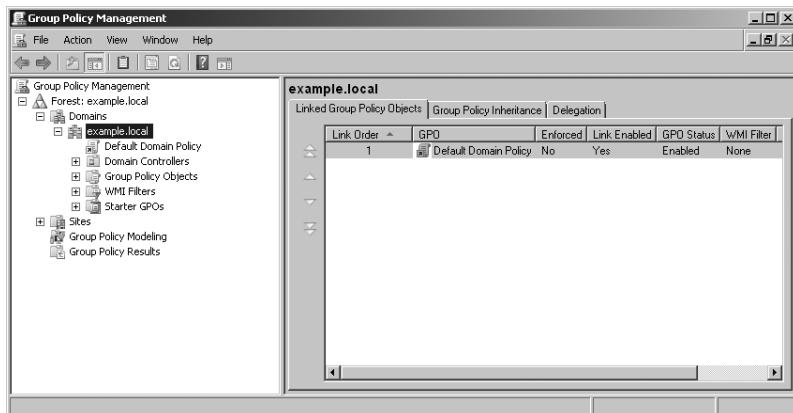


FIGURE 4-9 The Default Domain Policy link in the GPMC

Because of these links, all computer and user objects throughout the domain receive the settings in the Default Domain Policy GPO. Although it is not recommended that you do so, you could edit the Default Domain Policy GPO and add your own settings; they would then be disseminated throughout the domain in the same way.

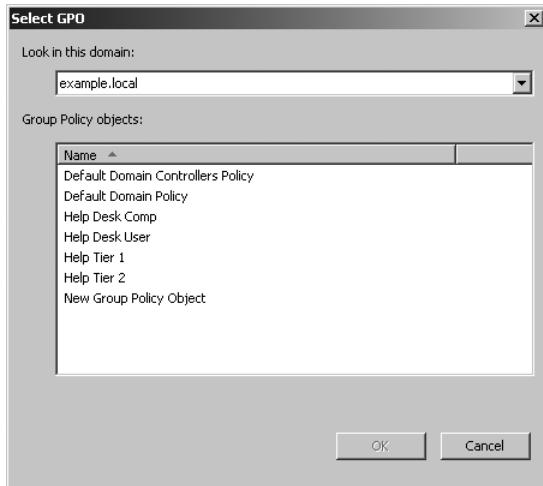
The objects in the Domain Controllers OU, however, receive the settings from both the Default Domain Policy GPO and the Default Domain Controllers Policy GPO. AD DS combines GPO settings in this way throughout the domain. You can link multiple GPOs to a single container or link them to containers at different levels in the AD DS hierarchy, and the objects in those containers will always receive the combined settings from all of the GPOs applicable to them.

### LINKING GPOS

After you create a GPO, you can link it to an AD DS container by using the following procedure:

1. Click Start, and then click Administrative Tools\Group Policy Management. The Group Policy Management Console appears.
2. Expand the Domains node and the node for your domain.

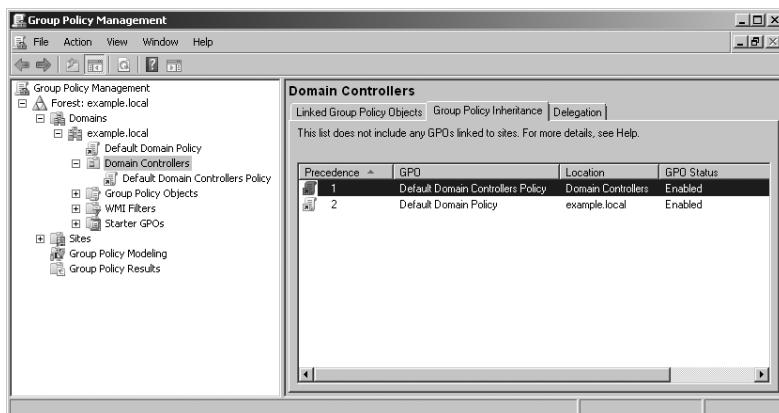
- Right-click the domain, site, or OU object to which you want to link the GPO and, from the context menu, select Link An Existing GPO. The Select GPO dialog box appears, as shown in Figure 4-10.
- From the Group Policy Objects list, select the GPO you want to link to the domain, site, or OU and click OK. The GPO appears on the Linked Group Policy Objects tab for the domain, site, or OU.



**FIGURE 4-10** The Select GPO dialog box

### UNDERSTANDING GROUP POLICY INHERITANCE

As noted earlier, the Domain Controllers OU receives settings from two GPOs, which are linked at different levels in the AD DS hierarchy. However, you can use GPMC to display all of the GPOs that apply to a particular container object, whether they are linked to domains or OUs, as shown in Figure 4-11.



**FIGURE 4-11** The Group Policy Inheritance tab for the Domain Controllers OU in GPMC

#### **NOTE UNDERSTANDING SITES**

As noted in the user interface, the Group Policy Inheritance tab in GPMC does not display GPOs that the container inherits from links to site objects. Sites are AD DS objects that administrators use to separate locations connected by relatively slow wide area network (WAN) technologies. By creating multiple sites, you can limit the amount of replication that occurs between domain controllers, thereby conserving bandwidth on the WAN. By default, AD DS installations have only a single site, and there are no GPOs linked to the site object.

The Default Domain Controllers Policy GPO exists mainly because domain controllers have a critical role in the enterprise and require more stringent security settings. This GPO contains settings that member servers and workstations do not need, so the default AD DS configuration places the computer objects for domain controllers in a separate OU and links this special GPO to that OU. The domain controllers therefore receive the Default Domain Policy settings that apply to all computers, and then they receive the function-specific settings from the Default Domain Controllers Policy GPO.

You can use this same technique when designing your own workstation configurations. By placing workstations with different requirements into separate OUs, you can link different GPOs to the OUs, which contain the settings for your various workstation configurations.

The problem with having multiple GPOs linked to a single container, whether at the same or different levels, is that those GPOs can contain policy settings that conflict. For example, you might have one GPO linked to a domain that contains a security policy with a relatively low setting, while a GPO linked to an OU in that same domain has the same security policy but with a higher setting. Objects in the OU will receive settings from both GPOs, but which will be the operative setting for that particular policy?

#### **UNDERSTANDING GROUP POLICY PRECEDENCE**

Group Policy precedence determines which value from conflicting GPO settings remains operative when processing is complete. When a workstation receives settings from multiple GPOs, the system applies the GPOs in a particular order, and the settings it applies last can overwrite those it has applied previously.

When a workstation receives GPOs from different levels in the AD DS hierarchy, the following precedence applies by default:

- 1. Organizational unit**
- 2. Domain**
- 3. Site**
- 4. Local**

Local GPOs, which have the lowest precedence, are applied first, and organizational unit GPOs, which have the highest precedence, are applied last. A workstation can belong to only one domain or site, but there can be multiple levels of OUs involved. When this is the case, GPOs linked to a workstation's immediate parent OU take precedence over those passed down from higher levels. Therefore, in an enterprise with two levels of OUs, a workstation in a second-level OU would apply GPO settings in the following order:

1. Local GPOs
2. Site GPOs
3. Domain GPOs
4. Grandparent GPOs
5. Parent GPOs

The settings in the GPOs linked to the parent OU therefore take precedence over all the other settings.

#### **MORE INFO PROCESSING LOCAL GPOS**

In workstation processing, GPOs linked to AD DS containers always take precedence over local GPOs, but there are multiple local GPOs as well, and they have their own precedence, as follows:

1. User-specific local GPO
2. Administrators local GPO or Non-Administrators local GPO
3. Local policy object

#### **ASSIGNING MULTIPLE GPOS TO ONE CONTAINER**

When you link multiple GPOs to a single container object, you determine the precedence by specifying a Link Order value for each GPO. By default, GPOs appear in the Linked Group Policy Objects list in the order you add them, with the last GPO you added having the highest Link Order value. This means that the last GPO you link to a particular object has the lowest precedence. To modify the Link Order values, you use the arrows on the left side of the Linked Group Policy Objects tab.

Somewhat counter-intuitively, the link order values in the GPMC reflect the precedence of the GPOs in the list, not the order in which computers apply them. For an OU with five linked GPOs, for example, the GPO with a link order value of 1 has the highest precedence and the one with a link order of 5 the lowest. This means, however, that when a computer applies the GPOs, it begins with the lowest precedence GPO, number 5, first, and applies the highest precedence GPO, number 1, last.

In the example shown in Figure 4-12, the Help Desk OU in an organization's IT department has a subordinate OU called Tier2, which contains the computer and user objects for the help desk technicians who receive escalated calls.

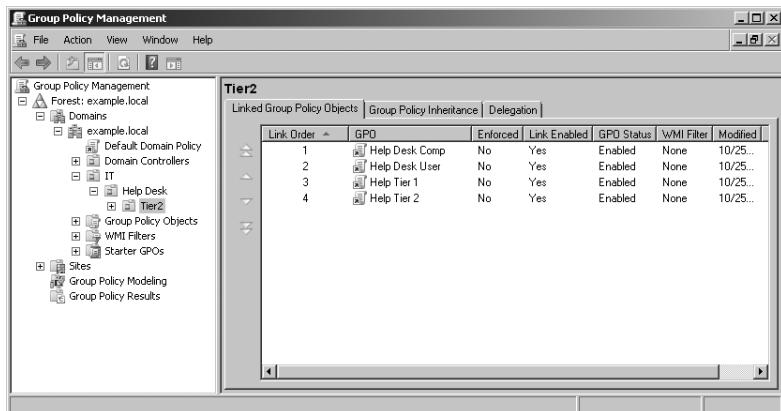
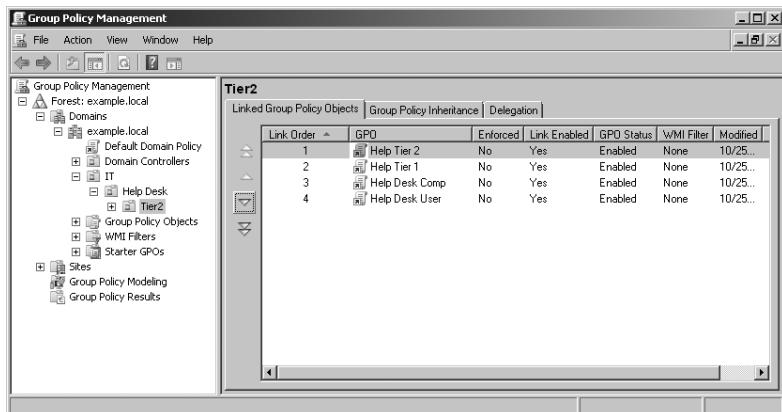


FIGURE 4-12 Multiple linked GPOs with Help Tier 2 having the lowest precedence

The Tier2 OU has four GPOs linked to it, as follows:

- **Help Desk Comp** Contains general Computer Configuration settings for all help desk computers
- **Help Desk User** Contains general User Configuration settings for all help desk users
- **Help Tier 1** Contains specific settings for Tier 1 help desk users, providing them with access to limited resources throughout the enterprise, which they might need for troubleshooting purposes
- **Help Tier 2** Contains specific settings for Tier 2 help desk users, providing them with access to extended resources throughout the enterprise, for troubleshooting purposes

When the administrator linked the GPOs to the Tier2 OU, she did so in the order you see in the figure. However, because the Help Tier 1 and Help Tier 2 GPOs contain some of the same settings with different values, the precedence orders shown are wrong. In this configuration, the Tier 2 workstations apply the Help Tier 2 GPO first, and then overwrite the Help Tier 2 settings with those in the Help Tier 1 GPO. This means that the more restrictive settings in Help Tier 1 are overwriting those in Help Tier 2. To resolve the problem, the administrator adjusts the Link Order values as shown in Figure 4-13 so that the Help Tier 2 GPO has the highest precedence.



**FIGURE 4-13** Multiple linked GPOs with Help Tier 2 having the highest precedence

## Controlling Group Policy Inheritance

The process of creating and deploying GPOs in an enterprise environment is interdependent with the design of the AD DS hierarchy. Ideally, administrators should consider GPO deployment as they create an Active Directory design because the structure of the OUs in a domain dictates how inherited GPO settings flow downward to the computer and user objects.

In many cases, however, no matter how careful the design, it is not possible or practical to subdivide an AD DS domain to accommodate all of the workstation configurations an enterprise needs. Having 20 different workstation configurations is not, in itself, a good enough reason to create 20 OUs. So you might need to exercise greater control over Group Policy inheritance. In other words, you might have to link a GPO to an OU and prevent some of the objects in the OU from inheriting its settings. You can choose from several ways in which you can do this, as described in the following sections.

### BLOCKING INHERITANCE

Blocking inheritance is a way of figuratively erecting a dam that prevents the downward flow of GPO settings through the AD DS hierarchy. You block inheritance in GPMC by right-clicking a domain or OU object and selecting **Block Inheritance** from the context menu. This prevents that OU, and all of its subordinate objects, from receiving any GPO settings from above.

After you block inheritance at a domain or OU, any GPOs you have linked directly to that domain or OU remain in effect. Only GPOs at levels above the blocked object are suppressed. The only way for subordinate objects to receive additional settings through AD DS is to link GPOs directly to their container objects.

### **IMPORTANT INHERITANCE BLOCKING AND LOCAL GPOS**

Blocking inheritance has no effect on local Group Policy objects. The block is effective only on GPOs in Active Directory Domain Services.

Blocking inheritance is a relatively drastic solution that many administrators try to avoid. You cannot block some GPOs and admit others; it's all or nothing. The block also complicates the Group Policy management process, much in the way that using Deny permissions does in the NTFS file system.

### **ENFORCING GPOS**

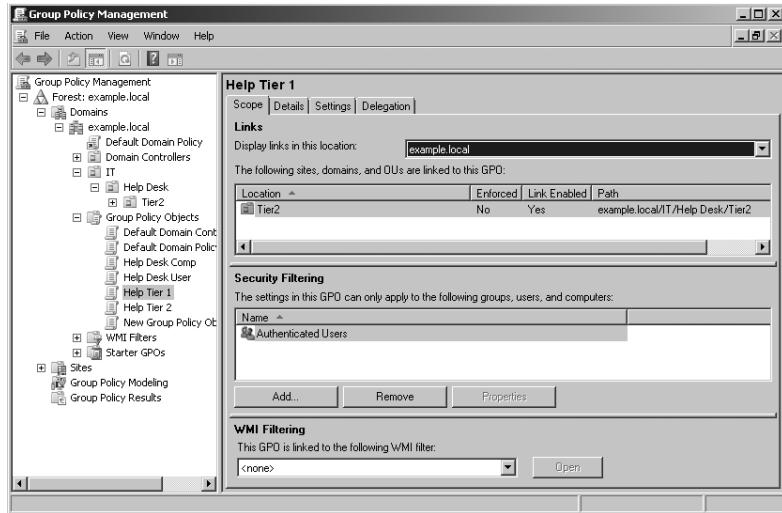
Enforcement is an alternative to inheritance blocking that enables you to prevent the blockage of specific GPOs. Unlike inheritance blocking, enforcement works at the GPO level, not the domain or OU level. When you right-click a GPO in GPMC and select Enforced from the context menu, that GPO cannot be blocked, and it automatically receives the highest precedence on all of the objects to which it applies. If a domain or OU has more than one enforced GPO linked to it, the GPO originating from the highest point in the AD DS hierarchy receives the highest precedence.

### **USING SECURITY FILTERING**

As with virtually all objects of any type in Windows Server, GPOs have an access control list (ACL), which specifies the permissions assigned to users, groups, and computers. A user or computer must have appropriate permissions to read from a GPO and apply the settings it contains. Security filtering is a method for controlling GPO dissemination by manipulating these permissions.

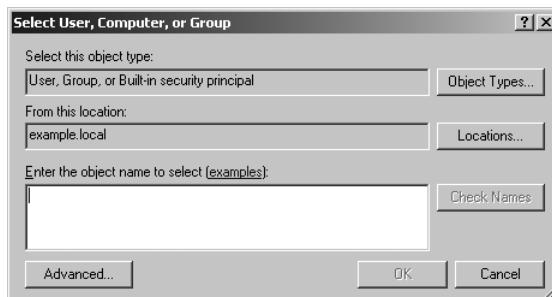
By default, all GPOs have the Allow Read and Allow Apply Group Policy permissions for the Authenticated Users security group. This enables any computer or user that successfully logs on to the domain to receive the settings in that GPO. To restrict the application of the settings in a GPO to more specific users and computers, you can modify these defaults, using the following procedure:

1. Click Start, and then click Administrative Tools\Group Policy Management\. The Group Policy Management Console appears.
2. Expand the Domains node and the node for your domain.
3. Expand the Group Policy Objects node and select the GPO whose permissions you want to modify, as shown in Figure 4-14.



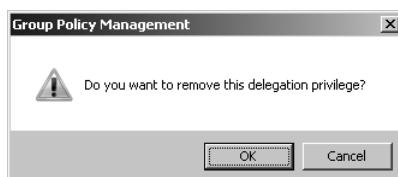
**FIGURE 4-14** The default Security Filtering list for a GPO in GPMC

- On the Scope tab, under Security Filtering, click Add. The Select User, Computer, or Group dialog box appears, as shown in Figure 4-15.



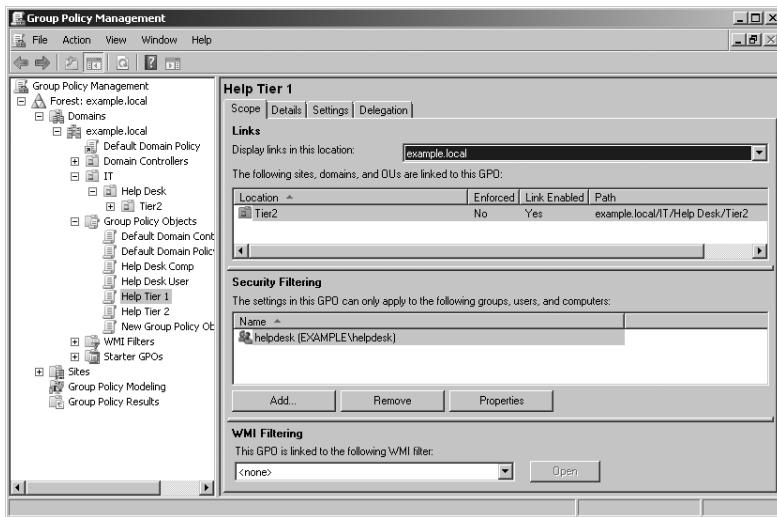
**FIGURE 4-15** Select User, Computer, or Group dialog box

- In the Enter The Object Name To Select text box, type the name of the user, computer, or group object to which you want to assign permissions, and click OK. The object appears in the Security Filtering list.
- Select the Authenticated Users group and click Remove. A Group Policy Management message box appears, as shown in Figure 4-16.



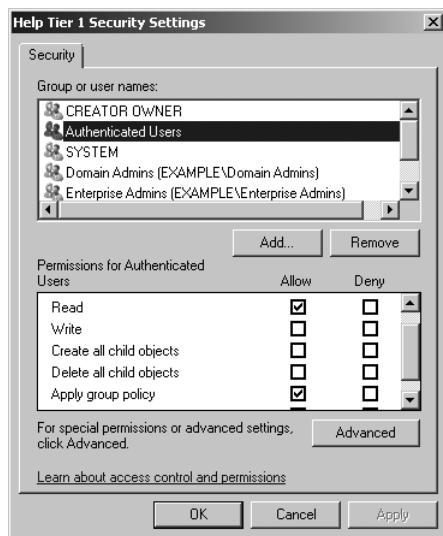
**FIGURE 4-16** The Group Policy Management message box

- Click OK. The Authenticated Users group is removed from the Security filtering list, leaving only the object you added, as shown in Figure 4-17.



**FIGURE 4-17** The modified Security Filtering list for a GPO in GPMC

You can also modify the permissions for the GPO directly by clicking Advanced on the Delegation tab to display the Security Settings dialog box for the GPO, as shown in Figure 4-18.



**FIGURE 4-18** The Security Settings dialog box for a GPO

## USING WMI FILTERING

The Windows Management Instrumentation (WMI) technology makes it possible to query computers for specific attributes. You can use WMI queries to apply GPOs by configuring them to locate the computers running a particular operating system or having other particular capabilities.

To use WMI filtering, you have to create the WMI filter itself, which exists as a separate file, and then link it to a GPO on the Scope tab for a GPO.

### MORE INFO CREATING WMI FILTERS

For more information about creating WMI filters, see the Microsoft Developer Network at <http://msdn.microsoft.com/en-us/library/aa286547.aspx>.

## Using Scripts

You can augment your use of Group Policy settings or replace them by configuring your workstations using scripts that execute at system startup and when a user logs on to the domain. Although scripts can't possibly replicate the more than 2,500 settings available in a Group Policy object, many administrators rely on scripts to configure settings that would otherwise require them to create and maintain a far larger number of GPOs.

### Choosing a Scripting Language

Windows 7 workstations support a number of scripting languages. You can choose a language from among them or combine them in various ways. The scripting languages that Windows 7 supports by default are as follows:

- **Batch files** A text file with a .bat or .cmd extension, which contains a series of commands that execute in sequence at the standard Windows command prompt. Batch files can contain calls to any internal command or command-line program available on the workstation, and can even use rudimentary "if" statements. Although some batch scripts can be quite elaborate, they are relatively limited in their capabilities. Many administrators quickly outgrow batch scripting and turn to other, more powerful, languages.
- **VBScript** A limited variation of the Visual Basic programming language that runs under Windows Script Host (WSH), a language-independent hosting engine that can provide Windows computers with support for various scripting languages. VBScript is a scripting language only; it does not have command-line capabilities. VBScript files have a .vbs extension; many administrators use them for startup/shutdown and logon/logoff scripts because the language is far more powerful than batch scripting, and all of the Windows operating systems since Windows 2000 support it.

- **Windows PowerShell** A relatively new command-line and scripting language that is based on the Microsoft .NET Framework technology. Windows PowerShell script files, which have a .ps1 extension, have access to all of the .NET libraries installed on the computer. Although it seems unlikely that Microsoft will drop support for WSH anytime soon, because many administrators rely on it, Microsoft clearly intends for Windows PowerShell to be the primary Windows scripting language.

#### BEST PRACTICES WORKING TO YOUR STRENGTHS

You should select a language for your scripts with an understanding of your own scripting capabilities. If you have experience programming with VBScript, use that. However, if you are new to scripting, your efforts are best spent on learning Windows PowerShell, and you should also consider adding Windows PowerShell support to all of your Windows computers that do not include it by default.

## Supporting Scripting Languages

The language (or languages) you use when creating startup/shutdown and logon/logoff scripts must be supported by the computers that will run them. If you still have computers on your network running the DOS-based versions of Windows, such as Windows ME, Windows 98, Windows 95, and Windows NT, your only choice for these computers is batch scripting.

For computers running Windows 2000 and later, WSH is an extensible hosting engine that can provide support for many languages, but Windows supports only VBScript and JScript by default. You can use other languages supported by WSH to create your scripts, but you must install the additional scripting engines on all of your client computers before they can execute the scripts.

In the same way, your workstations must support Windows PowerShell if you choose that language for your scripts. Windows 7 and Windows Server 2008 R2 include support for Windows PowerShell by default, but on Windows Server 2008, you must add it as a feature. On Windows Vista, Windows XP, and Windows Server 2003, you must download Windows PowerShell as a separate package and install it before the computers can run Windows PowerShell scripts.

## Deploying Scripts

There are two ways to deploy scripts to your workstations: by specifying them in user objects and by using Group Policy, as described in the following sections.

### DEPLOYING LOGON SCRIPTS IN USER OBJECTS

For computers running operating systems that do not support Group Policy, such as Windows NT, Windows ME, Windows 98, and Windows 95, the only way to assign a logon script is to add the filename to the Logon Script text box on the Profile tab of a user's Properties sheet in Active Directory Users And Computers or Local Users And Groups, as shown in Figure 4-19.

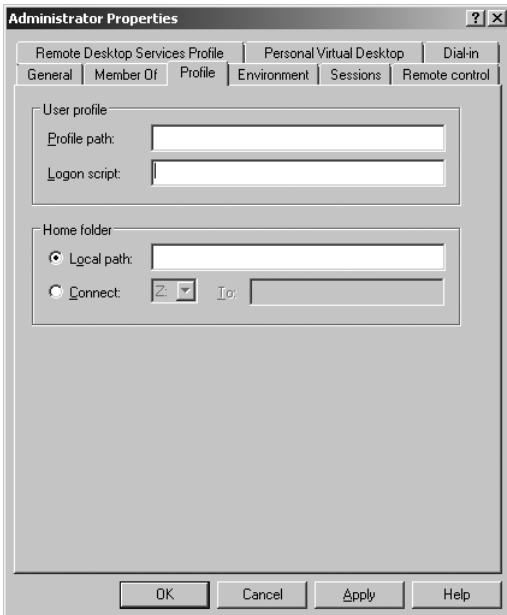


FIGURE 4-19 The Profile tab on a user's Properties sheet

For these older operating systems, you must use batch file logon scripts. The default location for the script files is the NetLogon share on the domain controller, which corresponds to the C:\Windows\SYSVOL\sysvol\<domain.com>\scripts\ folder, where <domain.com> is the AD DS domain name. This folder is replicated in all domain controllers for the domain, making the scripts you place there available to all users. To reference a script file in another location, you can insert a path name in the Logon Script text box, using the Universal Naming Convention (UNC) format. However, you must make sure that the location you specify is replicated in all of your domain controllers.

For computers running Windows 7 and other, newer, operating systems, you can continue to use this method, supplying batch file or VBScript scripts, although it can be impractical to configure large numbers of user accounts individually. In addition, this deployment method provides no means of running startup, shutdown, or logoff scripts. Some administrators create VBScripts that assign a logon script name to the *scriptPath* attribute of user objects in bulk, but most find it easier to use Group Policy to deploy scripts instead.

#### DEPLOYING SCRIPTS USING GROUP POLICY

GPOs include policies that enable you to assign startup, shutdown, logon, and logoff scripts to domain, site, or OU container objects, which cause all of the computers and users in those containers to execute the scripts. For a large enterprise, this is obviously easier than configuring each user individually, and you can use the filtering methods described earlier in this lesson to regulate the application of your scripts.

In Group Policy Management Editor, the Startup and Shutdown policies are located in the Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown) container, as shown in Figure 4-20. The Logon and Logoff policies are located in the User Configuration\Policies\Windows Settings\Scripts(Logon/Logoff) container.

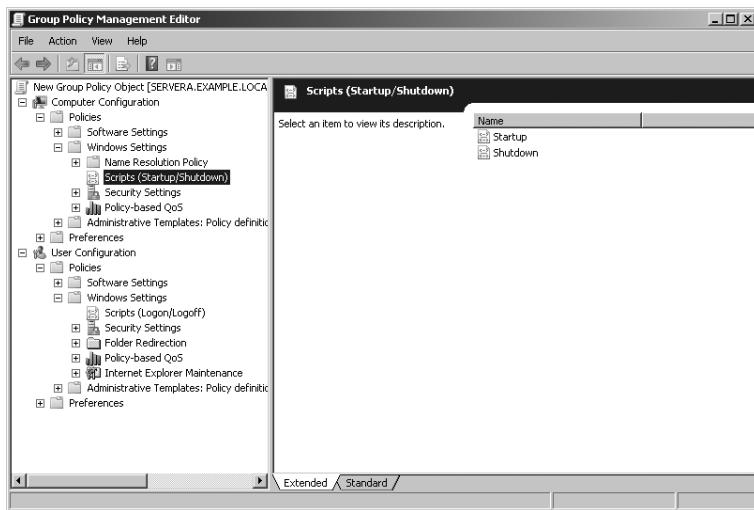


FIGURE 4-20 The Startup and Shutdown policies in a GPO

When you double-click one of the policies, its Properties sheet appears, as shown in Figure 4-21.

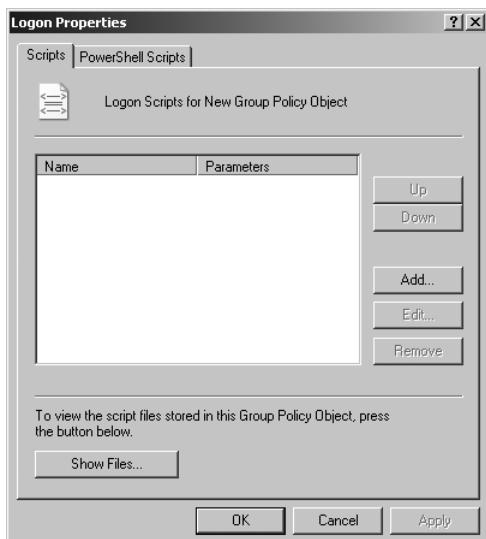


FIGURE 4-21 The Logon Properties sheet

Clicking Add displays the Add A Script dialog box, shown in Figure 4-22, in which you specify the name of your script and any parameters you might need to append to it. Clicking Show Files opens an Explorer window to the location of the script files, enabling you to access them directly from the interface.

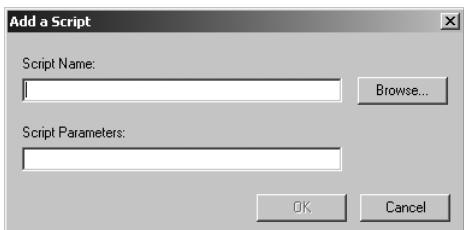


FIGURE 4-22 The Add A Script dialog box

For Windows PowerShell scripts, Windows Server 2008 R2 provides a new PowerShell Scripts tab on the Properties sheets, as shown in Figure 4-23. On this tab, you can add Windows PowerShell scripts and specify whether they should run before or after your regular scripts. Administrators who already have standard scripts in place that they do not want to change can now add Windows PowerShell commands to the existing solution.

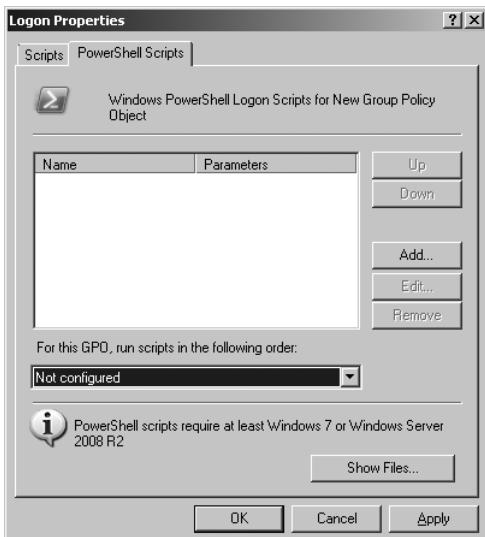


FIGURE 4-23 The PowerShell Scripts tab on the Logon Properties sheet

#### **NOTE COMBINING SCRIPTS**

The GPME provides one method for combining script languages by enabling you to execute a Windows PowerShell script either before or after your standard script. However, you can also call one script type from within another script. For example, you can create a batch file script containing a command that executes a VBScript or Windows PowerShell script. As long as the target computer is capable of running VBScript or Windows PowerShell and you have formatted the command to properly execute the required environment, the secondary script should run and, after it is finished, return control to the batch file script.

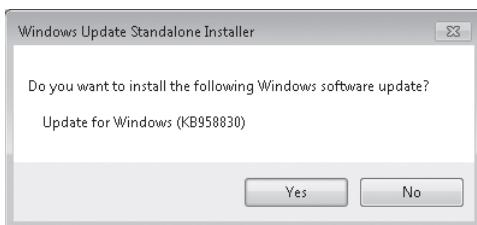
#### **PRACTICE Creating a GPO in Windows 7**

Before you can work with AD DS Group Policy objects on a Windows 7 workstation, you must download and install Group Policy Management Console. In this practice, you install GPMC and use it to create and edit a GPO.

#### **EXERCISE 1 Downloading and Installing GPMC**

Microsoft provides GPMC as part of the Remote Server Administration Tools for Windows 7 package free of charge from the Microsoft Downloads Center. To download and install the package, use the following procedure.

1. Open a browser window and, in the address box, type the following URL and press Enter:  
<http://go.microsoft.com/fwlink/?LinkId=130862>. The Remote Server Administration Tools for Windows 7 download page appears.
2. At the bottom of the page, click the Download button for the platform appropriate to your computer and save the amd64fre\_GRMRSATX\_MSU.msu or x86fre\_GRMRSATX\_MSU.msu file to a folder on your local drive.
3. In Windows Explorer, locate the file you downloaded and double-click it. A Windows Update Standalone Installer message box appears, as shown in Figure 4-24.



**FIGURE 4-24** The Windows Update Standalone Installer message box

4. Click Yes to install the update. The Read These License Terms page appears.
5. Click I Accept. The system installs the update, as shown in Figure 4-25, and then displays the Installation Complete page.

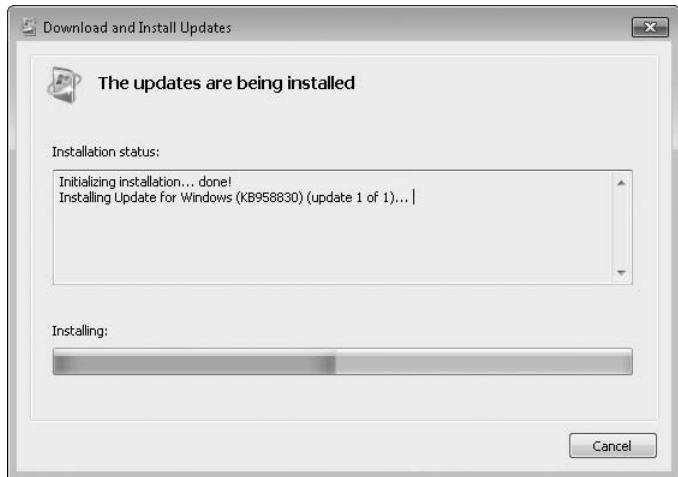


FIGURE 4-25 The Updates Are Being Installed page

6. Click Close.

## EXERCISE 2 Enabling Group Policy Management

Before you can use GPMC, you must enable the tools you just installed.

1. Click Start, and then click Control Panel. The Control Panel window appears.
2. Click Programs. The Programs window appears.
3. Click Turn Windows Features On And Off. The Windows Features dialog box appears.
4. Expand the Remote Server Administration Tools container and the Feature Administration Tools container, as shown in Figure 4-26.

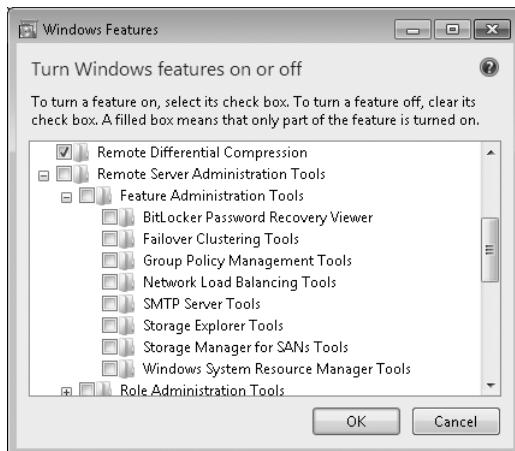


FIGURE 4-26 The Windows Features dialog box

5. Select the Group Policy Management Tools check box and click OK. Windows 7 enables the Group Policy Management Tools feature.

### EXERCISE 3 Creating a GPO

After you install and enable the Group Policy Management Tools feature, you can use GPMC to create a GPO.

1. Click Start, and then click Administrative Tools\Group Policy Management\. The Group Policy Management console appears.
2. Expand the Forest and Domains containers. Then expand the container that represents your domain and select Group Policy Objects, as shown in Figure 4-27.

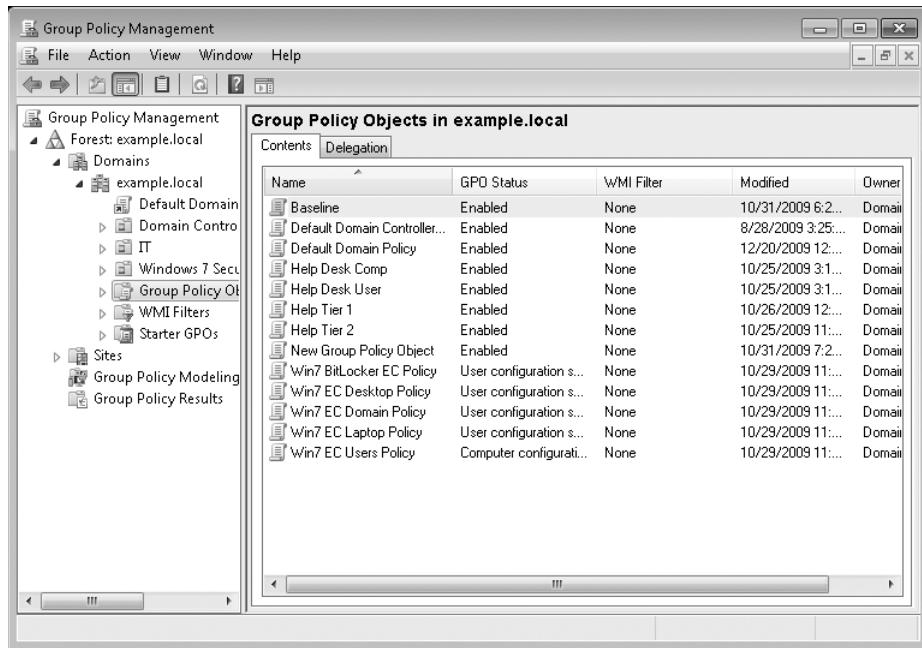


FIGURE 4-27 The Group Policy Objects container in the GPMC

3. Right-click the Group Policy Objects container and, from the context menu, select New. The New GPO dialog box appears, as shown in Figure 4-28.

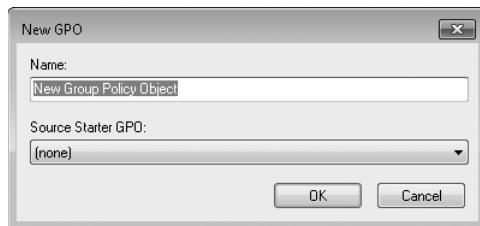


FIGURE 4-28 The New GPO dialog box

4. In the Name text box, type **Baseline** and click OK. The Baseline GPO appears in the Group Policy Objects list.

5. Right-click the Baseline GPO you created and, from the context menu, select Edit. The Group Policy Management Editor appears, as shown in Figure 4-29.

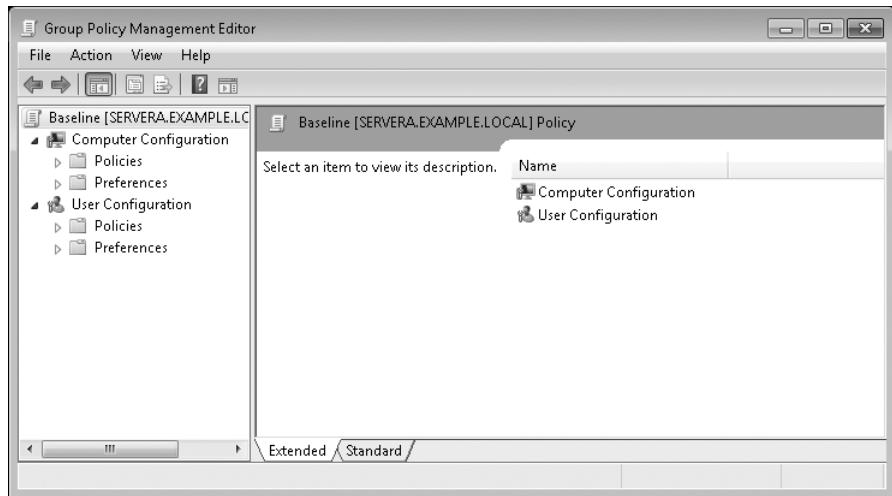


FIGURE 4-29 A new GPO in the Group Policy Management Editor

6. Close the Group Policy Management Editor and Group Policy Management Console windows.

## Lesson Summary

- An enterprise workstation deployment typically has a baseline configuration that applies to all of the computers. This configuration might consist of standard applications, but typically also includes configuration settings that control features such as error reporting, auditing, and user profiles.
- An enterprise is likely to have differing requirements for various groups of workstations. Administrators might therefore have different configuration settings for each of the workstation images they maintain.
- Defining workstation configuration settings should begin early in the Plan phase of the deployment project and be subject to the same planning, testing, and deployment procedures as the rest of the project.
- Windows 7 now supports more than 2,500 settings that you can configure using Group Policy, including a large number of preference settings that formerly were configurable only by using scripts.
- You can write scripts using batch or command files, Windows PowerShell commands, or any scripting language supported by the Windows Script Host (WSH), including VBScript and JScript.

## Lesson Review

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

### NOTE ANSWERS

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

1. Which of the following is not one of the primary tools desktop administrators typically use for the purpose of deploying configuration settings to a large number of workstations?
  - A. Group Policy Management Console
  - B. Local Group Policy Editor
  - C. Logon/logoff scripts
  - D. Startup/shutdown scripts
2. Which of the following are the primary differences between startup/shutdown scripts and logon/logoff scripts? (Choose all that apply.)
  - A. Logon/logoff scripts run under the account with which the user logged on and are relatively limited in the types of tasks they can perform.
  - B. Startup/shutdown scripts use the credentials of the computer object, have System privileges on the local computer, and can access the entire local file system and the registry.
  - C. Logon/logoff scripts run under the account with which the user logged on, have System privileges on the local computer, and can access the entire local file system and the registry.
  - D. Startup/shutdown scripts use the credentials of the computer object but are relatively limited in the types of tasks they can perform.
3. Which of the following are languages that you can use to create startup/shutdown and logon/logoff scripts? (Choose all that apply.)
  - A. Batch files
  - B. Windows Script Host
  - C. VBScript
  - D. Windows PowerShell

4. Which of the following statements about Group Policy processing speed is true?
  - A. Foreground processing is faster than background processing.
  - B. Monolithic GPOs always configure workstations faster than functional GPOs.
  - C. How often you modify GPOs has no effect on the speed at which workstations process them.
  - D. Asynchronous processing is faster than synchronous processing.
5. Which of the following is not true of functional GPOs?
  - A. Functional GPOs are numerous and contain relatively few settings.
  - B. Functional GPOs are dedicated to a specific area or type of setting.
  - C. Functional GPOs enable you to organize related settings into separate GPOs so that you can delegate responsibility for them to specific administrators.
  - D. Functional GPOs contain all of the settings a workstation needs, including Computer Configuration and User Configuration settings, Policies and Preferences settings, and Administrative Templates settings.

## Lesson 2: Creating a Client Baseline Configuration

After you decide how you are going to configure your Windows 7 workstations, you need to think about exactly what settings you are going to configure. Chapter 5, “Configuring Security and Internet Explorer,” discusses security settings and settings to configure Microsoft Internet Explorer. This lesson is devoted to settings that you are likely to want to configure on all of your Windows 7 workstations—standard settings that you can use to create a baseline configuration for all of your machines.

**After this lesson, you will be able to:**

- Configure standard settings to create a workstation baseline.

**Estimated lesson time:** 60 minutes

## Deploying a Baseline Configuration

A baseline is a starting point, and in this context it refers to a collection of configuration settings that you will apply to all of your workstations. After you have a baseline in place, you can build on it by adding settings suitable for specific job roles and workstation configurations. Many of the settings in a typical baseline configuration are security-related, and these are covered in more detail in Chapter 5. This lesson covers settings that report information to administrators and contribute to the client’s operational environment.

A baseline implementation can work in several ways. Some administrators create a single baseline GPO and link it to the domain object or to a high-level OU so that all of the computers on the network receive those settings. Then, to create configurations for more specific workstation types, administrators create additional, role-specific GPOs and link them to OUs farther down in the hierarchy, or they use filtering techniques to limit GPO dissemination to specific computers.

You can also create a baseline GPO and make multiple copies of it, modifying each copy by adding role-specific policies and settings. Each workstation configuration then has all of its settings in a single GPO.

## Using GPO Accelerator

Although many desktop administrators create their baseline configurations from scratch by creating new, empty GPOs, you can choose from other alternatives. The GPO Accelerator is a command-line tool provided by Microsoft that enables administrators to implement the EC or SSLF workstation environment automatically on an AD DS network.

The GPO Accelerator is a free download, included as part of the Security Compliance Management Toolkit. When you execute the GPOAccelerator.msi file on a Windows server or workstation, the installer adds a script file called GPOAccelerator.wsf and an executable called GPOAccelerator.exe.

In this case, the script file does all the work. The executable is just a wizard that enables you to select program features using a graphical interface, as shown in Figure 4-30. After you make your selections, the wizard executes the script from the command line, inserting the appropriate parameters.



FIGURE 4-30 The graphical interface for GPO Accelerator

When you run GPOAccelerator, the tool first creates the appropriate GPOs, as shown in Figure 4-31, and populates them with a standardized group of configuration settings for the environment you have chosen.

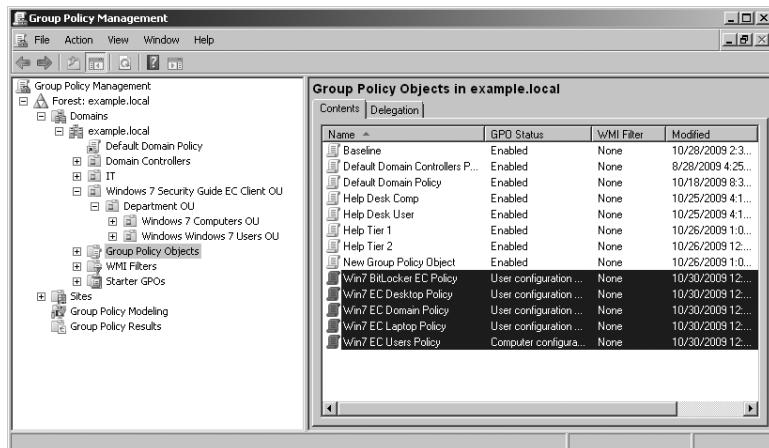


FIGURE 4-31 GPOs created by GPO Accelerator

Then the GPO Accelerator can create a hierarchy of OUs in your domain, as shown in Figure 4-32, and link the GPOs to the proper OUs.

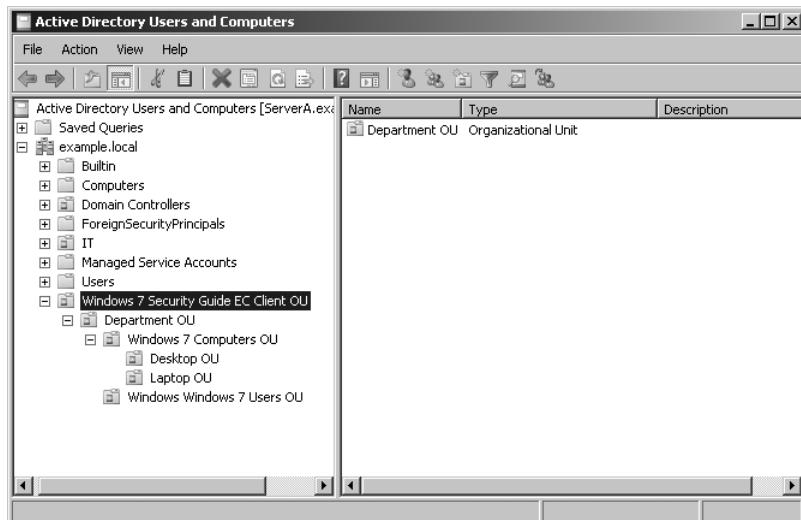


FIGURE 4-32 OUs created by GPO Accelerator

The GPOs that the GPOAccelerator tool creates contain a large variety of settings, including the following:

- Password policies that force users to change their passwords regularly
- Account lockout policies that prevent people from trying to guess user passwords
- Audit policies that monitor security events
- Event log settings that enlarge the sizes of the logs
- Windows Update settings that cause workstations to download updates and prompt for installation

These and many other settings implement the EC and SSLF environments described in the “Windows 7 Security Guide.” Although Microsoft has tested these environments in typical settings, you must test them thoroughly yourself on your own network before you implement them on a production network.

## Configuring Windows Error Reporting

Windows Error Reporting (WER) is the default exception handler client in Windows 7, which gathers information about user-mode and kernel-mode errors and sends it to Microsoft Dr. Watson servers on the Internet by default. Collectively, the client and servers are known as the Watson Feedback Platform (WFP).

In its default configuration, the WER client communicates directly with the Microsoft servers on the Internet, and users can configure the behavior of the client from the Windows Action Center, using the interface shown in Figure 4–33.

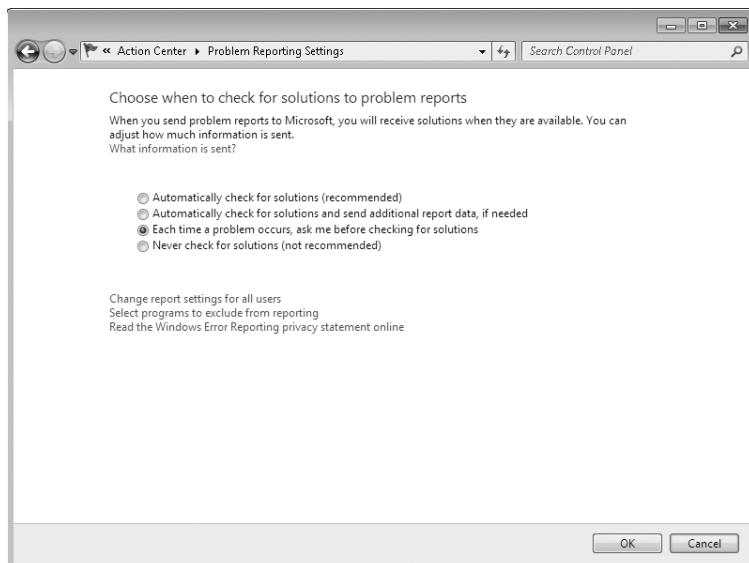


FIGURE 4-33 The Problem Reporting Settings interface in the Windows 7 Action Center

In an AD DS environment, however, you can also configure WER using Group Policy, and many administrators configure the WER client in their baseline GPOs. The policies that control WER are located in the following containers:

- Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\
- User Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\

Table 4-1 lists the settings you can configure for WER.

**TABLE 4-1** Group Policy Settings for Windows Error Reporting

POLICY NAME	USER OR COMPUTER	DESCRIPTION
Configure Error Reporting	Computer only	Disables WER configuration via Control Panel and enables administrators to specify a UNC path to a local server where WER clients will store their error data instead of sending it to the Microsoft servers on the Internet
Disable Logging	Both	Prevents WER from creating events for errors in the System log
Disable Windows Error Reporting	Both	Prevents WER from sending error information to the Microsoft servers on the Internet
Display Error Notification	Computer only	Enables administrators to control whether WER informs users of an error and provides the option to report the error
Do Not Send Additional Data	Both	Configures WER to deny requests for additional data from Microsoft servers on the Internet
Prevent Display of the User Interface For Critical Errors	Computer only	Prevents WER from displaying the error reporting interface when a critical error occurs
<b>ADVANCED ERROR REPORTING SETTINGS</b>		
Configure Corporate Windows Error Reporting	Computer only	Specifies the name of the server on the local network to which WER should send error data instead of the Microsoft servers on the Internet
Configure Report Archive	Both	Specifies how much information clients should store in the WER archive
Configure Report Queue	Both	Specifies whether WER clients should queue error reports or prompt to send them immediately
Default Application Reporting Settings	Computer only	Specifies whether WER should process general application errors

POLICY NAME	USER OR COMPUTER	DESCRIPTION
List of Applications to Always Report Errors For	Computer only	Specifies the applications that should be included in WER error reporting
List of Applications to be Excluded	Both	Specifies the applications that WER should exclude from its error reporting
List of Applications to Never Report Errors For	Computer only	Specifies the applications that WER should never include in its error reporting
Report Operating System Errors	Computer only	Specifies whether WER should process operating system errors
Report Unplanned Shutdown Events	Computer only	Specifies whether WER should process unplanned shutdowns as errors
<b>CONSENT</b>		
Configure Default Consent	Both	Specifies whether WER should prompt the user for consent before reporting errors
Customize Consent Settings	Both	Specifies whether WER should send the minimum error reporting data without consent and prompt the user for consent to send additional data
Ignore Custom Consent Settings	Both	Specifies whether the default consent settings should override the custom consent settings

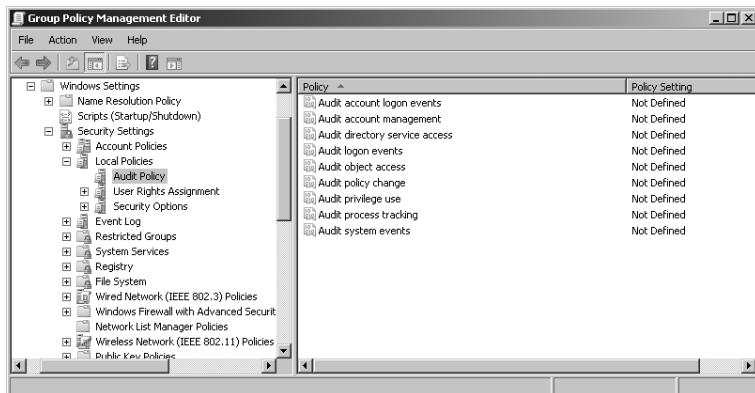
## Creating Auditing Policies

Auditing is one of the most powerful ways for administrators to monitor ongoing events on their workstations. When you configure auditing in Group Policy, workstations track specific types of events and record them in the computer's Security log for examination by administrators at a later time.

For example, if you configure your workstations to audit account logon failures, the system will create an event log entry each time a user types an incorrect password. If you see a large number of failed logon attempts, you can assume that someone is trying to guess a user's password and you can take appropriate measures to stop that person.

Windows has had auditing capabilities for a long time, but Windows 7 and Windows Server 2008 R2 have extended the operating system's auditing function, enabling administrators to audit events on a much more granular level.

The standard auditing policies, which you can apply to all Windows servers and workstations, are located in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy container of a GPO, as shown in Figure 4-34.



**FIGURE 4-34** The contents of the Audit Policy container in a Group Policy object

For all auditing policies, you can specify whether to monitor successes, failures, or both. The settings available in the Audit Policy container are as follows:

- **Audit account logon events** Monitors attempts to authenticate to the local computer across the network
- **Audit account management** Monitors attempts to create, modify, or delete user accounts and groups, as well as attempts to change user passwords
- **Audit directory service access** Monitors attempts to access Active Directory objects
- **Audit logon events** Monitors attempts to interactively log on to the local machine
- **Audit object access** Monitors attempts to access non–Active Directory objects, such as folders, files, or printers, for which you have enabled auditing
- **Audit policy change** Monitors attempts to modify user rights assignments, audit policies, account policies, or trust policies
- **Audit privilege use** Monitors attempts to exercise user rights
- **Audit process tracking** Monitors process-related events, including process creation and process termination
- **Audit system events** Monitors a variety of events that can affect the security of the system

For Windows 7 workstations, you can use a more advanced set of audit policy subcategories, which enable you to monitor more specific events. To use these subcategories, you must first enable the Audit: Force Audit Policy Subcategory Settings (Windows Vista or Later) To Override Audit Policy Category Settings policy, found in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options container.

After you enable this setting, you can use the settings found in the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies container, as shown in Figure 4-35.

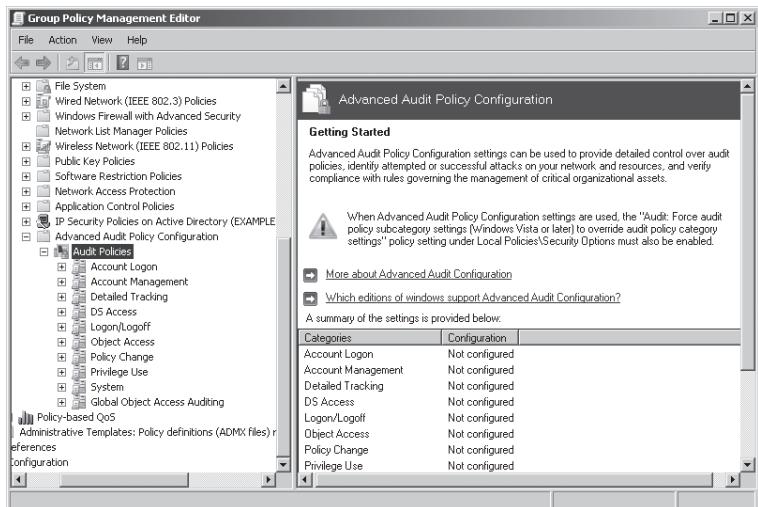


FIGURE 4-35 The Advanced Audit Policy Configuration container

This container has 10 subcategories with a total of 55 auditing policies, which enable you to monitor highly specific events. For example, the Account Logon subcategory contains four policies, instead of the one available in standard auditing, enabling you to monitor individual stages of the logon process, including credential validation, Kerberos Authentication Service transactions, Kerberos Service ticket operations, and others.

#### **IMPORTANT USING ADVANCED AUDIT POLICIES**

To create a GPO containing settings in the Advanced Audit Policy Configuration container, you must run GPMC on a computer running Windows 7 or Windows Server 2008 R2, and the computer must be targeting a domain controller running Windows Server 2008 R2. However, after you create the GPO, any domain controller can deploy it, so you do not have to have all Windows Server 2008 R2 domain controllers on your network.

If you have workstations running operating systems other than Windows 7, you must make sure that only the Windows 7 computers receive the GPO containing the Advanced Audit Policy Configuration settings. This means that you must put the Windows 7 computers in a separate OU or use filtering to prevent other operating systems from receiving the GPO.

## Creating a Folder Redirection Policy

Folder Redirection is a set of policies that administrators can use to control where users store their personal data. Many administrators prefer users to store their data on server drives, rather than local ones. This enables the administrators to secure the data, as well as back it up and recover it more easily. Storing data on servers also makes it possible to have roaming users; individuals can access the files they need from any computer on the network.

To make this possible without reconfiguring each workstation individually, administrators can use these Folder Redirection policies, which cause workstations to redirect specific folders to shares on the network. The policies are located in the User Configuration\Policies\Windows Settings\Folder Redirection container, as shown in Figure 4-36.

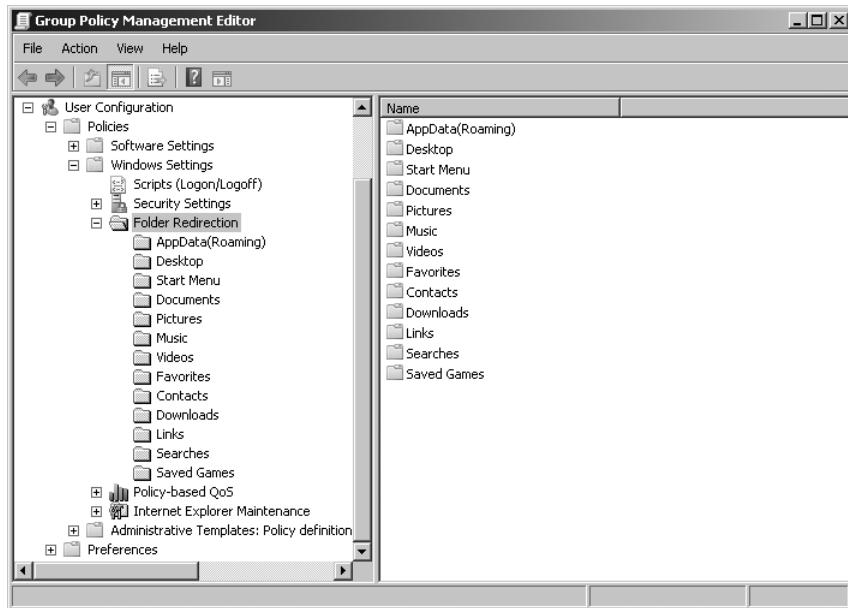


FIGURE 4-36 The Folder Redirection container in a GPO

When you configure one of the Folder Redirection policies, you see a Properties sheet like the one shown in Figure 4-37.

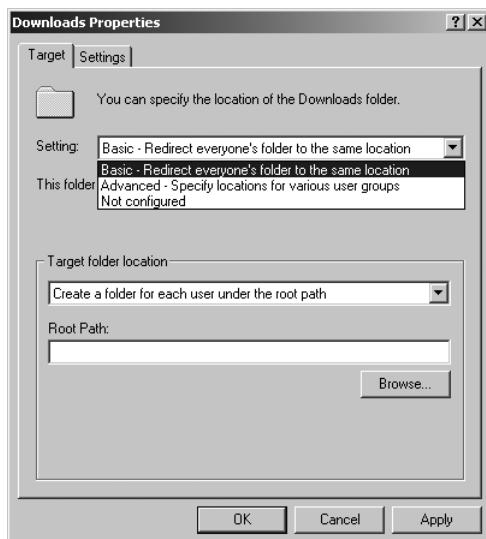


FIGURE 4-37 A folder redirection policy's Properties sheet

Each policy provides the following three options:

- **Basic** Redirects the folder to a specified location, to a folder named for the user at a specified location, to the home directory specified in the user's account, or to the local user profile location.
- **Advanced** Redirects the folder to different locations based on the user's group memberships.
- **Not Configured** The folder is not redirected and remains in its original location.

**NOTE REDIRECTING MEDIA**

You can choose a fourth option, **Follow The Documents Folder**, which appears only on the Properties sheets for the Pictures, Music, and Videos policies. This option causes the redirected folder to appear as a subfolder of the redirected Documents folder.

One of the most common configurations is for an administrator to create a folder called Users on a network share and use the Basic option with the Create A Folder For Each User Under The Root Path setting to redirect folders to that location. The policy then creates a separate subfolder for each user and stores the contents of the selected folder there.

## Designing a User Profile Strategy

A user profile is a collection of folders and registry settings that together provide the user environment on a Windows computer. By default, Windows 7 workstations create a separate profile in the C:\Users folder for each user that logs on to the computer. These are called local user profiles.

Many administrators prefer to store user profiles on servers, however, so that users can access them from any workstation. This makes it possible for users to maintain their own desktop environments, even in a workplace where they log on at a different computer each day. These are called roaming profiles. When a workstation is configured to use roaming profiles, it downloads the profile from the server each time the user logs on. Later, when the user logs off, the workstation copies any changes that the user made to the profile back to the copy on the server.

Some administrators also prefer to create a single server-based profile containing a standard desktop environment for all of their users and provide them with read-only access to it. The process is the same as for a roaming profile when the user logs on, but the workstation does not copy the changed profile back to the server at logoff. This enables the users to modify their environments during a session, but they lose those modifications when they log off. Each time they log on again, the workstation reloads the standard profile. This is called a mandatory profile.

One final variation, called a super-mandatory profile, requires users to access the server-based profile to log on. If the workstation cannot access the profile on the network, the logon fails.

### Quick Check

- Which of the user profile types described in this section can be used safely by multiple network users simultaneously?

### Quick Check Answer

- Multiple users can access mandatory and super-mandatory profiles simultaneously, because the workstations do not upload any changes to the profiles on the server. Standard roaming profiles are not suitable for multiple users because updates might conflict.

## Creating Roaming Profiles

To create roaming profiles and configure workstations to use them with Group Policy, use the following procedure:

1. Create a folder on the server where you want to store the profiles and share it.
2. Configure the profile folder with the NTFS permissions shown in Table 4-2.

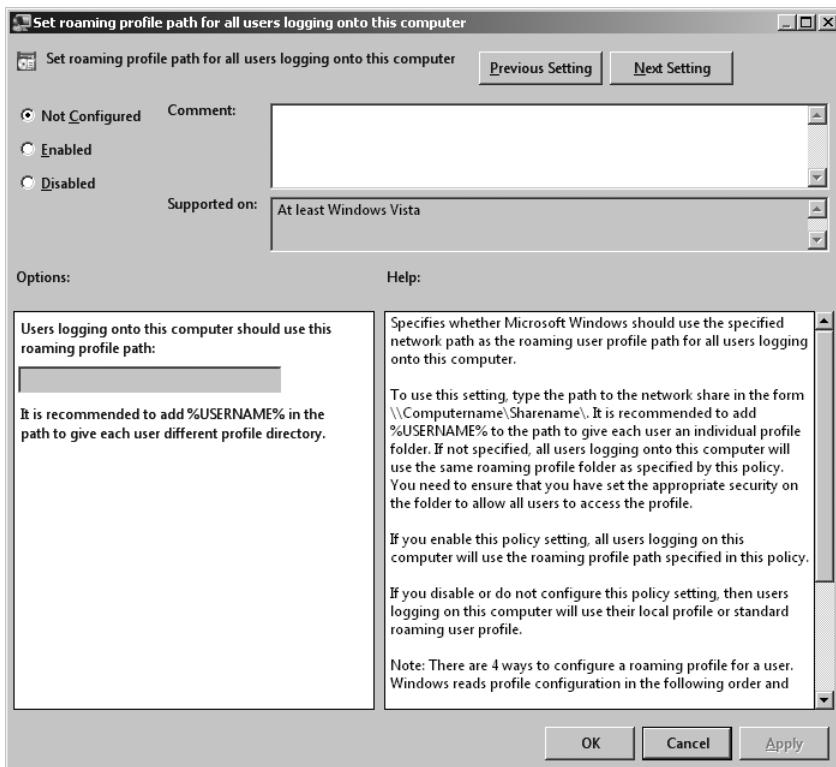
**TABLE 4-2** NTFS Permissions for a Roaming Profiles Folder

SECURITY PRINCIPAL	PERMISSIONS	APPLY TO
Creator/Owner	Allow Full Control	Subfolders and files only
Domain Users	Allow List Folder/Read Data Allow Create Folders/ Append Data	This folder only
LocalSystem	Allow Full Control	This folder, subfolders, and files
Administrator	No permissions	
Everyone	No permissions	

3. Configure the permissions for the profile share by granting the Allow Full Control permission to the Everyone special identity.
4. You can copy a default network profile to the NETLOGON share on a domain controller so that it will be replicated to all of the domain controllers for that domain.

This causes users to start with the default network profile when they log on for the first time, instead of using the default profile on the local disk.

5. In the Computer Configuration\Policies\Administrative Templates\User Profiles container of a GPO, enable the Set Roaming Profile Path For All Users Logging On To This Computer policy, as shown in Figure 4-38, and specify the path to the profile share you created, using the following format: \\servername\sharename%\%USERNAME%.



**FIGURE 4-38** The Set Roaming Profile Path For All Users Logging On To This Computer Properties sheet

This causes the workstation to create a folder on the share, named for the user logging on, in which the workstation stores the user's roaming profile.

You can configure workstations to use different roaming profile paths by creating multiple GPOs and applying them to different OUs or using filtering to apply them to different computers in a single OU. You can also configure profile paths for individual users by specifying a profile path on the Profile tab of a user's Properties sheet, as shown in Figure 4-39.

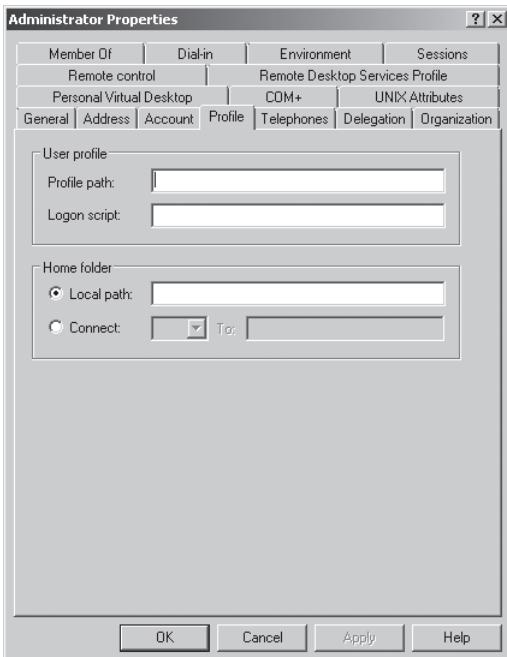


FIGURE 4-39 The Profile tab of a user's Properties sheet

**NOTE CREATING MANDATORY PROFILES**

Creating a mandatory profile is roughly the same as creating a roaming profile. The primary difference is that instead of giving users the Allow Full Control permission for the folder where the profile is stored, you give them the Allow Read permission only. This prevents the workstations from uploading changes to the profile stored on the server.

**PRACTICE Configuring Auditing**

To create a baseline GPO, you configure the standard Group Policy settings that you want to apply to all of your workstations, which could include auditing policies. This practice assumes that you have already completed the Lesson 1 practice, in which you downloaded, installed, and enabled GPMC, and then created a GPO called Baseline.

**EXERCISE 1 Configuring Standard Audit Policies**

After installing GPMC and creating a GPO, you can use Windows 7 to create a baseline workstation configuration.

1. Click Start, and then click Administrative Tools\Group Policy Management. The Group Policy Management console appears.

2. Expand the Forest and Domains containers. Then expand the container representing your domain and select Group Policy Objects.
3. Right-click the Baseline GPO you created earlier and, from the context menu, select Edit. The Group Policy Management Editor window appears.
4. Expand the Computer Configuration, Policies, Windows Settings, Security Settings, and Local Policies containers and select Audit Policy.
5. Double-click Audit Account Logon Events. The Audit Account Logon Events Properties sheet appears.
6. Select the Define These Policy Settings check box. The Audit These Attempts check boxes are activated.
7. Clear the Success check box and select the Failure check box. Then click OK.
8. Open the Audit Account Management Properties sheet.
9. Select the Define These Policy Settings check box, and then select both the Success and Failure check boxes and click OK.
10. Leave Group Policy Management Editor open for the next exercise.

## **EXERCISE 2 Configuring File and Folder Auditing**

The Audit Object Access policy enables you to audit specific types of access to specific objects by specific users groups. To do this, you must configure the policy and then configure auditing on the objects you want to monitor.

1. In the Group Policy Management Editor, in the Audit Policy container, double-click Audit Object Access. The Audit Object Access Properties sheet appears.
2. Select the Define These Policy Settings check box, and then choose both the Success and Failure check boxes and click OK.
3. Click Start. Then click All Programs\Accessories\Windows Explorer. The Windows Explorer window appears.
4. Expand Computer and Local Disk (C:).
5. Create a new folder called Data on the C: drive.
6. Right-click the C:\Data folder you created and, from the context menu, select Properties. The Data Properties sheet appears.
7. Click Security, and then click Advanced. The Advanced Security Settings For Data dialog box appears.
8. Click the Auditing tab, and then click Edit. A new Advanced Security Settings For Data dialog box appears, containing only an Auditing tab, as shown in Figure 4-40.

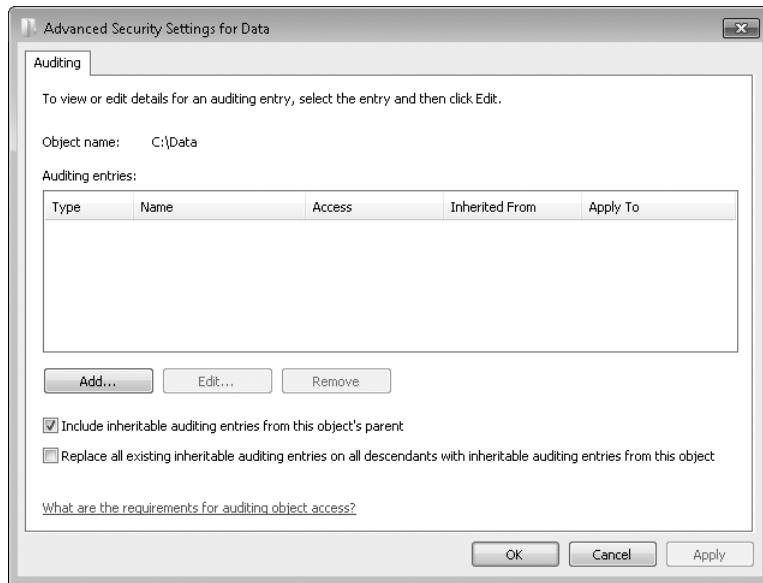


FIGURE 4-40 The Advanced Security Settings For Data dialog box

9. Click Add. The Select User, Computer, Service Account, Or Group dialog box appears.
10. In the Enter The Object Name To Select text box, type **Domain Users** and click OK. The Auditing Entry For Data dialog box appears, as shown in Figure 4-41.

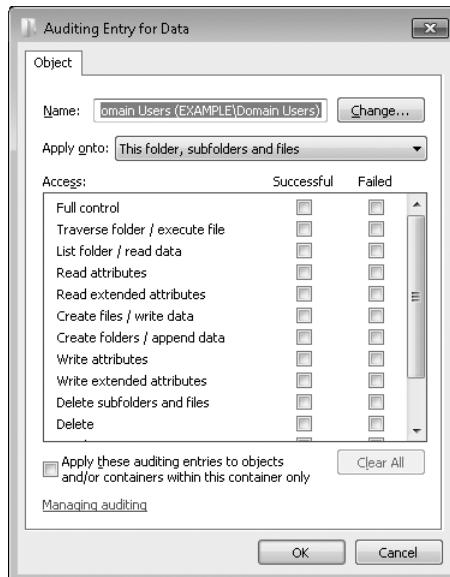


FIGURE 4-41 The Auditing Entry For Data dialog box

11. Select the Successful and Failed check boxes for the List Folder/Read Data permission and click OK. A new entry appears in the Auditing Entries list.
12. Click OK twice to close the two Advanced Security Settings For Data dialog boxes.
13. Click OK to close the Data Properties sheet.

## Lesson Summary

- A baseline configuration is a starting point, and in this context it refers to a collection of settings that you apply to all of your workstations.
- GPO Accelerator is a tool that automatically creates GPOs and OUs for the preconfigured EC and SSLF environments defined in the Windows Security Guides.
- Windows Error Reporting is a client/server technology that enables workstations to automatically send error information to a server. Administrators can configure WER using Group Policy.
- Auditing is the process by which computers are configured to create event log entries in response to specific security-related system activities. GPOs contain standard audit policies and advanced audit policies that apply only to Windows 7 and Windows Server 2008 R2.
- Folder redirection policies enable users to store their personal data on network servers so that administrators can secure and back up the data and users can access it from any workstation.
- A user profile is a collection of folders and registry settings that together provide the user environment on a Windows computer. Windows 7 workstations create local user profiles in the C:\Users folder for each user that logs on.
- Profiles stored on servers (so that users can access them from any workstation) are called roaming profiles. Read-only roaming profiles are called mandatory profiles. Mandatory profiles that must be accessible to users from the network for successful logons are called super-mandatory profiles.

## Lesson Review

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

### NOTE ANSWERS

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

- 1.** Which of the following folders can you make subdirectories of the Documents folder using Folder Redirection policies? (Choose all that apply.)
  - A.** Videos
  - B.** Music
  - C.** Saved Games
  - D.** Pictures
- 2.** Which of the following types of user profiles prevents the user from logging on if it is not accessible on the network?
  - A.** Local user profile
  - B.** Roaming profile
  - C.** Mandatory profile
  - D.** Super-mandatory profile

## Chapter Review

---

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

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

## Chapter Summary

- The primary method for deploying configuration settings to Windows 7 workstations in an enterprise environment is Group Policy. To do this, you create Group Policy objects using the Group Policy Management Console and link them to Active Directory Domain Services objects, such as domains, sites, and organizational units. You can also configure workstations using scripts that execute when the computer starts up or shuts down or when users log on or log off.
- A baseline workstation configuration consists of Group Policy settings that administrators want to deploy to all of the workstations on the network. These settings can include policies that configure Windows Error Reporting, auditing, folder redirection, and user profiles.

## 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.

- asynchronous processing
- functional GPO
- GPO Accelerator
- mandatory profile
- monolithic GPO
- roaming profile
- starter GPO
- super-mandatory profile
- synchronous processing
- user profile
- VBScript
- Windows Error Reporting

## Case Scenarios

In the following case scenarios, you will apply what you've learned about subjects of this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Deploying GPOs

Ed is creating GPOs for the workstations in the Sales department at A. Datum Corporation. In their Active Directory hierarchy, a Sales OU contains the computer and user objects for the entire department, except for the Order Entry team, which has its own OU subordinate to Sales. The workstations in the Order Entry department use a highly restricted environment, while the Sales workstations are relatively open. Ed has created two GPOs, one for Sales and one for Order Entry. The GPOs have precisely the same policies configured, but their settings are different. A Baseline GPO containing settings for all of the computers in the organization is also in the hierarchy and is linked to the Adatum.local domain object. Which of the following is the easiest way to deploy the GPOs to the appropriate workstations successfully?

- a. Link the Sales and Order Entry GPOs to the domain object.
- b. Link the Sales GPO to the Sales OU and the Order Entry GPO to the Order Entry OU.
- c. Link the Sales GPO to the Sales OU and the Order Entry GPO to the Order Entry OU, and then block Inheritance to the Order Entry OU.
- d. Create Sales and Order Entry groups and use security filters to apply the Sales and Order Entry GPOs to the appropriate computers.

## Case Scenario 2: Configuring Audit Policies

Alice is configuring auditing policies for her enterprise network, and she wants to use the Advanced Audit Policy Configuration settings for her Windows 7 workstations. However, the company also has workstations running Windows Vista and Windows XP SP2, and the various operating systems are distributed relatively evenly throughout the company and throughout the organization's Active Directory Domain Services hierarchy. Alice has created a separate GPO containing the Advanced Audit Policy Configuration settings. How can she deploy the GPO so that only the Windows 7 workstations receive these settings, without modifying the AD DS hierarchy?

## Suggested Practices

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

### Design Standard System Settings 1

In this practice, you configure Advanced Audit Policy Configuration settings for Windows 7 computers.

- **Practice 1** Open the Baseline GPO you created earlier in this chapter and enable the Audit: Force Audit Policy Subcategory Settings (Windows Vista or Later) To Override Audit Policy Category Settings policy in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options container.
- **Practice 2** Browse to the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies container. Then examine the various auditing policies available there and enable the ones that you think are appropriate for the network on which you are working.

### Design Standard System Settings 2

In this practice, you install the GPO Accelerator tool and use it to create GPOs for the SSLF environment.

- **Practice 1** Download the Security Compliance Management Toolkit from <http://www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e&displaylang=en> and install the GPO Accelerator program.
- **Practice 2** Run the GPO Accelerator script with the following command:  
`gpoaccelerator.wsf /win7 /sslf /tab`
- **Practice 3** Examine the settings in the GPOs created by the GPO Accelerator program.

## 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 70-686 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.



# Configuring Security and Internet Explorer

Organizations are far more likely to suffer loss of data through the carelessness of employees than they are through deliberate attacks by nefarious third parties. With this in mind, you should realize that configuring security is more than just configuring firewall rules to stop dangerous lurkers on the Internet from sneaking inside the perimeter network. Configuring security is about ensuring the integrity of your organization's data. This effort can include taking steps as simple as ensuring that a hard disk or sensitive file is encrypted. When you take this precaution, you stop unauthorized third parties from recovering data from a lost or stolen portable computer. Configuring security can also include making sure that the default Web browser, used to surf the dangerous tides of the Internet, is as sturdy as possible. Malicious software is far more likely to infect a computer through a browser than it is by means of an attacker randomly throwing packets against a firewall in the hope of finding a weakness in the network armor. In this chapter, you learn how to configure Windows 7 client security to meet the needs of your organization. You learn about encryption, firewall rules, application control policies, and account policies. You also learn how to use Group Policy and the Internet Explorer Administration Kit to configure Windows Internet Explorer to best meet the security needs of your organization.

## Exam objectives in this chapter:

- Define client security standards.
- Define Windows Internet Explorer settings.

## Lessons in this chapter:

- Lesson 1: Configuring Client Security **172**
- Lesson 2: Configuring Windows Internet Explorer **196**

## Before You Begin

To complete the exercises in the practice sessions in this chapter, you need to have completed the following steps:

- Installed the Windows 7 operating system on a stand-alone client PC named WKSTN1, as described in the Introduction at the beginning of this book.
- To perform Exercise 2 in Lesson 2, you will need an active connection to the Internet and need to download the Internet Explorer Administration Kit 8 from the following TechNet Web site: <http://technet.microsoft.com/en-us/ie/bb219517.aspx>.



### REAL WORLD

Orin Thomas

A laptop computer left at an airport screening station costs its owner far more than replacement hardware. When someone misplaces a company's laptop computer, the organization must assess what could happen if a third party with less-than-noble intentions recovers the data stored on that computer. To make that assessment, someone needs to perform an investigation to determine what data might have been exposed. Someone could publicly post or covertly use sensitive data that was stored on the laptop. Lost laptop computers may host the private personal data of other people. Having to admit to clients that their private information may now be public not only has a financial cost, but a cost to an organization in terms of loss of trust and reputation. This is why full volume encryption should be mandatory on the portable computers in your organization. If the hard disks on your portable computers are properly encrypted, an unauthorized third party will be unable to recover data from those computers. As a security administrator, you cannot prevent people in your organization from misplacing laptop computers any more than you can prevent them from losing their car keys. But you can correctly apply security settings that minimize the cost of losing a laptop.

## Lesson 1: Configuring Client Security

In the past, client computers, like servers, rarely moved from the office building because computers were big and heavy, and it took a fair amount of effort to move them from the desk on which they had been set up. Having physical computers tied to a single location provided an organization with a basic level of security. Unless someone broke into the premises and stole computers, only a certain amount of data left the office on a regular basis. Only so many documents could fit on a floppy disk! Today's security administrator faces greater challenges because the majority of computers being made and sold are laptops. In many organizations,

the computers that people use for their daily work are what they take home with them each evening. The mobility of portable computers and high-capacity thumb-size storage devices naturally increase the chance that a significant amount of data will fall out of your organization's control. Because administrators can do little to stop these devices being lost or stolen after they leave the office, they must take other actions to secure organizational data. This lesson looks at the client security policies that an administrator can configure to mitigate some of these problems. The lesson also covers other technologies available in Windows 7 that can form integrated parts of your organization's security strategy.

**After this lesson, you will be able to:**

- Configure Encrypting File System, BitLocker, and BitLocker To Go.
- Create Windows Firewall with Advanced Security rules.
- Define user account control policies.
- Manage user account policies.
- Restrict application execution.

**Estimated lesson time: 40 minutes**

## Using Encryption

Encryption encodes data. When encryption is applied properly, authorized people are able to decrypt the data and unauthorized people are unable to decrypt the data.

Windows 7 can implement encryption by means of two technologies: Encrypting File System and BitLocker Drive Encryption. Encrypting File System, available on Windows 7 Professional, Enterprise, and Ultimate, allows for file and folder encryption. BitLocker (and BitLocker To Go) are available in Windows 7 Enterprise and Ultimate and provide full volume encryption. This means that BitLocker encrypts the entire volume, not just specific files and folders. You can implement one or both of these technologies when designing a client security strategy.

## Configuring BitLocker

In addition to ensuring that all data stored on the client computer is encrypted, BitLocker can also protect the integrity of the boot environment by notifying users of any modifications, such as when the computer suffers an infection by boot sector Trojan malware. If a change to the boot environment occurs, the computer requires the user to enter the BitLocker recovery password to acknowledge the change. If the user has not made the change, the requirement to enter the recovery password serves as a notification that an unauthorized modification has occurred.

BitLocker does not protect data on a computer after the computer is fully active. After the computer starts successfully, BitLocker unlocks the volume. For this reason, it is important to consider BitLocker startup options when developing a client security standard. Startup options include configuring a combination of a Trusted Platform Module (TPM) chip, a personal

identification number (PIN), and a USB device that hosts a special cryptographically generated file, called a startup key. Startup options are configured through the Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require Additional Authentication At Startup Group Policy item, shown in Figure 5-1.

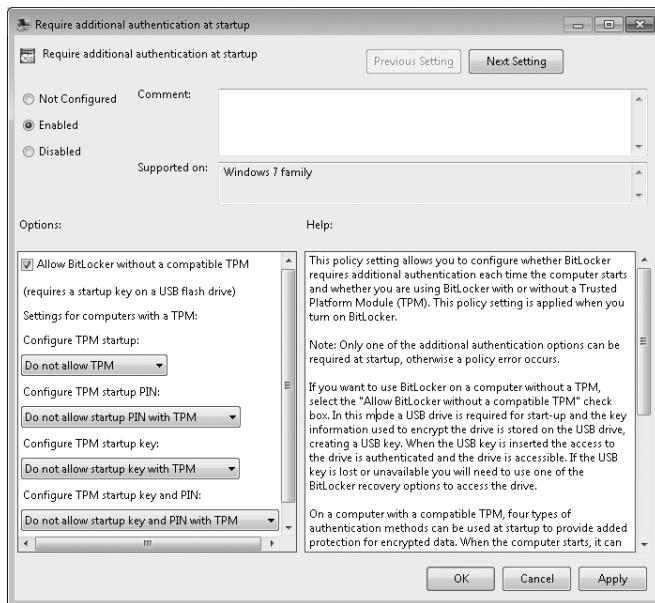


FIGURE 5-1 BitLocker Startup options

Using this policy, you can configure the following BitLocker startup options:

- **TPM-only mode** The user does not have to provide a password at startup. This is the least secure implementation of BitLocker because the hard disk is unlocked at startup.
- **TPM with startup key** User must have a USB startup key connected each time the computer performs a cold boot. If the USB startup key is not connected, the computer boots into recovery mode. Recovery mode is a special mode that allows the computer to start if the BitLocker recovery key is entered. The BitLocker recovery key is different from the startup PIN.
- **TPM with PIN** User must enter a PIN each time the computer performs a cold boot. Failure to enter the PIN forces the computer into recovery mode.
- **TPM with PIN and startup key** User must enter a startup PIN and have the startup key connected. If both these conditions are not met, the computer boots into recovery mode. This is the most secure implementation of BitLocker, but is also the least convenient from the user perspective.
- **BitLocker without TPM** This mode allows the use of BitLocker on a computer that does not have a compatible TPM chip but requires that a USB startup key be present each time the computer performs a cold boot.

Organizations tend to use the BitLocker USB startup key modes only on servers rather than portable computers because ensuring that a specific USB device is connected to a computer at boot time is cumbersome to the user of that computer. This is less of a problem for servers, for which restarts are less frequent than for client machines.

When configuring BitLocker as a part of your organization's client security policy, you should take care to consider how you will be able to recover BitLocker encrypted volumes. In an organizational environment, the most convenient way of recovering data from BitLocker-protected hard disk drives is to configure a data recovery agent. You can do this by assigning a specially configured data recovery agent certificate using the \Computer Configuration\Windows Settings\ Security Settings\Public Key Policies\BitLocker Drive Encryption key. You can also configure Group Policy so that BitLocker can be enabled on volumes only if the BitLocker recovery keys have been safely backed up to Active Directory directory services. This safeguard allows an administrator to recover the BitLocker recovery key from Active Directory in case a recovery operation becomes necessary. You can archive BitLocker keys in Active Directory as long as domain controllers in the environment are running Windows Server 2003 SP1 or later and the schema has been extended. You do not need to extend the schema if Windows Server 2008 domain controllers are in use in the domain.

To ensure that recovery keys are backed up to Active Directory, configure the following policies:

- Choose How BitLocker-Protected Operating System Drives Can Be Recovered
- Choose How BitLocker-Protected Fixed Drives Can Be Recovered

When configuring these policies, ensure that you enable the Do Not Enable BitLocker Until Recovery Information Is Stored To AD DS option, as shown at the bottom of Figure 5-2.

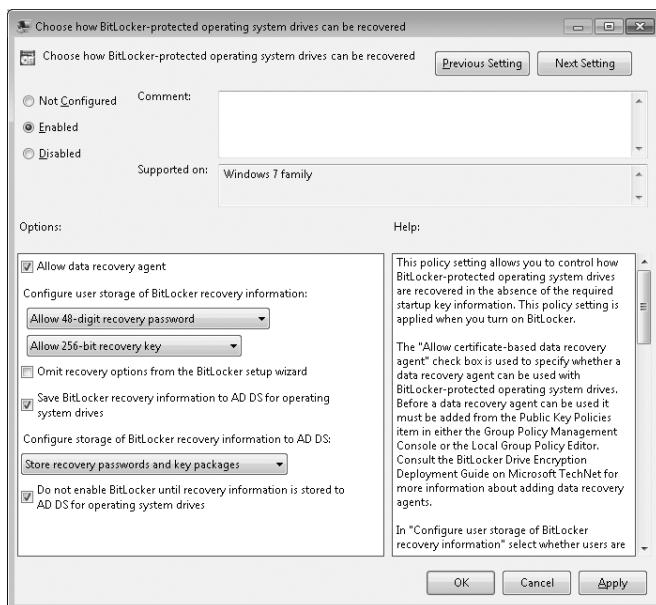


FIGURE 5-2 BitLocker recovery options

Another important part of any client security strategy is informing users of exactly how a specific encryption solution works. A common misconception about BitLocker is that data remains encrypted when copied from a BitLocker-protected drive. If a person copies data stored on a BitLocker-protected volume to a volume not protected by BitLocker, the data is no longer encrypted. Similarly, if a person attaches a file stored on a BitLocker-protected volume to an e-mail message and sends it, the file will not remain encrypted. Misconceptions about encryption are a significant cause of data breaches with users often believing something has remained encrypted when it has been inadvertently decrypted.

#### **MORE INFO BITLOCKER EXECUTIVE OVERVIEW**

For a more detailed summary of how you can make use of BitLocker as a part of your organization's client security standard, consult the following executive overview document hosted on Microsoft TechNet: [http://technet.microsoft.com/en-us/library/dd548341\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd548341(WS.10).aspx).

## **Configuring BitLocker To Go**

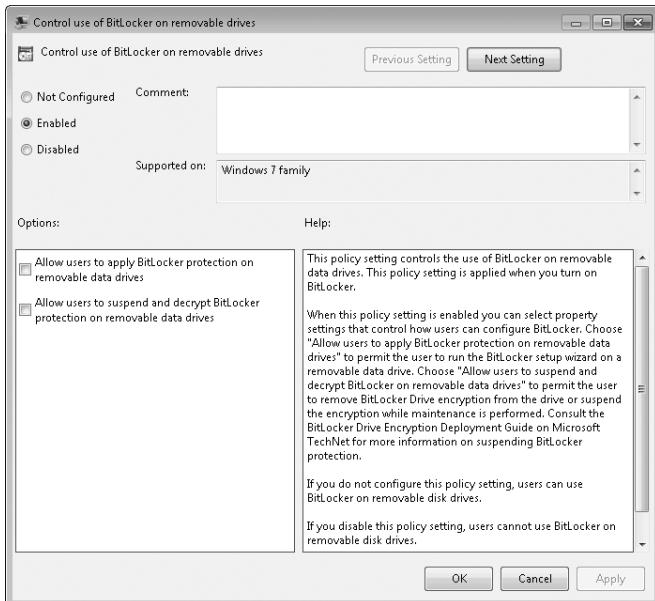
BitLocker To Go allows for the encryption of USB storage devices, such as flash drives and removable hard disk drives. Writing data to BitLocker To Go-protected devices is supported only on computers running Windows 7 Enterprise and Ultimate. With the appropriate password, you can read data from BitLocker To Go-protected devices on all editions of Windows 7, Windows Vista, and Windows XP operating systems. You can configure a removable storage device formatted with either the FAT32 or the NTFS file system to use BitLocker To Go.

BitLocker To Go protects the removable storage device with a single password. When the encrypted device is connected, the user who connects the device enters the password, after which she can access the data on the device. Data on the device cannot be accessed by a user who does not have the BitLocker To Go password. As is the case with BitLocker, the whole volume device is encrypted, which means that items copied to a protected device are automatically encrypted.

Organizations that are concerned about the security of data stored on portable devices are able to configure BitLocker To Go policies so that computer users are able to write data only to portable storage devices that are protected by BitLocker To Go. You can go even further than this and restrict access so that users can write data only to storage devices tagged with a specific organizational identifier and to configure Group Policy so that standard users cannot enable BitLocker To Go on their own removable storage devices. Configuring these policies allows an organization to control the use of removable storage devices by allowing people to use only authorized storage devices. You might want to block people from using their own devices for several reasons. Loss of small flash drives is a significant problem for many organizations. If such devices are provisioned centrally, users who lose these devices must inform someone before a replacement is issued. If people are using their own devices, they may not get around to informing anyone that a possible loss of data has occurred.

BitLocker To Go policies are found in the Computer Configuration\Administrative Templates\BitLocker Drive Encryption\Removable Data Drives node. Here are policies that you should consider configuring as a part of your organization's client security strategy:

- **Control Use Of BitLocker On Removable Drives** Enabling this policy enables the use of BitLocker To Go. You can also configure whether individual users are able to apply BitLocker protection to removable drives and whether they are allowed to suspend and decrypt BitLocker-protected drives, as shown in Figure 5-3.



**FIGURE 5-3** Controlling use of BitLocker To Go

- **Deny Write Access To Removable Drives Not Protected By BitLocker** Through this policy, you can block people from using drives that are not protected by BitLocker. Through this policy, you can also restrict users from writing to any devices that do not have a specific organizational identifier.
- **Allow Access To BitLocker-Protected Removable Data Drives From Earlier Versions Of Windows** This policy allows BitLocker To Go devices to be configured so that they are accessible to clients with the Windows XP and Windows Vista operating system installed.
- **Configure Use Of Passwords For Removable Data Drives** Use this policy to configure password complexity and length for BitLocker To Go passwords.
- **Choose How BitLocker-Protected Removable Drives Can Be Recovered** Use this policy to configure whether a data recovery agent is configured for BitLocker To Go as well as whether recovery data is written to Active Directory. When enabling backup of passwords to Active Directory, you can block BitLocker encrypting devices until successful password backup occurs.

In the practice exercise at the end of this lesson, you will configure BitLocker To Go so that users are able to write data only to protected devices with a specific organizational identifier.

## Configuring Encrypting File System

Encrypting File System (EFS) provides per-user file and folder encryption for client computers running Windows 7 Professional, Enterprise, and Ultimate. You can use EFS to encrypt sensitive folders, such as a user's documents folder, in case you cannot implement BitLocker. You can also use EFS in conjunction with BitLocker, with BitLocker providing volume encryption and EFS encrypting individual files and folders stored on that volume. EFS is different from BitLocker in the following important ways:

- EFS-encrypted files and folders retain their encrypted status only when copied to other NTFS formatted volumes. A file or folder that is hosted on a volume encrypted by BitLocker remains encrypted only when copied to another volume that is also encrypted by BitLocker. EFS-encrypted files are automatically decrypted when a user who is able to access the encrypted file copies it to a volume that does not support EFS, such as the FAT32 file system. EFS-encrypted files also do not remain encrypted if sent as e-mail attachments.
- You can use EFS-encrypted files and folders for different users of the same computer. For example, if Orin and Craig both use the same computer running Windows 7, EFS stops Orin from decrypting Craig's files and makes sure that Craig is unable to decrypt Orin's files. BitLocker and BitLocker To Go work on the volume level, which means that if Craig and Orin have access to the same computer, and NTFS permissions are set appropriately, they can access each other's files. It is possible to use EFS to encrypt a file for multiple users on a per-user basis, but files cannot be encrypted on a per-security-group basis.
- If a user tries to transfer an EFS-protected file to another computer using a removable storage device, he needs to import the associated EFS certificate on the destination computer. EFS-encrypted files can be accessed only if the certificate that was used to encrypt the file is accessible locally. For this reason, it is better to configure an enterprise certificate authority to issue EFS certificates centrally so that a single EFS certificate is used throughout the organization.

When configuring a client security standard using EFS, you should take care to implement a data recovery agent, a key recovery agent, or both types of recovery agent. You can configure an EFS data recovery agent through the Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System node of Group Policy. Key recovery agents are configured on an organization's certificate server.



## Quick Check

- What options do you have to use BitLocker to protect computers that do not have TPM chips?

## Quick Check Answer

- BitLocker can be configured to work on computers without a TPM chip if those computers are configured to boot with a specially prepared USB device.

## Creating Firewall Rules

Windows Firewall with Advanced Security rules can be configured through Group Policy and applied to client computers. This allows administrators to deploy specific firewall rules to all or some computers within an organizational environment. The Windows Firewall With Advanced Security Group Policy node is located under the Computer Configuration\Windows Settings\Security Settings node, as shown in Figure 5-4.

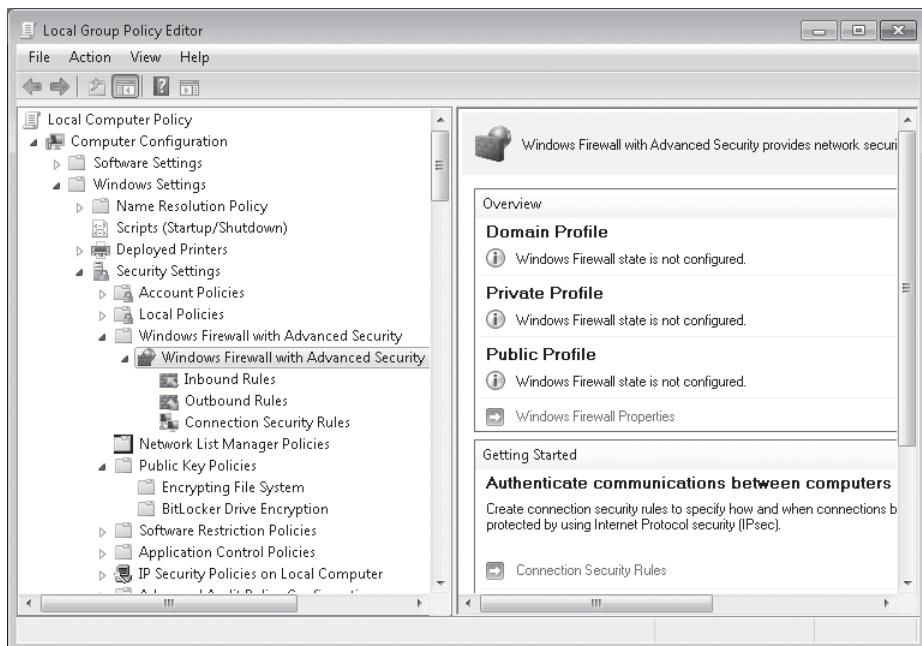


FIGURE 5-4 Windows Firewall with Advanced Security node

As a part of your organization's client security strategy, you can configure Windows Firewall with Advanced Security to perform the following tasks:

- Configure inbound and outbound rules that apply to groups of computers in the organization. This simplifies the process of configuring firewall settings for specific network-aware applications deployed to groups of client computers. For example, you can configure an outbound rule to block all outbound network communication from a specific application.
- Configure rules that apply to groups of computers based on protocol type and port address. For example, you can configure firewall rules to block all inbound SMTP traffic to hosts on the organizational network.
- Configure rules that apply to groups of computers based on a specific local service or application. Rather than just blocking protocols or ports, you can block specific applications or services from communicating with the network.
- Configure rule scope that limits traffic based on the traffic's source or destination. For example, administrators can allow an application to communicate with hosts on the organizational network but block the same application from communicating with hosts on the Internet.
- Configure rules that allow traffic only if it is authenticated in a specific manner. This allows administrators to limit connections to hosts that are members of the same Active Directory domain, rather than hosts that are merely on the same organizational TCP/IP subnet.

Connection security rules allow administrators to authenticate and encrypt connections.

For example, an administrator can use a connection security rule to configure all of the file servers in the organization to drop incoming connections unless the remote computer making the connection can prove its identity as a member of the same Active Directory domain. Connection security rules use the IPsec protocol for authentication and encryption. Connection security rules replace the IPsec policies that are available in previous versions of the Windows client operating system, although for compatibility reasons, both traditional IPsec policies and connection security rules can coexist in the same network environment. Connection security rules can be configured to request authentication for inbound and outbound communication, require authentication for inbound communication but request it for outbound communication, or require authentication for all communication. You can create the following types of connection security rules:

- **Isolation** Isolation rules allow you to limit communication to hosts that are able to authenticate using specific credentials. You would use an isolation rule to ensure that file servers communicate only with hosts that are members of the same AD DS domain.
- **Authentication exemption** This rule type is used to configure exemptions to existing connection security rules. Use these rules as fallback rules to allow connections from administrator computers to infrastructure servers, such as DHCP and DNS servers.

- **Server-to-server** This rule type allows you to protect connections between specific servers. These rules differ from isolation rules in that they apply to hosts at specific addresses rather than all connections.
- **Tunnel** This rule type is similar to the server-to-server rule type except that it applies to connections through tunnels to remote sites, such as over a WAN link.

## Defining Account Policies

Account policies in organizational environments are almost always set at the domain level and each domain can have only a single account policy. The exception to this is fine-grained password policies, which are beyond the scope of the 70-686 exam. The same Group Policy items define account policies at both the domain and local level. Domain policies apply to domain accounts, and local policies apply to accounts stored locally on the computer running Windows 7. Password policies and account lockout policies are located within the Computer Configuration\Windows Settings\Security Settings\Account Policies node of a Group Policy object.

Account policies determine how often a user must change his or her password, the properties of that password, and what happens when he or she enters an incorrect password. You can configure the following account policies:

- **Enforce Password History** This policy determines whether the operating system remembers a user's previous passwords. Enforcing password history stops users from rotating through a small number of remembered passwords and forces users to come up with new and unique passwords whenever they are prompted to change their passwords.
- **Maximum Password Age** This policy specifies the maximum age of a password before it must be changed.
- **Minimum Password Age** This policy specifies the minimum amount of time a user must keep a password before he or she is able to change it.
- **Minimum Password Length** This policy specifies the minimum number of characters a password must possess.
- **Password Must Meet Complexity Requirements** Enabling this policy means that user passwords must contain at least three of the following four elements: uppercase letters, lowercase letters, numbers, and symbols.
- **Account Lockout Duration** Determines how long a user is unable to log on after triggering an account lockout by entering incorrect passwords.
- **Account Lockout Threshold** The number of incorrect passwords entered that triggers an account lockout.
- **Reset Account Lockout After** The period after which the operating system forgets an incorrectly entered password.

When defining account control policies, you must balance security with convenience. Requiring users to change their passwords every week improves security but also leads to user annoyance. Configuring account lockout policies improves security but also can increase the load on help desk staff because they are required to unlock locked accounts when people inevitably forget their passwords.

## Defining User Account Control Policies

User Account Control (UAC) policies determine how user account control prompts appear to users when they perform an action that requires elevated privileges. These policies determine whether administrators simply have to click Yes when prompted for consent, whether they have to enter their user name and password, or whether they are prompted at all. Similarly, these policies determine whether the dialog box that the administrator has to respond to appears on the secure desktop, commanding attention until its query is resolved, or behaves like any other dialog box within Windows, not requiring an immediate response from the logged-on user.

User Account Control policies are located within the Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options node of a Group Policy object, as shown in Figure 5-5.

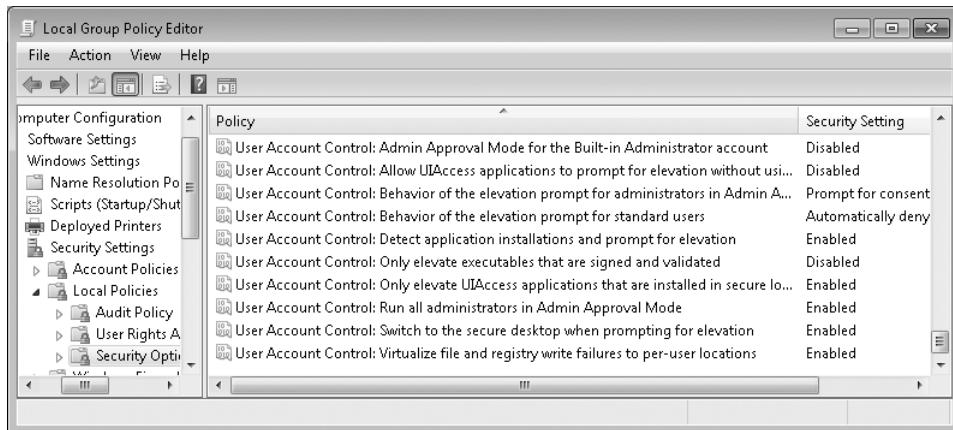


FIGURE 5-5 User Account Control policies

Important UAC policies include:

- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode** This policy determines whether an administrator is prompted for credentials or simply for consent on the secure desktop or within the normal Windows environment. It is also possible to use this policy to disable UAC entirely for administrators using this policy.

- **User Account Control: Behavior Of The Elevation Prompt For Standard Users**

Through this policy, it is possible to configure what occurs when a standard user performs an action which requires elevation. The default is to deny attempts at elevation. It is also possible to configure this policy so that a standard user is prompted for administrator credentials, either within the normal Windows environment or on the secure desktop.

- **User Account Control: Run All Administrators In Admin Approval Mode** Disabling this policy disables UAC for all users with administrative rights.

- **User Account Control: Switch To Secure Desktop When Prompting For Elevation**

This policy is enabled by default. If this policy is disabled, but other policies specify the use of secure desktop, secure desktop is still used.

For highly secure environments you should configure UAC to prompt administrators for credentials on the secure desktop. This ensures that an administrator has given their full consent and avoids the problem of another person performing administrative tasks if the administrator leaves their computer unattended while logged on with an administrator account. You should configure the Prompt For Credentials setting for the User Account Control: Behavior Of The Elevation Prompt For Standard Users policy in the event that administrators are assisting standard users through remote desktop and need to perform an administrative task.

#### **MORE INFO USER ACCOUNT CONTROL TECHNICAL REFERENCE**

To learn more about User Account Control, consult the following document on TechNet:  
[http://technet.microsoft.com/en-us/library/dd835546\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd835546(WS.10).aspx).

## Configuring User Rights and Security Policies

The User Rights Assignment node of Group Policy, located under Computer Configuration\Windows Settings\Security Settings\Local Policies and shown in Figure 5-6, allows you to delegate specific rights to specific users or groups. For example, you can use this set of policies to delegate the right to back up files and folders to one group of users and then delegate the right to restore files and folders to a separate group of users. In most organizations, the default rights configuration on client computers is adequate to ensure security. In high security environments, however, you may want to be more restrictive in the way that you allocate user rights, which requires that you be specific in the configuration of policies within this node.



FIGURE 5-6 User Rights Assignment policies

The Local Security Policy Editor, shown in Figure 5-7, allows you to configure security-specific policies, which can also be configured more generally through the Local Group Policy Editor. Both the Local Group Policy Editor and the Local Security Policy Editor allow you to import and export security policy settings as security templates. You can also use the Seedit.exe command-line utility to apply security templates. The advantage of using security templates is that they allow you to apply a consistent set of security settings to computers that are not members of a domain environment. For example, if you wanted to apply a consistent set of Windows Firewall With Advanced Security rules to a group of computers running Windows 7 that were not members of a domain, you could configure the rules on a reference computer, export the rules as a security template, and then apply that template to all of the stand-alone computers. You can also use a template with the Security Configuration And Analysis wizard to analyze a computer's current security configuration to determine how it deviates from the configuration in the template.

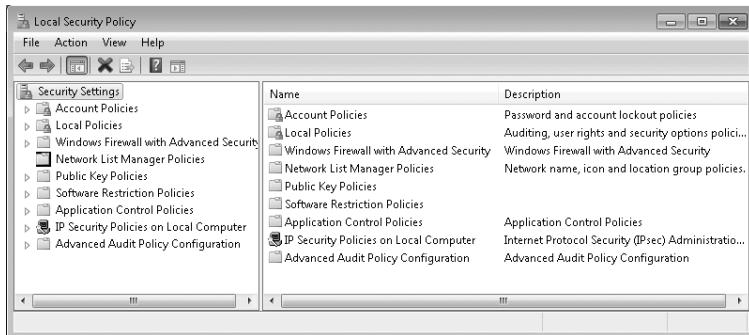


FIGURE 5-7 Local Security Policy

## Locking Down Services

In a default installation of Windows 7, services that are not required by the operating system are not configured to automatically start. When the operating system or an installed application requires a service, its startup type is set to Automatic or Manual. In environments where security is a significant concern, you can audit which services are necessary and set the startup type of any unnecessary services to Disabled. Disabling unnecessary services reduces the attack surface of a computer and reduces the chance that an unused service may be leveraged by an attacker to compromise the computer.

## Defining AppLocker Settings

AppLocker is available in Windows 7 Enterprise and Ultimate. AppLocker offers broadly similar functionality as the Software Restriction Policies that were available in earlier versions of Windows and that administrators can still use to restrict application execution in other editions of the Windows 7 operating system. AppLocker policies differ from Software Restriction Policies in that you are able to easily apply AppLocker policies on the basis of specific user or group accounts and you can create a rule that not only covers the current version of an application, but all future versions of that application. Accomplishing the same goal with Software Restriction Policies required you to filter Group Policy and create new policies whenever the application was updated.

AppLocker supports the following category restrictions:

- **Executable Rules** These rules apply to files that have the .exe and .com extensions. AppLocker applies primarily to this type of rule.
- **Windows Installer Rules** These rules apply to files with the .msi and .msp extensions.
- **Script Rules** These rules apply to files with the .ps1, .bat, .cmd, .vbs, and .js file extensions.
- **DLL Rules** These rules apply to files that have the .dll and .ocx extensions.

Within these category restrictions, you can configure the following types of AppLocker rules:

- **Publisher Rules** These rules identify files based on the digital signature applied to the file by the application vendor. Publisher rules allow an administrator to specify a specific version of a file and all future versions of that file, which means that it is not necessary to update publisher rules when an application update is applied.
- **Hash Rules** These rules use a digital fingerprint of a file that identifies it by its binary characteristics. The drawback of hash rules is that they must be updated whenever a software update is applied to the file that the hash identifies.
- **Path Rules** These rules identify files based on their location within the file system. Path rules are less secure than other rule types because an attacker can substitute malware for a known file if they have the ability to overwrite the original file at its location.

Another advantage that AppLocker has over Software Restriction Policies is that it can create rules automatically. An administrator can create a reference computer with allowed applications installed. The wizard automatically creates publisher rules for all files that have been digitally signed and provides the option of creating hash rules or path rules for any file that is not digitally signed. AppLocker policies can also be imported and exported in XML format, which simplifies the process of transferring an updated list of allowed applications from a reference computer to a Group Policy applied through Active Directory. When you create the first AppLocker rule, you are prompted to create a set of default rules to allow important system files to run, as shown in Figure 5-8.



FIGURE 5-8 Create default rules

More specific AppLocker rules, such as a publisher rule, override less specific ones, such as a path rule. Prior to enforcing AppLocker rules, you should audit rules using the auditing settings. You do this by editing the properties of the AppLocker policy, as shown in Figure 5-9. After you determine that the rules function as expected, you can change the policy from Audit Only to Enforce Rules. AppLocker auditing events are written to the AppLocker event log.

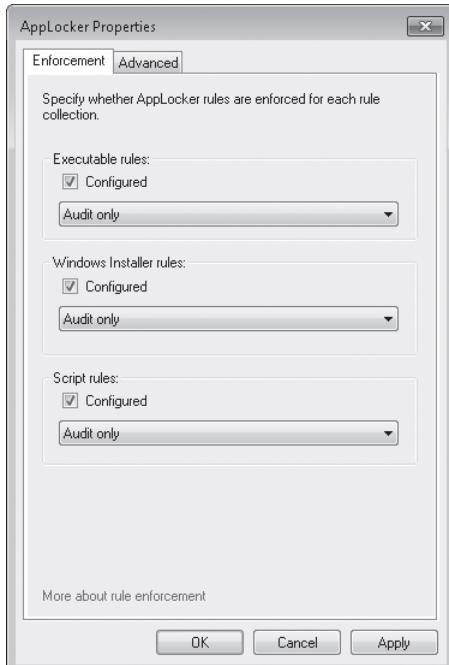


FIGURE 5-9 Configure AppLocker to Audit Only

#### MORE INFO APPLOCKER STEP-BY-STEP GUIDE

For more information on how to best configure AppLocker for your organization, consult the AppLocker Step-By-Step Guide, which is available on TechNet at [http://technet.microsoft.com/en-us/library/dd723686\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd723686(WS.10).aspx).

## Configuring Removable Drive Policies

Removable device policies allow you to configure read, write, and execute access to storage devices that can be classed as removable by the computer. As you learned earlier in this chapter, BitLocker To Go policies can be configured to allow you to block write access to removable storage devices that are not protected by BitLocker To Go. BitLocker To Go cannot be used to block access to removable storage devices, and it is still possible to load data and executable files from these devices. If you want to block users from loading executable files from DVDs or USB drives that they have brought into the office environment, you would configure a removable storage access policy.

Access to removable devices is configured through the Computer Configuration\Administrative Templates\System\Removable Storage Access node Group Policy. Figure 5-10 shows some of these policies.

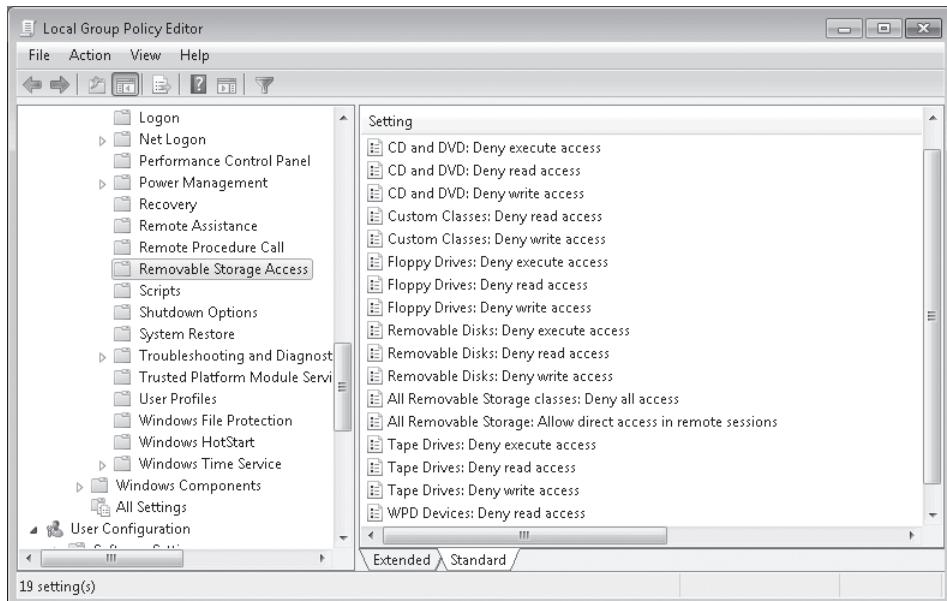


FIGURE 5-10 Removable Storage Access policy

You can apply removable device policies to deny execute, read, and write access to the following device types:

- CD and DVD.
- Floppy drives.
- Removable disks.
- Tape drives.
- WPD devices (media players and smart phones).
- Custom classes. You can deny access to devices that are not covered by other categories through these policies by configuring the setup class GUID.
- All removable storage classes. This denies access to all removable storage devices.

#### MORE INFO CONTROLLING ACCESS TO REMOVABLE DEVICES OR MEDIA

To learn more about removable device policies, consult the following document on TechNet:  
[http://technet.microsoft.com/en-us/library/cc730808\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc730808(WS.10).aspx).

## Modifying Network Security Settings

Windows 7 has introduced some changes to the way that the NTLM and Kerberos protocols function. These changes have been implemented to make Windows 7 more secure but may adversely affect the way that Windows 7 interacts with some network environments. In the event that the operating system default network security settings are not compatible with the existing environment, Administrators can edit Group Policy policies, to make Windows 7 interoperate with the existing network environment. You should note that you do not need to make these modifications in the vast majority of network environments.

To configure Windows 7 to support DES encryption for Kerberos, configure the Computer Configuration\Security Settings\Local Policies\Security Options\Network Security: Configure Encryption Types Allowed For Kerberos policy, as shown in Figure 5-11. If an encryption type is not explicitly allowed through this policy, it cannot be used for Kerberos authentication.



FIGURE 5-11 Allowed Kerberos encryption

NTLM authentication for computers running Windows 7 has also been strengthened with clients requiring 128-bit encryption when using the authentication protocol. In the event that 40-bit or 56-bit encryption is the maximum available with devices in an existing environment, you must remove the requirement for 128-bit encryption from the following policies:

- Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients
- Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers

Clients in environments that use Kerberos for authentication need to be configured so that the time on the client computer is very close to that of the server that authenticates the session. You should not modify the Maximum Tolerance For Computer Clock Synchronization Group Policy item beyond its default value of five minutes unless there are extenuating circumstances because you will reduce security on the network.

You can take several steps to ensure that all the client computers in your organization retain synchronized time settings. These steps include:

- Ensuring that the PDC emulator synchronizes with an external time server. If you are having trouble establishing a trust relationship between two domains, you should configure the PDC emulator for each domain to synchronize against the same external time server.
- The net time /set command can be used to synchronize time with a specific server. You must run this command from an elevated command prompt.
- The w32tm.exe /resync command allows you to resynchronize a computer's clock with that of another computer.

In some circumstances, a Kerberos ticket can become corrupted or invalid and needs to be removed. You can use the Klist.exe command-line utility to list and manage Kerberos tickets. Use Klist.exe with the purge option to remove problematic tickets in the event that authentication for a specific host is not functioning correctly.

#### **MORE INFORMATION CHANGES FOR IDENTITY AND AUTHENTICATION IN WINDOWS SERVER 2008 R2**

To learn more about the changes in network authentication in Windows 7, consult the following article on TechNet: [http://technet.microsoft.com/en-us/library/dd560654\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560654(WS.10).aspx).



#### **EXAM TIP**

Klist.exe can be used to manage Kerberos tickets in Windows Server 2008 environments; Kerbtray.exe was used in earlier versions of Windows.

#### **PRACTICE Implement Client Security Standards**

In this lesson, you have learned about the ways in which you can employ specific features of the Windows 7 operating system as part of an overall client security strategy. In the following practice exercises, you explore two facets of Windows 7 client security, BitLocker To Go policies and AppLocker policies.

## EXERCISE 1 Configuring BitLocker To Go to Limit USB Flash Storage Device Usage

Removable USB flash devices can store gigabytes of data and are easy to misplace. BitLocker To Go policies allow you to ensure that the only USB flash storage devices to which people in your organization are allowed to write data are those that are associated with your organization and are protected by BitLocker To Go.

1. Log on to computer WKSTN1 with the Mark Lee user account.
2. From the Start menu in the Search Programs And Files text box, type **gpedit.msc**. This opens the Local Group Policy Editor console.
3. Navigate to the Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption node.
4. Edit the Provide The Unique Identifiers For Your Organization policy. Enable the policy, and set the BitLocker Identification Field and Allowed BitLocker Identification Field to MySecretOrgID, as shown in Figure 5-12.

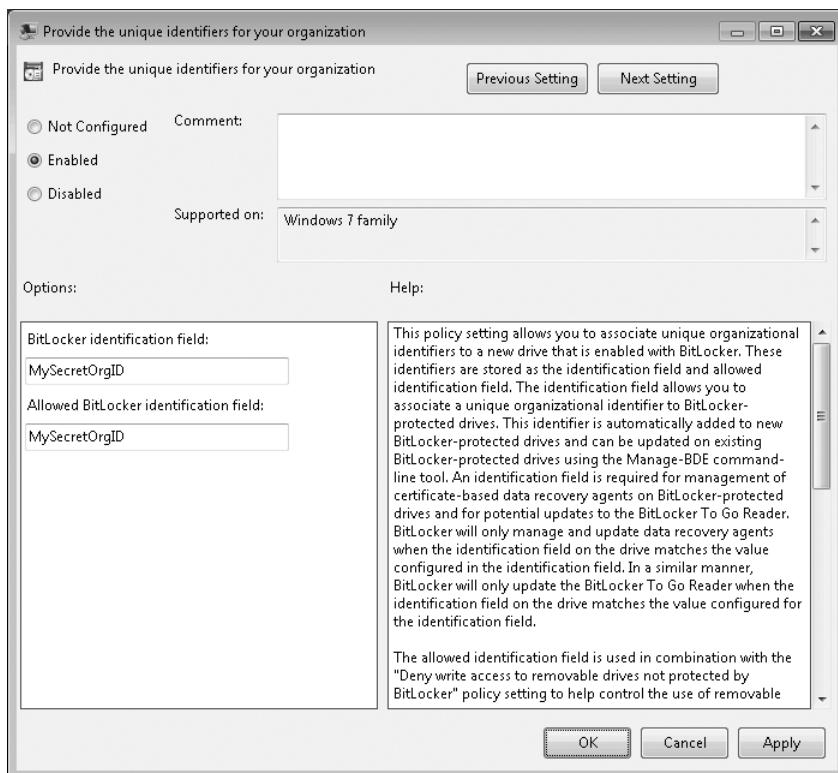
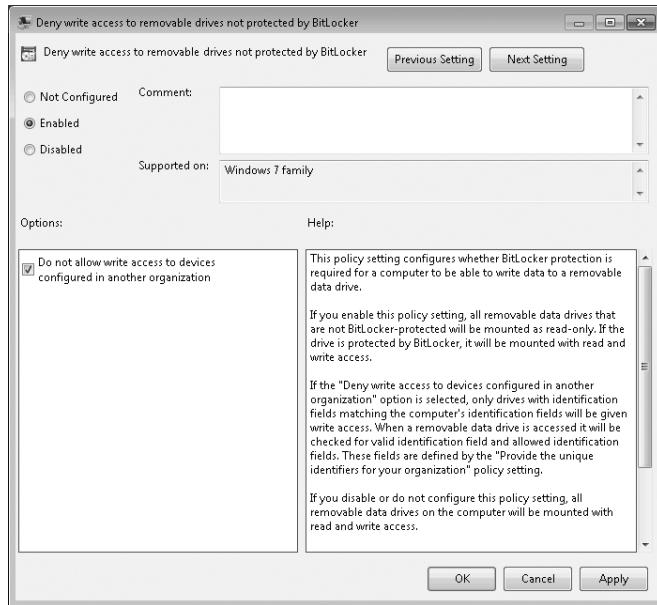


FIGURE 5-12 Configuring BitLocker organizational identifier

- Navigate to the Removable Data Drives node. Edit the Control Use Of BitLocker On Removable Drives policy. Set this policy to Enabled. Disable the Allow Users To Apply BitLocker Protection On Removable Data Drives and Allow Users To Suspend And Decrypt BitLocker Protection On Removable Data Drives options.
- Edit the Deny Write Access To Removable Drives Not Protected By BitLocker policy. Enable this policy, and set the Do Not Allow Write Access To Devices Configured In Another Organization option, as shown in Figure 5-13.



**FIGURE 5-13** Blocking access to devices from other organizations

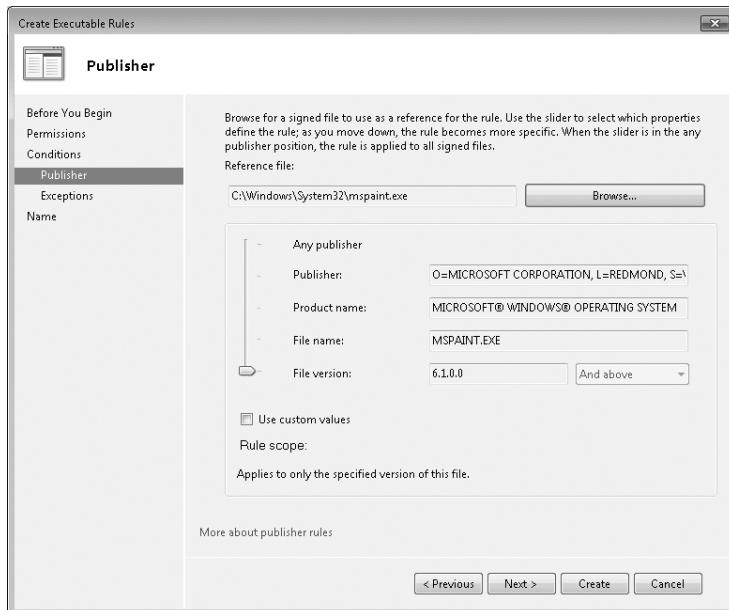
- Close the Local Group Policy Editor.

## EXERCISE 2 Configure AppLocker Policies

AppLocker policies can be configured to restrict the execution of applications on a client computer so that users can run only approved programs. In this exercise, you configure an AppLocker policy to block the execution of the Paint program.

- If you are not already logged on to computer WKSTN1, log on as Mark Lee.
- Click Start, and in the Search Programs And Files text box, type **Paint** and then press Enter. Verify that the Paint application opens. Close Paint.
- Open the services console and configure the properties of the Application Identity service. Set the startup type to Automatic. Start the service, and then close the dialog box.
- In the Search Programs And Files text box, type **gpedit.msc** to open the Local Group Policy Editor console.

- Navigate to the Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules node.
- Right-click Executable Rules, and then choose Create New Rule. On the Before You Begin page of the Create Executable Rules wizard, click Next.
- On the Permissions page, choose Deny, and then click Next.
- On the Conditions page, choose Publisher, and then click Next.
- On the Publisher page, click Browse. Navigate to the C:\Windows\System32\ folder, and then double-click mspaint.exe.
- Verify that the Publisher page of the wizard matches Figure 5-14, and then click Create.



**FIGURE 5-14** Configuring an Executable rule

- When prompted to create the default rules, click Yes. Close the Local Group Policy Editor and then restart the computer.
- When the computer restarts, log on using the Mark Lee user account and attempt to start the Paint program. You will receive a message telling you that the program is blocked by Group Policy.
- Open the services console, configure the properties of the Application Identity service. Set the startup type to Disabled. Stop the service.

## Lesson Summary

- BitLocker provides full volume encryption of internal hard disk drives. BitLocker To Go provides full volume encryption to removable storage drives. EFS provides per-user encryption to files and folders.
- AppLocker allows you to restrict the execution of applications in your environment based on application publisher, file hash, or file path.
- Account policies allow you to configure the properties of users' passwords, how often the users must change their passwords, and what happens if users enter an incorrect password a certain number of times.
- Windows Firewall with Advanced Security can be used to define inbound and outbound firewall rules based on port, protocol, service, or application. You can limit the scope of firewall rules to particular subnets. You can also limit connections, through connection security policies, to hosts that have met appropriate authentication criteria.
- User Account Control policy can be configured to require users with administrative rights to provide consent or provide credentials when attempting a task that requires elevated privileges.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. You are developing a client security standard for your organization. Which of the following organizational characteristics would dictate that you use Software Restriction Policies to restrict application execution as opposed to AppLocker policies? (Choose all that apply. Each answer forms a complete solution.)
  - A. There are computers in the organization running Windows 7 Professional.
  - B. The Active Directory Domain Services forest is set to the Windows Server 2003 functional level.
  - C. Line of business applications are not digitally signed.
  - D. There are computers in the organization running Windows Vista Enterprise.
2. You are in the process of developing a client security standard for your organization. You want to ensure that help desk staff are able to run programs using elevated privileges when connected through a remote assistance session to a computer where the user is

logged on with an account that is not a member of the local administrators group. Which of the following Group Policy items should you configure to implement this standard?

- A.** User Account Control: Behavior Of The Elevation Prompt For Standard Users.
  - B.** User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode.
  - C.** User Account Control: Detect Application Installations And Prompt For Elevation.
  - D.** User Account Control: Run All Administrators In Admin Approval Mode.
- 3.** You want to ensure that users change their passwords every 21 days and that users are locked out for 15 minutes if they enter an incorrect password three times in a 30-minute period. Which of the following Group Policy items must you configure to accomplish this goal? (Choose all that apply. Each answer forms part of a complete solution.)
- A.** Account Lockout Duration
  - B.** Enforce Password History
  - C.** Maximum Password Age
  - D.** Minimum Password Age
  - E.** Account Lockout Threshold
  - F.** Reset Account Lockout Counter After
- 4.** Your organization has 200 desktop computers that have the Windows 7 Enterprise edition operating system installed. You want to ensure that users in your organization are able to write data only to removable USB flash storage devices that you have specially protected using BitLocker To Go. Users should not be able to configure BitLocker To Go on removable USB flash storage devices themselves or use encrypted BitLocker To Go devices from other organizations. Which of the following policies should you configure to accomplish this goal? (Choose all that apply. Each answer forms a complete solution.)
- A.** Configure Use Of Passwords For Removable Data Drives
  - B.** Deny Write Access To Removable Drives Not Protected By BitLocker
  - C.** Provide The Unique Identifiers For Your Organization
  - D.** Control Use Of BitLocker On Removable Drives
- 5.** The portable computers in your organization do not have TPM chips. You want to enable file and folder encryption on these computers but do not want to require users to start up using a USB flash device. Users are restricted so that they can write documents only to specific folders on the volume hosted on the portable computer's internal hard disk. Which of the following encryption solutions can you implement to meet this goal?
- A.** BitLocker
  - B.** BitLocker To Go
  - C.** IPsec
  - D.** Encrypting File System

## Lesson 2: Configuring Windows Internet Explorer

Although most users pay little attention to the possible configuration options, Internet Explorer is one of the most customizable applications available for the Windows 7 operating system. Windows Internet Explorer 8 can be highly customized to suit the needs of your organization, with more than 1,300 individual settings that you can configure through Group Policy. You can use the Internet Explorer Administration Kit to configure settings when deploying Internet Explorer to stand-alone client computers that are not part of an Active Directory environment. In this lesson, you learn about how you can configure Internet Explorer security zone, cache, privacy, add on, and proxy server settings.

**After this lesson, you will be able to:**

- Use the Internet Explorer Administration Kit to configure Internet Explorer.
- Configure Internet Explorer through Group Policy.

**Estimated lesson time: 40 minutes**

### Internet Explorer Administration Kit

The Internet Explorer Administration Kit (IEAK) is a tool that allows you to deploy and manage Windows Internet Explorer. Although you can use IEAK to configure and manage Windows Internet Explorer settings in Windows 7 client environments that are managed by Active Directory Domain Services, the product is most often used to configure and manage settings in unmanaged environments, such as those where Active Directory is not present.

IEAK allows administrators to perform the following tasks:

- Centrally distribute and manage the installation of Windows Internet Explorer.
- Configure connection profiles for computers running the Windows 7 operating system.
- Customize all configurable aspects of Windows Internet Explorer.
- Organizationally brand Internet Explorer.

IEAK allows you to create a Windows Internet Explorer distribution that contains custom settings, working in much the same way that an unattended installation works. When a custom package is installed, Windows Internet Explorer installs with the settings assigned through the IEAK rather than with its default settings. You customize a Windows Internet Explorer package for distribution in the practice exercise at the end of this lesson.

IEAK is not limited to creating Windows Internet Explorer packages for distribution. IEAK allows you to create what is known as a configuration-only distribution using a tool known as the IEAK Profile Manager. The IEAK Profile Manager allows you to create an automatic configuration file that contains all of the settings you want to configure for Windows Internet Explorer. You place this file at an accessible location, and computers that are configured to use this configuration file automatically retrieve and apply their configuration based on the settings in this file.

The advantage of IEAK Profile Manager, shown in Figure 5-15, is that it holds most Internet Explorer configuration options in a central location. It can be difficult for administrators who are unused to navigating their way through Group Policy to locate all of the relevant Group Policy items for Internet Explorer configuration. IEAK Profile Manager simplifies this process.

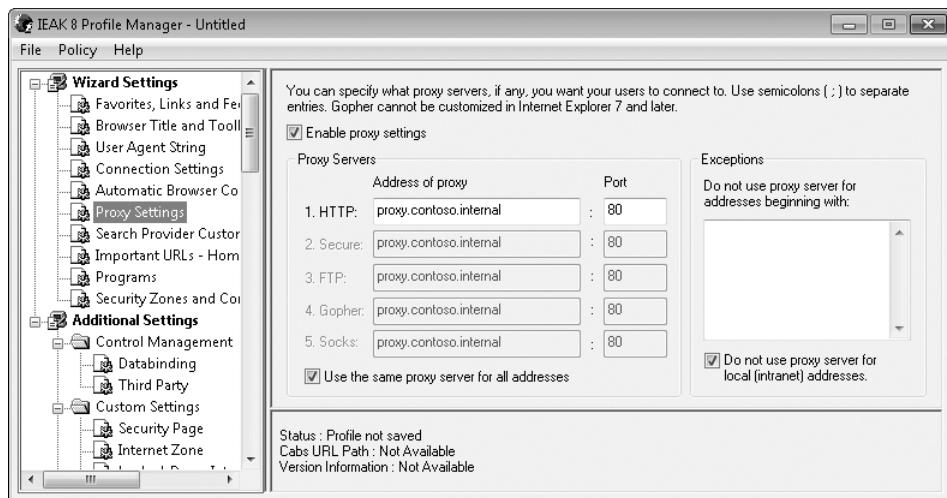
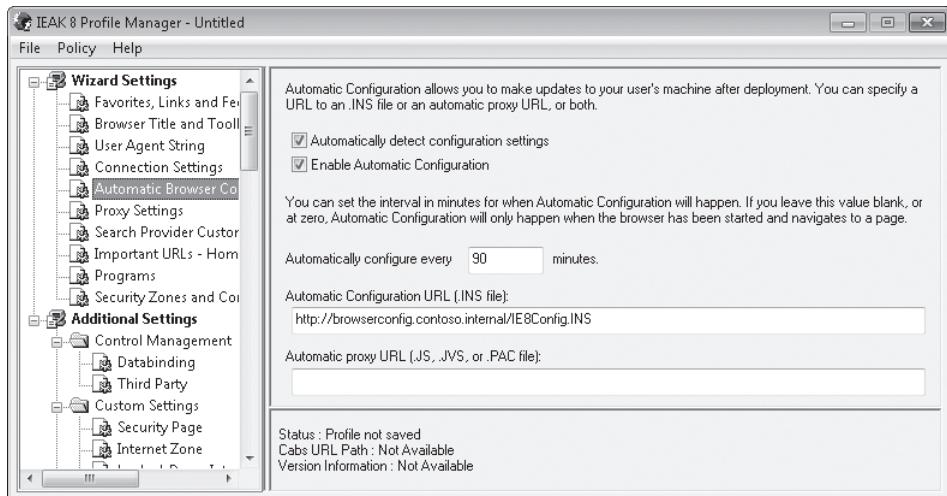


FIGURE 5-15 Configuring proxy settings using IEAK Profile Manager

To modify the location of the configuration file, edit the Automatic Browser Configuration settings, as shown in Figure 5-16, and enter the location of the new automatic configuration file. Publish the automatic configuration file with the new location to both the original location and the new location. After a suitable transition period, you can remove the automatic configuration file from the original location.



**FIGURE 5-16** Automatic configuration URL

You need to remember that you can use Group Policy to specify the location of an automatic configuration file generated using IEAK Profile Manager. You can do this through the User Configuration\Windows Settings\Internet Explorer Maintenance\Connection\Automatic Browser Configuration policy. This allows administrators to configure settings using IEAK Profile Manager for Windows 7 client computers when they must manage both clients that are members and clients that are not members of an Active Directory environment.

#### **MORE INFO INTERNET EXPLORER ADMINISTRATION KIT**

To find out more about the Internet Explorer Administration Kit, navigate to the Internet Explorer Administration Kit TechCenter hosted on TechNet at the following address:  
<http://technet.microsoft.com/en-us/ie/bb219517.aspx>.

#### **Quick Check**

- How can you configure Windows Internet Explorer using IEAK Profile Manager if Windows Internet Explorer was not deployed using the Internet Explorer Administration Kit?

#### **Quick Check Answer**

- You can place the automatic configuration file generated by IEAK Profile Manager at a location accessible to the clients and then use the User Configuration\Windows Settings\Internet Explorer Maintenance\Connection\Automatic Browser Configuration policy to point clients that fall under the scope of Group Policy at the automatic configuration URL.

## Windows Internet Explorer and Group Policy

The most common way to manage Windows Internet Explorer in enterprise environments is through Group Policy. Internet Explorer policies are located in the following areas of Group Policy:

- Computer Configuration\Administrative Templates\Windows Components\Internet Explorer.
- User Configuration\Windows Settings\Internet Explorer Maintenance. When Internet Explorer Maintenance is set to Preference mode, you can configure a large number of Internet Explorer policies that can be used to override any changes made by a user.
- Computer Configuration\Administrative Templates\Windows Components\Internet Explorer.

Although many of the policies that you can configure using the Computer Configuration area of Group Policy are available in the User Configuration area, a number of Group Policy items are unique to each specific area. With more than 1,300 policies related to Windows Internet Explorer in Group Policy, many administrators prefer to use IEAK Profile Manager to centralize and control configuration. At the release of Windows 7, there was not full parity between the options that can be configured through Group Policy and the options that can be configured through IEAK Profile Manager. Put another way, some configuration settings can be configured centrally using only one tool or the other. In some environments with specific configuration needs, you must use both IEAK Profile Manager and Group Policy to accomplish organizational objectives.

---

### EXAM TIP

Because of the extremely large number of policy and IEAK Profile Manager options, it is unlikely that the 70-686 exam will require you to know which settings can be configured only with a specific tool.

---

## Configuring Security Zones

Security zones determine the security settings that are applied to Web sites based on their address. For example, you can configure trusted sites that require greater privileges to run executable content to be members of the trusted sites zone. You can configure sites that you suspect of hosting malware, but which people in your organization need to visit nevertheless, as members of the Restricted Sites zone. Sites can be added to zones through Group Policy. You can also configure Group Policy to specify the security level of each zone if you want to alter it from the default settings. The four default zones are shown in Figure 5-17.

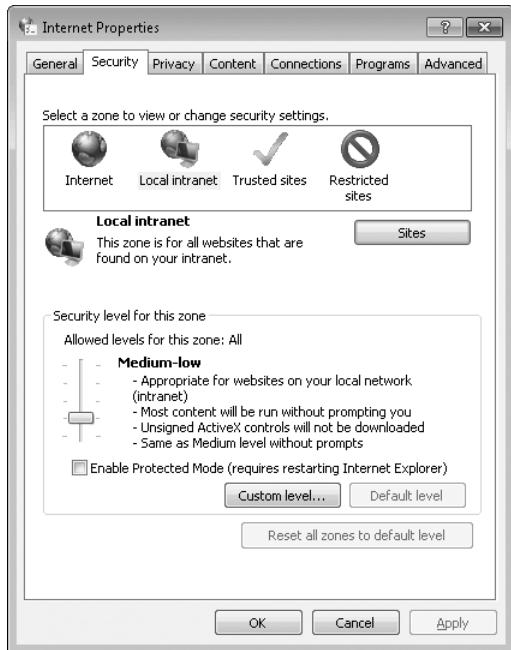


FIGURE 5-17 Available zones

The default Windows Internet Explorer zones are as follows:

- **Internet** This zone hosts all sites except those that have been added to the Trusted Sites and Restricted Sites zones. The security level of this zone is set to Medium-High and it is configured to use Protected Mode. The Internet Zone can be assigned only the Medium, Medium-High, and High security levels. You learn about levels and Protected Mode later in this lesson.
- **Local Intranet** Zones that are automatically detected on the local Intranet. You can configure intranet sites to be configured automatically or configure sites not listed in other zones, sites that bypass the proxy server and all UNC addresses, as shown in Figure 5-18. The security level of this zone is set to Medium-Low. All security levels can be assigned to this zone. This zone is not configured to use Protected Mode.

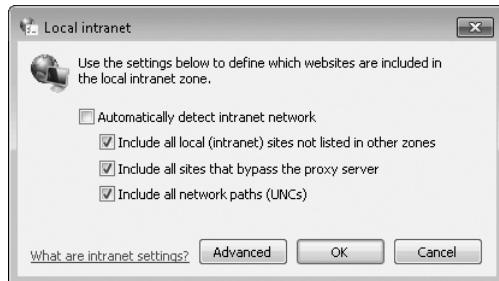


FIGURE 5-18 Local Intranet zone

- **Trusted Sites** This zone is used for sites that are trusted, but which are not located on the Local Intranet. It uses the Medium security level, which is between the level used for the Internet zone and the Local Intranet zone. All security levels can be assigned to this zone. The Trusted Sites zone does not use Protected Mode.
- **Restricted Sites** This zone is used for sites that you suspect of containing malware but which must be visited by people in your organization. The security level for this zone is set to High, and Protected Mode is enabled for this zone. Only the High security level is available for this zone.

Internet Explorer Protected Mode stops Windows Internet Explorer from modifying user or system files without explicit user consent. Protected Mode requires the user to consent to any attempt to store data or activate a program. Internet Explorer Protected Mode limits the chance that unauthorized software can be installed on the computer.

#### MORE INFO INTERNET EXPLORER PROTECTED MODE

To learn more about Internet Explorer Protected Mode, consult the following document on MSDN: [http://msdn.microsoft.com/en-us/library/bb250462\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb250462(VS.85).aspx).

As you learned earlier, security zones are associated with security levels. Some zones are unable to use all levels. The available levels are as follows:

- **Low** This level provides minimal safeguards and content can be downloaded and executed without prompts. All active Web page content is executed. This level is available only to the Local Intranet and Trusted Sites zones.
- **Medium-Low** Most content runs without prompting the logged-on user, but unsigned ActiveX controls cannot be downloaded. This level is available only to the Local Intranet and Trusted Sites zones.
- **Medium** When this level is set for a site, prompts are issued for all potentially unsafe content, and unsigned ActiveX controls cannot be downloaded. This level is available for all zones except the Restricted Sites zone.
- **Medium-High** This level is similar to the Medium level except that Internet Explorer is stricter in its interpretation of what constitutes unsafe content when prompting users to decide whether they want to run active content. This level is available for all zones except the Restricted Sites zone.
- **High** The High level provides a maximum level of safeguards by blocking the execution of active content. This level is available for all zones.

### Quick Check

- Users in your organization need to visit several sites that you suspect host malware. To which security zone should you add these sites to minimize the chance of them affecting users' computers?

### Quick Check Answer

- You should add sites that you suspect of hosting malware to the Restricted Sites zone.

## Managing Cache Settings

Windows 7 clients allocate 50 MB as the default size of the Temporary Internet Files folder. Through the Internet Options control panel, you can allocate up to 1024 MB of space to the Temporary Internet Files folder. You can configure the size of the Temporary Internet Files folder through Group Policy only if you enable Preference Mode. You enable Preference Mode by right-clicking the User Configuration\Windows Settings\Internet Explorer Maintenance mode and then clicking the Preference Mode item. This enables and displays the Advanced node, through which you can configure the size of the Temporary Internet Files folder. Alternatively, you can configure the size of this folder through the IEAK Profile Manager, as shown in Figure 5-19.

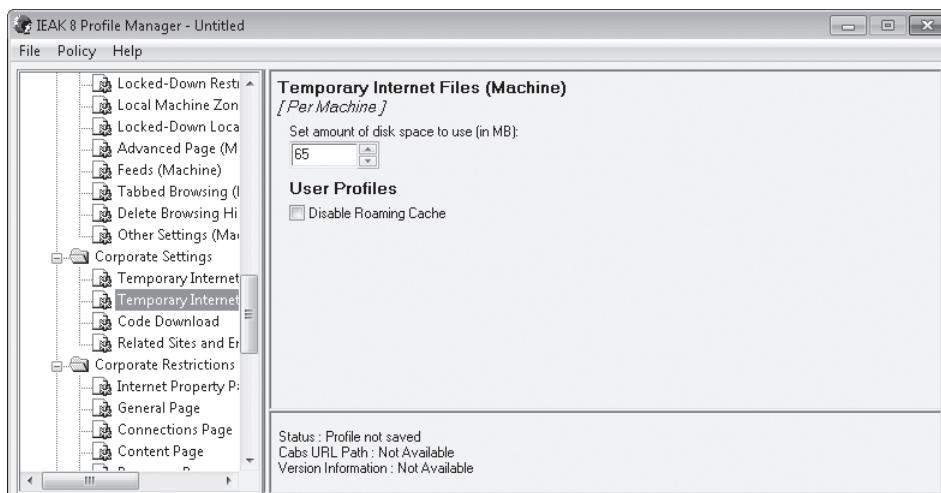


FIGURE 5-19 Temporary Internet File limits

You can configure the User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page\Empty Temporary Internet Files Folder When Browser Is Closed policy to automatically remove all data from the Temporary Internet Files folder whenever a Windows Internet Explorer session ends.

## Privacy Settings

The privacy settings in Internet Explorer manage how Internet Explorer reacts to requests by Web sites to store data in the form of cookies. Privacy settings are configured either through the Privacy tab of the Internet Properties dialog box, shown in Figure 5-20, or indirectly through the User Configuration\Windows Settings\Internet Explorer Maintenance\Security node of a Group Policy object.

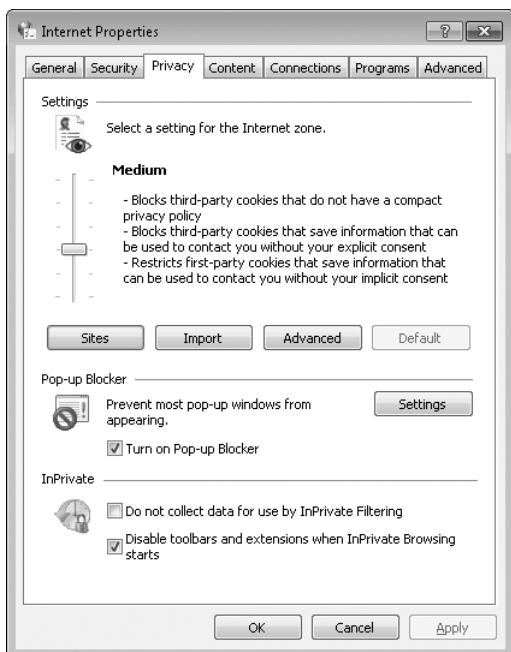


FIGURE 5-20 Internet Explorer Privacy tab

The privacy slider determines how cookies from the Internet zone are treated by Windows Internet Explorer. Cookies are files that Web sites use to store data about a user's session. Cookies can be read by the Web site that generated them, allowing that Web site to retain session data across different browsing sessions. Because cookies do retain data about a user's browsing, there can be privacy implications to the acceptance of cookies.

The default setting of medium blocks third-party cookies that do not have a compact privacy policy and blocks all cookies that save information that can be used to contact you without your consent. You can configure the privacy slider so that all cookies are accepted. Alternatively, you can configure the privacy slider so that all cookies are blocked and so that any cookies that are present on the computer cannot be read by Web sites.

Pop-ups are windows that often appear without prompting when you navigate to a Web site. Internet Explorer includes a pop-up blocker that blocks most automatic pop-ups. In some situations, you want to allow pop-ups from a specific site while retaining the block on

all other sites. You can do this centrally by employing the following policies, located in the Internet Explorer Group Policy node:

- **Pop-up Allow List** This list allows you to configure a collection of sites, which will always be allowed to display pop-up windows. This policy is shown in Figure 5-21.

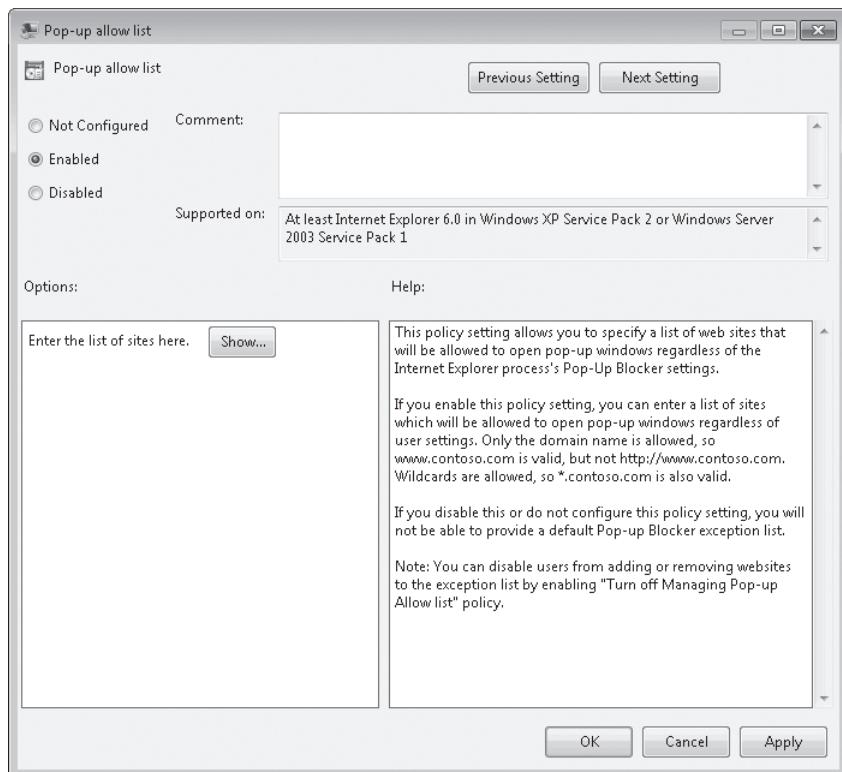


FIGURE 5-21 Configuring a list of allowed pop-ups

- **Turn Off Managing Pop-Up Allow List** This policy blocks users from adding or removing sites from the pop-up allow list.
- **Turn Off Pop-Up Management** This policy blocks access to the pop-up management feature entirely.

### Quick Check

- Should you use the security slider or the privacy slider for the Internet zone to block Internet Explorer from remembering user name and password data from sites on the Internet?

### Quick Check Answer

- Use the privacy slider to manage how Internet Explorer remembers user names and passwords from sites on the Internet.

## Managing Browsing History

By configuring Group Policy, you can prevent users from deleting their own browsing history. Although most organizations use a proxy server to track Web usage, you might need to have a copy of the browsing history data stored on the user's computer when you are attempting to prove that a user has visited sites that host illicit content. Configuring policies that prevent users from removing their browsing history can ensure that evidence remains present on the computer that the user might otherwise delete.

You can configure policy so that a user is simply unable to delete specific history items such as cookies and stored passwords. Alternatively, you can simply block the deletion of all history data, which includes everything stored by the browser about a browsing session. When setting policies to retain browsing history, ensure that you also disable InPrivate Browsing because InPrivate Browsing is a feature specifically designed to prevent the local computer from recording history data. A user who wants to hide their browsing history is more likely to try InPrivate Browsing before visiting sites that host illicit content than they are to visit the sites and then attempt to cover their tracks by deleting their browsing history. Browsing history policies are shown in Figure 5-22.

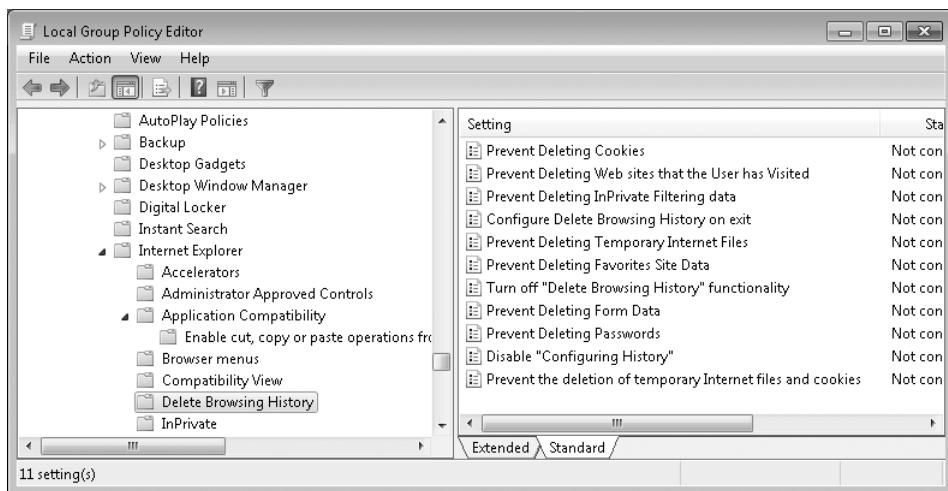


FIGURE 5-22 Managing browser history

## InPrivate Browsing

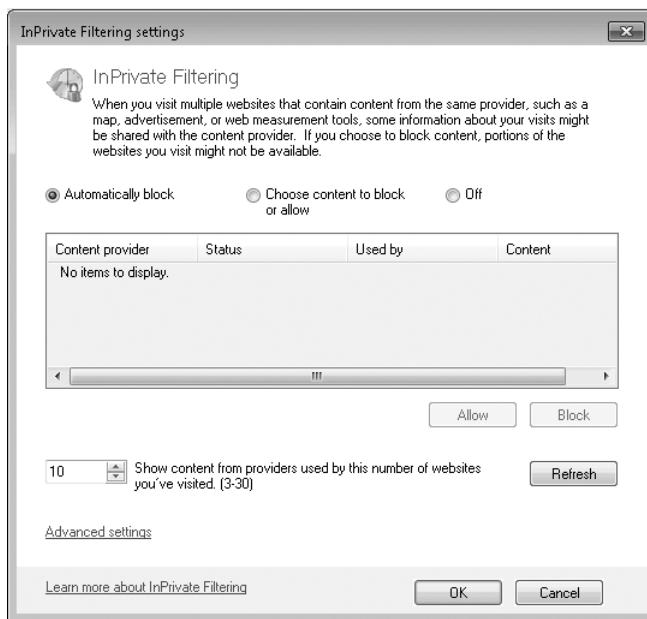
InPrivate Browsing restricts what data is recorded by the browser. Users can open an InPrivate Browsing window by clicking the InPrivate Browsing item on the Windows Internet Explorer safety menu. InPrivate Browsing blocks only data recorded by the browser and does not block proxy servers and other network technologies from tracking Web site activity. For example, assume a user enters InPrivate Browsing mode and then navigates to a Web site containing illicit images. Although there would be no record within the browser history, cache, or cookies of the visit to the site after the user closes the browser, any proxy server that the browser uses in

retrieving content from the Web site containing illicit images records precisely what traffic was accessed through the browser. You can block InPrivate Browsing by configuring the Administrative Templates\Windows Components\Internet Explorer\InPrivate\Turn Off InPrivate Browsing policy in either the Computer Configuration or User Configuration area of Group Policy.

## InPrivate Filtering

InPrivate filtering restricts the information about a browsing session that can be tracked by external third parties. For example, many Web sites display advertisements that they do not host themselves; the ads are hosted by an advertisement serving company. Through traffic analysis, these advertisement-serving companies can track a browsing session across multiple Web sites even if the Web sites that you are visiting have no direct relationship with one another. When you enable InPrivate Filtering, Internet Explorer blocks this type of tracking after it determines that a particular third-party site has tracked your activity over a threshold number of Web sites.

As with InPrivate Browsing, you must enable InPrivate Filtering during each session. This threshold value can be set by the user or administrator to a figure between 3 and 30 sites through the InPrivate Filtering Settings dialog box, available from the Safety menu of Internet Explorer, as shown in Figure 5-23.



**FIGURE 5-23** InPrivate Filtering settings

InPrivate Filtering can be disabled through Group Policy by configuring the Turn Off InPrivate Filtering policy. You can configure the InPrivate Filtering threshold through the InPrivate Filtering Threshold policy. These policies are located in the Administrative Templates\Windows Components\Internet Explorer\InPrivate node of both the Computer Configuration and User Configuration sections of Group Policy.

#### MORE INFO INPRIVATE FILTERING

To learn more about InPrivate Filtering, consult the following page on TechNet:  
<http://technet.microsoft.com/en-us/ie/dd878129.aspx>.

## Proxy Server Connections

Many organizational networks use a proxy server to reduce Internet traffic costs by caching frequently accessed content. Proxy servers also provide organizations with a way to centrally track people's Internet usage, with most proxy server software including significant traffic analysis functionality.

You can centrally manage Windows Internet Explorer proxy settings through two methods. If your organization has configured automatic proxy configuration, you can specify the location of the automatic configuration script through the Automatic Browser Configuration policy, located in the User Configuration\Windows Settings\Internet Explorer Maintenance\Connections node, as shown in Figure 5-24.

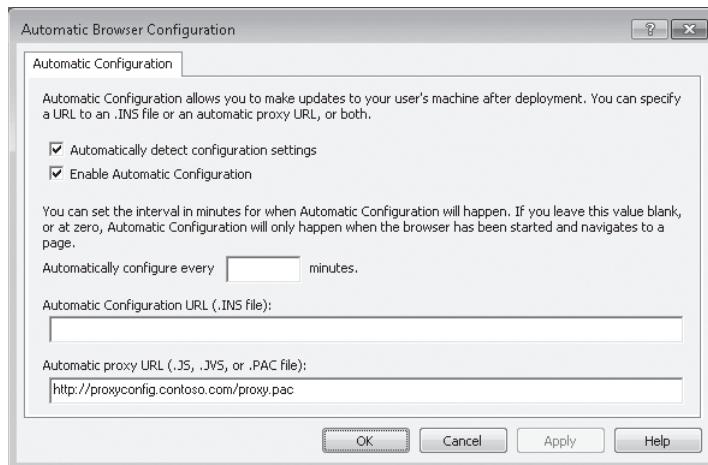


FIGURE 5-24 Automatic Proxy Configuration

In organizations that do not have automatic proxy configuration configured, you can configure proxy settings for each protocol through the User Configuration\Windows Settings\Internet Explorer Maintenance\Connections\Proxy Settings policy. Figure 5-25 shows this policy.

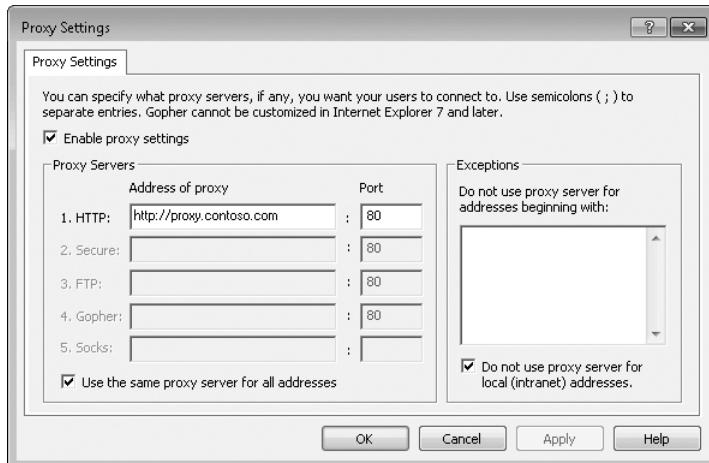


FIGURE 5-25 Proxy Settings

## Add-ons and Accelerators

Add-ons and accelerators extend the functionality of Windows Internet Explorer. For example, you can use the Add-Ons functionality of Internet Explorer to configure the browser to use a third-party search engine from the search bar, as long as there is an OpenSearch configuration file for the third-party search engine provider. Add-ons and accelerators can also present a security risk to your organization. If organizational policy is not configured correctly, add-ons and accelerators can forward sensitive data to untrusted third parties. Just as an organization controls the use of applications through AppLocker policies, add-on policies, located under the Windows Components\Internet Explorer\Security Features\Add-on Management node, allow control over the deployment of add-ons. The important policies for add-on management are:

- **Add-on List** This policy allows you to specify add-ons using add-on CLSID identifiers. You can specify whether an add-on is allowed or denied using this list.
- **Deny All Add-Ons Unless Specifically Allowed In The Add-On List** If you enable this policy, add-ons not listed in the Add-on List policy are blocked. If you do not enable this policy, Windows Internet Explorer allows add-ons not covered by the add-on list.

Accelerators differ from add-ons in that they must be executed by the user, rather than being loaded automatically by a Web page as is the case with an add-on. Accelerator policies are located under the Windows Components\Internet Explorer node of both the Computer Configuration and User Configuration Group Policy areas and have the following functionality:

- **Deploy Default Accelerators** This policy specifies the default accelerators for each category (Blog, E-mail, Map, and Translate). Users are able to use alternate accelerators where policy allows, but are unable to change the default accelerators.

- **Deploy Non-Default Accelerators** This policy enables administrators to deploy additional accelerators, which are provided as alternatives to the default accelerators. Users are unable to remove these accelerators.
- **Turn Off Accelerators** This policy disables all accelerators.
- **Use Policy Accelerators** This policy blocks the use of all accelerators except those that you have authorized through policy.

---

#### EXAM TIP

Understand how you can alter how Windows Internet Explorer interacts with Web sites by configuring security zones.

---

## PRACTICE Managing the Configuration of Internet Explorer

Internet Explorer offers administrators many options when it comes to enforcing a standardized configuration across the organization. You can choose from two methods through which you can enforce a standardized configuration: Internet Explorer Administration Kit profiles and Group Policy. In this practice, you use both methods to configure Internet Explorer.

### EXERCISE 1 Managing Windows Internet Explorer Add-Ons by Using Group Policy

Although add-ons and accelerators enhance the functionality of Internet Explorer, if policy is not configured effectively, users can download and install accelerators and add-ons from untrusted third parties that compromise browser security. In this practice, you configure a number of Internet Explorer 8 settings through Group Policy. To complete this exercise, perform the following steps:

1. Log on to computer WKSTN1 with the Mark Lee user account.
2. Open the Local Group Policy Editor and navigate to the Computer Configuration\ Administrative Templates\Windows Components\Internet Explorer node.
3. Enable the Do Not Allow Users To Enable Or Disable Add-Ons policy.
4. Enable the Disable Per-User Installation Of ActiveX Controls policy.
5. Enable the Disable Automatic Install Of Internet Explorer Components policy.
6. In the Accelerators node, enable the Turn Off Accelerators policy.
7. Close the Local Group Policy Editor.
8. Restart the computer and log on using the Mark Lee user account. Open Internet Explorer. From the Tools menu, select Manage Add-ons. Verify that you are unable to modify any of the default add-ons and are unable to install additional add-ons.
9. Return the Local Group Policy to its original configuration by setting the policies that you configured in steps 3, 4, 5, and 6 to the Not Configured setting.

## EXERCISE 2 Exploring the Internet Explorer Administration Kit

In this exercise, you install and configure the Internet Explorer Administration Kit and create a customized Windows Internet Explorer package for deployment.

### MORE INFO INTERN EXPLORER ADMINISTRATION KIT

To perform this exercise, you need to have downloaded the Internet Explorer Administration Kit. You can download this file from the following TechNet Web site:  
<http://technet.microsoft.com/en-us/ie/bb219517.aspx>.

To complete this practice, perform the following steps.

1. Log on to computer WKSTN1 with the Mark Lee user account.
2. Locate and run the file iekak.msi to begin the installation of the Internet Explorer Administration Kit. You are prompted by a security warning because the file has been downloaded from the Internet. At this warning, click Run.
3. On the wizard Welcome page, click Next. On the End-User License Agreement page, select the I Accept The Terms In The License Agreement page, and click Next.
4. On the Choose License Type page, select Internal Distribution Via A Corporate Intranet, as shown in Figure 5-26, and then click Next.

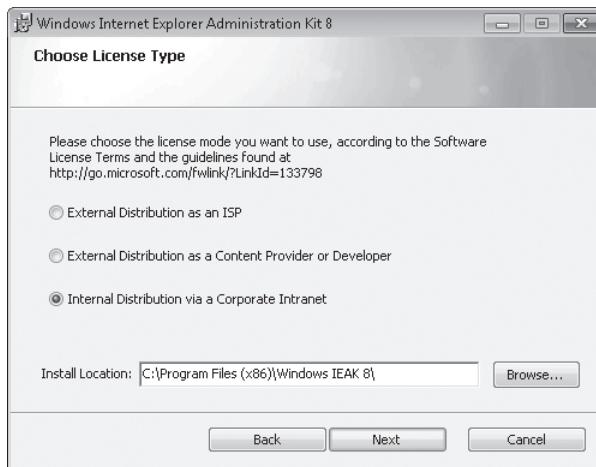
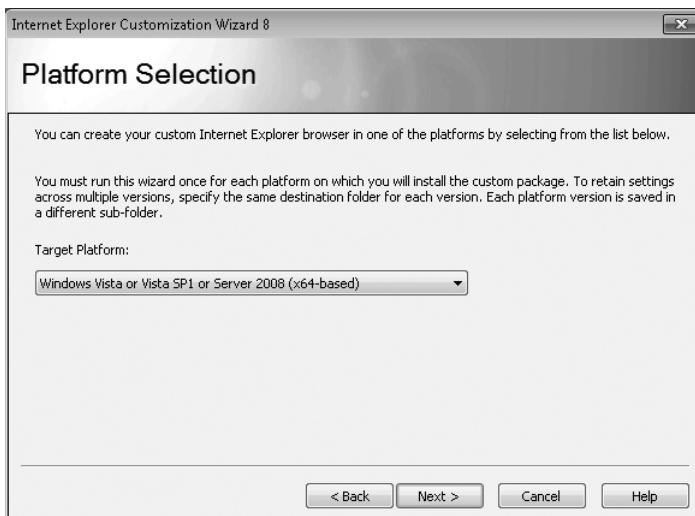


FIGURE 5-26 Selecting IEAK License Type

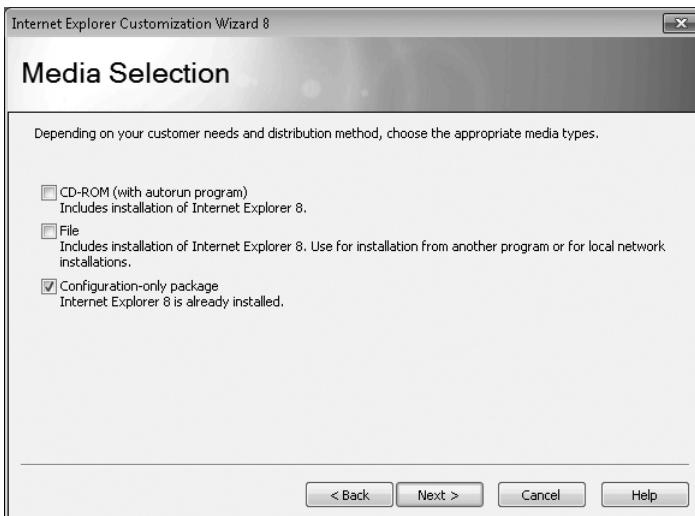
5. In the Organization Name text box, enter the name **Contoso Corp**, and then click Next. On the Ready To Install page, click Install.
6. On the Do You Want To Allow The Following Program To Install Software On This Computer page, click Yes. The Internet Explorer Administration Kit is now installed. To close the wizard, click Finish.
7. From the Start menu, click Internet Explorer Customization Wizard 8, which is located in the Windows IEAK 8 folder. Click Yes to dismiss the User Account Control dialog box.

8. On the Welcome page, click Next. On the File Locations page, accept the default value, which is the current date, and then click Next.
9. On the Platform Selection page, select Windows Vista Or Vista SP1 Or Server 2008 (x86-based), as shown in Figure 5-27, and then click Next.



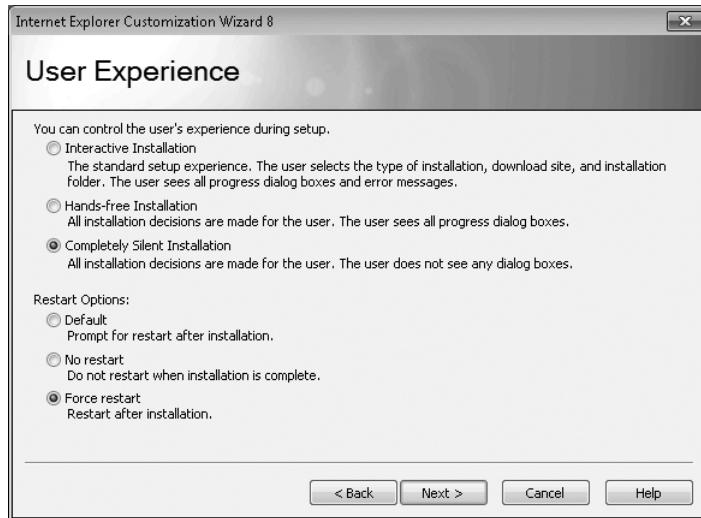
**FIGURE 5-27** Platform customization

10. After the wizard contacts the Microsoft Update servers on the Internet, accept the default target language selection, and then click Next.
11. On the Media Selection page, ensure that Configuration-only Package is selected, as shown in Figure 5-28. Click Next.



**FIGURE 5-28** Configuring media selection options

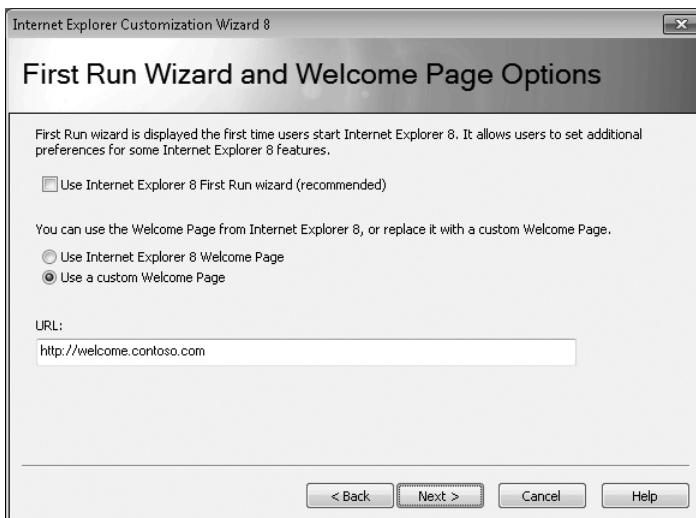
12. On the Feature Selection page, ensure that all features are selected, and then click Next.
13. The Automatic Version Synchronization page initiates synchronization, including a version check of the Internet Explorer 8 setup files. You need to click Run to allow synchronization to run and then click Synchronize to obtain the latest available version. You may need to click Run again when presented with another security warning. After synchronization has completed, click Next until you reach the User Experience page.
14. On the User Experience page, select the Completely Silent Installation and Force Restart options, as shown in Figure 5-29. Then click Next.



**FIGURE 5-29** User Experience options

15. On the Browser User Interface page, enable the Customize Title Bars option. In the Title Bar Text area, type **Contoso Corporation**. This brands the deployment of Internet Explorer. Click Next.
16. On the Search Providers page, click Import. This imports any search providers that are already installed on WKSTN1. Click Next.
17. On the Important URLs page, remove any existing URLs and add the URL **http://www.contoso.com**, and then click Next.
18. On the Accelerators page, click Import. This action imports any accelerators that are configured for Internet Explorer. Click Next.

19. Review the list of favorites, and then click Next. On the Browsing Options page, click Next.
20. On the First Run Wizard And Welcome Page Options page, ensure that the Use Internet Explorer 8 First Run Wizard option is not selected. Set the Welcome page to <http://welcome.contoso.com>, as shown in Figure 5-30. Then click Next.



**FIGURE 5-30** Configuring Welcome page

21. On the Compatibility View page, select the Use Internet Explorer 8 Mode (Default) option, and then click Next until you reach the Connection Settings page.
22. On the Connection Settings page, select the Do Not Customize Connection Settings option, and then click Next.
23. On the Automatic Configuration page, ensure that Automatically Detect Configuration Settings is enabled, and then click Next.
24. On the Proxy Settings page, review the default settings, and then click Next.
25. On the Security and Privacy Settings page, review the default settings, and then click Next.
26. On the Programs page, select Do Not Customize Program Settings, and then click Next.
27. Review the settings on the Additional Settings page, as shown in Figure 5-31. Then click Next.

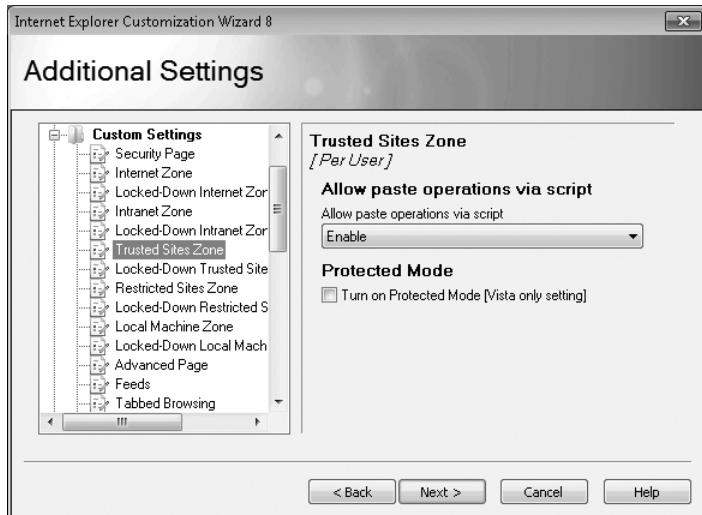


FIGURE 5-31 Additional settings

28. On the Wizard Complete page, click Next. This creates a custom package for the installation of Internet Explorer 8 on the Windows Vista x86 and Windows Server 2008 x86 operating systems. Make note of the folder in which the package is installed.
29. Review the installation files in the build folder using Windows Explorer.

## Lesson Summary

- Internet Explorer Administration Kit allows you to create customized Windows Internet Explorer packages.
- The Internet Explorer Administration Kit Profile Manager allows you to configure automatic configuration files for Windows Internet Explorer. These configuration files can be hosted at an accessible location.
- Add sites that you suspect of containing malware to the Restricted Sites zone. Add sites that you trust but that are not located on your organizational network to the Trusted Sites zone.
- You can allow specific add-ons while blocking all others by configuring Group Policy.

## Lesson Review

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

**NOTE ANSWERS**

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

1. You want to ensure that users in your organization are unable to add and remove Web site addresses from the Windows Internet Explorer Trusted Sites and Restricted Sites zones. Which of the following Group Policy items should you configure to accomplish this goal?
  - A. Security Zones: Use Only Machine Settings
  - B. Security Zones: Do Not Allow Users To Change Policies
  - C. Security Zones: Do Not Allow Users To Add/Delete Sites
  - D. Restrict Search Providers To A Specific List Of Providers
2. You want to limit Windows Internet Explorer accelerators to those that are configured through Group Policy. You do not want to add additional accelerators. Which of the following policies should you configure?
  - A. Deploy Non-Default Accelerators
  - B. Deploy Default Accelerators
  - C. Turn Off Accelerators
  - D. Use Policy Accelerators
3. You are in the process of creating a distribution plan for the deployment of Internet Explorer 8 using organization-specific configuration settings. Windows Internet Explorer must be deployed to 60 portable computers that are not part of your organization's Active Directory environment. Which of the following methods allows you to deploy organizational settings consistently to these computers with a minimum of administrative effort?
  - A. Local Group Policy
  - B. Security Policy
  - C. Domain-level Group Policy
  - D. Internet Explorer Administration Kit
4. You want to ensure that users are not able to remove temporary Internet files and cookies when browsing using Internet Explorer 8. Which of the following policies should you configure to accomplish this goal?
  - A. Prevent Deleting Passwords
  - B. Prevent Deleting InPrivate Filtering Data
  - C. Prevent Deleting Favorites Site Data
  - D. Prevent The Deletion Of Temporary Internet Files And Cookies

5. You want to ensure that users of Internet Explorer 8 in your organization are not able to browse in a way that avoids automatic recording of cookies and browsing history. Which of the following policies should you configure to accomplish this goal?
- A. Turn Off InPrivate Filtering
  - B. Turn Off InPrivate Browsing
  - C. Do Not Collect InPrivate Filtering Data
  - D. InPrivate Filtering Threshold

## Chapter Review

---

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

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

## Chapter Summary

- When defining a client security standard, select a technology that is appropriate to the outcome you want to accomplish.
- Use BitLocker and EFS to encrypt data and AppLocker policies to restrict application execution.
- Use account policies to set password policies and use user account control policies to determine how Windows treats requests for elevated privileges.
- Windows Internet Explorer can be configured through the Internet Explorer Administration Kit, through Group Policy or through a combination of both technologies.

## 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.

- AppLocker
- BitLocker
- InPrivate Browsing
- InPrivate Filtering

## Case Scenarios

In the following case scenarios, you apply what you've learned about subjects of this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Client Security at Contoso

You are in the process of developing a client security baseline policy for implementation on the computers running the Windows 7 operating system at Contoso Pharmaceuticals. You have recently installed the Windows 7 Enterprise edition operating system on all client computers at Contoso. Contoso has a policy of purchasing applications only from vendors who digitally sign the application binaries. As a part of its portable computer strategy, Contoso has just purchased 200 small form factor notebook computers. These netbook computers do not have a TPM (Trusted Platform Module) chip. You want to ensure that users are able to start their netbook computers without having to insert a USB key or use a startup PIN. You want to ensure that the contents of the C:\Documents folder on these netbook computers cannot be recovered by unauthorized third parties if the netbook computer is misplaced.

With these facts in mind, answer the following questions:

1. What encryption solution should you deploy to protect the C:\Documents folder on the netbook computers?
2. What steps should you take to prevent users from running applications that are not digitally signed by an approved vendor?
3. How can you ensure that computers running Windows 7 accept inbound communication only from computers that are members of the Contoso domain?

### Case Scenario 2: Internet Explorer Configuration

The legal department at Contoso Pharmaceuticals is concerned that the browsing habits of users at the organization are being tracked by third parties. After a security incident where sensitive intranet data was forwarded to an untrusted third-party Web site, your manager has recommended that you configure Internet Explorer to block add-ons and accelerators. Several users in your organization connect to a partner organization's internal network to interact with a Web application. They have noticed that some aspects of this Web application do not function with Internet Explorer 8. The partner organization reports that their users are able to fully utilize the Web application when it is accessed locally using Internet Explorer 8.

With these facts in mind, answer the following questions:

1. What steps can you take to ensure that user browsing sessions at Contoso Pharmaceuticals are not tracked across multiple sites by third parties?
2. What steps can you take to ensure that users are unable to install additional accelerators or add-ons on computers that have Internet Explorer 8 installed?
3. What steps can you take to ensure that users that connect to the Web application hosted by Fabrikam are able to run it without problems?

## Suggested Practices

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

### Define Client Security Standards

In this practice, you will perform two configuration tasks that are critical for those interested in developing client security standards for computers running the Windows 7 operating system.

- **Practice 1** Configure security policy so that a user is locked out for a period of 20 minutes if they enter an incorrect password three times in a 5-minute period. Also configure security policy so that users must change their passwords every 21 days and are unable to use any of their previous five passwords.
- **Practice 2** Configure security policy so that administrators and standard users must respond to all user account control prompts by entering credentials on the secure desktop.

### Define Windows Internet Explorer Settings

In this practice, you perform two configuration tasks related to the configuration of Internet Explorer.

- **Practice 1** Use the Internet Explorer Administration Kit to create custom Windows Internet Explorer deployment files for Windows XP x86 Service Pack 3. Install the resulting build in a Windows XP Mode deployment hosted on your computer running Windows 7.
- **Practice 2** Use Group Policy to configure browser history settings so that users are unable to delete their browsing history.

### 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 70-686 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.

# Designing a Windows 7 Client Deployment Strategy

Chapter 3, “Creating and Managing System Images,” discusses various methods for creating customized Windows Imaging files for deployment on an enterprise network. This chapter introduces the deployment process itself and helps you to decide which of the available deployment methods is most suitable for a particular organization. Lesson 1 lists the basic steps of a Windows 7 deployment and describes the permutations of the process that occur when you use the various Microsoft deployment tools. Lesson 2 provides the criteria administrators should use to decide what deployment method is best for their organizations.

## Exam objectives in this chapter:

- Analyze the environment and choose appropriate deployment methods.

## Lessons in this chapter:

- Lesson 1: Understanding the Windows 7 Deployment Process **220**
- Lesson 2: Choosing a Deployment Method **248**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- A computer running Windows 7 or Windows Server 2008 R2 on which you have installed Windows 7 AIK and MDT 2010, as described in the Chapter 3, Lesson 1 practice: “Downloading and Installing the Windows 7 AIK.”
- A Windows 7 installation DVD.



## REAL WORLD

Craig Zacker

There is a certain type of administrator who prefers to do things manually, uses command-line tools instead of graphical ones, and is determined to learn not just how things work, but why. Very often, this type of individual benefits from this inclination by learning to do things more quickly and efficiently than those who take the easy road.

The tools that Microsoft supplies for performing large-scale workstation deployments enable administrators to perform virtually every task in the process manually, if they want to, from creating answer files to capturing and deploying images. However, this is one instance when most administrators of that certain type should avoid their instinctive attraction to manual processes.

A completely manual deployment can be an incredibly complex and time-consuming process, and tools like Microsoft Deployment Toolkit 2010 are specifically designed to provide a framework of best practices that prevent administrators from having to “reinvent the wheel,” that is, build from scratch what has already been created for them.

## Lesson 1: Understanding the Windows 7 Deployment Process

Depending on the number of workstations you have to install, the requirements imposed by your organization, and the tools at your disposal, the process of deploying Windows 7 can be simple or extremely complex. This lesson explains the basic steps of the deployment process, and describes how the various Microsoft deployment tools implement those steps.

**After this lesson, you will be able to:**

- Understand the steps of a basic Windows 7 deployment and variations that result from the use of various deployment tools.

**Estimated lesson time: 60 minutes**

## Windows 7 Deployment Basics

In its simplest form, a Windows 7 deployment consists of a user starting a computer and inserting an installation disk into the DVD drive. After the user answers a few simple questions, the Windows 7 setup program takes over and installs the operating system. The process is completely automated until it is time for the user to provide an account name and log on for the first time. The user then configures various settings and installs various applications until the workstation has a working environment suitable for specific tasks.

Although much of it is transparent to the user, this interactive installation process is essentially the same as that performed in a complex Windows 7 deployment on an enterprise network. The computer starts, loads the Windows Preinstallation Environment (Windows PE), and applies a Windows Imaging file containing the operating system to the computer's local disk. The differences between an individual, interactive installation, and an enterprise deployment include the following:

- How the computer obtains the Windows PE boot files
- The configuration of the Windows Imaging file containing the operating system
- How the computer interacts with the setup program
- How the workstation receives the applications and configuration settings it needs

The main object of an enterprise deployment is to install Windows 7 in a standardized configuration on multiple computers with little or no interaction at the workstation site. At its most basic level, an enterprise workstation deployment consists of the following steps:

1. Build a deployment share.
2. Perform a reference computer installation.
3. Capture an image of the reference computer.
4. Boot the target computer by using Windows PE.
5. Apply the captured image containing Windows 7.

These steps are described in the following sections.

### Building a Deployment Share

A deployment share, as described in Chapter 3, is simply a shared folder on a Windows server where you store the Windows Image files and other software components that computers on the network need to access during the various phases of the deployment process. Although in a mass deployment, you can burn your customized images to DVD-ROM discs and distribute them to the target workstations that way, as in an individual installation, having the workstations access the images over the network is far easier.

There are performance factors to consider when deploying images over the network, however. Windows Imaging files are usually large, and hundreds of workstations downloading them simultaneously can flood the network, slowing down the deployment process and negatively affecting other users. For more information on benchmarking your networking and factoring performance issues into your deployment planning, see Lesson 2, "Choosing a Deployment Method," later in this chapter.

Windows Deployment Services (WDS), Windows 7 Automated Installation Kit (AIK), and Microsoft Deployment Toolkit (MDT) 2010 all provide mechanisms for creating deployment shares and populating them with image files and other software components. In WDS, you use the Windows Deployment Services console. In Windows 7 AIK, you use Windows System Image Manager (SIM), and in MDT 2010, you use Deployment Workbench. You can also create a share manually and use it to distribute your images, but these tools streamline the process considerably.

**NOTE DEPLOYMENT SHARES BY OTHER NAMES**

Although WDS, Windows AIK, and MDT 2010 can all create shares and populate them with deployment files, they refer to them by different names. MDT 2010 uses the term “deployment share,” while earlier versions of MDT and Windows 7 AIK refer to it as a “distribution share.” In WDS, you create a “remote installation folder.” The names are different, as are the tools that you use to create them, but the basic function is essentially the same.

## Performing a Reference Computer Installation

As described in Chapter 3, a reference computer is a workstation, installed and configured in a lab, which administrators use as a model for the workstations they plan to deploy on the production network. By creating a reference installation and then capturing an image of it, administrators can implement their own customized workstation configurations without having to configure each computer individually.

Windows 7 installation disks have image files on them, which contain the basic operating system files, but most administrators create their own customized images for mass deployments. You can use the Microsoft deployment tools to automate the process of installing and configuring a reference computer, but whether this is necessary for a particular deployment project is a decision each administrator must make individually.

For example, if you are planning a deployment of 500 workstations that are completely identical, you need only one reference computer, and you might find it easier to install and configure Windows 7 on the reference computer manually. If, however, you are deploying 500 workstations using 20 different configurations, you are not likely to want to perform 20 separate reference computer installations; automating the process can save a lot of time and effort.

The Microsoft deployment tools provide two ways of automating a reference computer installation. You can use the Windows SIM utility from Windows 7 AIK to create an answer file, which the Windows setup program uses to configure the installation process, or you can use Deployment Workbench from MDT 2010 to create a task sequence and a boot image. For more information on creating answer files and task sequences, see Chapter 3.

## Capturing an Image of the Reference Computer

After you install and configure a reference computer, you capture an image of it in Windows Imaging format, complete with all of its applications and customized settings. This is the image that you will deploy to your target workstations. Each of the Microsoft deployment tools has its own way of creating images, as follows:

- Windows 7 AIK includes the ImageX.exe utility, which you can use to create images from the command line.
- MDT 2010 creates boot images that include the Windows Deployment Wizard. When you run the wizard on the reference computer, you select the task sequence you want to use, and the wizard performs the Windows 7 installation and automatically captures an image of the resulting workstation.
- WDS enables you to create capture images, which when deployed on a reference computer, boot the system and capture an image of it.

Whichever method you choose, the program can upload the image it creates back to the deployment share for later distribution to the target workstations.

## Booting the Target Computer by Using Windows PE

Your target computers are the production workstations on which you want to deploy Windows 7. To install an operating system on any computer, you have to boot the system first, and in the case of a new, bare-metal computer, there are no boot files on the local disk. Windows PE is a stripped-down version of the Windows operating system that you can use to start a computer without installing an operating system to a local disk. During the default boot process, Windows PE loads the entire operating system from the boot disk into memory using a RAM disk, which is an area of memory to which the system assigns a drive letter and uses it like a disk. After Windows PE is loaded, you can remove, disconnect, or reformat the boot disk as needed to complete the installation.

The three Microsoft deployment tools support Windows PE in the following manner:

- Windows 7 AIK includes the Windows PE boot files and a script called Copype.cmd that you can use to create a Windows PE build directory. Then, you use a program called Oscdimg.exe to create a boot-disk image that you can burn to a removable medium, such as a CD-ROM or USB flash drive, or deploy over the network.
- MDT 2010 automates the process of creating a Windows PE boot image, which contains the Windows Deployment Wizard. As with the Windows 7 AIK boot image, you can deploy Windows PE on a removable medium or over the network.
- WDS provides the ability to deploy Windows PE boot images over the network to computers that support the Pre-Boot Execution Environment (PXE) standard. Instead of reading the boot files from a local device, such as a disk drive, the workstation connects to the WDS server and downloads a boot image.

#### **NOTE** BOOTING THREE TIMES USING WINDOWS PE

Windows PE can play three roles in a workstation deployment process. You use it to boot the reference computer, so you can install Windows 7. Then you use it to boot the reference computer in preparation for capturing an image. Finally, you use it to boot the target workstations, so you can install your custom images. In each of these three instances, you can boot the computer from a disk or by using a PXE boot.

## Accessing the Image and Installing Windows 7

The final stage of the deployment process is the application of the image you captured from the reference computer to the target computer. There are three ways to do this, as follows:

- **ImageX.exe** Using ImageX.exe from the Windows PE command line, you can apply an identical copy of the image to the hard disk on the target computer.
- **Setup.exe** Using the standard Windows 7 setup program, you can install an image with greater flexibility than ImageX.exe, by specifying an answer file, modifying the disk configuration, or adding drivers and applications.
- **WDS** Using Windows Deployment Services, target workstations running Windows PE can select and download image files for installation.

## Using Microsoft Deployment Tools

Windows 7 AIK, MDT 2010, and WDS are not three separate and independent sets of tools that all perform the same tasks. Deploying a large number of Windows 7 workstations is not just a matter of choosing one package over the others. They are, to be sure, three separate sets of tools, but they are all designed to work together, and administrators can pick and choose among them at will.

For example, although you can complete a deployment using Windows 7 AIK on its own, to use MDT 2010 you must also install Windows 7 AIK. In addition, you can use the services provided by WDS alongside Windows 7 AIK and MDT 2010, as needed. Although each of the three packages has its own procedures and documentation, administrators often achieve their own synthesis between them, using the tools and processes that best suit their environments and their temperaments.

The following sections examine the workstation deployment process as implemented using each of these three packages; they might help you decide which package works best for you at each stage of the process.

# Using Windows Deployment Services

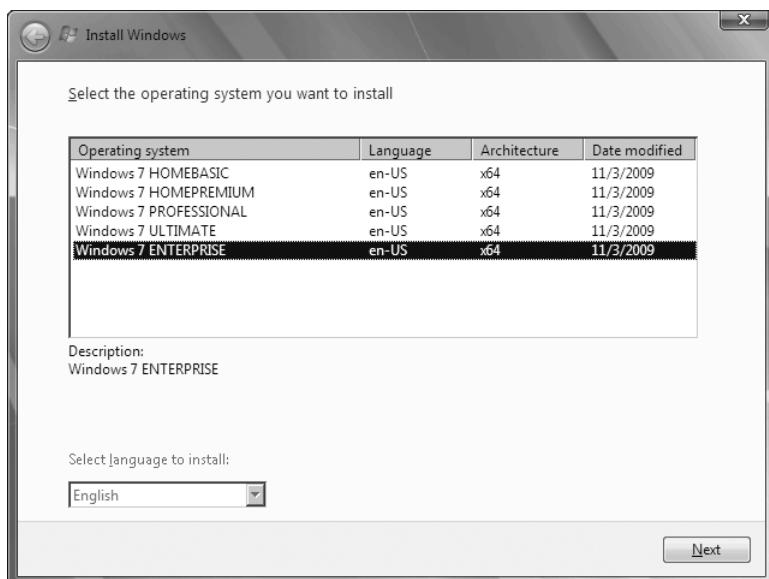
Unlike Windows 7 AIK and MDT 2010, which are stand-alone products largely devoted to the design and creation of images, WDS is a service included in Windows Server 2008 R2 and Windows Server 2008 that is dedicated primarily to the task of deploying images across the network. Using WDS, you can boot bare-metal reference and target computers across the network without having to burn CDs or create bootable flash drives. Once started, a reference or target computer can then download a workstation image file from the WDS server and install it using the Setup.exe program.

## Understanding WDS Communications

For a bare-metal computer to start without a local boot device, it must have a network interface adapter that is compliant with the Pre-Boot Execution Environment (PXE) standard. PXE includes a basic TCP/IP (Transmission Control Protocol/Internet Protocol) client that includes support for the Dynamic Host Configuration Protocol (DHCP). When the computer starts and finds no local boot device, it transmits broadcast messages that search for a DHCP server on the network.

The normal function of a DHCP server is to provide clients with IP addresses and other TCP/IP configuration parameters. In this case, however, the DHCP server, which can run on the same server as WDS, also supplies the client computer with the location of the WDS server on the network. After the PXE network adapter has configured its TCP/IP client, it connects to the WDS server and downloads a boot image by using the Trivial File Transfer Protocol (TFTP).

The boot image contains Windows PE startup files and a setup client that enables the user at the reference or target computer to select and install a workstation image from those stored on the WDS server, as shown in Figure 6-1.



**FIGURE 6-1** The Install Windows Wizard generated by Windows Deployment Services

## Configuring a WDS Server

In Windows Server 2008 R2 and Windows Server 2008, WDS takes the form of a Windows Deployment Services role that you must install with the Server Manager console, as shown in Figure 6-2. The server must be a member of—or a domain controller for—an Active Directory Domain Services (AD DS) domain, and there must be a DHCP server and a Domain Name System (DNS) server on the network.

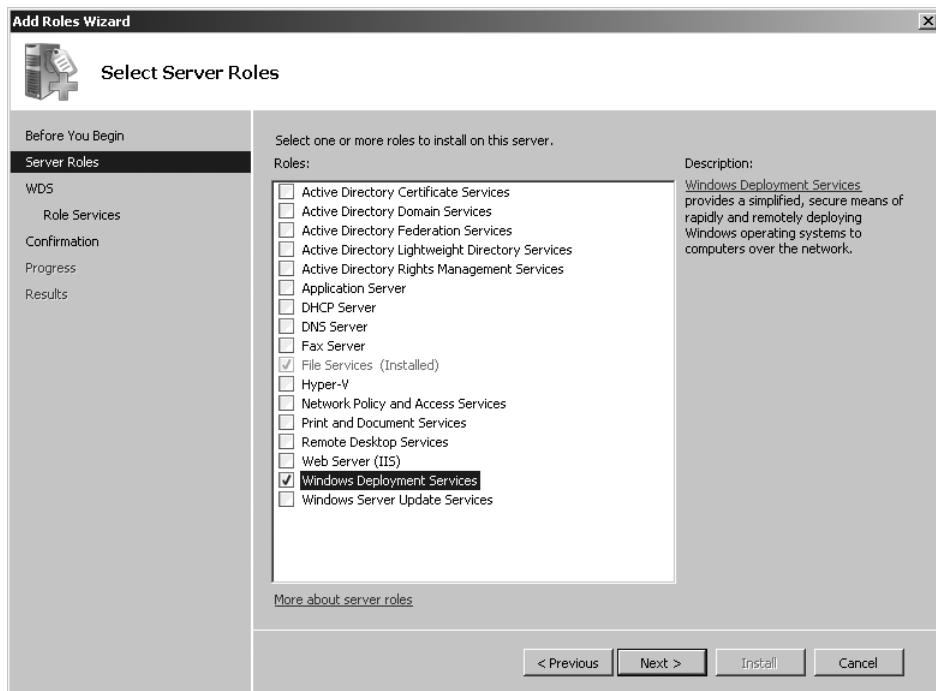


FIGURE 6-2 The Add Roles Wizard in the Server Manager console

After you install the role, you configure WDS by using the Windows Deployment Services console. During the configuration process, you specify the location of the remote installation folder, which is the deployment share that computers on the network use to obtain images. The configuration wizard shares the folder using the share name REMINST, and it creates the directory structure that contains the images and other files, as shown in Figure 6-3.

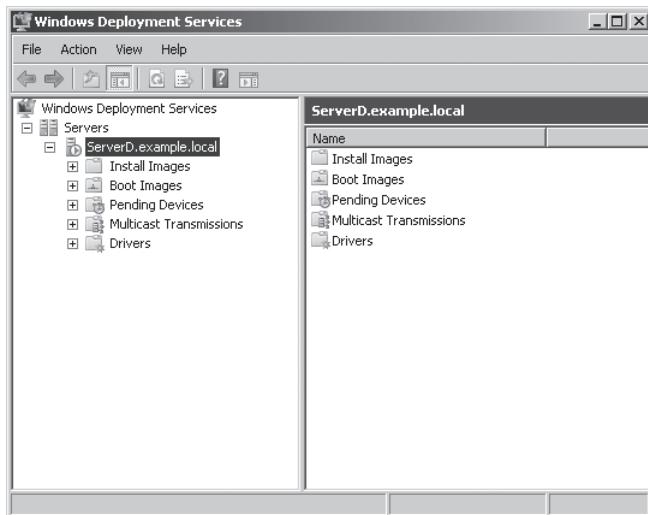


FIGURE 6-3 The directory structure created by Windows Deployment Services

With the deployment share in place, you can begin populating it with images. WDS requires you to add at least one boot image and one install image. A boot image is a Windows Imaging file that contains Windows PE boot files and the setup program that WDS uses on the client desktop. An install image contains the installation files for an operating system.

#### MORE INFO USING WDS

For more information on installing, configuring, and populating WDS, see Chapter 3, “Deploying System Images,” in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7*, by Ian MacLean and Orin Thomas (Microsoft Press, 2009).

### Using WDS as a Complete Deployment Solution

Every Windows 7 installation disk contains, in the Sources folder, a boot image file called Boot.wim and an install image called Install.wim. These are the default images containing the Windows PE boot files and the Windows 7 operating system installation files, respectively. For a small deployment project, or one in which you do not intend to create your own images, you can simply add the Boot.wim and Install.wim images in the Windows Deployment Services console and proceed to start your PXE-enabled workstations. This saves you from having to insert a DVD or other distribution disk into the workstation drive, and it even enables you to install Windows 7 on workstations with no DVD drives at all.

## USING WDS WITH NON-PXE CLIENTS

Not all computers have network interface adapters that support PXE, but you can still use WDS to deploy install images to computers that cannot download a boot image over the network. Using the Windows Deployment Services console, you can convert the standard Boot.wim image into a discover image.

A discover image contains boot files and also enables the client to locate and connect to the WDS server. After the client connects to the server, the process of selecting and installing an install image is the same as on a PXE-compliant workstation.

Discover images do not offer much value to administrators deploying the default Install.wim image because they might as well boot from the original Windows 7 installation disk. However, when you are deploying customized images, creating generic boot CDs containing a discover image can be much easier than burning a lot of individual images to DVDs. You also might find it a valuable alternative when deploying to older workstations that have CD, but not DVD, drives.

## CAPTURING IMAGES WITH WDS

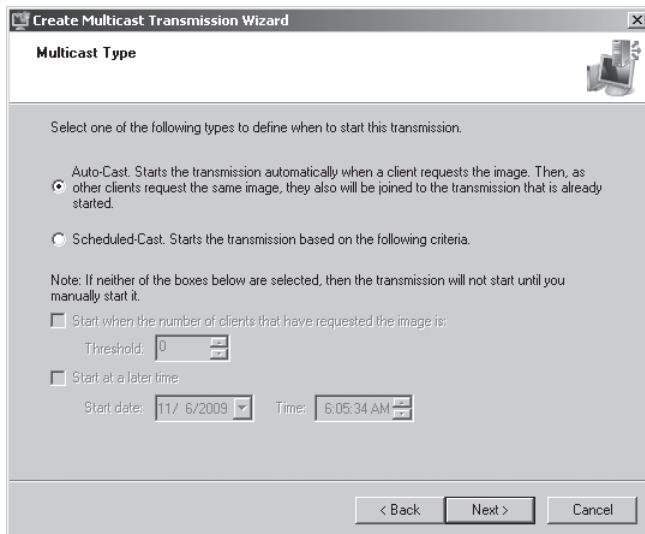
WDS does not provide tools for creating customized reference computer installations; for this, you must use MDT 2010 and/or Windows 7 AIK. However, you can use WDS as an alternative to the ImageX.exe utility to capture an image of a reference computer. With the files in the Boot.wim image from a Windows 7 disk or the WinPE.wim boot image from Windows 7 AIK, you can use WDS to create a capture image. A capture image is a bootable image that launches the Windows Deployment Services Image Capture Wizard on the reference computer. Using the wizard, you can select the volume you want to capture and automatically upload the install image back to the WDS server.

## DEPLOYING IMAGES BY USING MULTICASTS

For large-scale workstation deployments, one of the most useful features in WDS is its ability to deploy images by using multicast transmissions. Multicasting is a feature of the Internet Protocol (IP) that enables one system to transmit data to multiple destinations simultaneously. This is sometimes called a one-to-many transmission.

Using unicasts—also called one-to-one transmissions—deploying an image to 10 computers requires the WDS server to transmit the same file 10 times to 10 different IP addresses. Because image files can be several gigabytes in size, this method can consume a large amount of network bandwidth. Deploying hundreds of workstations can therefore bring even the fastest network to a standstill.

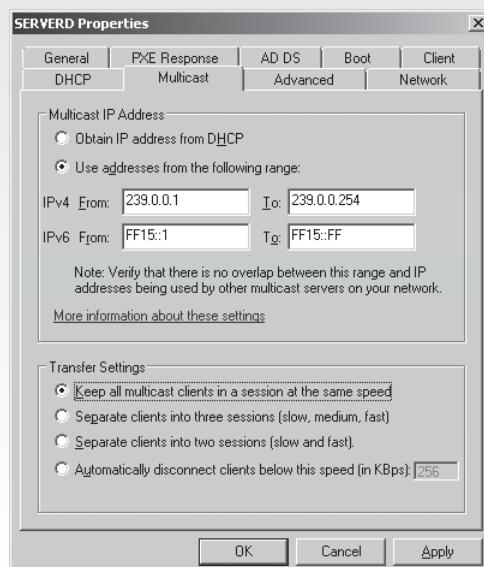
In WDS multicasting, the server transmits the image file only once, to a special multicast group address. The workstations to be deployed, on connecting to the server, join the group and begin receiving the transmission. When you configure a WDS server to use multicasting, you select an image file and specify how you want to initiate the transmission. Multicasts can start automatically when the first client requests the image, you can start them manually, or you can schedule them to start at a specific time, using the interface shown in Figure 6-4.



**FIGURE 6-4** Scheduling multicasts in Windows Deployment Services

#### **NOTE NEW IN WINDOWS SERVER 2008 R2 WDS**

In Windows Server 2008 R2, WDS has additional multicasting capabilities, such as support for IPv6 multicasts. You can also configure WDS to automatically disconnect clients that are running below a specified network transmission speed, or you can split the transmission into two or three sessions, running fast and slow, or fast, medium, and slow, using the Transfer Settings options shown in Figure 6-5. These options enable you to prevent one workstation from affecting the others in the multicast.



**FIGURE 6-5** Multicast Transfer Settings in Windows Deployment Services

## Using WDS with Windows 7 AIK or MDT 2010

Whenever you have to deploy images to workstations on your network, no matter what means you used to create those images, you can deploy them using WDS. Using WDS frees you from having to create boot disks and installation disks, and it also enables you to take advantage of its multicasting capabilities, thereby reducing the impact of the network deployment process on your network.

When you use Windows 7 AIK or MDT 2010 to deploy workstations, you have to boot them several times. First, you have to boot your reference computer to install Windows 7. Then, you have to boot the reference computer again to capture an image of it. Finally, you have to boot the target workstations to deploy your images on them. You can use WDS to perform any of these boots, and as long as your workstations are PXE-compliant, you do not ever have to burn a boot disk. You can use the Boot.wim image from a Windows 7 installation disk, the WinPE.wim image provided with Windows 7 AIK, or a customized boot image created using MDT 2010.

If you create your install images manually, using the tools in Windows 7 AIK, you can deploy them using WDS, just as you would the standard Install.wim image. If you use MDT 2010, you can boot your workstations by using WDS, but because MDT 2010 creates its own deployment share, there is no need to use WDS to deploy the install images.

## Using Windows 7 Automated Installation Kit

The Windows 7 Automated Installation Kit is a collection of tools and documentation that enable you to perform all the tasks essential to a Windows 7 workstation deployment. The same can be said of Microsoft Deployment Toolkit 2010, except that Windows 7 AIK does not include the planning and coordination framework for complex, high-volume deployment projects.

The most important tools included in Windows 7 AIK are as follows:

- **Windows System Image Manager (Windows SIM)** A graphical tool that creates distribution shares and answer files that administrators can use to customize Windows 7 installations
- **ImageX.exe** A command-line tool that can capture, modify, and apply image files in Windows Imaging format
- **Deployment Image Servicing and Management (DISM.exe)** A command-line tool that can mount, edit, and upgrade image files in the Windows Imaging format
- **Windows PE** Core operating system files used to create bootable media
- **System Preparation (Sysprep.exe)** A command-line program that prepares Windows 7 workstations for imaging, auditing, and deployment

Because Windows 7 AIK is a set of free-standing tools, it is highly flexible in its deployment capabilities. The basic deployment framework described earlier in this lesson applies, but with the Windows SIM tool, you can customize and automate your reference computer and target computer installations by creating answer files. Windows 7 AIK was largely created with original equipment manufacturers (OEMs) in mind, and it defines in its documentation two basic types of deployment:

- **Build-to-plan (BTP)** Intended for building workstations in a standard, uniform configuration, the BTP deployment is one in which administrators build the reference computer by using an answer file and create an image, which they deploy to the target workstations unaltered.
- **Build-to-order (BTO)** Intended for customized workstation builds, a BTO deployment is one in which administrators use an answer file to build the reference computer, deploy the resulting image on the target computers, and then boot the computers in audit mode to make further customizations.

The usefulness of these deployment types in an enterprise deployment depends on the types of images you plan to create, as discussed in Chapter 3. If you create a separate, thick image for each of your workstation configurations, you can deploy them to the target computers as is, using BTP deployment. If you choose to create thin images, or a single generic image that you plan to customize for each workstation type, you can use the BTO method and customize the target computers after you deploy the image.

The procedure for a BTO deployment of a bare-metal workstation using only the Windows 7 AIK tools can consist of the following steps:

1. Install Windows 7 AIK on a build computer.

The build computer is where you will create your answer files by using Windows SIM and your Windows PE boot media.

2. Create a distribution share by using Windows SIM, as shown in Figure 6-6.

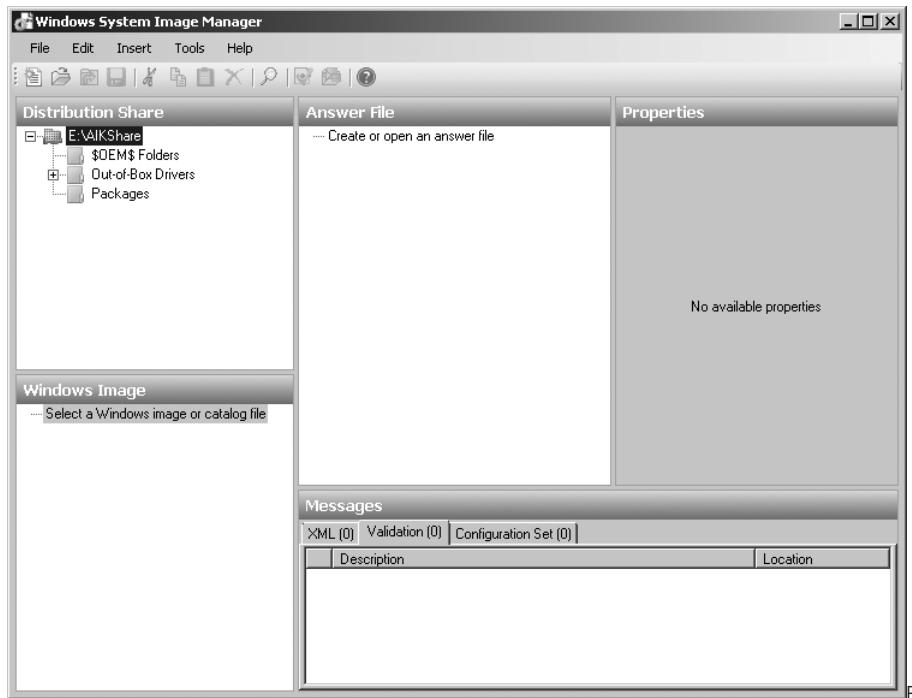


FIGURE 6-6 A distribution share in Windows System Image Manager

In Windows 7 AIK, a distribution share is a directory structure where you store any device drivers and applications that you want to deploy using the answer file. Unlike WDS and MDT 2010, this is not a deployment share where you store the image files you intend to deploy to your reference and target computers. Windows 7 AIK does not have a built-in deployment infrastructure. You either have to manage the image distribution process manually or use WDS or MDT 2010 to deploy your images.

**3. Populate the distribution share.**

Add the device drivers and applications you want to install using the answer file to the appropriate directories in the distribution share, creating subdirectories for each drive and application.

**4. Create and validate an answer file for the reference computer by using Windows SIM.**

Using an answer file, you can add device drivers and applications to the Windows setup procedure, as well as configure a multitude of operating system settings. You must also add the appropriate settings for the software components you stored in the distribution share, as well as any component settings you want to use to configure the operating system installation on the reference computer.

#### MORE INFO CREATING ANSWER FILES

For more information on creating answer files, see Chapter 2, "Configuring System Images," in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7*. For complete documentation of the answer file creation process, see the Windows System Image Manager Technical Reference help file. For complete documentation of all answer file component and package settings, see the Unattended Windows Setup Reference for Windows 7 help file. Both of these help files are supplied with the Windows 7 AIK.

5. Create a configuration set using Windows SIM, using the interface shown in Figure 6-7.

A configuration set is a self-contained version of the files from the distribution share you referenced in the answer file, as well as the answer file itself. After you have created the configuration set, copy it to a removable medium, such as a USB flash drive.

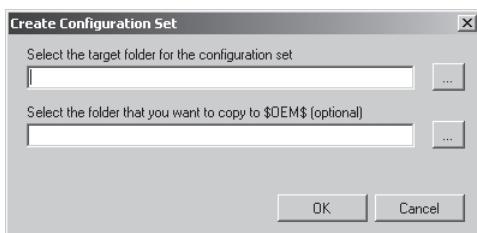


FIGURE 6-7 The Create Configuration Set dialog box in Windows SIM

6. Boot the reference computer by using a Windows 7 installation disk and insert the removable medium containing the configuration set.

The Windows 7 Setup.exe program automatically searches the removable drives on the system, locates the answer file, and installs Windows 7 on the reference computer using your customizations.

#### NOTE INSTALLING THE REFERENCE COMPUTER OVER THE NETWORK

If necessary, you can also install the reference computer by placing the configuration set and the Windows 7 installation files on a network share. After booting the reference computer with a Windows PE boot disk, you map a drive letter to the share using the NET USE command and start the Setup.exe file manually, specifying the path to the answer file on the command line.

7. Switch the reference computer to audit mode and prepare it for image capture using Sysprep.exe.

Running Sysprep.exe with the */generalize* parameter removes the computer-specific and user-specific settings from the installation, and the */audit* parameter switches it from out-of-box experience (OOBE) mode to audit mode.

- 8.** Create a Windows PE boot disk containing the ImageX.exe utility.

Windows 7 AIK includes the Windows PE boot files, but it does not provide a means of deploying boot files over the network. Therefore, to boot your workstations using only Windows 7 AIK tools, you must use the Copype.cmd batch file to create a build directory, add ImageX.exe, and then use the Oscdimg.exe program to package the build directory as a sector-based image file with an .iso extension. Then, you must burn the boot image file to a removable medium, such as a CD-ROM, DVD-ROM, or USB flash drive, using a third-party tool, which Windows 7 AIK does not provide.
- 9.** Boot the reference computer by using the Windows PE disk and capture an image of the reference computer by using ImageX.exe.

Running ImageX.exe with the */capture* command enables you to capture an image of the system and save it to a Windows Imaging file on a local disk, after which you can map a drive to your distribution share and copy the image file there.
- 10.** Boot the target computer by using the Windows PE disk and create a disk partition by using the Diskpart.exe command line utility.

Windows Imaging files require you to create a formatted partition of appropriate size before you can deploy them. When you install a workstation by using the Windows Setup.exe program, you can configure the answer file to create the partition. When you use ImageX.exe to deploy an image, you must create the partition manually.
- 11.** From the Windows PE command line, apply the captured reference computer image to the target computer by using the ImageX.exe utility.

To access the image file from a network share, you must map a drive letter to the share first, and then run ImageX.exe with the */apply* parameter, specifying the path to the image file.
- 12.** Restart the target computer and allow it to boot in audit mode and make any additional configuration modifications.

Audit mode enables you to start the workstation without completing the Windows Welcome user interface pages. You can then configure operating system settings or install applications on the target computer to create a customized configuration.
- 13.** Switch the reference computer back to OOBE mode and prepare it for delivery by using Sysprep.exe.

Running Sysprep.exe with the */oobe* parameter switches the computer from audit mode back to OOBE (Windows Welcome) mode. The */generalize* and */shutdown* parameters then leave the system ready for delivery to the end user.

This procedure describes one permutation of the deployment process using the Windows 7 AIK tools. Depending on the number of workstations you have to deploy and the degree of customization you require, you can modify this procedure considerably. For example, you can conceivably omit the reference computer installation entirely and use an answer file to install the target workstations.

It is relatively rare for administrators to complete a large workstation deployment with Windows 7 AIK alone. Many use WDS to deploy images over the network, or MDT 2010 for a more integrated solution, or both. However, it is difficult to deploy a large number of computers without using some of the tools in Windows 7 AIK, so it is well worth familiarizing yourself with them.

## Using Microsoft Deployment Toolkit 2010

Compared to Windows 7 AIK, which is a set of individual tools, MDT 2010 is more of a unified deployment environment. However, MDT 2010 is also a superset of Windows 7 AIK. You must install Windows 7 AIK along with MDT 2010, and the MDT procedures utilize the AIK tools.

At the highest level, the MDT deployment procedure is essentially the same as that with Windows 7 AIK. You create and configure a reference computer, capture an image from it, and then deploy the image to your target workstations. However, MDT 2010 streamlines the method by which you perform these tasks, thanks to the capabilities of the Deployment Workbench tool.

MDT 2010 supports two deployment models, the Lite-Touch Installation (LTI) and the Zero-Touch Installation (ZTI). As the names imply, an LTI deployment requires a minimal amount of user intervention at the workstation, while the ZTI requires none. For more details on these deployment models, see Lesson 2, later in this chapter, and Chapter 7, “Designing Lite-Touch and Zero-Touch Deployments.”

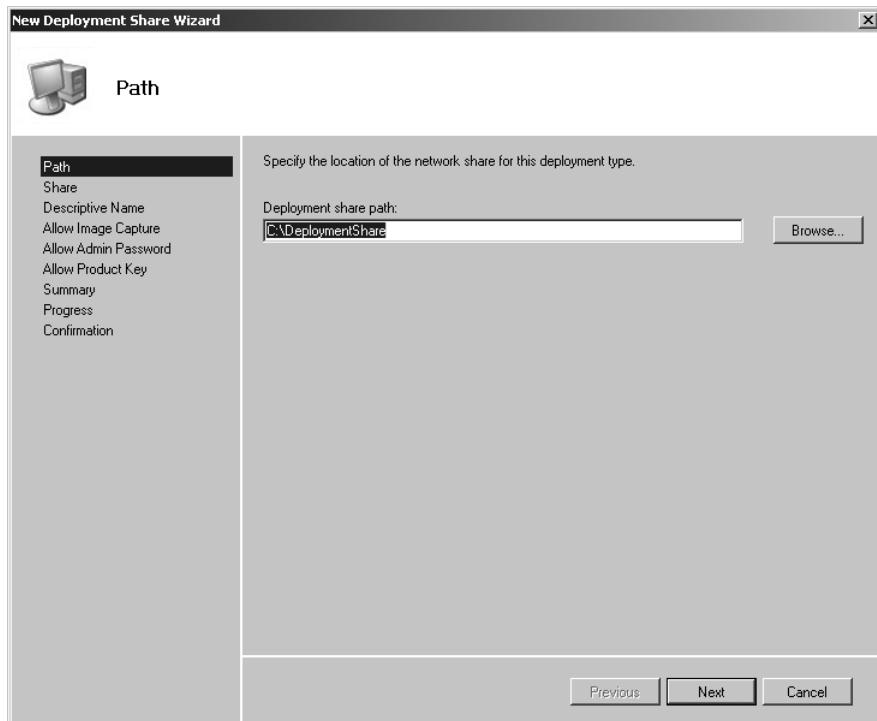
The basic steps in an MDT 2010 LTI workstation deployment are as follows:

1. Create a build computer.

As with Windows 7 AIK, you need a computer on which to install MDT 2010 and the other software it requires, including Windows 7 AIK.

2. Create a deployment share.

Using Deployment Workbench, you create a share, using the New Deployment Share Wizard shown in Figure 6-8. Unlike the distribution share created by Windows SIM, workstations can actually access image files from the MDT deployment share.



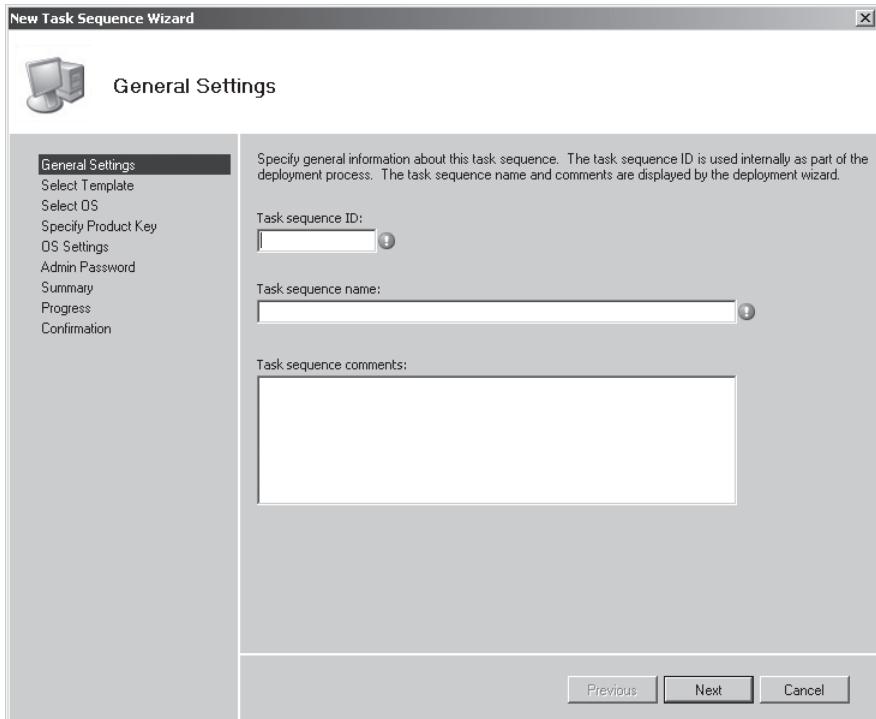
**FIGURE 6-8** The New Deployment Share Wizard in Deployment Workbench

**3.** Populate the deployment share.

Deployment Workbench enables you to add operating systems, applications, device drivers, and other software packages, which you can integrate into your installations. For a reference computer installation, you typically use the Install.wim image from a Windows 7 installation disk.

**4.** Create a task sequence for the reference computer installation.

The MDT task sequencer is responsible for performing the various steps in a Windows installation. When you create a task sequence in Deployment Workbench using the New Task Sequence Wizard shown in Figure 6-9, the wizard automatically creates an answer file that the Windows setup program uses to install the operating system. However, task sequences can also perform additional operations outside of the installation, including automatically capturing an image of the newly installed workstation.



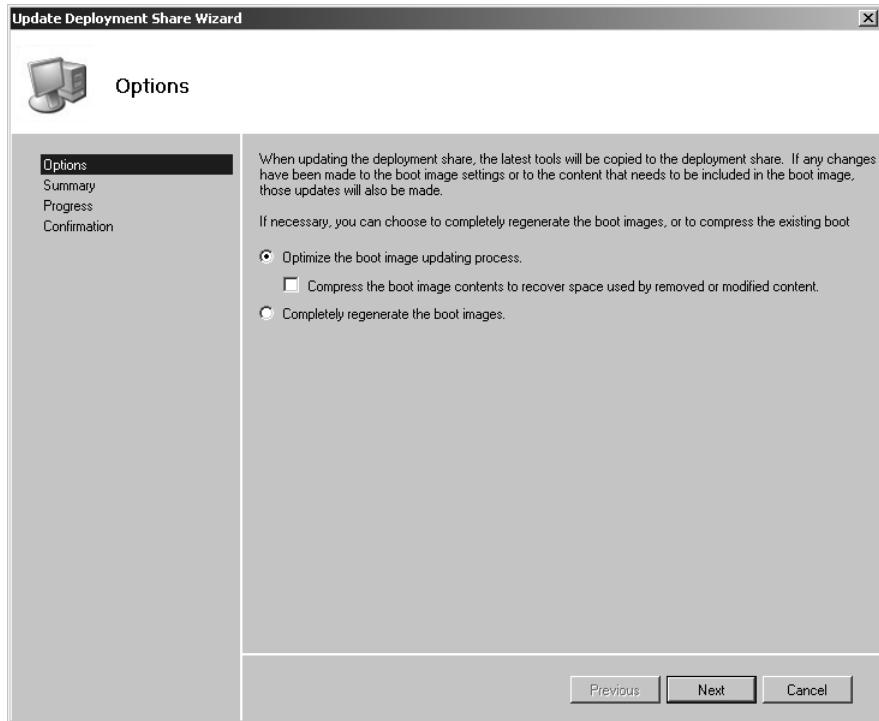
**FIGURE 6-9** The New Task Sequence Wizard in Deployment Workbench

#### **MORE INFO CREATING A TASK SEQUENCE**

For more information on creating a task sequence, see Chapter 3, “Deploying System Images,” in *MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7*. For complete documentation of the task sequence creation and editing processes, see the Microsoft Deployment Toolkit Documentation Library help file, supplied with MDT 2010.

#### **5. Update the deployment share.**

When you update the deployment share in Deployment Workbench, using the Update Deployment Share Wizard shown in Figure 6-10, the wizard creates a boot image using the Windows PE files from the Windows 7 AIK. Unlike the Copype.cmd script from Windows 7 AIK, however, the wizard creates a customized boot image that enables the workstation to access the deployment share over the network.



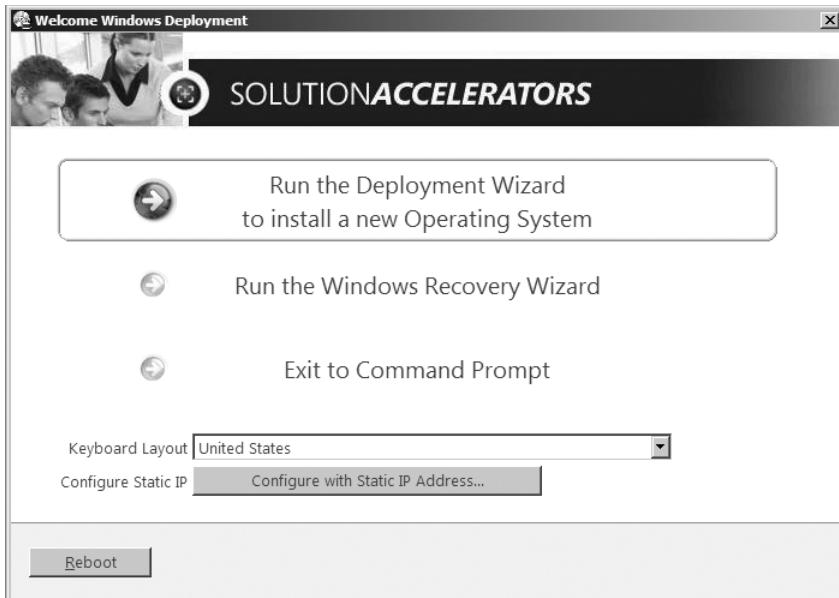
**FIGURE 6-10** The Update Deployment Share Wizard in Deployment Workbench

**6.** Deploy the boot image to the reference computer.

MDT 2010 creates a customized boot image, but it cannot deploy this image to a workstation. However, because the Update Deployment Share Wizard creates the boot image in both file-based (with a .wim extension) and sector-based (with an .iso extension) formats, you can deploy the image to the reference computer by using WDS or by creating a boot disk.

**7.** Install the reference computer.

Starting the reference computer by using the boot image automatically connects the system to the deployment share and launches the Windows Deployment Wizard, as shown in Figure 6-11, from which you can select the task sequence you created earlier.



**FIGURE 6-11** The Windows Deployment Wizard on the reference computer

**8.** Capture an image of the reference computer.

You can configure a task sequence to automatically capture an image of the reference computer after it completes the Windows 7 installation and save it back to the build computer.

**9.** Add the captured image to the deployment share.

After capturing an image of your reference computer, you must add it to the deployment share, so that you can deploy it to your target workstations.

**10.** Create a task sequence for the target computer installation.

In an LTI deployment, the process of deploying your captured image to your target workstations is roughly the same as the reference computer deployment. When creating the task sequence for the target computer deployment, you select your captured reference computer image. You can also configure the task sequence to perform additional installation and configuration procedures on the target workstations.

**11.** Deploy the reference computer image to the target computers.

After creating the task sequence, you update the deployment share and deploy the resulting boot image using WDS or boot disks, just as you did earlier, but this time to the target computers.

A ZTI deployment differs primarily in that it uses System Center Configuration Manager to deploy the images to the workstations. This complicates the deployment process considerably, both in the infrastructure required and in the staging of the reference computer and target computer installations, but it enables administrators to deploy large numbers of workstations without any interaction at each workstation.

## PRACTICE Using Windows System Image Manager

Windows System Image Manager enables you to create distribution shares and answer files that help to automate the Windows 7 deployment process.

### EXERCISE 1 Creating a Distribution Share

A Windows SIM distribution share provides a directory structure in which you can store device drivers and other files you want to deploy to a workstation.

1. Click Start. Then click All Programs | Microsoft Windows AIK | Windows System Image Manager. The Windows System Image Manager console appears.
2. Right-click Select A Distribution Share, and from the context menu, select Create Distribution Share. The Create A Distribution Share dialog box appears.
3. Create a new folder on a local drive, select it, and click Open. The folder appears in the Distribution Share box, as shown in Figure 6-12.

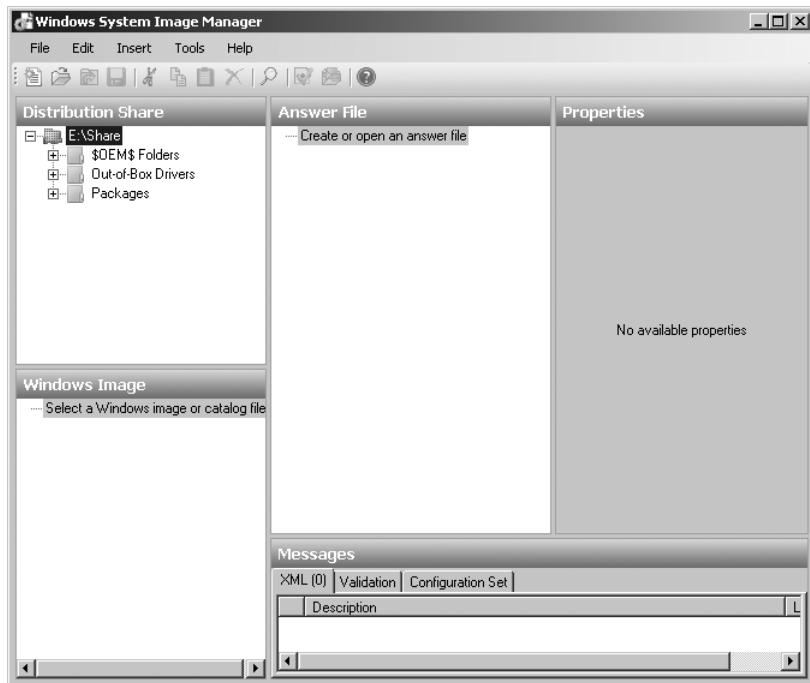
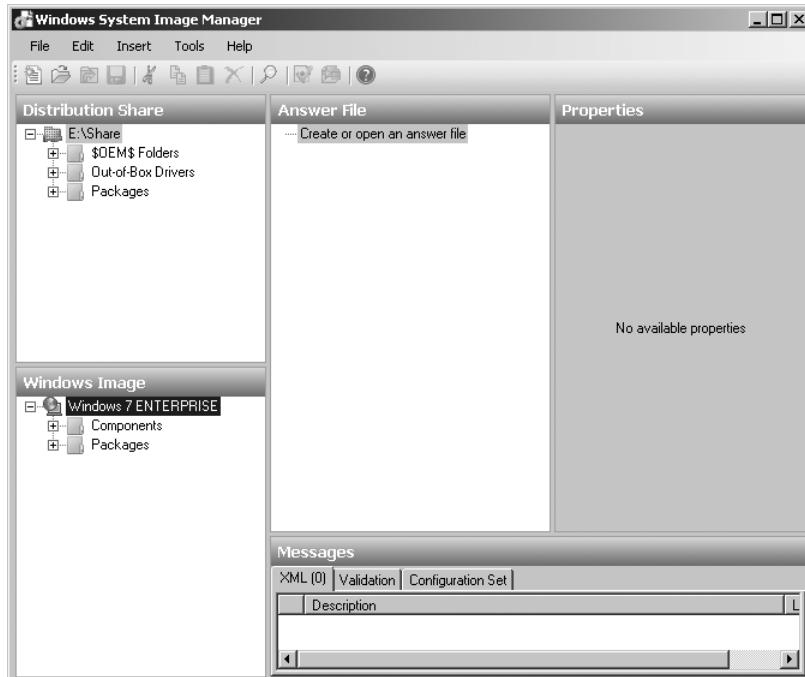


FIGURE 6-12 Creating a distribution share in Windows SIM

- Right-click Select A Windows Image Or Catalog File, and from the context menu, choose Select Windows Image. The Select A Windows Image dialog box appears.
- Insert the Windows 7 installation disk into the DVD drive, browse to the Sources folder on the disk, select the Install.wim file, and click Open. The image appears in the Windows Image box, as shown in Figure 6-13. Depending on the installation disk you use, you might have to select a specific Windows 7 image from those on the disk.



**FIGURE 6-13** Selecting a Windows Image in Windows SIM

- Right-click Create Or Open An Answer File, and from the context menu, select New Answer File. The contents of the new answer file appear in the Answer file box, as shown in Figure 6-14.

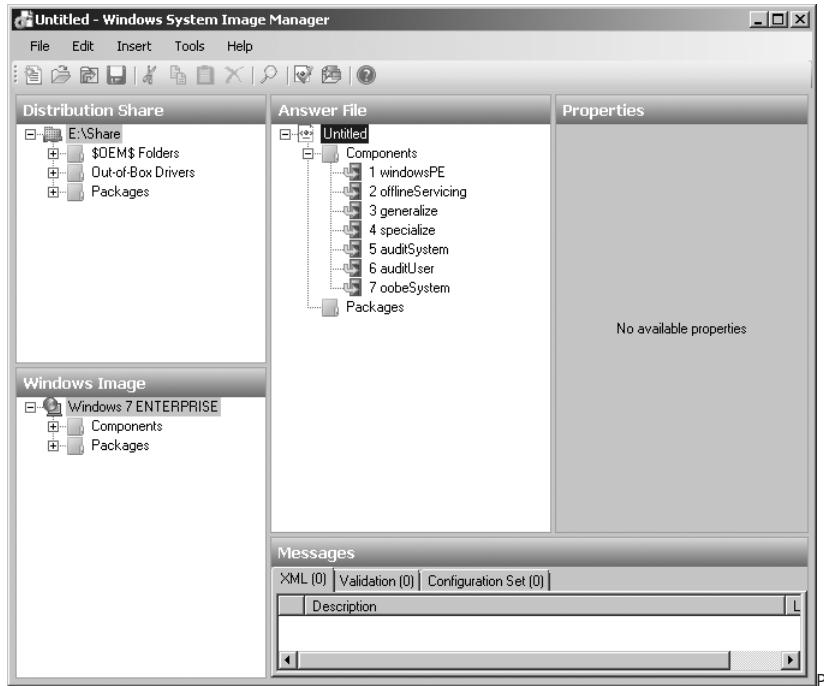


FIGURE 6-14 Creating an answer file in Windows SIM

## EXERCISE 2 Partitioning a Disk with an Answer File

When deploying Windows 7, you can use an answer file to automate the process of partitioning the disk on which you intend to install Windows 7.

1. In Windows SIM, in the Windows Image box, browse to the Microsoft-Windows-Setup\_6.1.7600.16385\_neutral\DiskConfiguration\Disk\CreatePartitions\CreatePartition container, as shown in Figure 6-15. The exact folder name varies depending on the Windows 7 version you are using.

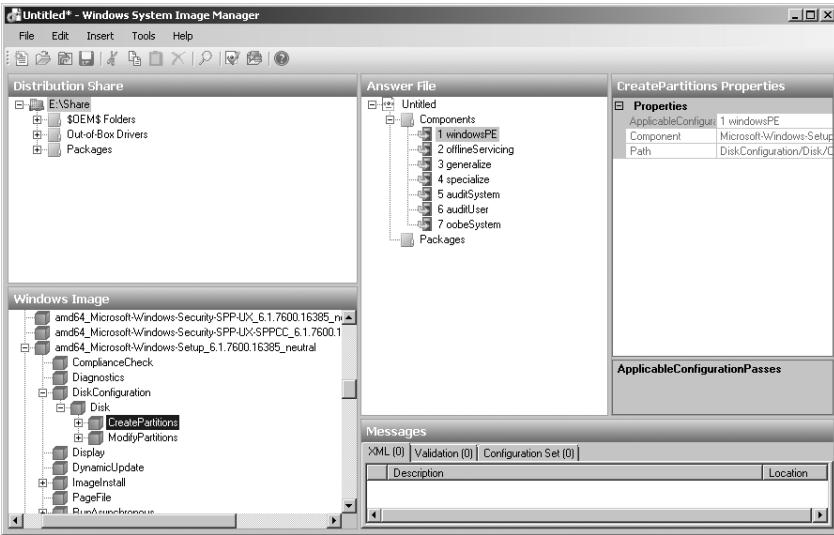


FIGURE 6-15 Locating Disk Configuration components

2. Right-click CreatePartition, and from the context menu, select Add Setting To Pass 1 WindowsPE. The CreatePartition setting appears in the Answer File box, as shown in Figure 6-16.

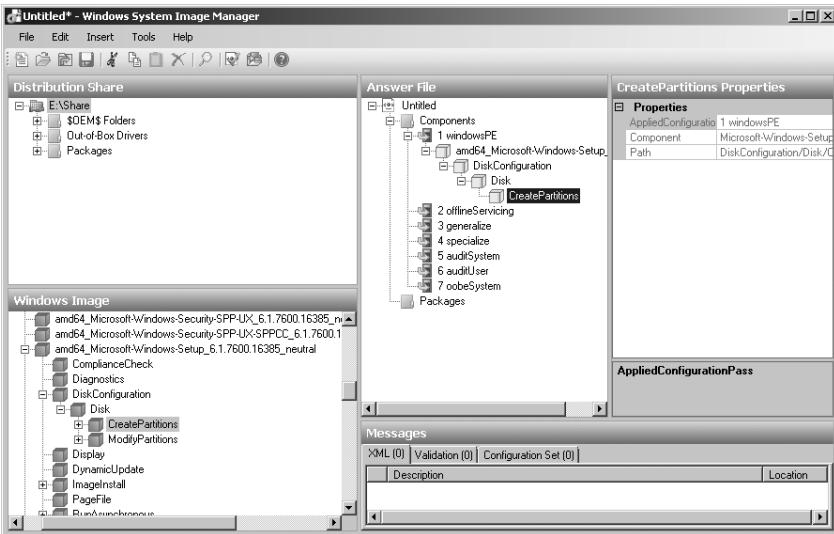


FIGURE 6-16 Adding components to an answer file

3. Expand the ModifyPartitions container, right-click ModifyPartition, and from the context menu, select Add Setting To Pass 1 WindowsPE. The ModifyPartition setting appears in the Answer File box.
4. In the Answer File box, select Disk.
5. In the Disk Properties box, under Settings, configure the following settings, as shown in Figure 6-17:
  - DiskID = 0
  - WillWipeDisk = true

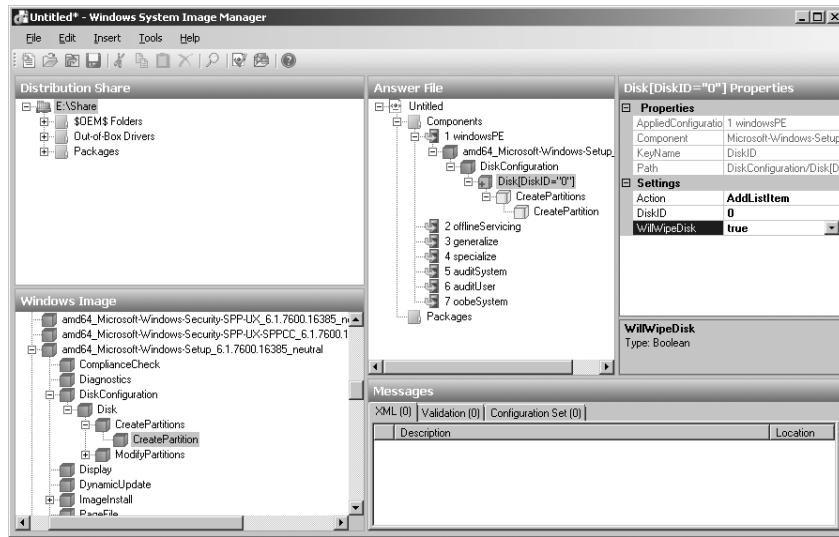
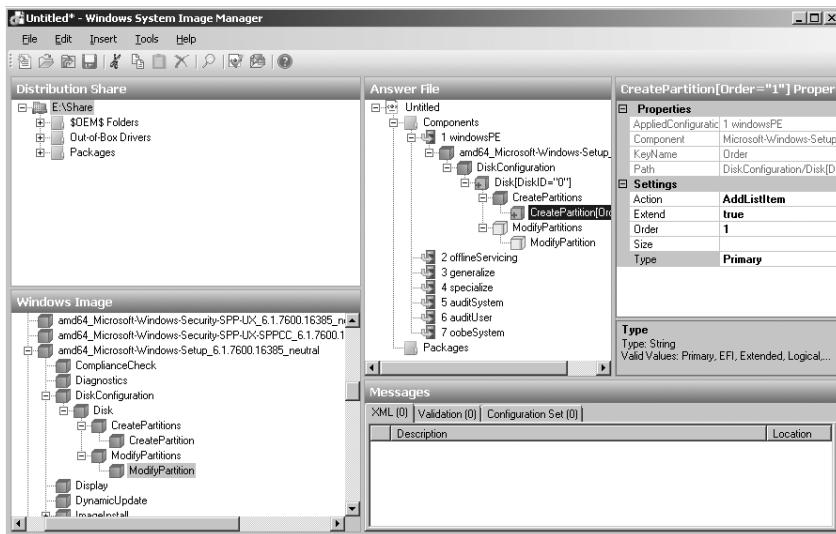


FIGURE 6-17 Configuring Disk settings

6. In the Answer File box, select CreatePartition.

7. In the CreatePartition Properties box, under Settings, configure the following settings, as shown in Figure 6-18:
- Extend = true
  - Order = 1
  - Type = Primary



**FIGURE 6-18** Configuring CreatePartition settings

8. In the Answer File box, select ModifyPartition.
9. In the ModifyPartition Properties box, under Settings, configure the following settings, as shown in Figure 6-19:
- Active = true
  - Format = NTFS
  - Label = Windows
  - Letter = C
  - Order = 1
  - PartitionID = 1

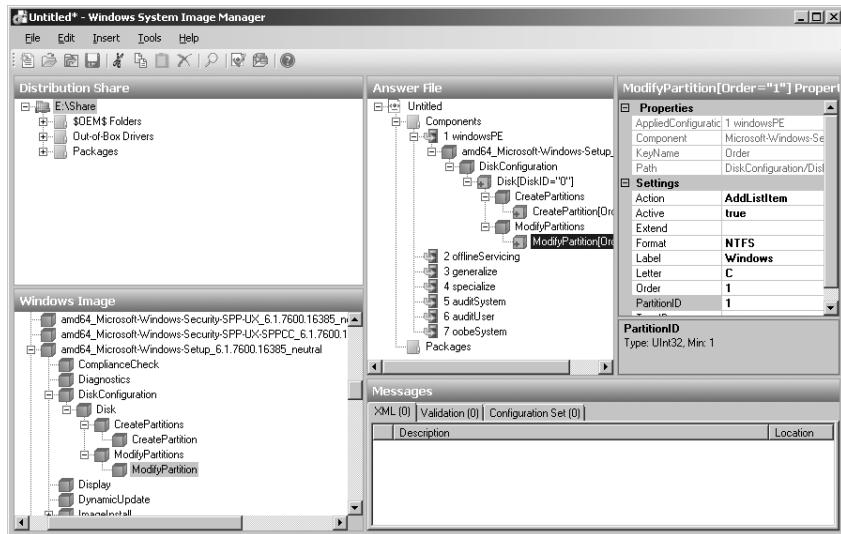


FIGURE 6-19 Configuring ModifyPartition settings

10. From the Tools menu, select Validate Answer File. The Messages box reads No Warnings or Errors.

## Lesson Summary

- In its simplest form, a Windows 7 deployment consists of a user starting a computer and inserting an installation disk into the DVD drive. After the user answers a few simple questions, the Windows 7 setup program takes over and installs the operating system.
- At its most basic level, an enterprise workstation deployment consists of the following steps: build a deployment share, perform a reference computer installation, capture an image of the reference computer, boot the target computer by using Windows PE, and apply the image containing Windows 7.
- WDS is a service included in Windows Server 2008 R2 and Windows Server 2008 that is dedicated primarily to the task of deploying images across the network. Using WDS, you can boot bare-metal reference and target computers across the network without having to burn CDs or create bootable flash drives. Once started, a reference or target computer can then download a workstation image file from the WDS server and install it using the Setup.exe program.
- The Windows 7 AIK is a collection of tools and documentation that enable you to perform all the tasks essential to a Windows 7 workstation deployment. The same can be said of Microsoft Deployment Toolkit 2010, except that Windows 7 AIK does not include the planning and coordination framework for complex, high-volume deployment projects.

- Windows 7 AIK defines in its documentation two basic types of deployment: build-to-plan (BTP), in which administrators build the reference computer by using an answer file and create an image, which they deploy to the target workstations unaltered; and build-to-order (BTO), in which administrators use an answer file to build the reference computer, deploy the resulting image on the target computers, and then boot the computers in audit mode to make further customizations.
- In the MDT deployment procedure, you create and configure a reference computer, capture an image from it, and then deploy the image to your target workstations, just as with Windows 7 AIK. However, the method by which you perform these tasks is more streamlined in MDT 2010, thanks to the capabilities of the Deployment Workbench tool.
- MDT 2010 supports two deployment models, the Lite-Touch Installation (LTI) and the Zero-Touch Installation (ZTI). An LTI deployment requires a minimal amount of user intervention at the workstation, while the ZTI requires none.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, “Understanding the Windows 7 Deployment Process.” 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. To boot a workstation by using WDS, the workstation must have which of the following?
  - A Windows 7 installation disk
  - A PXE-compliant network interface adapter
  - A USB flash drive
  - A Windows PE boot disk
2. Which of the following statements is true about MDT 2010 task sequences? (Choose all that apply.)
  - Task sequences can do things that answer files cannot.
  - Creating an answer file in Deployment Workbench automatically creates a task sequence.
  - Task sequences can automatically capture an image of an installed workstation and upload it to the MDT deployment share.
  - You can use a task sequence when installing a reference computer, but not when installing a target computer.

3. Which of the following Sysprep.exe parameters enables you to start a workstation without completing the Windows Welcome user interface pages?
  - A. /oobe
  - B. /generalize
  - C. /shutdown
  - D. /audit
4. Which of the following programs is not included in Windows 7 AIK?
  - A. Deployment Workbench
  - B. ImageX.exe
  - C. Deployment Image Servicing and Management
  - D. Windows System Image Manager

## Lesson 2: Choosing a Deployment Method

---

As you can tell from Lesson 1 of this chapter, the method for deploying Windows 7 to a large number of workstations is relatively simple, but you need to choose from the many tools you can use to implement that method and choose from the many ways to use those tools. During the early planning stage of your deployment project, you must decide your method for deploying your workstations, based on your needs and your temperament, and then you must build your project around that method. This lesson discusses the criteria you should examine when deciding how you intend to deploy your workstations.

**After this lesson, you will be able to:**

- Understand the criteria for selecting a deployment method.

**Estimated lesson time: 30 minutes**

### Understanding Deployment Options

In Lesson 1, you learned about the primary tools you can use to perform workstation deployments, and to some degree, how those tools can work together. However, there are any number of ways you can combine the tools to suit a specific network environment, and it is likely that your particular situation differs from the preplanned scenarios supplied by Microsoft in their documentation.

## Using Local Installations

The simplest and most basic option, of course, is to have no mass deployment plan at all and simply deploy each workstation manually by inserting a Windows 7 disk into the drive and letting Setup.exe perform the installation. For a small number of workstations, this is the most logical solution. Planning and implementing a mass workstation deployment is usually a complex and time-consuming process, and it is up to the individual administrator to decide at what point a mass deployment saves time and effort over individual installations.

The more applications, updates, and customized settings you have to apply to each workstation, the longer an individual installation takes. For example, if you are rolling out 10 bare-metal Windows 7 workstations with Microsoft Office 2007 and no other customizations, you might be better off installing them manually. However, if you have a dozen applications to install and a large number of settings to configure on those same 10 workstations, you might be able to save time and effort by building a reference computer, capturing an image of it, and deploying that image to the workstations.

## Using Customized Target Computer Installations

There is also a middle ground between a manual installation and a mass deployment using reference computers. You can perform customized target computer installations without using a reference computer, in the following ways:

- **Modify the default `Install.wim` image file by using `DISM.exe`** You can mount an image file while it is offline and add device drivers and updates to it or configure operating system settings by using the DISM.exe command-line program. Then, you can deploy the modified image directly to the target computers. For more information on this process, see Chapter 3.
- **Customize the `Install.wim` installation process by using an answer file or a task sequence** You can use an answer file created with Windows SIM or a task sequence created with Deployment Workbench to customize a target computer installation without creating a reference computer first.

Modifying a single image file or creating a single answer file is faster and easier than planning a full deployment project, as described earlier in Lesson 1. However, both of these options assume that the customizations you intend to make are relatively minor and that you are working with a relatively small number of workstation configurations.

## Using Reference Computers

As noted in the previous sections, the first decision administrators have to make when approaching a workstation installation project is whether to perform individual or customized local installations or design a full-featured deployment using reference computers to capture images.

In an enterprise environment, full deployments are more common. This is not only because there are typically large numbers of workstations to install, but also because the time and effort of designing and planning the deployment can be amortized against future workstation rollouts. You can take the image files, task sequences, answer files, and other elements you create for a deployment now and use them again for future deployments.

After you have decided that local, individual installations are not practical and that you will be building reference computers and capturing new image files, the next questions are how many images you will need and how to create them. These questions are discussed in Chapter 3. Then you must also consider what tools you will use to deploy the images and how you will use those tools.

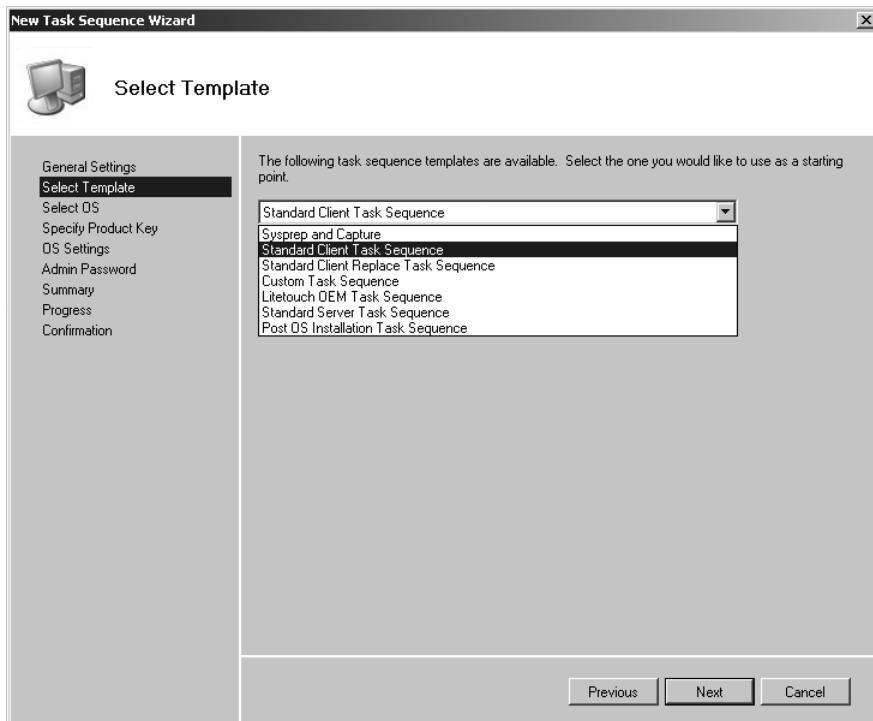
In most cases, there are no compelling reasons not to use Microsoft Deployment Toolkit 2010 as the basis of a large-scale enterprise workstation deployment. MDT 2010 is a free product, as is Windows 7 AIK, its prerequisite, so there are no cost issues to consider. MDT provides support for several different deployment scenarios, as well as extensive documentation to aid in the planning and implementation of a deployment strategy. Assuming, therefore, that you will use MDT 2010 as the basis of your enterprise deployment, the remaining question is how you are going to use it, and what other tools you are going to use with it, as discussed in the following sections.

## Understanding Deployment Scenarios

So far, the discussion of large-scale Windows 7 workstation deployments has centered around bare-metal installations, that is, brand-new computers with no operating system on them. In many deployments, this is the most common scenario. Computer OEMs have to install Windows 7 on hundreds or thousands of new computers, and the more automation they can bring to the process, the better. However, in the case of corporate deployments, this is not always the case.

Corporate IT departments deploying Windows 7 do not always have new computers to work with, so MDT 2010 defines four deployment scenarios, as described in the following sections. The main difference among the scenarios concerns the varying needs for and methods of preserving existing user state data. The User State Migration Tool (USMT) is a Microsoft utility you use to save user state data by copying it to a different location. For more information about USMT, see Lesson 3 in Chapter 2, “Designing a Client Life Cycle.”

To implement these scenarios, you might have to perform certain predeployment tasks on the target workstation and select different templates when creating your task sequences in Deployment Workbench, as shown in Figure 6-20.



**FIGURE 6-20** Selecting a task sequence template in Deployment Workbench

## Using the New Computer Scenario

As described previously in this chapter, the new computer scenario is when you use MDT 2010 to deploy Windows 7 onto a brand-new, bare-metal computer with a clean hard disk. Because there is no existing user data, no applications, and no file system on the target workstation, there is nothing to preserve prior to the deployment. To perform a new computer deployment, you run the Windows Deployment Wizard using a task sequence you create in Deployment Workbench using the Standard Client Task Sequence template.

## Using the Upgrade Computer Scenario

In the upgrade computer scenario, you use MDT 2010 to deploy Windows 7 onto a computer with another operating system already installed on it. The Windows 7 upgrade procedure preserves the existing user state data, applications, and file system, so you do not need to prepare the workstation before the deployment. To perform a new computer deployment, you use a task sequence created with the Standard Client Task Sequence template, just as in the new computer scenario.

#### **NOTE UPGRADING TO WINDOWS 7**

The main limitation of the upgrade computer scenario is that the upgrade paths for Windows 7 are limited. If your workstations are running Windows Vista with Service Pack 1 or Service Pack 2, you can use the upgrade computer scenario to perform an in-place upgrade to Windows 7. However, for workstations running Windows XP or earlier, in-place upgrades are not possible. The only option is to save the user state data with USMT and perform a new operating system installation, either on the same workstation, using the refresh computer scenario, or on a new workstation, using the replace computer scenario.

#### **IMPORTANT UPGRADES AND ZTI**

MDT 2010 supports only the upgrade computer scenario when you perform an LTI deployment. You cannot upgrade workstations using a ZTI deployment.

## **Using the Replace Computer Scenario**

The replace computer scenario describes a means for deploying new workstations while preserving the user state data from your existing workstations. In this scenario, you save the user state data from the existing workstation to a removable medium or network share by running the Windows Deployment Wizard and applying a task sequence created with the Standard Client Replace Task Sequence template. Then, you deploy Windows 7 by running the Windows Deployment Wizard again on the new workstation by using a task sequence created with the Standard Client Task Sequence template, which also restores the user state data you saved previously. Because you are moving only the user state data, the applications and the file system are left on the existing workstation and not transferred to the new one.

## **Using the Refresh Computer Scenario**

In the refresh computer scenario, you use MDT 2010 to deploy Windows 7 on an existing workstation, to standardize the configuration or repair a problem while retaining the user state data. For this scenario, you run the Windows Deployment Wizard only once, using a task sequence based on the Standard Client Task Sequence template. This single task sequence saves the user state data to another location, installs Windows 7, and then restores that same data after the operating system installation is complete. This procedure deletes the existing file system in the process, so all applications and data are lost except for the user state data you saved before the installation.



## REAL WORLD

Craig Zacker

**M**ost IT projects—deployments included—end up being much less simple than they appear on paper. In a perfect deployment, administrators have identical, brand-new computers, onto which they can deploy Windows 7 in a single configuration. In reality, however, a deployment project is likely to require some, or even all, of the four scenarios, which adds another complicating factor to an already complicated project. For example, you might have some Windows Vista workstations that you can upgrade, as well as Windows XP workstations that you must refresh or replace.

To streamline the deployment process somewhat, you might find it preferable to select one scenario for all your existing workstations. If, for example, you are going to refresh your Windows XP computers, you might find it easier to refresh the Windows Vista workstations as well, rather than implement a separate upgrade scenario.

## Evaluating the Infrastructure

As noted earlier in this chapter, the Microsoft deployment tools are not mutually exclusive. You can combine them in a variety of ways, depending on the nature of your deployment project. In many cases, the infrastructure in which you are working can dictate how you use MDT 2010 and the other tools.

You have already seen how the MDT deployment scenarios you use depend on whether you are deploying to new or existing workstations. Other elements of your existing infrastructure can affect how you deploy workstations in other ways.

## Using Windows Deployment Services

Windows Deployment Services provides the most convenient means of deploying MDT 2010 boot images to reference computers and target computers over the network. Without WDS, you must create boot media to start your workstations, in the form of CD-ROMs or DVD-ROMs or USB flash drives. In a large deployment project, this can be extremely inconvenient. However, to use WDS, there are several infrastructure requirements, as follows:

- **Windows Server** WDS is a role included in Windows Server 2008 R2 and Windows Server 2008. You must therefore have a server on your network running one of these operating systems, on which you have installed the Windows Deployment Services role.

- **PXE compliance** The workstations to which you will deploy boot images using WDS must have network interface adapters that are compliant with the PXE standard. There is no need for WDS discover images in an MDT 2010 deployment because if you are going to create boot disks, you can just use the boot images that MDT creates.
- **Network connectivity** To deploy large image files over the network, workstations must have a persistent, high-speed connection to the server running WDS. Wireless connections are not sufficient for this purpose, nor are connections that span relatively slow wide area network (WAN) links.

#### **BEST PRACTICES DEPLOYMENTS AND NETWORK SPEED**

For a large-scale Windows 7 deployment, the workstations and the computers hosting the deployment shares, including the build computer and the server running WDS, should all be connected to a wired network running at a minimum speed of 100 megabits per second (Mb/sec). The computers can be on different subnets, as long as the subnets are not connected by a slow link. If you have wireless computers to deploy, such as laptops assigned to traveling users, your choices are either to use a removable boot device or to connect the computer to the wired network for the duration of the deployment process. For computers at remote locations, you can temporarily move the workstations to the location of the server, or move the server to the workstations.

## Using Lite-Touch vs. Zero-Touch Deployments

As noted earlier in this chapter, MDT 2010 supports two different types of deployments: Lite-Touch Installation (LTI) and the Zero-Touch Installation (ZTI), and most of the product documentation is based on the administrator having chosen one of these two options.

Selecting the LTI or ZTI deployment type is usually not a difficult decision. From an infrastructure perspective, the primary difference between the two is that a ZTI deployment requires Microsoft System Center Configuration Manager (SCCM) 2007 and an LTI deployment does not. In most cases, if you already have SCCM 2007 installed on your network, a ZTI deployment is preferable; if you do not have SCCM, you are better off using an LTI deployment.



#### **EXAM TIP**

Although the 70-686 exam can include coverage of any of the deployment methods discussed in this chapter, the primary emphasis is likely to be on Microsoft Deployment Toolkit 2010 and its two primary deployment types: LTI and ZTI. You should be familiar with the differences between the two and the infrastructure requirements for each.

Other differences between the two deployment types are as follows:

- **User interaction** The primary advantage of a ZTI deployment is that it requires no interaction at the workstation while the operating system installation is occurring. This streamlines the deployment process and reduces the incidence of configuration errors. LTI deployments, at the very least, require someone to initiate the installation at the workstation site and can require additional interaction as the installation proceeds. This means that the on-site technicians require more training and administrative credentials, and human interaction introduces a potential source of configuration errors.
- **Flexibility** Most of the alternative deployment strategies discussed throughout this chapter are limited to LTI deployments. ZTI is a more structured deployment method, with fewer options.
- **Complexity** ZTI deployments typically require more time and effort to configure than LTI deployments, mainly because a ZTI performs more tasks on the workstations being deployed.
- **Connectivity** ZTI supports only network-based deployments; you cannot use removable media. Therefore, all of the workstations you deploy using ZTI must have a persistent, high-speed connection to the MDT build computer and all of the servers involved, including the SCCM, SQL, and WDS servers. In an LTI deployment, the workstations do not even have to be networked, although it is preferable that they are.
- **Security** Because no interaction is required at the workstation during a ZTI deployment, it is not necessary to provide users or site technicians with administrative credentials, as it is with LTI. However, to use ZTI, you must configure the network security and firewall policies to allow automatic software installation and permit Remote Procedure Call (RPC) traffic between the workstations and the deployment servers. By contrast, you can perform an LTI deployment to workstations that prohibit automatic software installation and are secured behind a firewall.
- **Upgrades** Unlike LTI, ZTI does not support the upgrade computer deployment scenario.

## BEST PRACTICES IMPLEMENTING SYSTEM CENTER CONFIGURATION MANAGER 2007

SCCM 2007 is a comprehensive network management application that can provide a wide array of administrative services, including software distribution. As a general rule, however, it is not worthwhile to implement SCCM on a network solely to perform workstation deployments. There are several reasons why this is so, including the following:

- **Prerequisites** SCCM 2007 requires a Microsoft SQL Server database to function, and you cannot use the free SQL Server Express Edition for this purpose. This adds considerably to the complexity of the installation and the cost of implementing the product.
- **Installation** Installing SCCM is not simply a matter of inserting a DVD into a drive and running a setup program. There are many optional components and a significant amount of prior planning is required.
- **Client agents** SCCM requires an agent program on each computer that it manages, which adds to the complexity of the installation as well as the cost.
- **Price** Unlike MDT 2010 and the other deployment products, SCCM 2007 is not free. You must purchase the product itself and the SQL Server product it requires to function. In addition, you must purchase a license for each client computer you intend to manage. As a result, the cost of implementing SCCM on a large enterprise network can be considerable.

If you are considering an SCCM implementation on your network, it should be for reasons in addition to performing ZTI workstation deployments.

## Scaling the Client Deployment Process

One of the most critical factors in selecting a Windows 7 deployment method is how many workstations you have to deploy and the conditions under which you will be deploying them.

In an ideal situation, you are deploying new computers on a new network with an unlimited amount of time to complete the project. In the real world, however, administrators rarely have all of these advantages. In fact, they often have none of them. Therefore, you must consider the questions in the following sections and how they affect the selection of a deployment method.

### How Many Workstations?

Obviously, the number of workstations you have to deploy is one of the basic issues in the selection of a deployment method. As discussed earlier in this lesson, small-scale deployments can sometimes proceed without any special methodology at all, but after you get to the point at which you decide that some automation is required, the size of the deployment process can still make a difference.

The number of workstations you have to deploy can affect the overall project in two fundamental ways. If you have several different workstation configurations to deploy, you must consider modifications to your image creation process, as discussed in Chapter 3. However, if the issue is how many workstations of each configuration you have to deploy, the issues are different.

When you have 500 workstations of a specific configuration to deploy, as opposed to 50, the process of installing the reference computer and capturing an image need not change, but the process of deploying the image to the target computers might. Depending on the deployment method you choose, this part of the process can require more network bandwidth, to transfer the image files to the workstations; more personnel, to set up the workstations and possibly initiate the installation on each one; and time, to complete the entire deployment process.

The more workstations you have to install, the more compelling the argument for additional automation becomes. For example, at some point in an enterprise environment, the manpower required to perform an LTI deployment on a large number of workstations offsets the cost of implementing SCCM 2007 and performing a ZTI deployment instead. It might not be worth the effort and the expense to install SCCM for 50 workstations, but for 500, it might be a viable option, particularly when you consider the ongoing benefits of a network management system. However, if you will be shipping those 500 workstations to branch offices at remote locations, where centralized network management is not practical or desirable, then LTI might still be the better choice.

## How Much Bandwidth?

If you are deploying your Windows 7 workstations over the network, you must consider the amount of bandwidth it will take to transmit image files to each computer. Image files can be several gigabytes in size, and deploying dozens or hundreds of computers at once can easily flood a network, slowing the entire process down to a crawl. This can be particularly problematic if you are deploying workstations on a network that other people are using for their everyday work at the same time. When performing a deployment on a working network, you must consider not only the amount of bandwidth the infrastructure is capable of delivering, but also the amount of bandwidth available above the requirements of the working users.

There are several ways you can address competing claims on bandwidth during a workstation deployment, including the following:

- **Stagger deployments** If you must deploy your target computers while other users are working, you can consider installing a few at a time, to avoid flooding the network with deployment traffic. This increases the amount of time needed to complete the project, but in an LTI deployment, it has the added benefit of reducing the manpower needed to perform the installations.
- **Schedule deployments for off hours** For a network that is not in production around the clock, performing deployments at night or at other times when the network is not in use minimizes their effect on bandwidth utilization. However, this can increase manpower costs significantly because of overtime rates.

- **Use a dedicated deployment network** Temporarily connecting the target computers to a separate network used only for deployment eliminates the impact on the production network. This solution is particularly viable if you are using the new computer or replace computer scenario because you can set up, deploy, and test the workstations on an IT network prior to delivering them to the end users. For the upgrade computer and refresh computer scenarios, however, this can be impractical if it requires large numbers of computers to be moved long distances.
- **Use multicasting** Deploying image files by using WDS multicasts can minimize the amount of bandwidth consumed, as long as the entire infrastructure supports multi-cast transmissions, including any routers located between the target computers and the deployment servers.

## PRACTICE Creating Task Sequences

---

In this practice, you create the two task sequences needed to deploy a workstation by using the replace computer scenario. This practice assumes that you have installed MDT 2010 and Windows 7 AIK and created a deployment share, as described in Chapter 3.

### EXERCISE 1 Creating a Task Sequence to Save User State Data

When you create a task sequence using the Standard Client Replace Task Sequence template, the New Task Sequence Wizard configures the sequence to run a script called ZTILUserState.wcf with the /capture parameter, which saves the user state data.

1. Click Start, then click All Programs | Microsoft Deployment Toolkit | Deployment Workbench. The Deployment Workbench console appears.
2. Browse to the deployment share you created in the Chapter 3 practice and select the Task Sequences container.
3. Right-click the Task Sequences container, and from the context menu, select New Task Sequence. The New Task Sequence Wizard appears, displaying the General Settings page.
4. Type **101** in the Task Sequence ID text box and **Replace-Save** in the Task Sequence Name text box. Then click Next. The Select Template page appears.
5. In the drop-down list, select the Standard Client Replace Task Sequence template and click Next. The Summary page appears.
6. Click Next. The wizard creates and imports the task sequence and the Confirmation page appears.
7. Click Finish. The new task sequence appears in the Task Sequences container.
8. Leave the Deployment Workbench console open for the next exercise.

## **EXERCISE 2 Creating a Task Sequence to Install Windows 7 and Restore User State Data**

When you create a task sequence by using the Standard Client Task Sequence template, the task sequence again includes a command to run the ZTIUserState.wcf script, but this time with the */restore* parameter, which applies the saved user state data to the new workstation.

1. If Deployment Workbench is not already open, click Start, then click All Programs | Microsoft Deployment Toolkit | Deployment Workbench. The Deployment Workbench console appears.
2. Browse to the deployment share you created in the Chapter 3 practice, and select the Task Sequences container.
3. Right-click the Task Sequences container again, and from the context menu, select New Task Sequence. The New Task Sequence Wizard appears, displaying the General Settings page.
4. Type **102** in the Task Sequence ID text box and **Replace-Deploy** in the Task Sequence Name text box. Then click Next. The Select Template page appears.
5. In the drop-down list, select the Standard Client Task Sequence template and click Next. The Select OS page appears.
6. Select the operating system you want to install and click Next. The Specify Product Key page appears.
7. Click Next to accept the default option. The OS Settings page appears.
8. Change the default value in the Full Name text box, if desired, and type an appropriate value in the Organization text box. Then click Next. The Admin Password page appears.
9. Select the Do Not Specify An Administrator Password At This Time option and click Next. The Summary page appears.
10. Click Next. The wizard creates and imports the task sequence, and the Confirmation page appears.
11. Click Finish. The new task sequence appears in the Task Sequences container.

## **Lesson Summary**

- The simplest and most basic deployment option is to have no mass deployment plan at all and simply deploy each workstation manually by inserting a Windows 7 disk into the drive and letting the Setup.exe perform the installation.
- There is a middle ground between a manual installation and a mass deployment using reference computers. You can perform customized target computer installations by modifying the default Install.wim image file by using DISM.exe or by customizing the Install.wim installation process using an answer file or a task sequence.
- In most cases, there are no compelling reasons not to use Microsoft Deployment Toolkit 2010 as the basis of a large-scale enterprise workstation deployment. MDT 2010 is a free product, as is Windows 7 AIK, its prerequisite, so you have no cost issues to consider.

- MDT 2010 defines four deployment scenarios: new computer, upgrade computer, replace computer, and refresh computer.
- Windows Deployment Services provides the most convenient means of deploying MDT 2010 boot images to reference computers and target computers over the network.
- The primary difference between an LTI deployment and a ZTI deployment is that a ZTI deployment requires Microsoft System Center Configuration Manager (SCCM) 2007 and an LTI deployment does not. In most cases, if you already have SCCM 2007 installed on your network, a ZTI deployment is preferable; if you do not have SCCM, you are better off using an LTI deployment.

## Lesson Review

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

### **NOTE** ANSWERS

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

1. Which of the following deployment scenarios is not supported in a ZTI deployment?
  - A. New computer
  - B. Upgrade computer
  - C. Refresh computer
  - D. Replace computer
2. Which of the following statements about ZTI deployments is not true?
  - A. ZTI deployments can be network-based or media-based.
  - B. ZTI deployments never require interaction at the workstation site.
  - C. ZTI deployments use RPC communications between the servers and the workstations.
  - D. ZTI deployments are more difficult to configure than LTI deployments.
3. Which of the following deployment scenarios both captures and restores the user state data in the same task sequence?
  - A. New computer
  - B. Upgrade computer
  - C. Refresh computer
  - D. Replace computer

4. Which of the following elements are required to deploy MDT 2010 boot images over a network by using Windows Deployment Services? (Choose all that apply.)
- A. A computer running Windows Server
  - B. PXE-compliant workstation network adapters
  - C. Persistent, high-speed network connection
  - D. Routers that support multicast traffic

## Chapter Review

---

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

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

## Chapter Summary

- The main object of an enterprise deployment is to install Windows 7 in a standardized configuration on multiple computers with little or no interaction at the workstation site. At its most basic level, an enterprise workstation deployment requires that you follow these steps: build a deployment share, perform a reference computer installation, capture an image of the reference computer, boot the target computer by using Windows PE, and apply the image containing Windows 7.
- Although the method for deploying Windows 7 to a large number of workstations is relatively simple, there are many tools you can use to implement that method, and many ways to use those tools. During the early planning stage of your deployment project, you must decide on a method for deploying your workstations, based on your needs and your temperament, and build your project around that method.

## 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.

- build-to-order (BTO)
- build-to-plan (BTP)
- capture image
- discover image
- Lite-Touch Installation (LTI)
- multicast
- Pre-Boot Execution Environment (PXE)
- Windows Deployment Services
- Zero-Touch Installation (ZTI)

## Case Scenarios

In the following case scenarios, you will apply what you have learned about subjects of this chapter. You can find answers to these questions in the “Answers” section at the end of this book.

### Case Scenario 1: Capturing an Image by Using WDS

Ralph is an IT administrator who has been assigned the task of deploying Windows 7 on 20 new computers just received by his company. He has just completed a manual installation of one of the computers, including all of the required applications, updates, and configuration settings. Now he wants to copy that installation to the remaining computers. Ralph is unaware of the Windows 7 AIK tools, but he does have a server running Windows Server 2008 R2 on the network, and the new workstations have PXE-compliant network adapters. List the steps Ralph has to perform to capture an image of the newly installed workstation by using Windows Deployment Services.

### Case Scenario 2: Refreshing Workstations

Alice is responsible for upgrading 250 workstations in the Order Entry department from Windows XP to Windows 7. Because she cannot perform an actual upgrade, she has decided to use the MDT 2010 refresh computer deployment scenario to save the user state data on the computers, install Windows 7, and then restore the user state data. She has already created an image of a reference computer and added it to her MDT deployment share by using Deployment Workbench. She has also created the necessary task sequence for the target computer deployment in Deployment Workbench and updated the deployment share, to create the necessary boot image. Because the workstations are PXE-compliant, her plan is to deploy the MDT boot image to the workstations over the network by using Windows Deployment Services. She has already added the boot image to the Windows Deployment Services console.

Alice's main problem at this point is that the Order Entry department at her company works three shifts, around the clock, and she is concerned about overloading the network during the workstation deployment process. A network outage would prevent the department workers from taking orders, which would mean reduced revenue for the company and big trouble for Alice. To minimize the bandwidth utilized by the deployment process, Alice has decided to use the multicasting capability in WDS. She adds the workstation install image she captured to the Windows Deployment Services console and uses the Create Multicast Transmission Wizard to configure multicasting for it.

Before installing all of the computers, Alice decides to perform a test deployment on five workstations simultaneously. She gives instructions to the five users to restart their computers at the same time, boot from the network, and select the MDT boot image from the boot menu. All seems to go well. The workstations start and the Windows Deployment Wizard runs, enabling the users to install the captured image.

However, while monitoring the network during the test deployment, Alice notices an alarming rise in traffic as each of the five workstations downloads the install image individually. Why isn't the multicasting that Alice configured working as expected, and how will she be able to deploy the rest of the computers without compromising network performance?

## Suggested Practices

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

### Choosing an Appropriate Deployment Method 1

In this practice, you install and configure Windows Deployment Services on a computer running Windows Server 2008 R2.

- **Practice 1** On a computer running Windows Server 2008 R2, launch Server Manager and install the Windows Deployment Services role.
- **Practice 2** Open the Windows Deployment Services console, right-click the server, and from the context menu, select Configure Server. Complete the Windows Deployment Services Configuration Wizard.

### Choosing an Appropriate Deployment Method 2

In this practice, you add image files to your Windows Deployment Services installation.

- **Practice 1** Insert your Windows 7 installation disk into the DVD drive. Then, in the Windows Deployment Services console, browse to the Boot Images container. Right-click Boot Images, and from the context menu, select Add Boot Image. In the Add Image Wizard, browse to the Sources folder on the Windows 7 disk and add the Boot.wim file.
- **Practice 2** Browse to the Install Images container. Right-click Install Images, and from the context menu, select Add Install Image. In the Add Image Wizard, browse to the Sources folder on the Windows 7 disk and add the Install.wim file.

## 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 70-686 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.

# Designing Lite-Touch and Zero-Touch Deployments

Chapter 6, “Designing a Windows 7 Client Deployment Strategy,” describes the basic steps involved in a mass client deployment and examines the tools that Microsoft provides to help automate the process. This chapter assumes that you have decided to use one of the deployment strategies provided in Microsoft Deployment Toolkit (MDT) 2010: Lite-Touch Installation (LTI) or Zero-Touch Installation (ZTI), and it examines the actual process of implementing the deployment and customizing it to your needs.

## Exam objectives in this chapter:

- Design a lite-touch deployment strategy.
- Design a zero-touch deployment strategy.

## Lessons in this chapter:

- Lesson 1: Designing a Lite-Touch Deployment **266**
- Lesson 2: Designing a Zero-Touch Deployment **298**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- A computer running Windows 7 or Windows Server 2008 R2 on which you have installed Windows 7 Automated Installation Kit (Windows AIK) and MDT 2010 and created a deployment share, as described in the Chapter 3, Lesson 1 practice: “Creating a Deployment Share.”



## REAL WORLD

Craig Zacker

When you decide to perform a Zero-Touch Installation (ZTI) deployment of Windows 7 workstations, you are committing yourself to the tasks involved in creating an entirely automated process, and these tasks can be extensive. A Lite-Touch Installation (LTI) deployment provides a good deal more flexibility, and it is up to you to decide how much time you should spend developing the deployment process and how much you should spend performing the deployment itself. This decision is typically based on factors such as the number of workstations to be deployed, the number and complexity of the workstation configurations, and the time and expertise of the staff available to perform the deployment.

By customizing the `CustomSettings.ini` files for your deployment shares, you can reduce the amount of interaction required at each target workstation, effectively making a light touch an even lighter touch. For a large LTI deployment, the time spent learning about the `CustomSettings.ini` syntax and modifying the file might be well worth it, if it saves you substantial time and keystrokes on each of 500 workstations. For a more modest deployment, however, you can easily spend more time working on the `CustomSettings.ini` file than you would save by automating the deployments.

## Lesson 1: Designing a Lite-Touch Deployment

As noted in Chapter 6, “Designing a Windows 7 Client Deployment Strategy,” by selecting the LTI deployment option, you are committing to having someone at each target workstation to initiate the Windows 7 installation process. Beyond that requirement, the LTI deployment process is quite flexible. This lesson examines the LTI deployment process in detail and explains how you can customize the process to your organization’s needs.

### After this lesson, you will be able to:

- Understand the steps of an LTI deployment.
- Customize an LTI deployment to suit your development and installation requirements.
- Create task sequences for target computer deployments.
- Modify the `CustomSettings.ini` file to automate deployment tasks.

**Estimated lesson time: 60 minutes**

# **Understanding Lite-Touch Deployment Requirements**

The majority of the LTI deployment process occurs in a lab environment. It is not until you are ready to actually deploy Windows 7 onto your target workstations that the production network is involved. The first step in the LTI deployment process is to assemble the components you need to create your lab environment.

## **Having a Plan**

As you learned in Chapter 1, “Preparing to Deploy Windows 7,” careful planning is an essential part of any deployment project, and you should have a complete plan in hand before you begin any of the LTI implementation steps discussed in this lesson.

For example, you should at this point have already decided how many workstation configurations you intend to deploy and how many target computers are to receive each one. You should have a timetable prepared that specifies how long you have to create and test your image files before you must deploy them to the target workstations. You should be conscious of where the target computers will be during the deployment and how the deployment process might affect the production network. These and dozens of other issues must be considered, discussed, and documented before the actual deployment process even begins.

## **Gathering Your Hardware**

The central hardware component of an LTI deployment project is the build computer, which is where you install Microsoft Deployment Toolkit (MDT) 2010 and Windows 7 Automated Installation Kit (Windows AIK). The build computer can be a Windows server or workstation; its requirements depend on how you have designed your deployment lab.

### **LOCATING THE DEPLOYMENT SHARE**

As part of the LTI deployment process, you must create a deployment share, which is where you will store the installation and image files your other computers will need during the deployment process. If you use the build computer to host the deployment share, you must equip it with an appropriate amount of storage and be conscious of the fact that your target computers will eventually be downloading image files that are several gigabytes in size from this computer. You should also consider whether you will be using Windows Deployment Services (WDS) as part of your deployment strategy because WDS is supplied as a role in the Windows Server 2008 and Windows Server 2008 R2 operating systems.

At minimum, the build computer can be a basic workstation running Windows 7 (or Windows Vista), which uses an existing server to host the deployment share and WDS. The workstation therefore would need only the resources required to run the MDT 2010 and Windows 7 AIK tools. If you want to create a build computer that handles all aspects of the deployment, a server would be preferable and might in fact be essential if you plan to deploy many target computers simultaneously or use WDS.

## ALLOCATING STORAGE SPACE

Wherever you choose to host the deployment share, you must be conscious of the amount of storage space the deployment process requires. The deployment share first must have sufficient space to hold all of the components needed to install the reference computers. This includes the operating system distribution files, as well as operating system language packs, device drivers, and applications. In addition, the share needs sufficient space to hold the images you capture of the reference computers. Keep in mind that every operating system version, edition, and processor type requires a separate set of distribution files and a separate image.

### **NOTE** STORING USER STATE DATA

Another storage factor to consider is whether you want to perform deployments using the Replace Computer or Refresh Computer scenario, both of which include task sequence commands that save the user state data from the existing Windows workstations to an alternative location. If you use the computer hosting the deployment share for this purpose, you must plan for that additional storage space as well.

## SELECTING REFERENCE COMPUTERS

The other hardware component of your LTI deployment lab is one or more reference computers, which you will use to capture images of your workstation configurations. This component is flexible also. If you are planning to deploy target computers with different hardware configurations, and particularly computers with devices requiring different drivers, your lab should have at least one reference computer for each configuration.

If your workstation configurations differ only in their software, such as different combinations of applications, the number of reference computers you need is based more on the time and personnel available for the deployment project. You could have just one reference computer in the lab and use it to install and capture each workstation configuration sequentially. Alternatively, you could equip the lab with a separate reference computer for each workstation configuration and have technicians install and capture them all simultaneously.

For deployment projects with a definitive endpoint, the reference computers can be workstations that you eventually deploy on the production network as target computers. Some projects are ongoing, however, in which case it might be preferable to have lab systems permanently allocated as reference computers.

## Gathering Your Software

For the build computer itself, you must download MDT 2010 from the Microsoft Web site, along with Windows 7 AIK, which MDT requires to function. To populate the deployment share, you need the distribution files for all of the Windows 7 editions and processor platforms you plan to install, as well as the device drivers, language packs, and installation packages you plan to deploy with the operating system.

## **Building the Lab**

All of the phases of the deployment project until the actual target computer deployment can take place in a laboratory environment that is completely separate from the production network. The primary function of the lab is to create the image files that you eventually deploy to your target computers. Although you can use the same build computer to deploy the reference computers and later deploy your captured images to the target computers, this does not have to be so. You can create multiple build computers, with one on the isolated lab network and another on the production network, or you can create multiple deployment shares on a single build computer, with different servers hosting them.

If you decide to create an isolated lab, remember that it must have the same infrastructure services as your production network, including an Active Directory Domain Services (AD DS) domain controller, a Domain Name System (DNS) server, and a Dynamic Host Configuration Protocol (DHCP) server. For more information on constructing an image creation lab, see Chapter 3, "Creating and Managing System Images."

## **Building Reference Computers**

In the LTI deployment documentation, the process of building reference computers and capturing images of them is automated using a task sequence, as described in Chapter 3 in "Creating Images with MDT 2010." However, it is not essential that you proceed in this manner.

The sole reason for building reference computers is to capture the images that you eventually deploy to your target computers. As long as you successfully create baseline installations on the reference computers that are suitable for image capture, how you perform those installations is irrelevant. Therefore, if you prefer to install and configure the reference computers manually, which might be preferable in a deployment project with a relatively small number of workstation configurations, you can do so.

## **Deploying Images to Target Computers**

Whatever method you use to build and capture your reference computers, the result should be the image files that you want to deploy to your target computers. The basic steps of this final deployment process are almost the same as those for building the reference computer, as described in Chapter 3. These steps are as follows:

- Add the captured image to the deployment share.
- Create a task sequence for the target computer installation.
- Start the target computer with an MDT 2010 boot image and initiate the installation.

Although these steps might seem simple, especially when you have just used the same basic procedure to build your reference computers, deploying images to large numbers of target computers can complicate the process enormously. MDT 2010 and the Windows operating systems provide many ways to customize the deployment process to accommodate the specific needs of your network, your IT staff, and your users.

## Adding Captured Images to the Deployment Share

The process of adding an image to an MDT 2010 deployment share is a simple one, but there are other factors to consider when deploying images to target computers. The first consideration is access to the production network itself. If you constructed your image creation lab on an isolated network, you must see to it that your target computers can access the deployment share containing your captured images.

Your two options in this respect are as follows:

- **Connect the build computer to the production network** Move the build computer to the production network or add a connection to the production network, using a second network interface adapter. If you elect to move the build computer and your deployment share is hosted by another system, you must move that computer as well.
- **Create a new build computer on the production network** Install MDT 2010 on a computer connected to the production network and use that system to host a deployment share containing your images and the task sequences for your target computer deployments.

The need for additional components on the target deployment share depends on the type of images you chose to create. If you created thick images, the deployment share does not need any other software, but if you created thin or hybrid images, you might have to add drivers, language packs, updates, or applications to the share so that you can deploy them to the target computers.

### REPLICATING DEPLOYMENT SHARES

If you elect to create multiple build computers or multiple deployment shares on a single build computer, you can configure Deployment Workbench to replicate the contents of one share to another. This way, you can use a deployment share on an isolated lab network to install and capture your reference computers and create your target deployment task sequences, and then replicate the data to another share on your production network for the target computer deployment. To initiate the replication process, you use Deployment Workbench to link the deployment shares and then create selection profiles to specify the files on the share that you want to replicate.

### ENSURING NETWORK BANDWIDTH

The image files you will be deploying to the target computers are typically several gigabytes in size, so the amount of bandwidth available between the build server and the target computers is an important consideration. MDT 2010 is not designed to deploy target computers over wireless networks or relatively slow wide area network (WAN) links. Attempts to perform deployments over slow links would take an inordinately long time and likely flood those links, preventing any other traffic from using them.

For deployments to target computers that have no high-speed link to a build computer, consider the following alternatives:

- Move the build computer to the target computers' network temporarily, perform the deployment, and then move the build computer back. This option might be complicated by the need to provide server resources on the target computer network, including DHCP and WDS.
- Move the target computers to the build computer's network temporarily, perform the deployment, and then move the target computers back.
- Perform the deployment using removable media, such as DVDs or USB flash drives.

Even on high-speed networks, a large-scale deployment can consume enough bandwidth to interfere with regular traffic. Project administrators should be conscious of every network's current traffic situation, and they should use that data to determine how many workstations they can deploy at one time without interfering with other users. This is known as a staggered deployment. Other strategies are to deploy workstations only during nonproduction hours or to use multicasting, which reduces the amount of bandwidth consumed by the deployment process.

#### **MORE INFO USING MULTICASTING**

For more information about using multicasting with LTI deployments, see "Multicasting LTI Deployments," later in this chapter.

## **Creating a Task Sequence for Target Deployment**

To deploy Windows 7 to a target computer using MDT 2010, you must create a task sequence using the New Task Sequence Wizard, just as you did for the reference computer installation. However, the target computer deployment is often more complicated than that for the reference computer. Depending on which of the deployment scenarios you are using, you might have to create a task sequence that saves the user state data from the target workstation before installing Windows 7 and restores the user state data to the target workstation afterward. You might even have to create multiple task sequences that save the user state data from existing workstations and then restore the data to new workstations after installing Windows 7.

For a target deployment using the New Computer, Upgrade Computer, or Refresh Computer scenarios, you create a task sequence using the Standard Client Task Sequence template. The wizard then prompts you for the operating system you want to install and some other optional information, such as the product key and Administrator password you want to use on the workstation.

After you have created the task sequence, you can view and modify its various settings by opening its Properties sheet and selecting the Task Sequence tab, as shown in Figure 7-1.

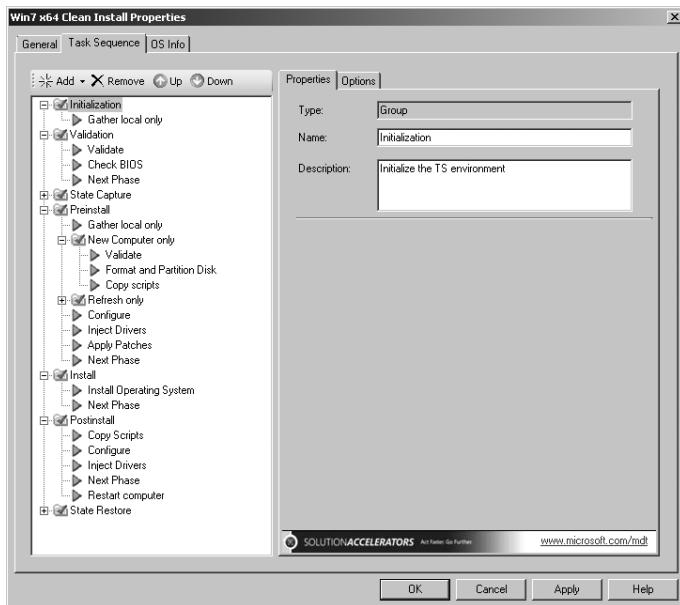


FIGURE 7-1 A task sequence based on the Standard Client Task Sequence template

A task sequence consists of a succession of commands that perform various actions on the target computer, on which it runs. Some of the commands execute scripts, while others interact directly with the target computer. The template you select when you create the task sequence inserts a default group of commands into the task sequence; on the Task Sequence tab, you can modify the defaults and add or remove commands as you need to.

Most of the task sequences for LTI deployments are based on the Standard Client Task Sequence template because this template enables the installer to implement a variety of features on the target computer. Because a Lite-Touch deployment requires some interaction at the client site, as opposed to the Zero-Touch deployment, which requires none, the task sequence can contain actions that the target workstation does not always need.

For example, the Standard Client Task Sequence template includes the Capture User State action, which can save the user state data on a target computer to a remote location for later retrieval. In a deployment using the New Computer or Upgrade Computer scenario, this action is not needed and the installer can disable it at the target computer before the installation begins. When using the Refresh Computer scenario, however, the installer must configure the Windows Deployment Wizard to save the user state data before installing Windows 7. In a ZTI deployment, the task sequence must be precisely configured to perform all of the required actions on the target computer because there is no installer interaction. Task sequences for LTI deployments are therefore easier to create.

The one LTI scenario that requires a different task sequence template is the Replace Computer scenario. In this type of deployment, you are saving the user state data from an existing workstation and then restoring it to a new workstation after installing Windows 7. Because you are working with two computers, you need two separate task sequences. The first one, based on the Standard Client Replace Task Sequence template, contains the Capture User State command and skips the process of installing Windows 7, as shown in Figure 7-2. In the second task sequence, which runs on the new computer, the installer skips the Capture User State command, installs Windows 7, and then performs the Restore User State command to copy the user state data from the existing computer to the new one.

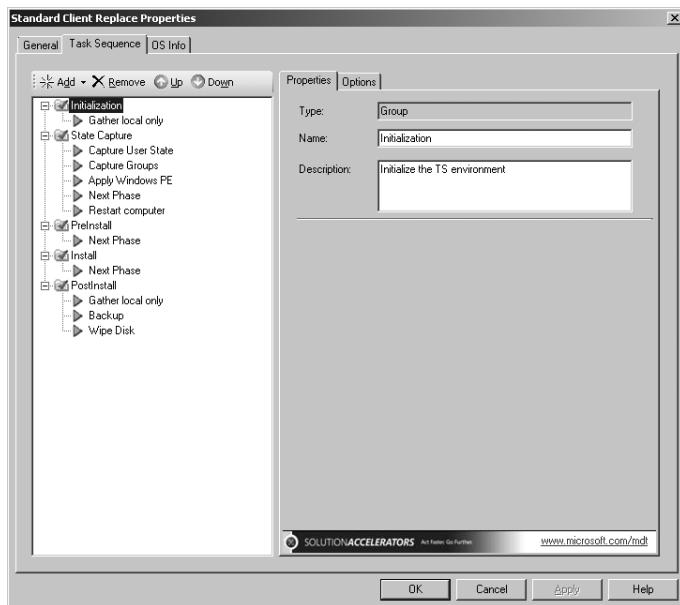


FIGURE 7-2 A task sequence based on the Standard Client Replace Task Sequence template

Technical specialists who have special needs and who are familiar with the task sequence format can also use the Custom Task Sequence template to create a sequence from scratch.

## Updating the Deployment Share

After you have created the task sequences that you need to deploy your captured images to the target computers, you must update your deployment share, if you have not done so already. Updating the deployment share creates the boot images that enable the target workstations to connect to the deployment share on the build computer.

**NOTE UPDATING THE DEPLOYMENT SHARE**

If you updated the deployment share when you deployed your reference computers, you have no reason to do so again unless you modified the boot image settings in Deployment Workbench since then.

Updating the deployment share creates boot images in the Boot folder of the deployment share in both Windows Imaging (wim) and ISO formats, in 32-bit and 64-bit versions, using the following file names:

- LiteTouchPE\_x64.wim
- LiteTouchPE\_x64.iso
- LiteTouchPE\_x86.wim
- LiteTouchPE\_x86.iso



**Quick Check**

- Which of the deployment share images listed can you use to create a bootable DVD or USB flash drive?

**Quick Check Answer**

- LiteTouchPE\_x64.iso or LiteTouchPE\_x86.iso, because ISO is a bit-based image format.

## Choosing a Client Boot Method

The image files that Deployment Workbench creates when you update the deployment share contain the Windows PE boot files and the Windows Deployment Wizard. This wizard runs on the target computer and enables the installer to control the individual deployment process for each workstation. The next decision that the administrators must make is how they intend to boot each of the target computers.

### USING FILE-BASED IMAGES

The LiteTouchPE\_x32.iso and LiteTouchPE\_x64.iso files that Deployment Workbench creates contain all the boot files the target computer requires in a single, file-based image. You can burn these images to CDs, DVDs, or USB flash drive and use them to boot the target workstations. The resulting boot disks include all of the software necessary to start a computer, load the Windows Deployment Wizard, and connect to the deployment share on the build computer.

**NOTE BURNING BOOT DISKS**

The Windows operating systems do not include the software needed to burn an ISO file to a CD, DVD, or flash drive. You must obtain a third-party software product to do this.

The advantage to this boot method is that the target computers require no special hardware other than a disk drive or a USB port from which the system can boot. The disadvantage is that you must have a boot disk for each target computer you want to install. However, you do not necessarily have to create a separate boot disk for each workstation because the disks are not system-specific.

After the Windows Deployment Wizard loads, remove the disk or drive and use it to boot another computer. Because some interaction is required at each target computer anyway in an LTI deployment to initiate the installation process, using boot disks to start each workstation is not a terrible inconvenience.

### USING WINDOWS IMAGING FILES

The other boot method for target workstations is to deploy the LiteTouchPE\_x86.wim and LiteTouchPE\_x64.wim files over the network by using Windows Deployment Services (WDS). This method is much faster and eliminates the need to burn boot disks and carry them to the individual workstations. You can also install large numbers of target computers simultaneously.

The disadvantages are that every target computer must be equipped with a network interface adapter that supports the Preboot Execution Environment (PXE) standard. The network must also have a WDS server and a DHCP server that is configured to support WDS. You can run both of these services on your build computer or on a separate server.

### USING VISUAL BASIC SCRIPTING EDITION

You can also launch the Windows Deployment Wizard from a computer that is already running an operating system by connecting to the deployment share over the network and running the Litetouch.vbs script, located in the Scripts folder. One example of the commands used to do this appears as follows:

```
net use s: \\server\deploymentshare$  
s:  
cd scripts  
cscript litetouch.vbs
```

This method of launching the wizard is required when your task sequence needs access to the currently installed operating system on the target computer. For example, in the Refresh Computer scenario, the wizard must capture the target computer's user state and save it to a remote location before it installs Windows 7. If you use one of the Windows PE boot methods to start the target computer, the wizard skips the Capture User State task because it does not have access to the installed operating system. Starting the wizard with the Litetouch.vbs script while the existing operating system is running enables it to locate the required files and perform the Capture User State task.

## Starting the Target Computer

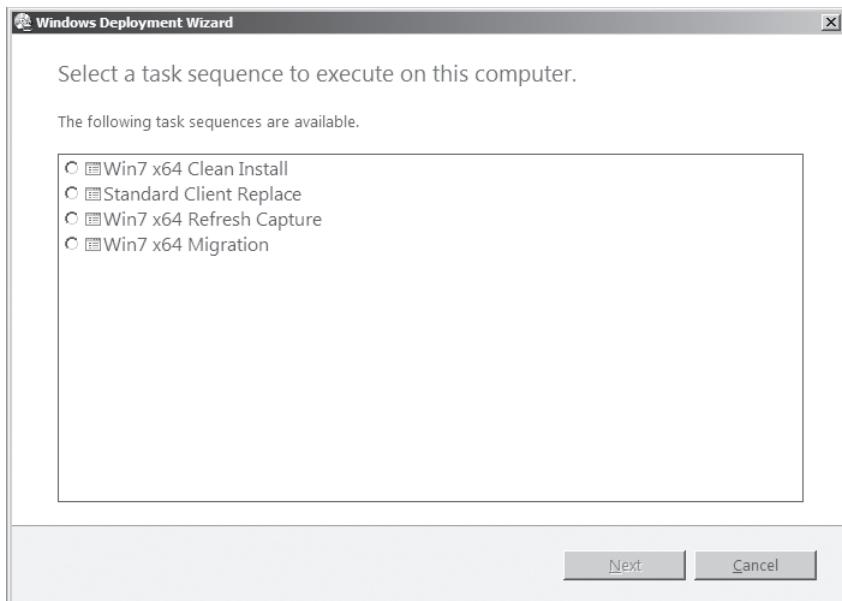
When you boot the target computer using one of the LiteTouchPE image files, the MDT 2010 Solution Accelerators interface appears, as shown in Figure 7-3. When you boot the computer using one of the ISO images, the initial interface is included on the disk. When you deploy the Windows Imaging file using WDS, the target computer obtains the address of the WDS server from the DHCP server on the network and then downloads the boot files and the interface from the WDS server. Whichever method the target computer uses, the interface is the same, as is the process of deploying Windows 7.



**FIGURE 7-3** The MDT 2010 Solution Accelerators interface

After the interface appears, you can click Run The Deployment Wizard To Install A New Operating System. The User Credentials window appears, in which you must type domain or local credentials in the User Name, Password, and Domain text boxes that provide access to the deployment share.

At this point, the Windows Deployment Wizard appears displaying the Select A Task Sequence To Execute On This Computer page, as shown in Figure 7-4. If you run the Litetouch.vbs script from within a running operating system, the wizard loads using the credentials with which you logged on to the target computer.



**FIGURE 7-4** The Select A Task Sequence To Execute On This Computer page in the Windows Deployment Wizard

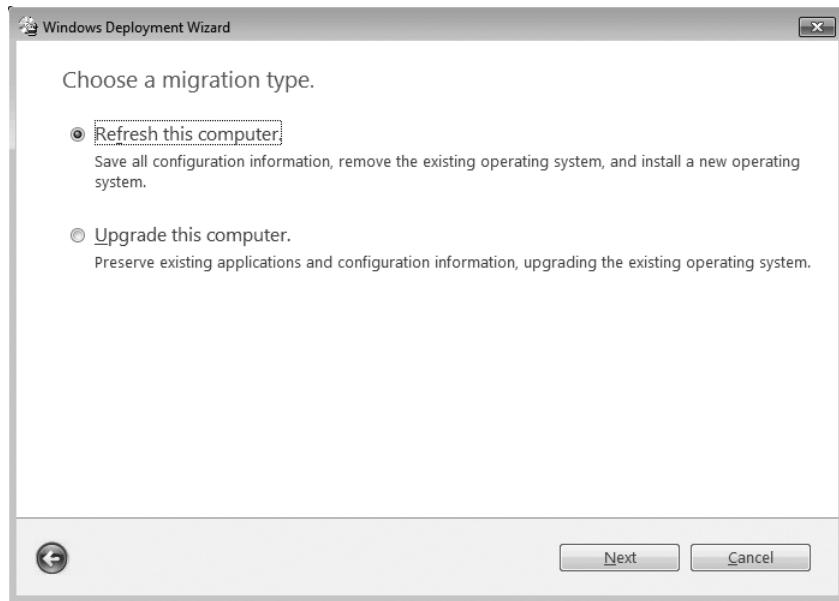
The installer can now proceed with the LTI deployment process as follows:

1. In the Select A Task Sequence To Execute On This Computer page, select the task sequence to run on the target computer and click Next.

#### **NOTE SELECTING A TASK SEQUENCE**

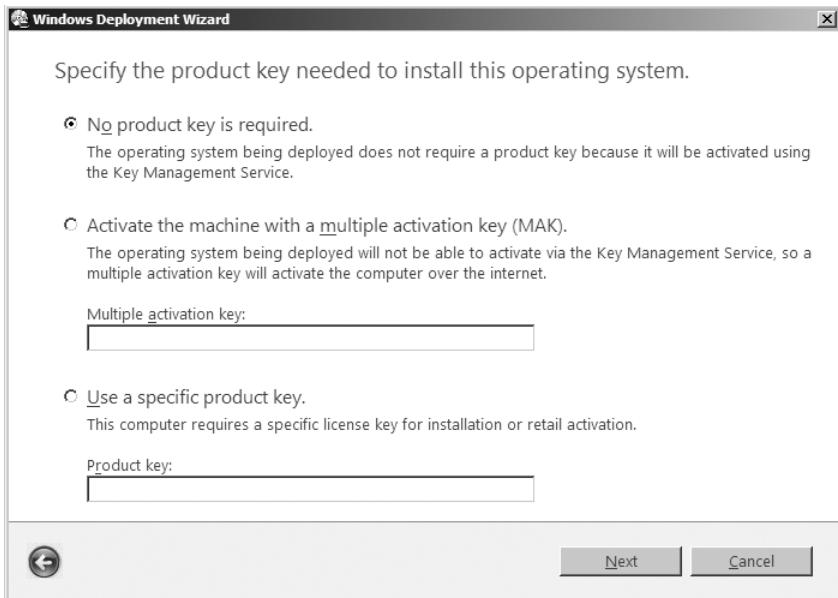
The Select A Task Sequence To Execute On This Computer page contains all of the task sequences created in Deployment Workbench on the build computer that are available to the target computer. If the target computer is running a 64-bit operating system, for example, task sequences configured to install 32-bit operating systems do not appear in the list.

2. If you have launched the wizard from a running operating system, the Choose A Migration Type page appears, as shown in Figure 7-5. Specify what scenario you want to use for the target computer deployment by selecting the appropriate option.



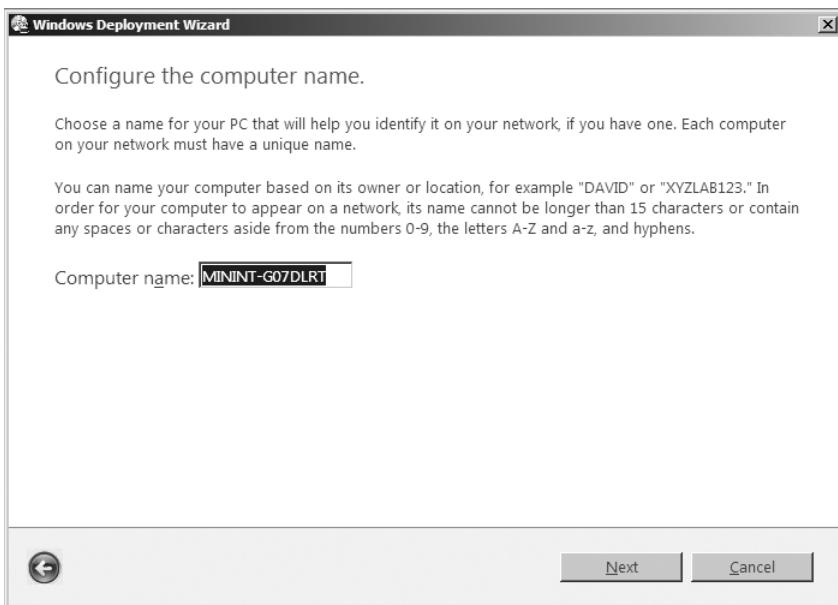
**FIGURE 7-5** The Choose A Migration Type page in the Windows Deployment Wizard

3. Click Next. The Specify The Product Key Needed To Install This Operating System page appears, as shown in Figure 7-6. To specify an individual Windows 7 product key or a Multiple Activation Key (MAK) for the installation, select the appropriate option and type the key in the text box provided.



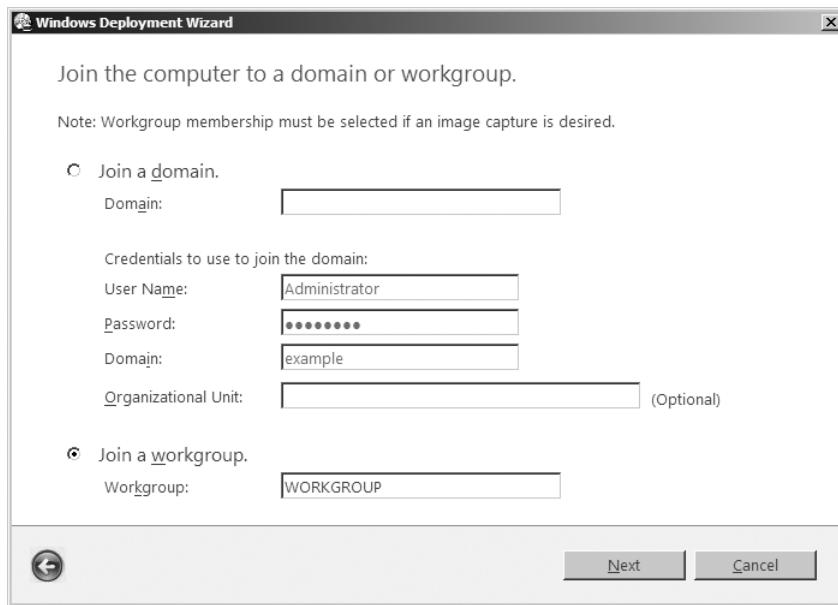
**FIGURE 7-6** The Specify The Product Key Needed To Install This Operating System page in the Windows Deployment Wizard

4. Click Next. The Configure The Computer Name page appears, as shown in Figure 7-7.



**FIGURE 7-7** The Configure The Computer Name page in the Windows Deployment Wizard

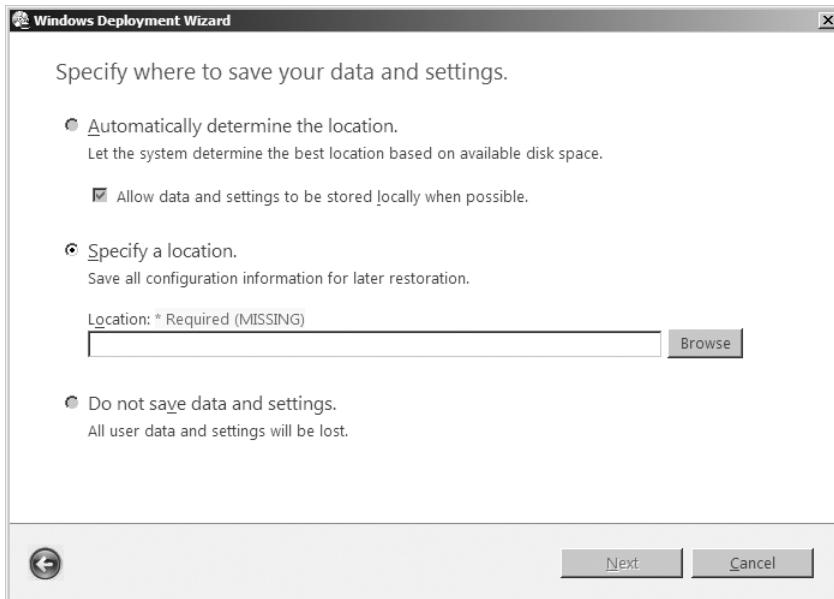
5. In the Computer Name text box, specify the name you want to assign to the new workstation and click Next. The Join The Computer To A Domain Or Workgroup page appears, as shown in Figure 7-8.



**FIGURE 7-8** The Join The Computer To A Domain Or Workgroup page in the Windows Deployment Wizard

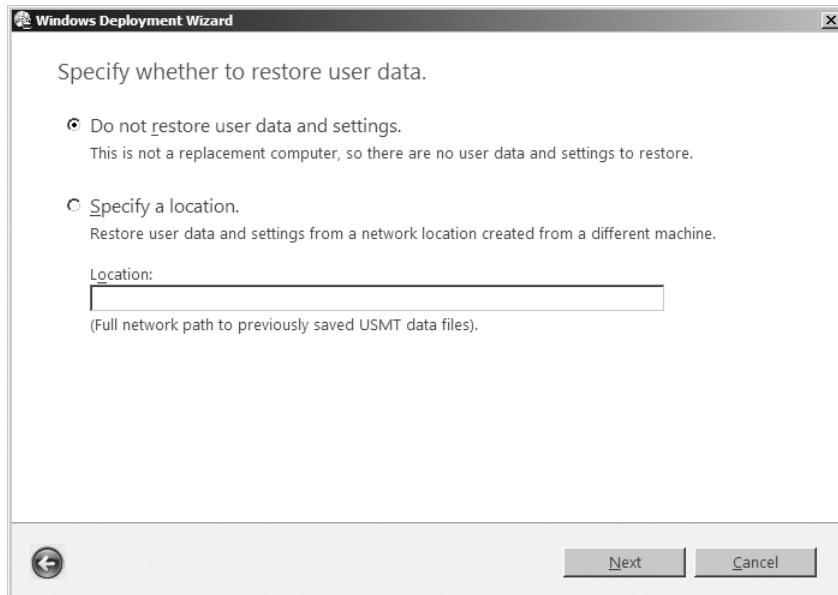
6. To join the target computer to a domain after the Windows 7 installation, select the Join A Domain option and, in the Domain text box, type the name of the domain you want the computer to join and click Next.
- The credentials you supplied earlier appear by default in the User Name, Password, and Domain text boxes. If these credentials do not provide administrative access to the AD DS domain you specified, you must change them.
  - If you want the wizard to create the computer object in a specific organizational unit, rather than the Computers container, type its name in the Organizational Unit text box.
  - To join the target computer to a workgroup, leave the Join A Workgroup option selected and type the name of the workgroup you want the computer to join in the Workgroup text box.

7. If you are using the Refresh Computer scenario, the Specify Where To Save Your Data And Settings page appears, as shown in Figure 7-9. Select the Specify A Location option, and in the Location text box, type a path to the folder to which you want the wizard to copy the user state data from the target computer. Then click Next.



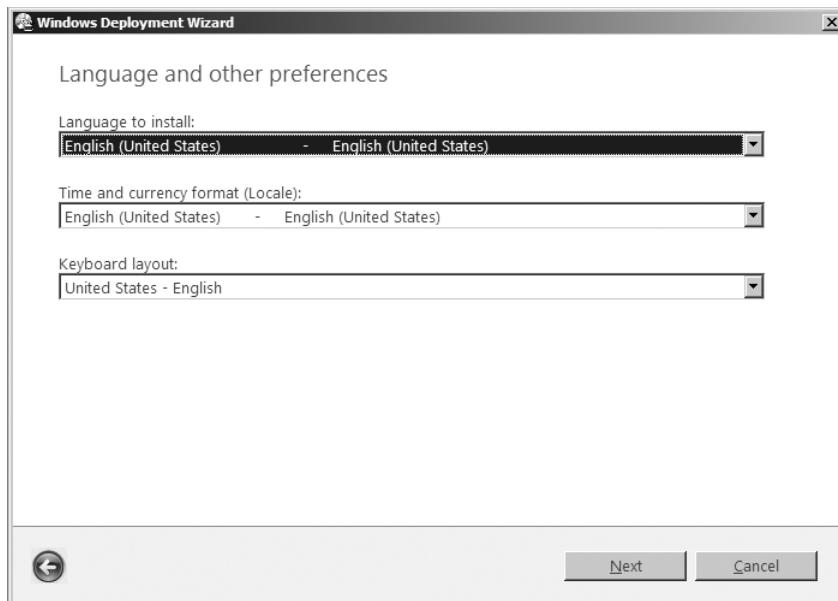
**FIGURE 7-9** The Specify Where To Save Your Data And Settings page in the Windows Deployment Wizard

8. If you are using the Replace Computer or Refresh Computer scenario, the Specify Whether To Restore User Data page appears, as shown in Figure 7-10. Select the Specify A Location option and, in the Location text box, type the path to the location in which you saved the user state data you want to restore.



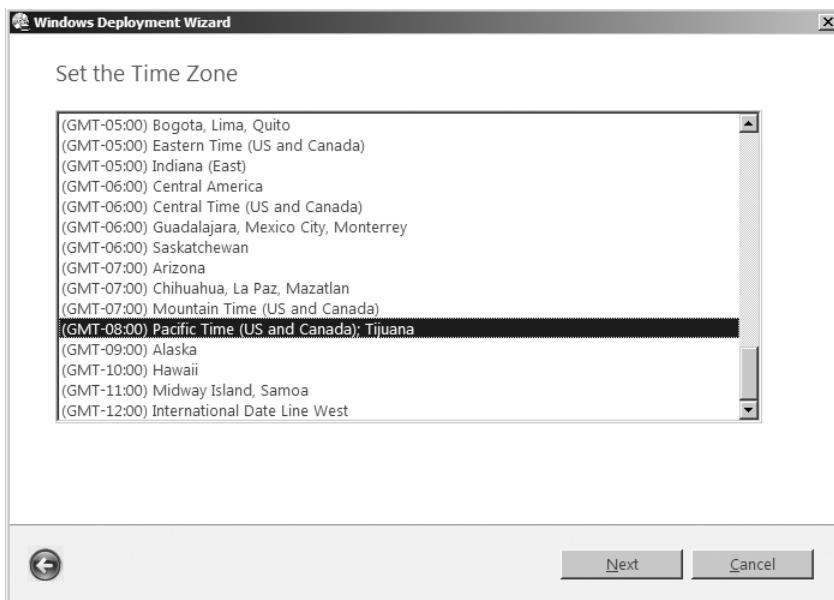
**FIGURE 7-10** The Specify Whether To Restore User Data page in the Windows Deployment Wizard

9. Click Next. The Language And Other Preferences page appears, as shown in Figure 7-11.



**FIGURE 7-11** The Language And Other Preferences page in the Windows Deployment Wizard

- 10.** Click Next to accept the default language, country, and keyboard layout settings, or if you need to make changes, choose the correct values from the three drop-down lists. Then click Next. The Set The Time Zone page appears, as shown in Figure 7-12.



**FIGURE 7-12** The Set The Time Zone page in the Windows Deployment Wizard

- 11.** Select the time zone for the target computer's ultimate location and click Next. The Administrator Password page appears, as shown in Figure 7-13.

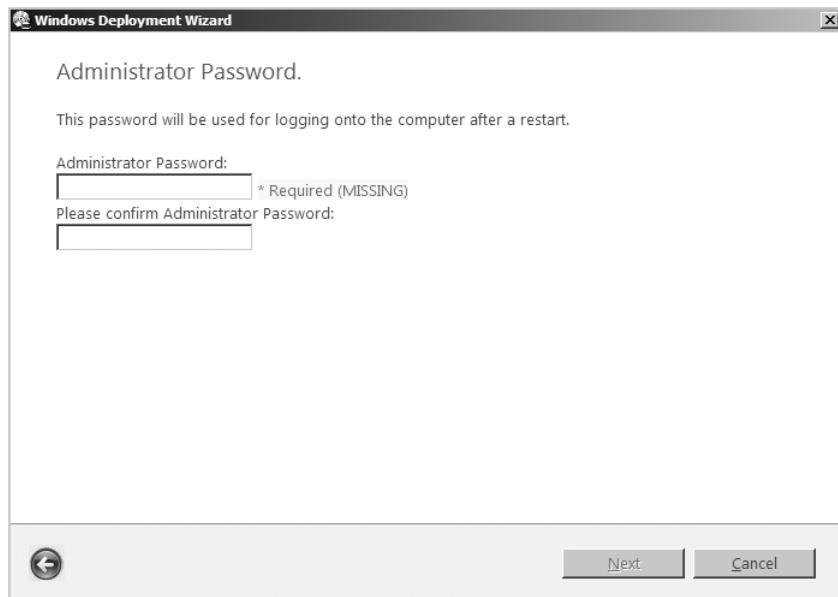


FIGURE 7-13 The Administrator Password page in the Windows Deployment Wizard

12. In the Administrator Password and Please Confirm Administrator Password text boxes, type the password you want the target computer to use and click Next. The Specify The BitLocker Configuration page appears, as shown in Figure 7-14.

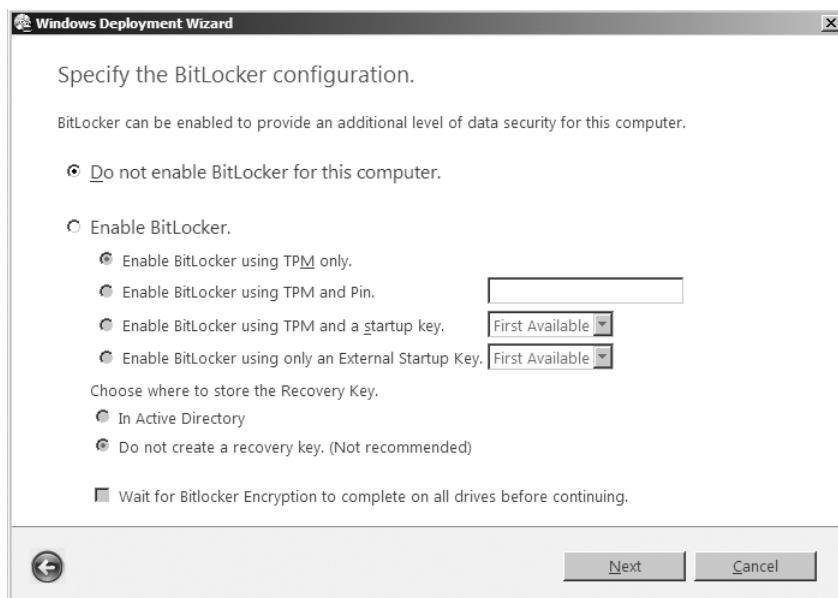


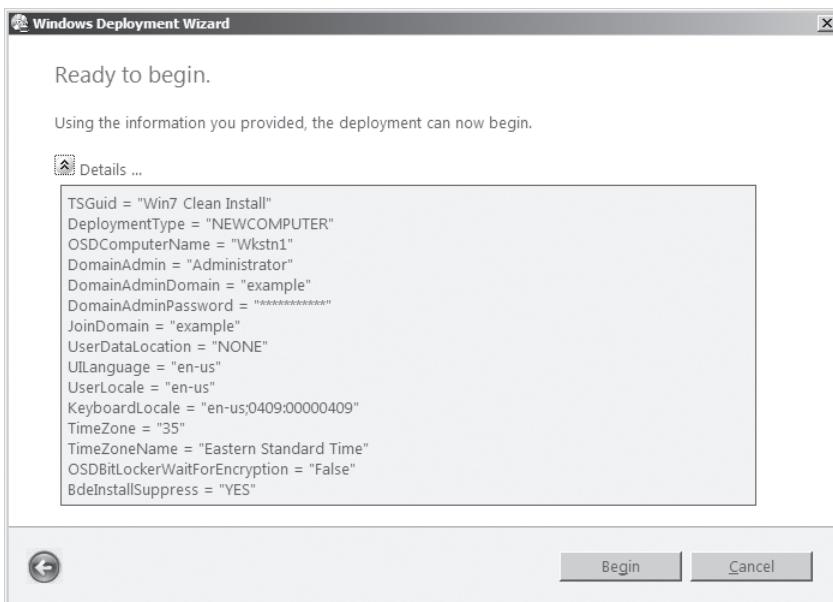
FIGURE 7-14 The Specify The BitLocker Configuration page in the Windows Deployment Wizard

- 13.** To enable BitLocker Drive Encryption on the target computer, select the Enable BitLocker option and choose one of the configuration options. Then click Next. The Ready To Begin page appears.
- If you select the option requiring a PIN, specify a value in the provided text box. If you select an option requiring a startup key, select the drive letter that the USB flash drive will be assigned or, if there will be only one flash drive in the computer, leave the default First Available option selected.
  - If you have configured the target computer to join a domain, you can select the In Active Directory option to store the recovery key in Active Directory.
  - Select the Wait For BitLocker Encryption To Complete On All Drives Before Continuing check box to prevent the deployment process from continuing until BitLocker finishes encrypting the computer's drives.

**NOTE ENABLING BITLOCKER**

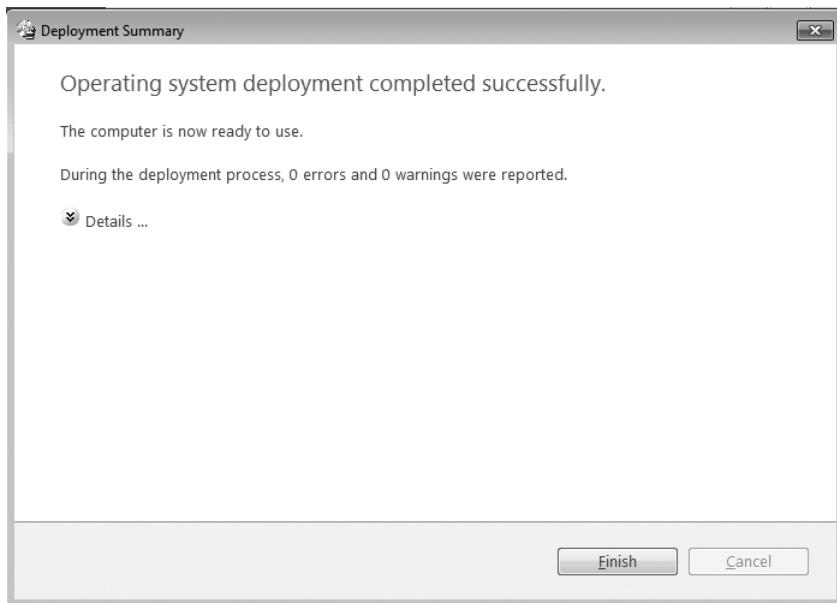
At this time, the Windows Discovery Wizard presents all of the available options for BitLocker configuration and does not perform a hardware check on the target computer. It is up to the installer to know whether the computer is equipped with a Trusted Platform Module (TPM) chip and whether a startup key is present when the installer is selecting options that call for those components.

- 14.** Click the Details arrow to display a summary of the settings you configured, as shown in Figure 7-15.



**FIGURE 7-15** The Ready To Begin page in the Windows Deployment Wizard

- 15.** Click Begin. An Installation Progress window appears, tracking the various procedures of the installation.
- 16.** When the installation is completed, the Operating System Deployment Completed Successfully page appears, as shown in Figure 7-16.



**FIGURE 7-16** The Operating System Deployment Completed Successfully page in the Windows Deployment Wizard

- 17.** Click Finish.

## Customizing Target Deployments

The previous section describes the basic LTI deployment process, but at first glance, many administrators would not consider the interaction required to be especially light. In fact, there is quite a bit of interaction involved, and performing the entire sequence on hundreds of computers can be nearly as tedious and time-consuming as installing Windows 7 manually. Fortunately, MDT 2010 provides a method for automating the deployment process even further.

## Using CustomSettings.ini

CustomSettings.ini is the main configuration file for MDT 2010. Each deployment share has its own CustomSettings.ini file, located in the Control folder. Target computers read the file when they load the Windows Deployment Wizard, and the settings inside control the behavior of the wizard and the deployment process.

The format of CustomSettings.ini is the same as most Windows Configuration files. Section headings are enclosed in square brackets, and properties under each heading are separated from their values by equal signs, as in the following sample:

```
[Heading]  
Property=value
```

Many of the properties that CustomSettings.ini supports take binary values in the form of YES or NO, such as SkipProductKey=YES. Others take alphanumeric values, such as AdminPassword=Pa\$\$w0rd.

### **NOTE EXPRESSING BINARY PROPERTY VALUES**

CustomSettings.ini properties that take the binary values YES and NO must use uppercase text for the values, as in the following example:

```
SkipAdminPassword=YES
```

This is so that the deployment scripts running on the target computers can properly process the values.

When you create a deployment share, the New Deployment Share Wizard creates a CustomSettings.ini file, based on your responses to the wizard's prompts. For example, if you select the Ask User For A Product Key check box, the wizard adds the SkipProductKey=NO command to the CustomSettings.ini file. Later, when the Windows Deployment Wizard running on the target computers reads that command, it causes the wizard to suppress the appearance of the Specify The Product Key Needed To Install This Operating System page.

A typical default CustomSettings.ini file contains the following commands:

```
[Settings]  
Priority=Default  
Properties=MyCustomProperty  
  
[Default]  
OSInstall=Y  
SkipAppsOnUpgrade=YES  
SkipCapture=NO  
SkipAdminPassword=NO  
SkipProductKey=NO
```

The SkipCapture, SkipAdminPassword, and SkipProductKey commands correspond to the Allow Image Capture, Allow Admin Password, and Allow Product Key pages in the New Deployment Share Wizard, reflecting the responses you supplied when creating the share. If you ever want to change these defaults, you can simply modify the commands in CustomSettings.ini by changing the NO values to YES.

You can edit the CustomSettings.ini file manually, using Notepad or any other text editor, but you can also view and edit the file in Deployment Workbench. To access CustomSettings.ini for a particular deployment share, right-click the share in Deployment Workbench and, from the context menu, select Properties. When the Properties sheet for the deployment share appears, select the Rules tab, as shown in Figure 7-17.

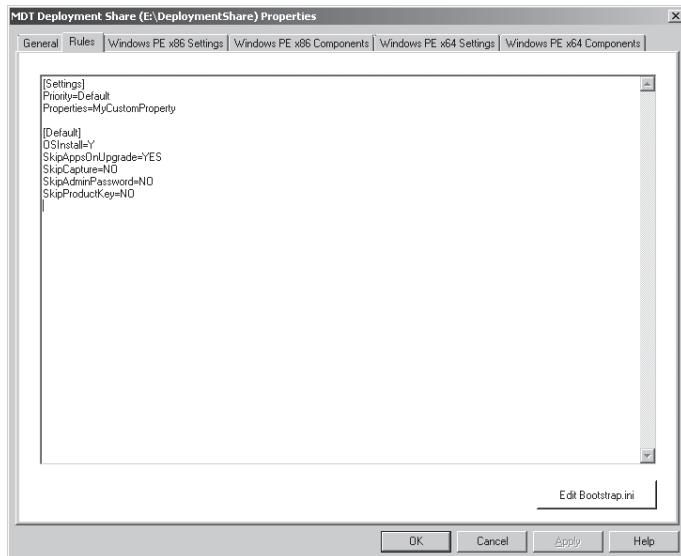


FIGURE 7-17 The Rules tab in a deployment share's Properties sheet

In addition to modifying the existing commands in a CustomSettings.ini file, you can add hundreds of others to customize your deployments. The following sections describe some of the ways in which you can use CustomSettings.ini to reduce the amount of interaction required during a workstation deployment.

#### MORE INFO CUSTOMSETTINGS.INI REFERENCE

For a complete list of the properties you can use in a CustomSettings.ini file, along with explanations and examples of their syntax, open the Microsoft Deployment Toolkit Documentation Library help file included with MDT 2010 and browse to the Properties heading in the Microsoft Deployment Toolkit Reference section.

## SUPPRESSING WINDOWS DEPLOYMENT WIZARD PAGES

In many cases, the interactive pages that appear in the Windows Deployment Wizard are nothing more than chores to the installer sitting at the target computers. For example, if you are deploying 100 computers, all into the same domain, requiring the installer to type the domain name and administrative credentials on every workstation is time-consuming and redundant. Using CustomSettings.ini properties, you can automate the required inputs and suppress the appearance of the Join The Computer To A Domain Or Workgroup page in the Windows Deployment Wizard. The commands you must add to CustomSettings.ini to do this are as follows:

```
JoinDomain=domain_name  
DomainAdmin=domain_administrator_name  
DomainAdminPassword=domain_administrator_password  
DomainAdminDomain=domain_administrator_domain  
SkipDomainMembership=YES
```

The CustomSettings.ini commands that you can use to replace each of the replaceable pages in the deployment procedure are listed in Table 7-1.

TABLE 7-1 CustomSettings.ini Properties for Windows Deployment Wizard

WINDOWS DEPLOYMENT WIZARD PAGE	ADD THIS PROPERTY TO SUPPRESS THE WIZARD PAGE	ADD THESE PROPERTIES TO REPLACE THE CONTROLS ON THE WIZARD PAGE
Specify credentials for connecting to network shares	<i>None</i>	UserID UserDomain UserPassword
Select a task sequence to execute on this computer	SkipTaskSequence	TaskSequenceID
Choose a migration type	SkipDeploymentType	DeploymentType
Specify the product key	SkipProductKey	ProductKey <i>or</i> OverrideProductKey
Configure the computer name	SkipComputerName	OSDComputerName
Join the computer to a domain or workgroup	SkipDomainMembership	JoinDomain DomainAdmin DomainAdminPassword DomainAdminDomain <i>or</i> JoinWorkgroup
Specify where to save your data and settings	SkipUserData	UDDir UDShare UserDataLocation

(continued)

WINDOWS DEPLOYMENT WIZARD PAGE	ADD THIS PROPERTY TO SUPPRESS THE WIZARD PAGE	ADD THESE PROPERTIES TO REPLACE THE CONTROLS ON THE WIZARD PAGE
Specify whether to restore user data	SkipUserData	UDDir UDShare UserDataLocation
Language and other preferences	SkipLocaleSelection	KeyboardLocale UserLocale UILanguage
Set the time zone	SkipTimeZone	TimeZoneName
Administrator Password	SkipAdminPassword	AdminPassword
Specify the BitLocker configuration	SkipBitLocker	BDEDriveLetter BDEDriveSize BDEInstall BDEInstallSuppress BDERecoveryKey TPMOwnerPassword OSDBitLockerStartupKeyDrive OSDBitLockerWaitForEncryption
Ready to begin	SkipSummary	None
Operating system deployment completed successfully	SkipFinalSummary	None

### GROUPING TARGET COMPUTERS

When you place commands in the [Default] section of the CustomSettings.ini file, they apply to all target computers that access the deployment share. However, this does not mean that you can't use CustomSettings.ini commands if you have to assign different property values to some of your computers. You can define groups in a CustomSettings.ini file and assign properties with different values to the computers in each group.

MDT 2010 enables you to group your target computers by location or according to hardware or software attributes. For example, to create groups based on locations in a CustomSettings.ini file, you assign group names to the default gateway addresses of the subnets on your network, as in the following sample:

```
[Default Gateway]
192.168.1.1=Boston
192.168.2.1=Chicago
192.168.3.1=Seattle
```

You then create sections named for the groups and place your group-specific properties in those sections. For example, the following commands join the target computers to a different domain depending on the city where they are located:

```
[Boston]
JoinDomain=boston.example.local
DomainAdmin=Alice
DomainAdminPassword=Pa$$w0rd
DomainAdminDomain=boston.example.local

[Chicago]
JoinDomain=chicago.example.local
DomainAdmin=Ralph
DomainAdminPassword=Pa$$w0rd
DomainAdminDomain=chicago.example.local

[Seattle]
JoinDomain=seattle.example.local
DomainAdmin=Ed
DomainAdminPassword=Pa$$w0rd
DomainAdminDomain=seattle.example.local
```

## CONFIGURING INDIVIDUAL COMPUTERS

Some properties require values that must be unique on every computer, such as the OSDComputerName property, which specifies the computer name assigned to a target computer during the Windows 7 installation. To assign properties like these to individual computers, you must create separate sections for each computer in the CustomSettings.ini file. As with the group capabilities, you can use different criteria to identify individual computers, including hardware, software, and user-defined attributes.

For example, to identify target computers using the media access control (MAC) addresses assigned to their network interface adapters, you create a section for each computer named using the six-byte hexadecimal value of its MAC address. Then you add the computer-specific properties into each section, as shown in the following example:

```
[Settings]
Priority=MACAddress, Default

[00:1a:6b:3c:ba:1f]
OSDComputerName=Wkstn1

[00:0c:29:ab:07:a2]
OSDComputerName=Wkstn2
```

#### **NOTE** DISPLAYING MAC ADDRESSES

To display the MAC address of a Windows computer, open a Command Prompt window and run the `Ipconfig.exe` program using the `/all` parameter.

In the [Settings] section, the Priority property specifies the order in which the Windows Deployment Wizard on the target computer should parse the settings in the `CustomSettings.ini` file. Adding the `MACAddress` property to the Priority command causes the computers to apply the commands in the MAC address sections first, and then to apply the commands in the [Default] section.

#### **NOTE** USING A MICROSOFT SQL SERVER DATABASE WITH MDT 2010

Automating a truly large deployment project using `CustomSettings.ini` files alone can still be a huge task. For this reason, MDT 2010 also provides the ability to use a SQL Server database to store the settings for individual computers and define group settings as well. Deployment Workbench includes the ability to create and interact with a database on a computer running SQL Server.

## Multicasting LTI Deployments

A large operating system deployment product normally requires the build computer to transmit a separate copy of the captured install image to each target computer. Because these images can run to several gigabytes in size, the amount of network traffic generated by the deployment process can be enormous. Part of your initial planning for your project should include issues such as when you plan to perform the target computer deployment, how much network bandwidth is available, and how many workstations you can safely deploy at the same time.

One way to reduce the amount of network bandwidth the deployment process consumes is to use multicast transmissions to deliver the image files to the target computers. A multicast is a type of TCP/IP transmission that delivers a single copy of the data to multiple destinations. Most TCP/IP transmissions are unicasts, which are transmissions to a single destination, or broadcasts, which are transmissions to all possible destinations. A multicast falls between these two by transmitting to a selected group of destinations—in this case, a group of target computers that you want to receive a single transmission of an image at the same time.

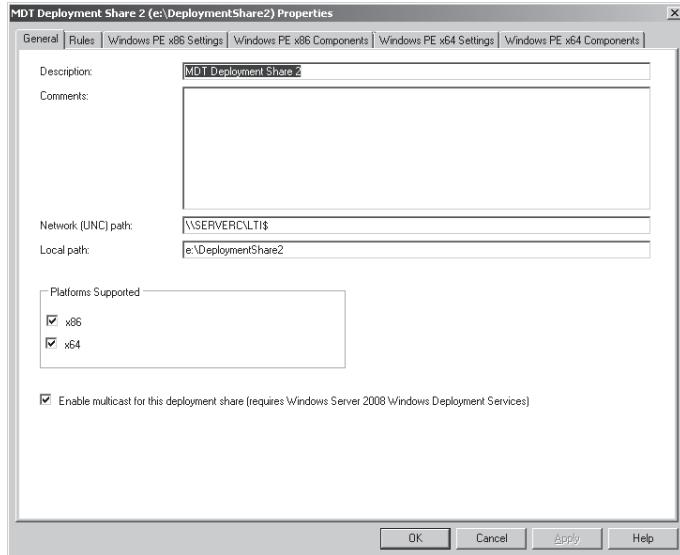
As discussed in Chapter 6, the versions of Windows Deployment Services included in Windows Server 2008 and Windows Server 2008 R2 have multicasting capabilities, and you can use WDS to deploy your captured images directly to target computers using multicasts. However, this method bypasses the MDT 2010 deployment share, which prevents you from using task sequences to control your deployments.

Fortunately, MDT 2010 is capable of utilizing the multicasting capabilities of WDS when transmitting images from its own deployment share. To do this, your build server must be running Windows Server 2008 or Windows Server 2008 R2, and must have Windows Deployment Services, Windows Automated Installation Kit 2.0, and Microsoft Deployment Toolkit 2010 installed and configured. You must also create an MDT 2010 deployment share that uses the share name LTI\$.

After configuring WDS and MDT in the usual manner, you configure the deployment share to use multicasting by opening the share's Properties sheet and, on the General tab, selecting the Enable Multicast For This Deployment Share check box, as shown in Figure 7-18. Then you must update the deployment share in the usual way to create boot images that support multicasting.

**NOTE SUPPORTING MULTICASTING**

To use multicasting successfully with MDT 2010, you must be using Windows AIK version 1.1 or later on your build server. This is because earlier versions of Windows AIK include Windows PE boot files that do not support multicasting.



**FIGURE 7-18** The Enable Multicast For This Deployment Share check box in an MDT 2010 deployment share

This action in Deployment Workbench triggers the creation of a Multicast Transmission in WDS, as shown in Figure 7-19. You can then add the MDT 2010 boot images to the Windows Deployment Services console. This process does not add the MDT 2010 install images to WDS, but it does enable the MDT deployment share to use WDS multicasting for its transmissions.

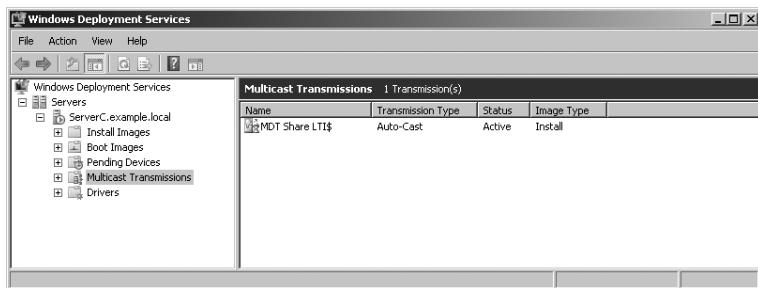


FIGURE 7-19 The WDS multicast transmission created by MDT 2010

WDS supports two types of multicasting, as follows:

- **Auto-cast** The server initiates a multicast transmission when an eligible client connects and requests an install image. If, while the transmission is in progress, other clients on the network request the same image, they are added to the multicast group and receive the same transmission as the first client.
- **Scheduled-cast** The server initiates a multicast transmission when a predetermined number of clients request the same image or when a scheduled date and time occurs. An administrator can also start a scheduled-cast transmission manually.

MDT 2010 supports the creation of only auto-cast multicast transmissions. To use scheduled-cast multicasting, you must deploy your images by using WDS directly, and not through MDT 2010.

To use multicasting effectively, any routers located between the build server and the target servers must support multicasting using the Internet Group Management Protocol (IGMP). Routers that do not support multicasts treat the transmissions as broadcasts, sending them to all of the computers on the network, instead of to only the ones requesting the transmission.

## PRACTICE Customizing a CustomSettings.ini File

By working with the CustomSettings.ini file, you can automate elements of the LTI deployment process that by default require interaction on each target workstation.

### EXERCISE 1 Modifying the Default Commands

A Windows SIM distribution share provides a directory structure in which you can store device drivers and other files you want to deploy to a workstation.

1. Click Start. Then click All Programs | Microsoft Deployment Toolkit | Deployment Workbench. The Deployment Workbench console appears.

2. Expand the Deployment Shares folder.
3. Right-click your deployment share and, from the context menu, select Properties. The Properties sheet appears.
4. Click the Rules tab.
5. You want to assign the same Administrator password to all your target workstations, so in the [Default] section, make sure that the value assigned to the SkipAdminPassword property is YES.
6. Specify an Administrator password to assign to your target computers by adding the following command to the [Default] section.

`AdminPassword=Pa$$w0rd`

7. You will not be using MDT 2010 to capture reference computer images, so set the SkipCapture value to YES.
8. Change the value of the SkipProductKey property to NO so that the installer can specify a unique key on every deployed workstation.
9. Click OK.

## **EXERCISE 2 Suppressing Windows Deployment Wizard Pages**

Create your own CustomSettings.ini file based on the default commands created by the New Deployment Share Wizard, adding the code needed to accomplish the following tasks.

1. To suppress the Specify Credentials For Connecting To Network Shares page, add commands that supply the credentials needed to access your deployment share, as follows:

```
UserID=<user_name>
UserPassword=<password>
UserDomain=<user_domain_name>Note Supplying Customized Values
```

Replace the bracketed placeholders in this exercise with values appropriate for your network.

2. To suppress the Join The Computer To A Domain Or Workgroup page, add commands that will join the target computer to your domain, as follows:

```
SkipDomainMembership=YES
JoinDomain=YES
DomainAdmin=<user_name>
DomainAdminPassword=<password>
DomainAdminDomain=<user_domain_name>
```

3. To suppress the Specify Where To Save Your Data And Settings and Specify Whether To Restore User Data pages so that the target computers do not capture or restore user state data, add the following command:

`SkipUserData=YES`

- To suppress the Specify The BitLocker Configuration page and add commands that implement BitLocker on the target computers using TPM and a startup key on drive L, storing the recovery key in Active Directory, use the following code:

```
BDEInstall=TPMKey  
BDEInstallSuppress=NO  
BDERecoveryKey=AD  
OSDBitLockerStartupKeyDrive=L:
```

- To suppress the Configure The Computer Name page and add commands to specify the name Client1 for your computer only, based on its MAC address, use the following code:

```
[Settings]  
Priority=MACAddress, Default  
  
[<xx:xx:xx:xx:xx:xx>]  
SkipComputerName=YES  
OSDComputerName=Client1
```

## Lesson Summary

- The central hardware component of an LTI deployment project is the build computer, which is where you install Microsoft Deployment Toolkit (MDT) 2010 and Windows 7 Automated Installation Kit (Windows AIK).
- The other hardware component of your LTI deployment lab is one or more reference computers, which you will use to capture images of your workstation configurations.
- To deploy Windows 7 to a target computer using MDT 2010, you must create a task sequence using the New Task Sequence Wizard. After you have created the task sequences, you must update your deployment share.
- The image files that Deployment Workbench creates when you update the deployment share contain the Windows PE boot files and the Windows Deployment Wizard.
- You can launch the Windows Deployment Wizard from a computer that is already running an operating system, by running the Litetouch.vbs script.
- When you boot the target computer using one of the LiteTouchPE image files, the MDT 2010 Solution Accelerators interface appears. After the interface appears, you can run the Windows Deployment Wizard.
- CustomSettings.ini is the main configuration file for MDT 2010. Target computers read the file when they load the Windows Deployment Wizard, and the settings inside control the deployment process.
- When you place commands in the [Default] section of the CustomSettings.ini file, they apply to all target computers that access the deployment share.
- One way of minimizing the amount of network bandwidth the deployment process consumes is to use multicast transmissions to deliver the image files to the target computers.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Designing a Lite-Touch Deployment." The questions are also available on the companion CD if you prefer to review them in electronic form.

### NOTE ANSWERS

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

1. Which of the following MDT 2010 deployment scenarios requires a task sequence to save the user state data from the target computer?
  - A. New Computer
  - B. Refresh Computer
  - C. Replace Computer
  - D. Upgrade Computer
2. Which of the following Windows Deployment Wizard pages can be suppressed without adding a Skip command to the CustomSettings.ini file?
  - A. Select a task sequence to execute on this computer.
  - B. Join the computer to a domain or workgroup.
  - C. Specify credentials for connecting to network shares.
  - D. Operating system deployment completed successfully.
3. Which of the following CustomSettings.ini commands always require a unique value for every target computer? (Choose all answers that are correct.)
  - A. UserID
  - B. ProductKey
  - C. TaskSequenceID
  - D. OSDComputerName
4. Which of the following client boot files makes it possible for a task sequence to save user state data before installing Windows 7?
  - A. Litetouch.vbs
  - B. LiteTouchPE\_x64.wim
  - C. LiteTouchPE\_x32.iso
  - D. LiteTouchPE\_x64.iso

## Lesson 2: Designing a Zero-Touch Deployment

As mentioned earlier and in previous chapters, a Zero-Touch Installation follows the same basic steps as a Lite-Touch Installation. You still install reference computers, capture images of them, and deploy those images to your target computers. However, a ZTI target computer deployment differs from an LTI deployment in that it requires no interaction at all at the workstation. In Lesson 1 of this chapter, you saw how the effort you put into the preparation of an LTI deployment was repaid by reduced interaction later. To reduce the interaction to zero requires even more preparation, as well as a significantly more complex infrastructure.

**After this lesson, you will be able to:**

- Prepare the infrastructure for a ZTI deployment
- Create task sequences for target computer deployments
- Customize a ZTI deployment to suit your development and installation requirements
- Create SCCM collections and advertisements

**Estimated lesson time: 60 minutes**

## Using System Center Configuration Manager

Unlike an LTI deployment, the preparation for a ZTI deployment is not optional. MDT 2010 can provide a zero-touch deployment only because it is able to take advantage of the capabilities built into Microsoft System Center Configuration Manager (SCCM) 2007. You therefore must have SCCM 2007 installed on the computer on which you plan to install MDT 2010.

In a ZTI deployment, SCCM takes over many of the tasks performed by MDT 2010 in an LTI deployment. You still must create task sequences to install reference computers and target computers, but in a ZTI deployment, you use the SCCM Configuration Manager utility to perform all of the tasks of the Deployment Workbench program in an LTI, except for the management of the MDT database.

### Understanding the Infrastructure Prerequisites

SCCM 2007 is a full-featured network management package that is designed to perform a wide variety of tasks. Operating system deployment is one of the product's major capabilities, but for most network managers, it is not worth the time, effort, and expense required to install SCCM just for that purpose.

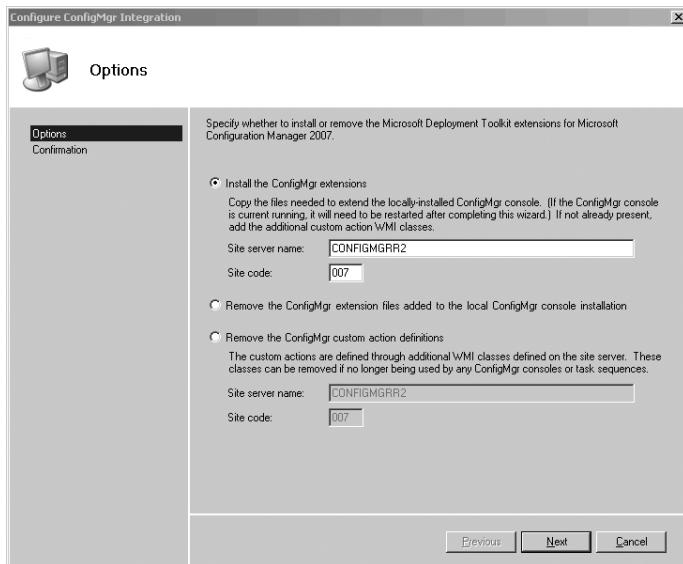
Implementing SCCM on a large network is a formidable task in itself, before you even consider using it with MDT. The product requires a substantial software infrastructure, including a variety of Windows Server roles and features and a SQL Server database. You can distribute the various services among different computers, but to use a single server to perform a ZTI deployment, you must install and configure all of the following servers, roles, features, and other elements:

- Windows Server 2008 or Windows Server 2008 R2
  - Active Directory Domain Services
  - DNS Server
  - DHCP Server
  - Internet Information Services (IIS)
  - Windows Deployment Services
  - BITS Server Extensions
  - Remote Differential Compression
- System Center Configuration Manager 2007
- SQL Server 2005 SP2 or later
- Windows 7 Automated Installation Kit
- Microsoft Deployment Toolkit 2010

## Configuring Configuration Manager Integration

After you have installed and configured SCCM 2007 and all of the other software required to run it, you can install Windows 7 AIK and MDT 2010, just as you would for an LTI deployment. Then, to enable the interaction between the SCCM Configuration Manager console and MDT 2010, you must run the Configure ConfigMgr Integration Wizard, as in the following procedure:

1. Click Start. Then click All Programs | Microsoft Deployment Toolkit | Configure ConfigMgr Integration. The Configure ConfigMgr Integration Wizard appears, displaying the Options page, as shown in Figure 7-20.



**FIGURE 7-20** The Configure ConfigMgr Integration Wizard

2. Select the Install The ConfigMgr Extensions option.
3. In the Site Server Name text box, type the name of the server on which SCCM is installed.
4. In the Site Code text box, type the SCCM server's site code number and click Next. The Confirmation page appears.
5. Click Finish.

This wizard copies the MDT integration files to the Configuration Manager root folder (C:\Program Files\Microsoft System Center Configuration Manager, by default) and adds new Windows Management Instrumentation (WMI) classes for MDT functions.

## Creating Task Sequences Using SCCM

SCCM 2007 uses task sequences to define the activities it performs on clients, just as MDT 2010 does. In a ZTI deployment, you must create task sequences to deploy Windows 7 on reference computers and target computers, just as in an LTI deployment. Although the terminology is the same, the procedure for creating the task sequences in Configuration Manager is substantially different.



#### EXAM TIP

LTI and ZTI deployments use some of the same terminology for their components, such as packages and task sequences, but the terms do not always refer to the same elements. Be careful to distinguish between the LTI and ZTI environments when reading exam questions.

Software distribution is one of the primary functions of SCCM, which the product does by creating software packages and transmitting them to clients all over the network. When you create a task sequence in Configuration Manager, you create a number of separate packages in the process, containing the various software elements needed to install the target computer.

The process of creating a task sequence for a ZTI target computer deployment is as follows:

1. Click Start. Then click All Programs | Microsoft System Center | Configuration Manager 2007 | ConfigMgr Console. The Configuration Manager Console appears, as shown in Figure 7-21.

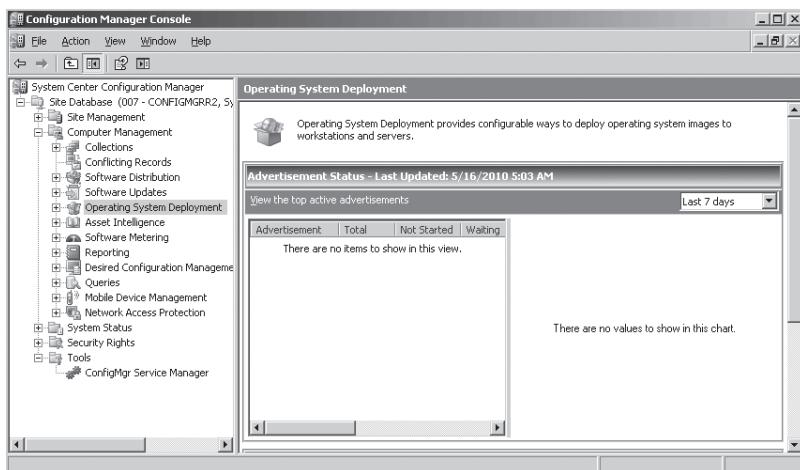
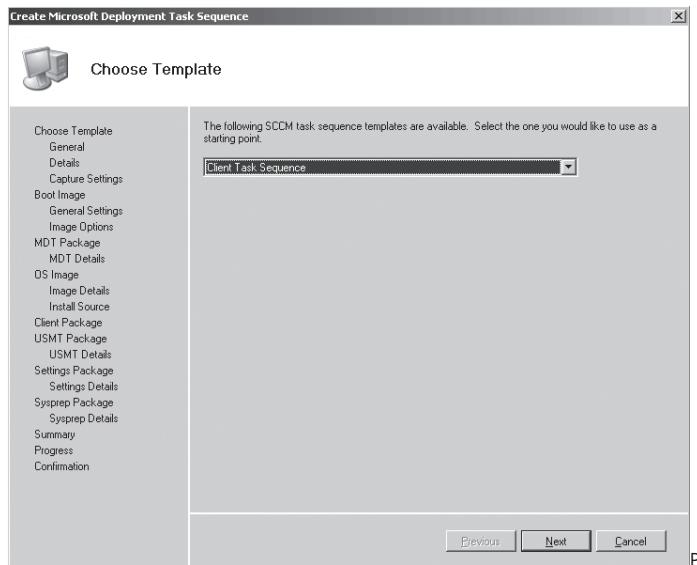


FIGURE 7-21 The Configuration Manager Console

2. Expand the Computer Management\Operating System Deployment node. Then right-click Task Sequences and, in the context menu, select Create Microsoft Deployment Task Sequence. The Create Microsoft Deployment Task Sequence Wizard appears, displaying the Choose Template page, as shown in Figure 7-22.

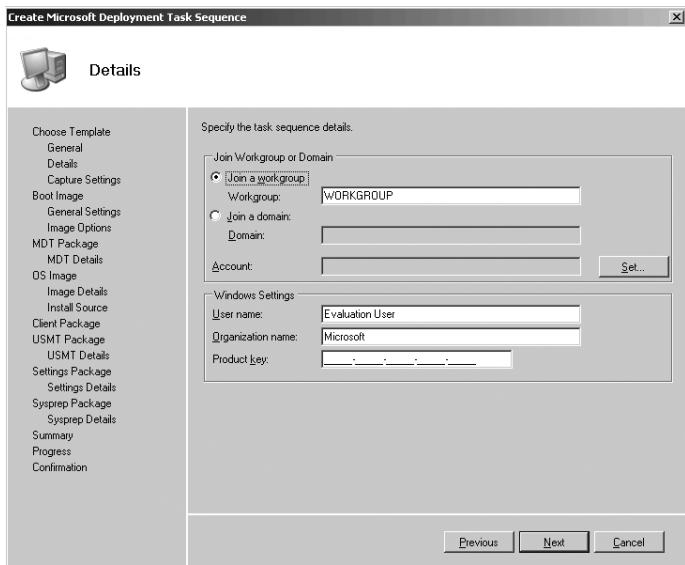


**FIGURE 7-22** The Choose Template page of the Create Microsoft Deployment Task Sequence Wizard

**NOTE CREATING MICROSOFT DEPLOYMENT TASK SEQUENCES**

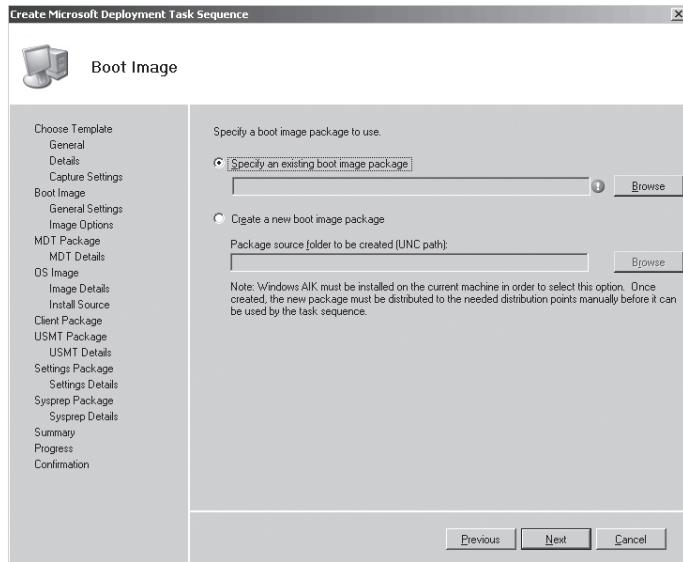
SCCM 2007 also uses task sequences for operating system deployments independent of MDT 2010. Therefore, be sure to select Create Microsoft Deployment Task Sequence from the context menu, and not the New | Task Sequence option.

3. Leave the Client Task Sequence template selected and click Next. The General page appears.
4. In the Task Sequence Name text box, type a descriptive name, such as **Windows 7 Target Deployment**, and click Next. The Details page appears, as shown in Figure 7-23.



**FIGURE 7-23** The Details page of the Create Microsoft Deployment Task Sequence Wizard

5. Select the Join A Domain option, and in the Domain text box, type the name of the domain you want the target computer to join.
6. Click Set. The Windows User Account dialog box appears.
7. In the User Name, Password, and Confirm Password text boxes, type the administrative credentials that the target computer will use to join the domain. Then click OK.
8. In the Windows Settings box, type the User Name, Organization Name, and Product Key values that the target computer should use when installing Windows 7. Then click Next. The Capture Settings page appears.
9. Leave the option named The Task Sequence Will Never Be Used To Capture An Image selected and click Next. The Boot Image page appears, as shown in Figure 7-24.



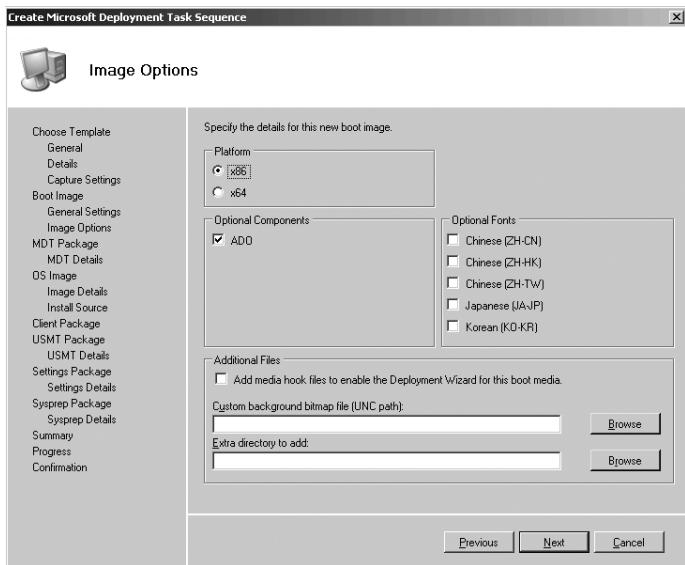
**FIGURE 7-24** The Boot Image page of the Create Microsoft Deployment Task Sequence Wizard

10. Select the Create A New Boot Image Package option and in the Package Source Folder To Be Created text box, type the path to a shared folder where the wizard will create the image. Then click Next. The General Settings page appears.

#### **NOTE CREATING NEW PACKAGES**

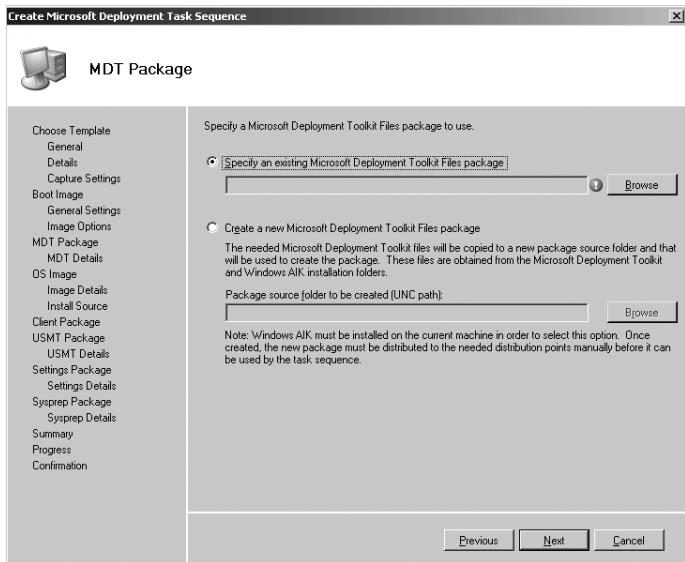
If you have already created a boot image package for your reference computer deployment, you can choose the Specify An Existing Boot Image Package option and select that same boot image for your target computer deployment. The same is true for the other packages that the task sequence offers to create. You can reuse existing packages in as many task sequences as you want.

11. In the Name text box, type a name for the boot image and click Next. The Image Options page appears, as shown in Figure 7-25.



**FIGURE 7-25** The Image Options page of the Create Microsoft Deployment Task Sequence Wizard

- 12.** Select the Platform option for the target computer you want to install and click Next. The MDT Package page appears, as shown in Figure 7-26.



**FIGURE 7-26** The MDT Package page of the Create Microsoft Deployment Task Sequence Wizard

13. Select the Create A New Microsoft Deployment Toolkit Files Package option and, in the Package Source Folder To Be Created text box, type the path to a shared folder where the wizard will create the package. Then click Next. The MDT Details page appears.

**NOTE CREATING A MICROSOFT DEPLOYMENT TOOLKIT FILES PACKAGE**

The Microsoft Deployment Toolkit Files package enables the target computer to access the MDT 2010 software on the build computer during the SCCM distribution process.

14. In the Name text box, type a name for the MDT package and click Next. The OS Image page appears, as shown in Figure 7-27.

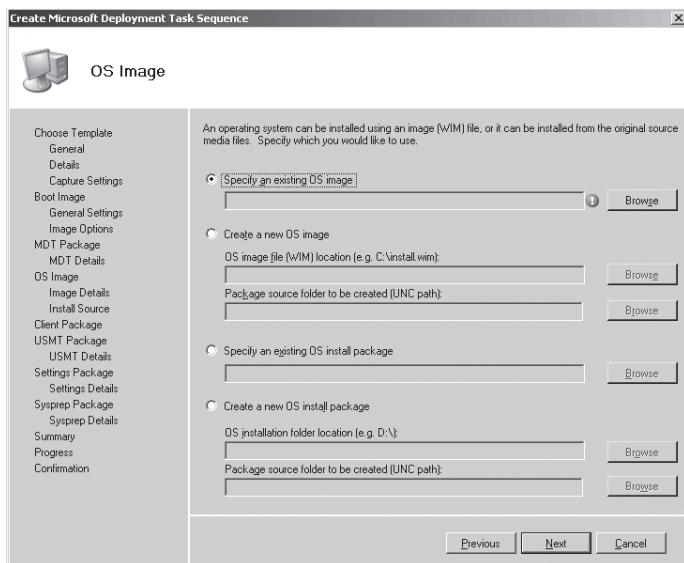
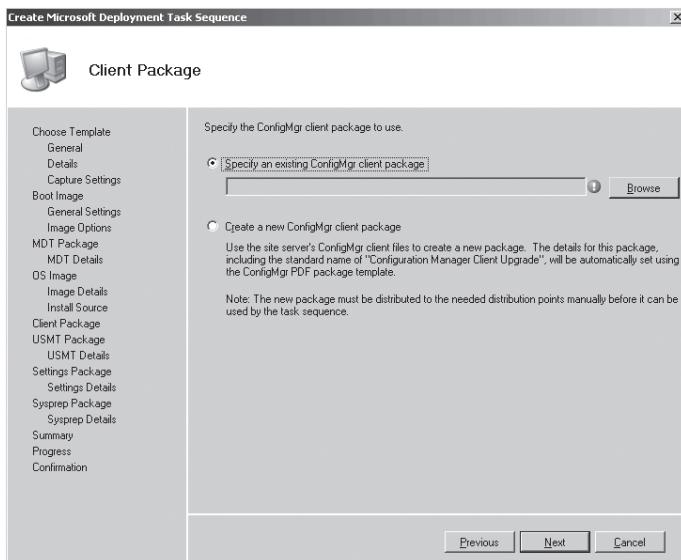


FIGURE 7-27 The OS Image page of the Create Microsoft Deployment Task Sequence Wizard

15. Select the Create A New OS Image option.
16. In the OS Image File (WIM) Location text box, type the path to the image you captured from your reference computer.

17. In the Package Source Folder To Be Created text box, type the path to a shared folder where the wizard will create the package. Then click Next. The Install Details page appears.
18. In the Name text box, type a name for the reference OS image and click Next. The Client Package page appears, as shown in Figure 7-28.

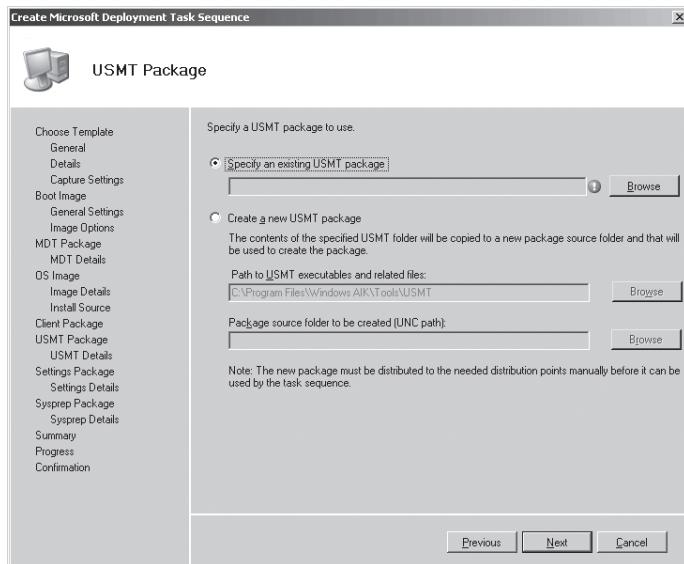


**FIGURE 7-28** The Client Package page of the Create Microsoft Deployment Task Sequence Wizard

19. Select the Create A New ConfigMgr Client Package option and click Next. The USMT Package page appears, as shown in Figure 7-29.

**NOTE** **INSTALLING THE SCCM CLIENT**

The SCCM client package, which will be installed on the target computer after the operating system, enables administrators to manage the workstation remotely from the Configuration Manager Console.



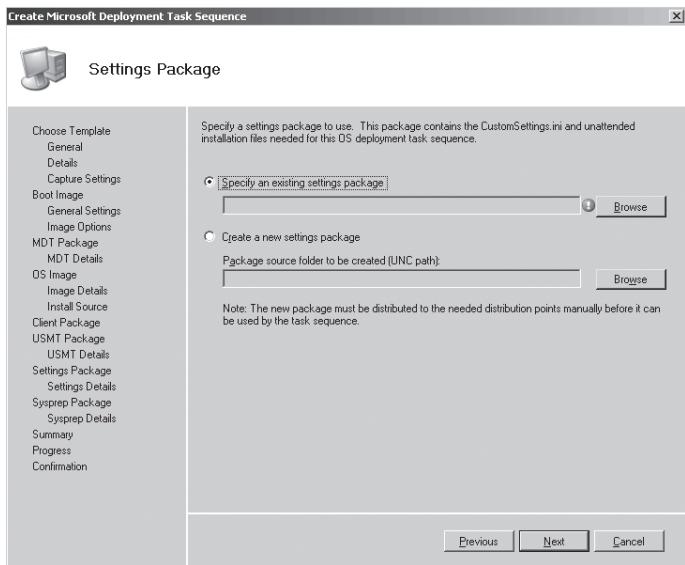
**FIGURE 7-29** The USMT Package page of the Create Microsoft Deployment Task Sequence Wizard

20. Select the Create A New USMT Package option.
21. In the Package Source Folder To Be Created text box, type the path to a shared folder where the wizard will create the USMT package. Then click Next. The USMT Details page appears.

#### **NOTE CREATING A USMT PACKAGE**

The USMT package provides the target computer with the User State Migration Tool programs, `Savestate.exe` and `Loadstate.exe`, which the system uses to save and restore user state data.

22. In the Name text box, type a name for the USMT package and click Next. The Settings Package page appears, as shown in Figure 7-30.



**FIGURE 7-30** The Settings Package page of the Create Microsoft Deployment Task Sequence Wizard

23. Select the Create A New Settings Package option.
24. In the Package Source Folder To Be Created text box, type the path to a shared folder where the wizard will create the Settings package. Then click Next. The Settings Details page appears.

**NOTE CUSTOMIZING SETTINGS**

When the Create Microsoft Deployment Task Sequence Wizard is completed, you will find a CustomSettings.ini file in the folder you specified as the location for the Settings package. You can modify this file just as you would in an LTI deployment, to configure elements of the target computer installation. The Microsoft Deployment Toolkit Reference in the Microsoft Deployment Toolkit Documentation Library help file indicates which of the properties you can use in a CustomSettings.ini file are supported in ZTI deployments.

- 25.** In the Name text box, type a name for the Settings package and click Next. The Sysprep Package page appears.
- 26.** Leave the No Sysprep Package Is Required option selected and click Next. The Summary page appears.
- 27.** Click Next. The Progress page appears, as the wizard creates the various packages.
- 28.** When the process is completed, the wizard closes and the task sequence appears in the Task Sequences container.

## Deploying ZTI Task Sequences to Target Computers

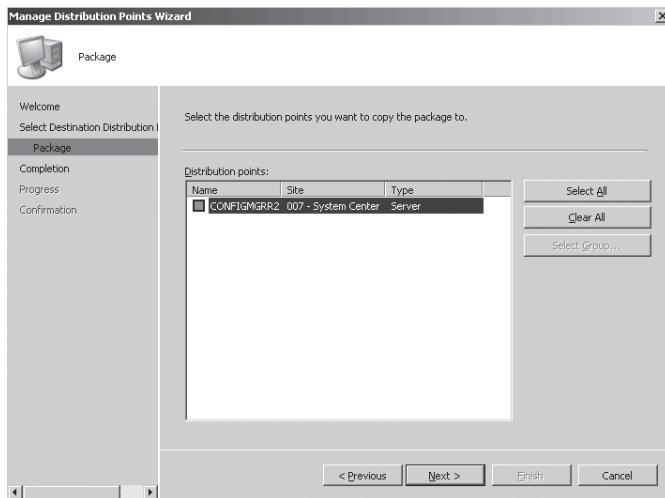
After creating the task sequence and the packages and images containing the software the target computers need, you must complete a number of additional steps to deploy the task sequence to the target computers. Eventually, you will be able to simply boot the target computers and walk away as SCCM and MDT complete the entire workstation installation with no further interaction. The following sections describe what you must do to get to that point.

### Creating Distribution Points

SCCM 2007 is a highly scalable application that you can use to manage hundreds or thousands of computers all over an enterprise network. To deploy software to computers at different sites, SCCM uses distribution points. A distribution point is a computer that is designated as a storehouse for packages and images. To perform a truly large ZTI deployment, you might have to use multiple distribution points, and Configuration Manager enables you to select those points and control the replication of the distribution packages and images to them.

To select the distribution point you want to use for your ZTI deployment, you must run the Manage Distribution Points Wizard by browsing to the Site Database/Computer Management/Software Distribution/Packages folder, right-clicking the Settings package you created with the task sequence and, from the context menu, selecting Manage Distribution Points.

On the Package page of the wizard, as shown in Figure 7-31, you select one or more distribution points. If you select more than one, the wizard replicates the package to all of the points, in preparation for the deployment.



**FIGURE 7-31** The Package page of the Manage Distribution Points Wizard

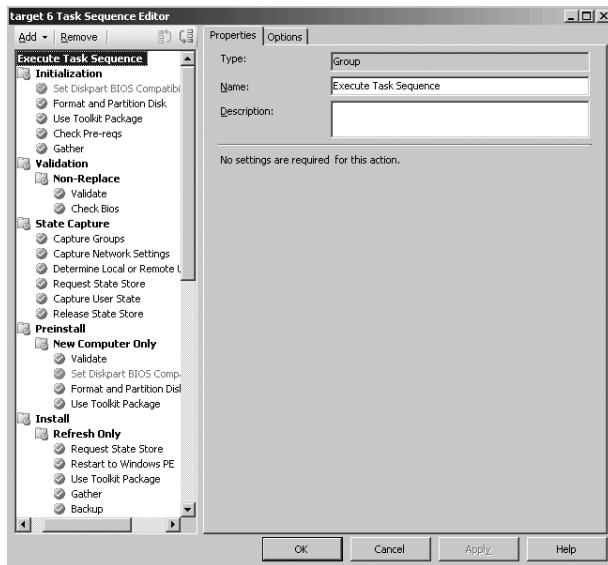
#### **IMPORTANT UPDATING DISTRIBUTION POINTS**

If you modify the CustomSettings.ini file at any point after you select the distribution points you want to use, you must update the distribution points to replicate your changes before you actually deploy your target computers.

When the wizard is completed, you must then browse to the Site Database/Computer Management/Operating System Deployment/Operating System Images folder and do the same thing to select distribution points for the operating system image you created with the task sequence.

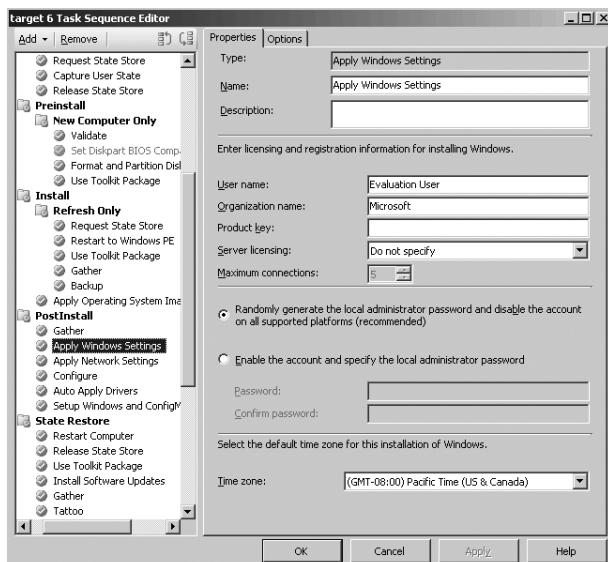
### **Customizing Task Sequences**

As in an LTI deployment, you can modify the task sequences you create in Configuration Manager to customize them, although the interface is slightly different. To edit a task sequence, browse to the Site Database/Computer Management/Operating System Deployment/Task Sequences folder in Configuration Manager, right-click the task sequence you created and, from the context menu, select Edit. The Task Sequence Editor appears, as shown in Figure 7-32.



**FIGURE 7-32** The SCCM Task Sequence Editor

An SCCM task sequence, in its default configuration, usually needs no modification to perform an entire workstation deployment. However, using this interface, you can modify all aspects of the workstation installation, if necessary. For example, the default task sequence disables the target computer's Administrator account and assigns it a random password. To modify that behavior and specify a password of your own, you can browse to the PostInstall/Apply Windows Settings page and select the Enable The Account And Specify The Local Administrator Password option, as shown in Figure 7-33.



**FIGURE 7-33** The Apply Windows Settings page of the SCCM Task Sequence Editor

## Adding the Target Computer to the Site Database

SCCM 2007 is designed to manage computers by communicating with a client installed on each one. The ZTI task sequence includes the installation of the client so that administrators can manage the workstation after the deployment is complete. However, this client/server communication cannot take place if there is no client. Therefore, when you deploy target computers using the New Computer scenario, you must add the computer to the SCCM site database so that it can communicate with the build server.

If you are using one of the other deployment scenarios, such as Refresh Computer, Replace Computer, or Upgrade Computer, and your workstations already have an operating system and the client installed and running, SCCM can automatically discover them and initiate the deployment, so there is no need to manually add them to the database.

To add New Computer targets to the data, browse to the Site Database/Computer Management/Operating System Deployment/Computer Association folder, right-click it and, from the context menu, select Import Computer Information. The Import Computer Information Wizard appears and offers two options for importing computer information, as follows:

- **Import computers using a file** To add a large number of target computers to the database, you can create a comma-delimited text file with each line containing a computer name and either an SMBIOS GUID value or the MAC address of the network adapter in the computer. You then use the wizard's Choose Mapping page, as shown in Figure 7-34, to specify the database field into which the wizard should add the values in each column of your file.

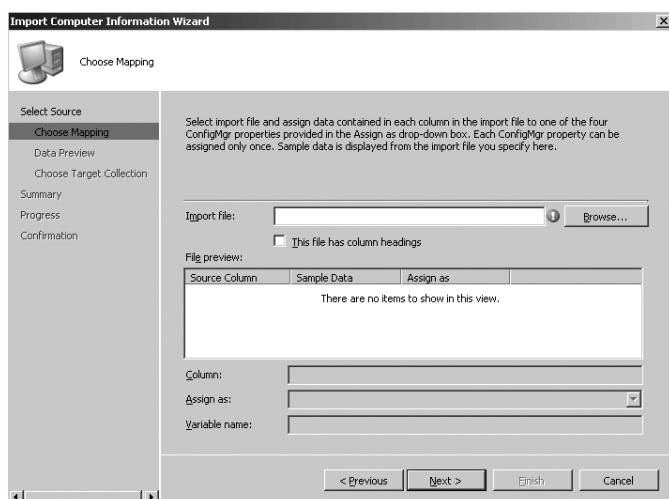


FIGURE 7-34 The Choose Mapping page of the Import Computer Information Wizard

- **Import single computer** To add a single target workstation to the database, you use the wizard's Single Computer page, as shown in Figure 7-35, to enter the computer name and either an SMBIOS GUID value or the MAC address of the network adapter in the computer.

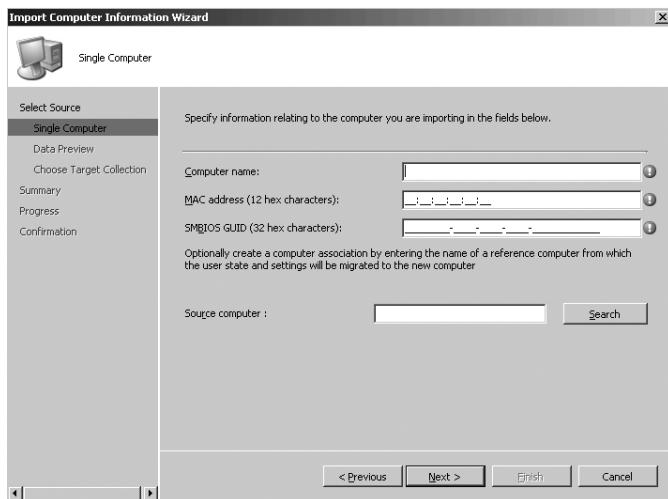
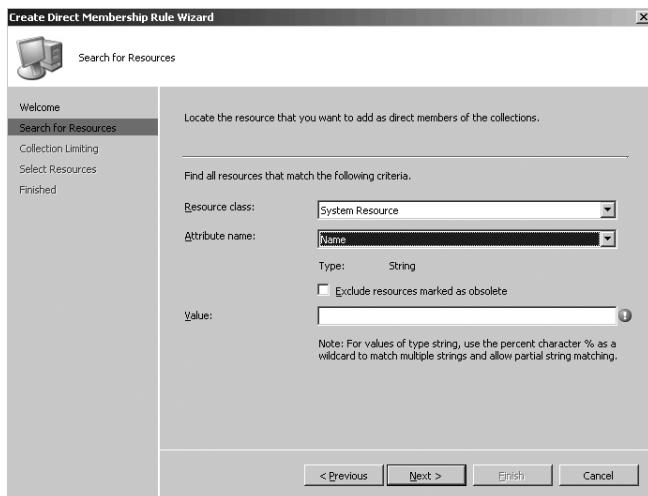


FIGURE 7-35 The Single Computer page of the Import Computer Information Wizard

## Creating Collections

In SCCM, a collection is an organizational tool that enables administrators to perform tasks on a specific set of computers, users, or groups. To perform a ZTI deployment, you must add the target computers that you want to deploy to a collection. The computers in the collection then receive an advertisement from SCCM that informs them of the installation to be completed.

To create a collection, browse to the Site Database/Computer Management/Collections folder in Configuration Manager. The console includes a number of preconfigured collections, but you can add as many new ones as you need. Right-click the Collections folder and, from the context menu, select New Collection. This launches the New Collection Wizard, which in turn launches the Create Direct Membership Rule Wizard, which you can use to select computers in the database by searching for specific attribute values, such as names and MAC addresses, as shown in Figure 7-36.



**FIGURE 7-36** The Search For Resources page of the Create Direct Membership Rule Wizard

Collections are one way to regulate the progress of your deployment project. By creating multiple collections, you can limit the number of workstations you deploy at any one time, to prevent your networks from being flooded with traffic. For example, if you determine that your subnets can handle up to five simultaneous workstation deployments, you can create a number of collections, each of which contains five target computers from every subnet. You can then configure SCCM to advertise each collection at a different time so that the collection deployments never overlap.

## Creating Advertisements

Advertisements are the mechanisms by which SCCM makes software packages available to collections of computers, users, or groups. In a ZTI deployment, you use advertisements to make your task sequences available to the target computers in your collections.

To create an advertisement, open Configuration Manager and browse to the Site Database/Computer Management/Operating System Deployment/Task Sequences folder. Right-click the task sequence you want to advertise and, from the context menu, select Advertise. The New Advertisement Wizard appears, displaying the General page, as shown in Figure 7-37. On this page, you specify the name of the collection to which you want to advertise the task sequence.

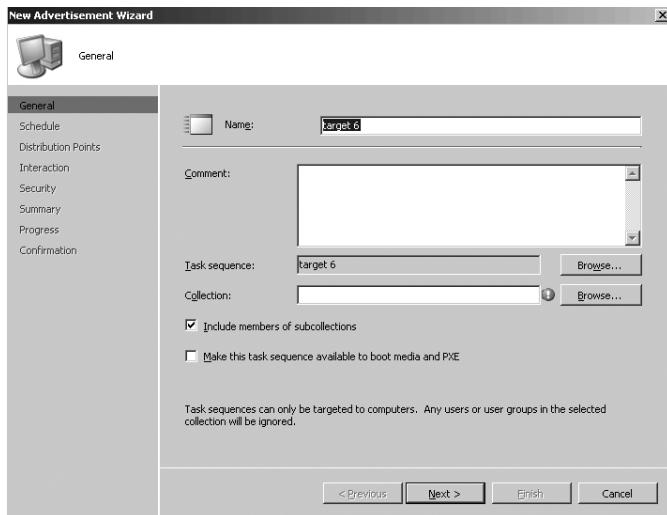


FIGURE 7-37 The General page of the New Advertisement Wizard

The default values on the rest of the wizard pages will suffice in many cases, but you can also use the Schedule page, as shown in Figure 7-38, to regulate when your task sequences are advertised, thus providing another way to restrict the amount of traffic generated by the deployment process.

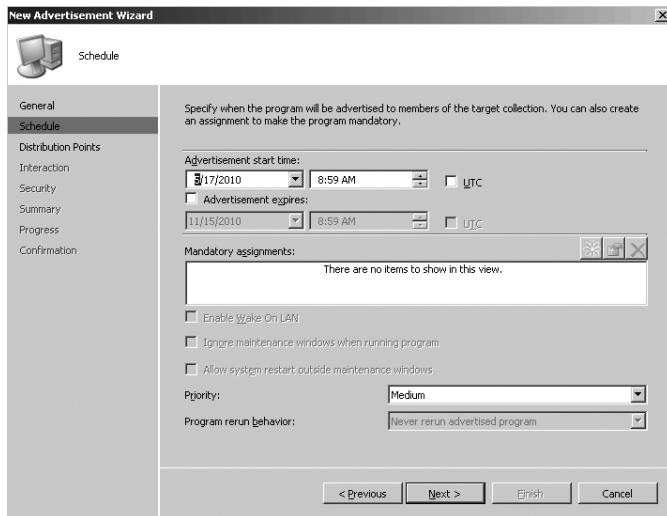


FIGURE 7-38 The Schedule page of the New Advertisement Wizard

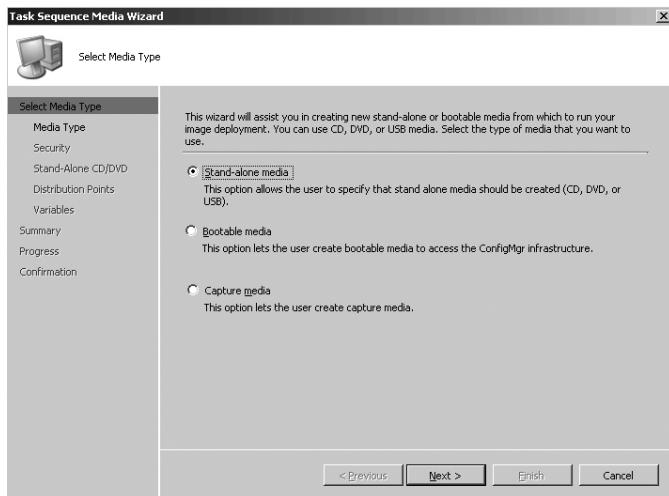
## Creating Boot Media

With the SCCM server prepared, all that remains is to boot the target computers. After they are started, the target computers connect to the server, and the installation of the packages and images you prepared earlier proceeds automatically.

As with an LTI deployment, you can start the target computers using removable boot media, such as DVDs, CDs, or USB flash drives, or you can use Windows Deployment Services for workstations that are PXE-enabled.

To create task sequence bootable media, use the following procedure:

1. Open Configuration Manager and browse to the Site Database/Computer Management/Operating System Deployment/Task Sequences folder.
2. Right-click a task sequence and, from the context menu, select Create Task Sequence Media. The Task Sequence Media Wizard appears, displaying the Select Media Type page, as shown in Figure 7-39.



**FIGURE 7-39** The Select Media Type page of the Task Sequence Media Wizard

3. Select the Bootable Media option and click Next. The Media Type page appears, as shown in Figure 7-40.

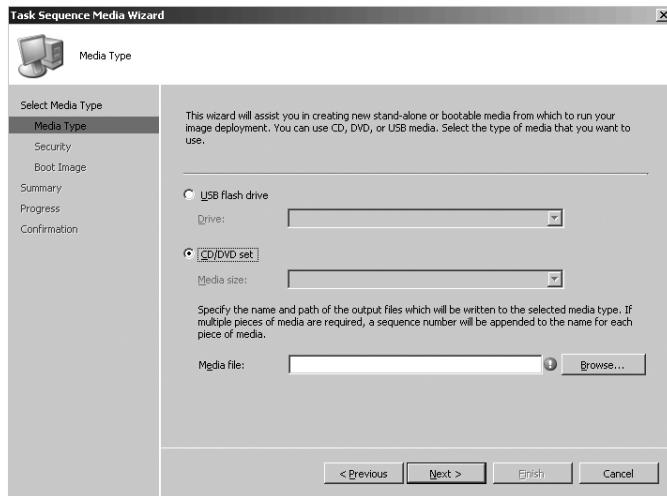


FIGURE 7-40 The Media Type page of the Task Sequence Media Wizard

4. Select one of the following options:
  - **SB flash drive** Insert the flash drive and select the drive letter. The wizard burns the task sequence medium directly to the drive.
  - **D/DVD set** Specify the name of the media file the wizard will create and the path to the folder in which you want to create it. The wizard creates an ISO file that you can burn to a CD or DVD.
5. Click Next. The Security page appears, as shown in Figure 7-41.

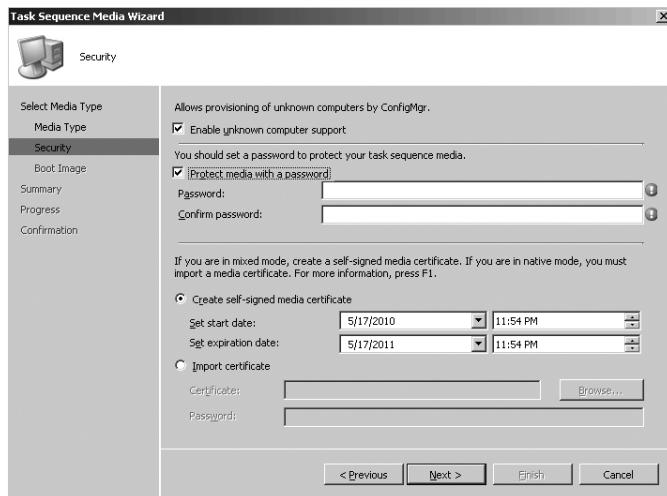


FIGURE 7-41 The Security page of the Task Sequence Media Wizard

6. In the Password and Confirm Password text boxes, type a password to protect the task sequence medium and click Next. The Boot Image page appears, as shown in Figure 7-42.

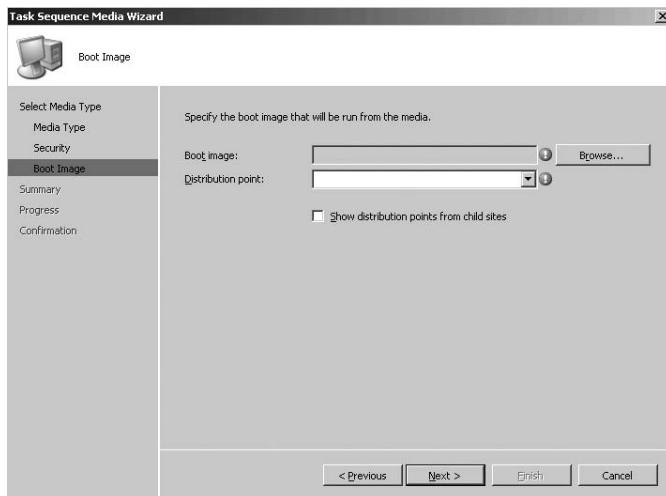


FIGURE 7-42 The Boot Image page of the Task Sequence Media Wizard

7. Click Browse. The Select A Boot Image dialog box appears.
8. Select the boot image you created with the Create Microsoft Deployment Task Sequence Wizard and click OK.
9. In the distribution point drop-down list, select the distribution point from which the target computer will access the boot image and click Next. The Summary page appears.
10. Click Next. The wizard creates the boot medium and displays the Wizard Completed page.

To boot the target workstations using WDS, you must configure SCCM to function as a PXE service point so that the server can respond to boot requests generated by the target computers. By right-clicking the Site Database/Site Management/<site>/Site Settings/Site Systems/<server> folder and selecting New Roles, you launch the New Site Role Wizard, with which you can add the PXE service point role, as shown in Figure 7-43.

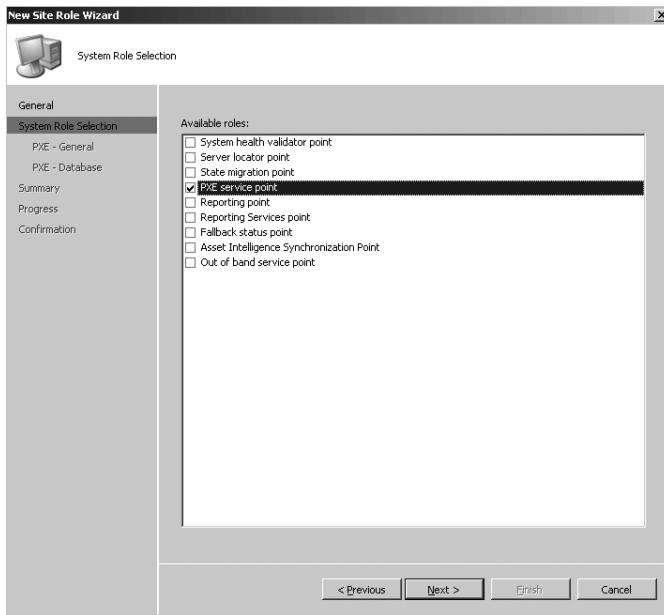


FIGURE 7-43 The New Site Role Wizard

## PRACTICE Comparing SCCM Deployment Scenarios

Because a self-taught student cannot be expected to have access to a System Center Configuration Manager server, the practice for this student consists of SCCM videos produced by Microsoft.

### EXERCISE 1 Viewing a “Using Configuration Manager to Deploy Windows 7” Video

Use a Windows computer with Internet access to view a video demonstration of a Windows 7 deployment using SCCM in its native mode.

1. Launch Windows Internet Explorer.
2. In the address box, type <http://go.microsoft.com/fwlink/?LinkId=196560> and press Enter.
3. Click the Play button in the video window to start the clip.

### EXERCISE 2 Viewing a “Deploying Windows 7 with the Microsoft Deployment Toolkit for Configuration Manager” Video

Use a Windows computer with Internet access to view a video demonstration of a Windows 7 deployment using Microsoft Deployment Toolkit 2010 with SCCM.

1. Launch Internet Explorer.

2. In the address box, type **http://go.microsoft.com/fwlink/?LinkId=196561** and press Enter.
3. Click the Play button in the video window to start the clip.

## Lesson Summary

- A ZTI target computer deployment differs from an LTI deployment in that it requires no interaction at all at the workstation.
- In a ZTI deployment, SCCM takes over many of the tasks performed by MDT 2010 in an LTI deployment. You use the SCCM Configuration Manager utility to perform all of the tasks of the Deployment Workbench program in an LTI, except for the management of the MDT database.
- To enable the interaction between the SCCM Configuration Manager console and MDT 2010, you must run the Configure ConfigMgr Integration Wizard.
- SCCM 2007 is a highly scalable application that you can use to manage hundreds or thousands of computers all over an enterprise network. To deploy software to computers at different sites, SCCM uses distribution points.
- When deploying target computers using the New Computer scenario, you must add the computer to the SCCM site database so that it can communicate with the build server.
- In SCCM, a collection is an organizational tool that enables administrators to perform tasks on a specific set of computers, users, or groups. To perform a ZTI deployment, you must add the target computers that you want to deploy to a collection.
- Advertisements are the mechanisms by which SCCM makes software packages available to collections of computers, users, or groups. In a ZTI deployment, you use advertisements to make your task sequences available to the target computers in your collections.
- As with an LTI deployment, you can start the target computers using removable boot media, such as DVDs, CDs, or USB flash drives, or you can use Windows Deployment Services for workstations that are PXE-enabled.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Designing a Zero-Touch Deployment." The questions are also available on the companion CD if you prefer to review them in electronic form.

### NOTE ANSWERS

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

- 1.** Which of the following packages created by an SCCM task sequence enables a target computer to save and restore user state data?
  - A.** MDT Files package
  - B.** USMT package
  - C.** Client package
  - D.** Settings package
- 2.** For which of the following ZTI deployment scenarios must you add the target computer to the site database?
  - A.** New Computer
  - B.** Refresh Computer
  - C.** Replace Computer
  - D.** Upgrade Computer
- 3.** Which of the following SCCM components enables you to deploy Windows 7 to target computers located at remote sites, all over the enterprise?
  - A.** Site databases
  - B.** Collections
  - C.** Advertisements
  - D.** Distribution points

## Chapter Review

---

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

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

## Chapter Summary

- To deploy captured reference images using the MDT 2010 Lite-Touch Installation method, you must create a task sequence, provide your target computers with access to your build server, and then decide how you intend to boot your target computers and launch the Windows Deployment Wizard.

- The MDT 2010 Zero-Touch Installation method requires much more preparation and infrastructure than a Lite-Touch Installation, but the benefits to network administrators, both during and after the actual deployment, can be significant. To prepare for a ZTI deployment using captured reference images, you must create a task sequence, select distribution points, add the target computers to a collection, create an advertisement, and finally create task sequence boot media.

## 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.

- advertisement
- collection
- CustomSettings.ini
- distribution point
- multicast

## Case Scenarios

In the following case scenario, you will apply what you've learned about subjects of this chapter. You can find answers to the scenario questions in the "Answers" section at the end of this book.

### Case Scenario 1: Multitasking an LTI Deployment

Ed is a newly hired IT staffer working on a project to expand the Inside Sales department of his company by adding 100 new Windows 7 workstations. He is going to have to deploy Windows 7 onto the new workstations while the department is running and salespeople are using the network. Ed has been told that he must use multicasting when deploying the workstations to prevent the network from being flooded with deployment traffic.

Ed designs an LTI deployment using a single build server running Windows Server 2008 R2. The department already has reference computer images from a previous deployment that he can use. He adds the Windows Deployment Services role to the server and installs the latest versions of Windows 7 Automated Installation Kit and Microsoft Deployment Toolkit 2010.

Using Deployment Workbench, Ed creates a new deployment share on his server, using the default folder names and settings. He then populates the deployment share with his reference images, creates a task sequence, and makes sure that multicasting is enabled in the deployment share's Properties sheet. Finally he updates the deployment share and deploys the resulting boot images using WDS.

After a test deployment consisting of five workstations, Ed determines that each workstation is receiving unicast transmissions; no multicasting is occurring. Checking the Windows Deployment Services console, Ed sees no multicast transmissions.

Why is the build server not multitasking and what can Ed do to fix it?

## Suggested Practices

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

### Designing a Lite-Touch Deployment

- **Practice 1** Using the documentation supplied with Microsoft Deployment Toolkit 2010, review the “Quick Start Guide for Lite-Touch Installation” and compare the procedure with that for the Zero-Touch Installation.

### Designing a Zero-Touch Deployment

- **Practice 1** Using the documentation supplied with Microsoft Deployment Toolkit 2010, review the “Quick Start Guide for Zero-Touch Installation” and compare the procedure with that for the Lite-Touch Installation.
- **Practice 2** Using the Microsoft Web site at <http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-os-deployment.aspx>, study the capabilities of System Center Configuration Manager other than operating system deployment and the cost of purchasing SCCM for a medium-sized to large-sized network. Try to determine at what point the benefits provided by the product warrant the expenditure.

## 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 70-686 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.

# Planning a Windows 7 Client Update Strategy

Windows Server Update Services (WSUS) is a role service that you can install on computers running the Windows Server 2008 R2 operating system. It is also freely available software that you can download and install on computers running versions of the Windows Server operating system prior to Windows Server 2008 R2. WSUS functions as a local Microsoft Update server on an organization's network. This tool allows organizations to optimize their bandwidth usage, with only a single computer on the network downloading update files from the Internet rather than having each computer on the network download the same update files. WSUS also allows network administrators to control update approval, disseminating updates at times that are convenient to the organization rather than having them downloaded and installed automatically whenever Microsoft publishes them on the Microsoft Update servers. When you run WSUS 3 SP3 on a computer that has the Windows Server 2008 R2 operating system installed, you can take advantage of BranchCache technology. This reduces the number of WSUS servers that you need to deploy in branch offices because updates can be cached and shared among branch office computers rather than requiring a dedicated local server to host them.

## Exam objectives in this chapter:

- Plan and manage software updates.

## Lessons in this chapter:

- Lesson 1: Designing an Update Management Strategy **326**
- Lesson 2: Deploying Updates to Clients **343**

## Before You Begin

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

- Installed the Windows 7 operating system on a stand-alone client PC named WKSTN1, as described in the Introduction.
- For the practice exercise at the end of Lesson 1, download the Microsoft Baseline Security Analyzer 2.1.1 or later installation files from the following location on the Microsoft Web site: <http://www.microsoft.com/mbsa>.



### REAL WORLD

Orin Thomas

No administrator wants to be the person who deployed an update that was so incompatible with the organization's existing software configuration that it took everyone's computer offline. Although such situations are rare, they do occur and should serve as a reminder to those that aspire to be responsible for the deployment of software updates that such updates should be thoroughly tested before being deployed. Testing updates prior to deploying them generally will not catch every possible conflict that might occur between the update and your established configuration, but it is likely to catch the most serious conflicts. If you do not notice a conflict after an update has been deployed on a test computer when that computer has been used for a normal week of work, the inconvenience caused by that update is likely to be minor. An update testing infrastructure will not catch every conflict, but it will catch the big ones that would have caused you hours of headaches trying to roll back the deployment of an update.

## Lesson 1: Designing an Update Management Strategy

An important part of being an Enterprise Desktop Administrator is ensuring that you keep the client computers that you are responsible for current with the latest updates published by Microsoft and third-party vendors. A large part of accomplishing this objective is ensuring that you have an update management strategy that is appropriate for your environment. The default configuration of computers running Windows 7 is for the computer to automatically download and install updates published on the Microsoft Update servers. Although this configuration might be appropriate for some organizations, you probably want more control over the distribution of updates. If you are responsible for a small number of computers, you can choose to install updates manually from a network share or removable USB drive. If you are in a larger organization, you might decide to use a centralized update

management solution like Windows Server Update Services or System Center Configuration Manager. The method you choose for updating client computers depends significantly on your needs. Choosing the right update management strategy saves you time and saves your organization money.

**After this lesson, you will be able to:**

- Understand updates.
- Design an update infrastructure.
- Determine update compliance.

**Estimated lesson time: 40 minutes**

## Understanding Updates

Updates are files that address functionality issues and address security vulnerabilities in operating systems and applications. Because vulnerabilities can be quickly exploited after the details of the vulnerability are published, you must ensure that updates that address the vulnerabilities are deployed to computers in your organization with reasonable haste.

Unfortunately, updates do alter a computer's configuration, and an update that addresses one issue in an application or operating system can cause problems with other parts of the configuration. These problems might become apparent only after the update is deployed. As an enterprise desktop administrator, you must seek a balance, ensuring that you test updates adequately prior to deployment, but also ensuring that updates are deployed in a timely and effective manner.

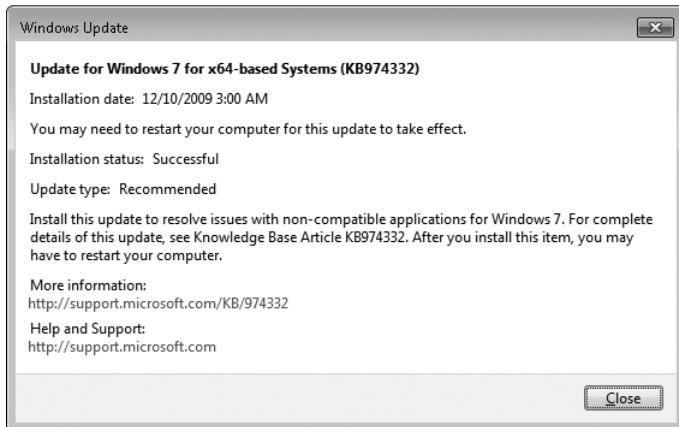
### Update Classification

Microsoft assigns a classification to each update it publishes. The classification allows you to prioritize the deployment of updates, and you should test and deploy updates that have a more urgent classification before testing and deploying updates with less urgent classifications. The update bulletin provides details on its classification as well as the location from which you can obtain the update files if an automated update solution is not in place.

Updates published by Microsoft can have one of the following three classifications:

- **Important Updates** These updates address critical security issues such as those an attacker can use remotely to take control of a computer. In some cases, Important updates address security issues for which exploit code has already been published on the Internet. In cases for which exploit code is not available, attackers quickly reverse-engineer updates in an attempt to determine which vulnerabilities the update might address and use this as the basis of developing their own exploit code. You should prioritize the deployment of updates with this classification over the deployment of other updates.

- **Recommended Updates** These updates often address issues related to the existing functionality of the computer. Figure 8-1 shows a Recommended update that relates to application compatibility. Recommended updates are of lower priority than Important updates, But you should still deploy updates with this classification to computers in your organization in a timely manner.



**FIGURE 8-1** Recommended update

- **Optional Updates** These updates include items such as language packs and driver updates. Optional updates often extend the functionality of the computer. Optional updates are strictly optional. Organizations should assess the changes that Optional updates introduce to the software ecosystem prior to rolling the updates out to desktop computers. The deployment of Optional updates is rarely time-sensitive in the way that the deployment of other updates is.

## Update Deployment

When the Windows 7 operating system is installed on a computer, the installation routine queries you about how you want to treat automatic updates. This dialog box is shown in Figure 8-2. The default setting is for updates classified as Important and Recommended to be automatically downloaded and installed on the computer as they are released by Microsoft. When a computer running Windows 7 is configured using the default settings, the Windows Update client on the computer regularly checks with the Microsoft Update servers on the Internet to see whether any new updates have been published. If a new update has been published, the Windows Update client downloads and installs the update and then reboots the computer if that is a necessary part of the update installation process.



**FIGURE 8-2** Configuring update settings during installation

In many small-size to medium-size organizations, this default configuration for Windows Updates is acceptable. As organizations get larger, they are more likely to want to take control of the deployment and approval of updates. The next pages tell you about the solutions that are available to an organization that wants to take control of the update management process.

## Installing Updates Manually

The first update management option that organizations can implement is manually deploying updates, rather than having the updates downloaded directly by clients from the Internet. You can download update files from the Microsoft Web site and install them manually using the Wusa.exe command-line utility. Update files have the .msu extension.

Manual installation of updates might be necessary for computers located on secure isolated networks, or for stand-alone computers that are not connected to any network. In some cases, it will be necessary to install multiple updates. One problem with manual update installation is that many updates require the computer to be restarted for the installation process to complete. As a way of dealing with this problem, you can chain the installation of updates using the /norestart parameter. A script that installs three updates with a single command would have a format similar to the following:

```
Wusa.exe i:\windows6.1-kb123456-x64.msu /quiet /norestart  
Wusa.exe i:\windows6.1-kb123457-x64.msu /quiet /norestart  
Wusa.exe i:\windows6.1-kb123458-x64.msu /quiet
```

Manual update installation can be a tedious process because an administrator must ensure that update files are placed in a location accessible to the computer being updated; the administrator also must type out long update file names in a command-line window. In some cases though, installing updates manually is the only way that you can deploy updates to computers running the Windows 7 operating system.

**MORE INFO** **WINDOWS UPDATE STAND-ALONE INSTALLER**

To find out more about the Windows Update Stand-alone installer (Wusa.exe), consult the following article on the Microsoft Web site: <http://support.microsoft.com/kb/934307>.

## Windows Server Update Services

Windows Server Update Services (WSUS) is a free update management solution from Microsoft. WSUS allows for the central distribution and deployment of updates and functions as a local area network version of the Microsoft Update servers located on the Internet. WSUS 3.0 Service Pack 2 (SP2) is a role that you can add to a computer running the Windows Server 2008 R2 operating system. You can also download and install WSUS on computers running previous versions of the Windows Server operating system, though in this case WSUS is an add-on program rather than a role built into the operating system, as is the case with Windows Server 2008 R2.

You can accomplish update deployment goals by deploying WSUS:

- WSUS allows you to control which updates you deploy to computers in your organization. Updates published by Microsoft are not deployed to clients unless specifically approved by the WSUS administrator.
- WSUS allows an organization to make more efficient use of Internet bandwidth. Rather than have update files downloaded separately to each computer, updates are downloaded to the WSUS server and distributed centrally.

As Figure 8-3 shows, WSUS can be used to deploy critical updates, definition updates, drivers, feature packs, security updates, service packs, tools, update rollups, and updates. By default, WSUS synchronizes only Critical Updates, Definition Updates, and Security Updates. WSUS does not allow you to deploy updates for third-party applications.

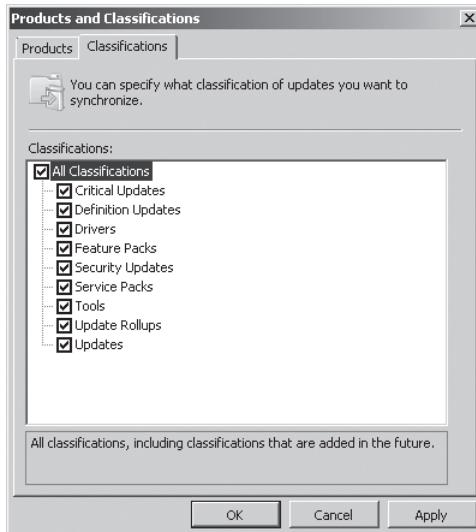


FIGURE 8-3 WSUS update classifications



### Quick Check

- What type of application updates cannot be distributed from a WSUS server?

### Quick Check Answer

- WSUS cannot be used to distribute updates from third-party application vendors.

## WSUS Servers as Update Locations

Clients running the Windows 7 operating system can retrieve updates from a WSUS server or from the Microsoft Update servers. Sometimes the Microsoft Update servers are preferable to a server on the organizational network. For example, if a worker is using a portable computer from her home office for an extended period of time, she should download updates from the Microsoft Update servers rather than across a VPN or DirectAccess connection. The client's bandwidth to the Microsoft Update servers through her ISP is likely to provide more capacity than her bandwidth to the WSUS server on the organizational network.

As an Enterprise Desktop Administrator, you have the following choices for deploying and approving updates for the Windows 7 clients in your organization:

- **Microsoft Update used as source of update files and approvals** This is the default configuration of computers running Windows 7. In this configuration, an administrator does not have central control over which updates are approved or disallowed.

- **Microsoft Update used as source of update files** WSUS server used for update approvals. You configure computers to use this option by setting them to use the WSUS server and then configuring the WSUS server so that it does not store updates locally.
- **WSUS server used as source of update files and approvals** The typical WSUS deployment has both updates and approvals coming from the same location. You configure clients to use the WSUS server through Group Policy. You learn how to configure the appropriate policy in Lesson 2 of this chapter.

## WSUS Topologies

You can choose from several ways to deploy WSUS. The way that you choose often depends on issues of bandwidth utilization and administrative responsibility. In a single WSUS deployment, you deploy a WSUS server on the organizational network that synchronizes with the Microsoft Update servers on the Internet. Clients on the organizational network retrieve updates directly from this server. The WSUS server administrator approves updates for distribution. This is the most common type of WSUS deployment, and a single WSUS 3.0 SP2 server can function as the update server for up to 25,000 computers running the Windows 7 operating system.

In general, this type of deployment does not work well for organizations that have a large number of branch offices because branch office client computers each have to retrieve updates from the central WSUS server over a WAN link. Although you can configure clients in branch offices to retrieve only approval data from the head office WSUS server, a single WSUS server can function either as an approvals-only server or as an approvals and updates server. A single WSUS server cannot function as an approvals-only server for one group of clients and an approvals and updates server for another group of clients. This is why many organizations deploy multiple WSUS servers, allowing bandwidth efficiencies to be realized in each branch office.

The options for the deployment of multiple WSUS servers are as follows:

- **Replica WSUS server** A replica WSUS server is a server that retrieves the list of update approvals and WSUS groups from a WSUS server above it in the WSUS hierarchy. This method is appropriate when update approvals are handled centrally for the organization. A replica WSUS server can obtain updates from the parent WSUS server or from the Microsoft Update servers on the Internet, or it can force WSUS clients to retrieve approved updates from the Microsoft Update servers.
- **Autonomous WSUS server** An autonomous WSUS server can retrieve update files from a WSUS server above it in the WSUS hierarchy, but approvals are handled by a local administrator. This allows local administrators to manage the approval process but also allows efficiencies in terms of update bandwidth utilization.
- **Independent WSUS server** WSUS servers are managed independently from one another and do not draw updates or approvals from a source on the organizational network.



## Quick Check

- What type of WSUS server receives approvals from another WSUS server on the organizational network?

## Quick Check Answer

- WSUS servers configured in replica mode receive approval data from another WSUS server on the organizational network.

## WSUS and BranchCache

When WSUS 3.0 SP2 is installed on a computer running the Windows Server 2008 R2 operating system, the BranchCache feature can be enabled. This allows Windows 7 Enterprise and Ultimate clients located in branch offices to leverage peer caching as a method of optimizing update distribution. Rather than clients on the branch office network independently downloading the same update from the head office WSUS server, one client downloads the update and then shares the update installation files with other clients on the branch office network. This allows organizations to deploy a single WSUS server in a head office location and still enjoy the bandwidth efficiencies at branch office sites.

You can use BranchCache in hosted cache mode in branch office locations where there is a computer running the Windows Server 2008 R2 operating system. Hosted cache mode makes peer caching more reliable than the alternative, which is distributed cache mode. Hosted cache mode is more reliable because a server (which is in theory always available) hosts a copy of the cache. In branch office locations where there is no computer running the Windows Server 2008 R2 operating system, you can use only BranchCache distributed cache mode. Distributed cache mode is not as reliable as hosted cache mode because clients hosting updates in their local cache might be switched off when other clients attempt to access the same update, requiring those clients to contact the head office WSUS server.

You should note that clients that have the Windows 7 Professional or Windows Vista operating systems installed cannot access updates through BranchCache. Clients using these operating systems must retrieve updates directly from WSUS or Microsoft Update servers.

To use BranchCache with WSUS, ensure that you have performed the following steps:

1. Ensure that the WSUS server has the Windows Server 2008 R2 operating system installed. Ensure that the BranchCache feature is enabled.
2. Configure the clients at the branch office to retrieve updates from the BranchCache-enabled WSUS server using the Specify Intranet Microsoft Update Service Location policy.
3. Configure the clients at the branch office with the appropriate BranchCache policies. If there is a server with the Windows Server 2008 R2 operating system located at the branch office, you can use the Hosted Cache mode. If no branch office Windows Server 2008 R2 server is present, clients will need to use Distributed Cache mode.

#### MORE INFORMATION BRANCHCACHE

To find out more about how to use BranchCache, consult the following TechNet Web page:  
<http://technet.microsoft.com/en-us/network/dd425028.aspx>.

## WSUS Groups

When you approve an update on a WSUS server, you choose the WSUS groups that the update deploys to. WSUS groups are collections of computer accounts that allow you to stagger the deployment of updates to computers; you do not have to deploy them to every computer at the same time. WSUS servers have two computer groups by default: the All Computers and the Unassigned Computers group. When clients are set so that they use a specific WSUS server without additional configuration, they are automatically added to the Unassigned Computers group. WSUS computer groups have the following properties:

- **WSUS groups can be organized hierarchically.** Groups lower in the hierarchy automatically inherit update approvals from groups closer to the top of the hierarchy, although you can also configure inheritance blocks where necessary.
- **You can assign computers to multiple WSUS groups.** Assigning computers to multiple WSUS groups allows you to be more selective about the deployment of updates. For example, in an organization that has only a single WSUS server, you could create a group structure that allowed approval based on which department the computer was in and approval based on location. Figure 8-4 shows a computer assigned to multiple WSUS groups.

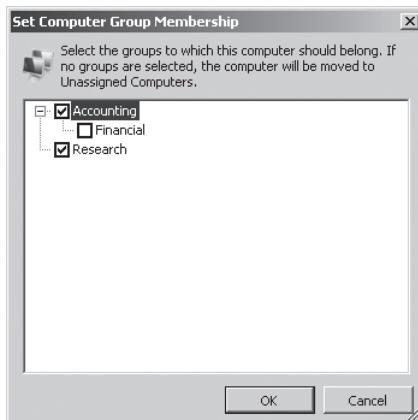
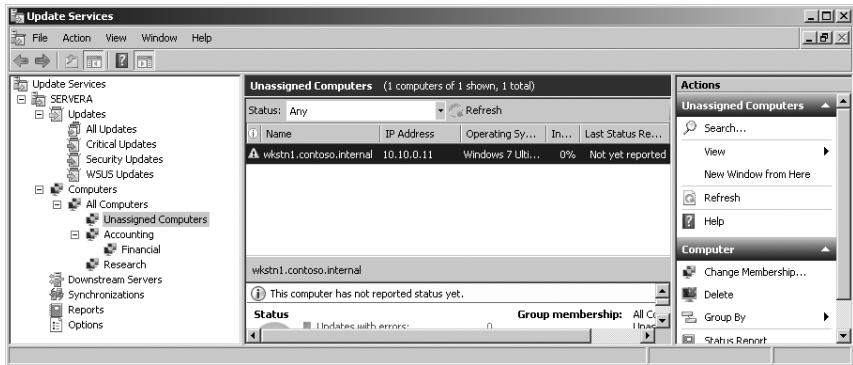


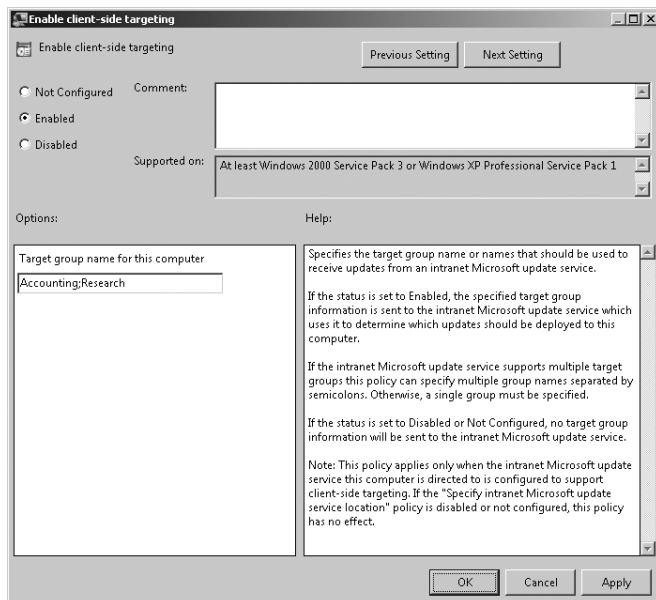
FIGURE 8-4 Computer assigned to multiple groups

- **Computers are assigned to the Unassigned Computers group by default.** Unless a computer is already assigned to a WSUS group, it belongs to the Unassigned Computers group, as shown in Figure 8-5.



**FIGURE 8-5** Using WSUS groups to stagger updates

WSUS groups are separate from Active Directory security groups. Administrators can manually assign computers to groups using the WSUS console after the computer has contacted the WSUS server. Large numbers of computers can be added to existing WSUS groups using the Enable Client-Side Targeting Group Policy item. Figure 8-6 shows the Enable Client-Side Targeting policy configured so that the computers that the policy applies to are made members of both the Accounting and Research WSUS groups. If a group that does not exist on the WSUS server is specified in the client-side targeting policy, the WSUS computer account is added to the Unassigned Computers group.



**FIGURE 8-6** Client-side targeting

## Configuring an Update Testing Infrastructure

Although Microsoft tests updates rigorously before releasing them publicly, no one can test every possible software and hardware configuration for adverse side effects that might result when an update is applied. For this reason, you should deploy updates to a small group of computers prior to deploying updates to all computers in your organization and test those computers to determine whether a newly released update conflicts with your organization's specific software configuration.

You should ensure that the small group of computers on which you test updates match the software and hardware configuration of computers in your organization and that the computers used for testing are actually used by real people to perform their everyday job-related tasks. You need to do this because you will not be able to detect all possible problems by simply installing the update on a computer that no one actually uses. Only through testing the updates under real-world conditions do any conflicts or other problems become evident.

You should ensure that you deploy updates to the test computers long enough that you have confidence that the updates do not cause problems when deployed generally. You must balance this with not waiting so long that the computers in your organization become vulnerable to the issue that the update addresses. In many organizations, updates are deployed to test computers between 7 to 10 days before being deployed to all other computers in the organization. This period provides enough time to test that the updates do not cause obvious problems with the existing configuration before rolling the updates out more generally.

A basic update testing infrastructure would have a separate computer group containing the WSUS computer accounts for all test computers. A WSUS automatic approval rule for all new updates would apply to this WSUS computer group. The WSUS administrator would manually approve updates for the All Computers group after a seven-day period in which no issues had been reported by users of computers that are located in the test group.

## Verifying Update Deployment

The final component in a successful update strategy is ensuring that updates deploy correctly to client computers. There are many reasons why updates might not deploy correctly to client computers, including but not limited to the computer being switched off for a lengthy period of time, synchronization problems, and lack of disk space on the client.

One of the simplest ways that you can verify the updates that are installed on local and remote computers running Windows 7 and which are members of the same domain is to manually use the *Get-Hotfix* Windows PowerShell command. You can use the *-Computername* option to specify the address of the remote computers that you want to check.

For example, the command

```
Get-HotFix -Computername wkstn1,wkstn2,wkstn3,wkstn4
```

provides a report on all of the updates installed on computers wkstn1, wkstn2, wkstn3, and wkstn4. Although this is a quick way to verify which updates are installed on a small number

of computers, it is not an effective technique for determining the status of missing updates across a large number of computers. This is because the output will tell you only which updates are present on the target computers and will not tell you which updates are missing from the target computers.

## WSUS Reports

One way you can determine which updates are missing from client computers in your organization is to use WSUS reports. WSUS servers generate reports based on information forwarded to the WSUS server from the server's WSUS clients. When a WSUS client retrieves and successfully installs an update, it reports this success back to the WSUS server.

WSUS servers do not query clients to determine whether specifically approved updates are missing and they can use only information that active clients report back to them. This distinction is important because you cannot learn anything about the update status of client computers that have not reported to the WSUS server. To find out whether a client computer has suffered some unforeseen configuration problem it has not reported, you must use a tool such as the Microsoft Baseline Security Analyzer, covered later in this lesson, to query client computers to determine whether specific updates are missing.

You can access WSUS reports from the Reports node of the WSUS console, as shown in Figure 8-7. WSUS reports can be printed or exported to Microsoft Office Excel or PDF format. Because WSUS data can be forwarded to a SQL Server database, you can also perform a separate analysis using your own database queries. There are several basic categories of reports that allow you to view how successful the deployment of a specific update has been or the update status of specific WSUS server clients.

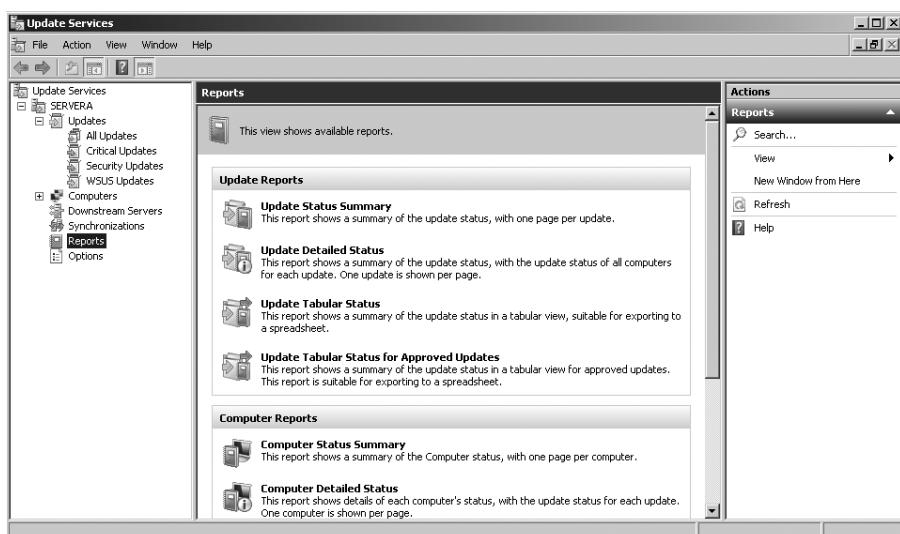


FIGURE 8-7 WSUS reports

## Microsoft Baseline Security Analyzer

As mentioned, you can use Microsoft Baseline Security Analyzer (MBSA) to scan client computers in an organization to determine whether they are missing software updates. You can configure the MBSA tool to check whether a computer is up to date with the updates published by Microsoft through the Microsoft Update servers. You can also configure the MBSA tool to check against the list of approved updates hosted on a local WSUS server. This practice allows you to determine whether a computer is up to date with the updates that have been approved for your specific environment. When used to scan against a WSUS server approval list, the MBSA tool scans using the WSUS server assigned to the scanning computer through policy.

The person performing the scan of remote computers must do so with a user account that is a member of the local administrators group on each remotely scanned computer. This requirement ensures that nefarious third parties cannot use the MBSA tool to determine what vulnerabilities computers might have. The MBSA tool can also be used to locate common administrative vulnerabilities incurred by problematic configuration practices.

You can use the MBSA tool to scan all computers that are members of a specific domain or all computers that are located in a particular IP address range, as shown by Figure 8-8. When scanning computers, ensure that the Check For Security Updates option is configured. Then you need to choose between configuring the scan to use Microsoft Update or the WSUS server that is configured for the computer performing the scan.

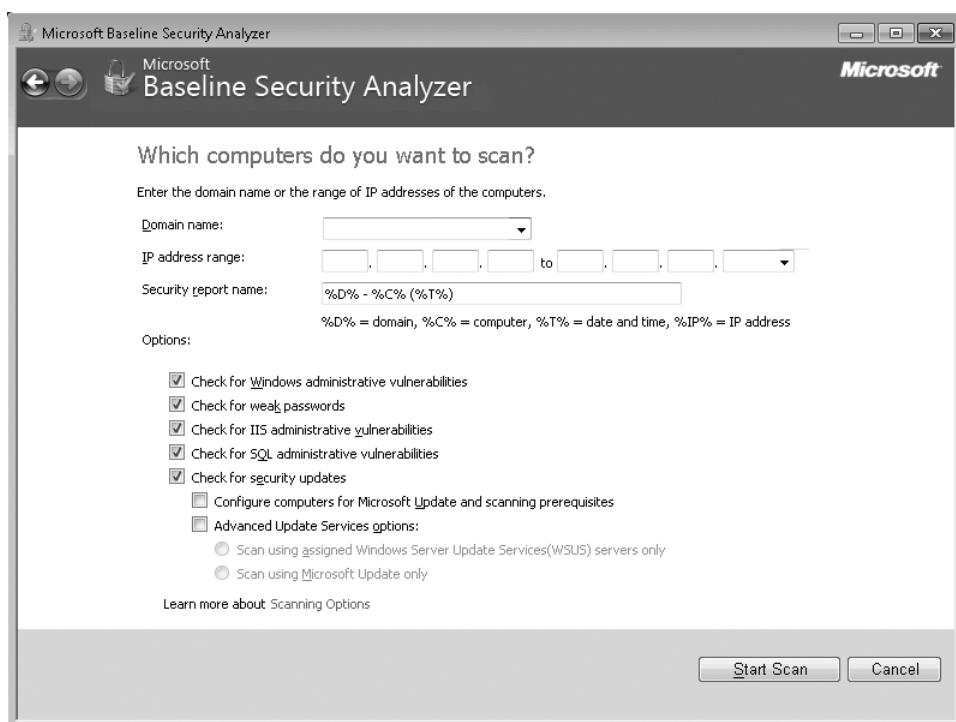


FIGURE 8-8 Scanning multiple computers with the MBSA tool

Keep in mind that only Microsoft Baseline Security Analyzer 2.11 and later are compatible with the Windows 7 operating system. You install and use the Microsoft Baseline Security Analyzer in the practice exercise at the end of this lesson.

#### MORE INFORMATION MICROSOFT BASELINE SECURITY ANALYZER

To learn more about the Microsoft Baseline Security Analyzer, consult the following Microsoft TechNet Web page: <http://technet.microsoft.com/en-us/security/cc184924.aspx>.

## Updating with System Center Configuration Manager

System Center Configuration Manager is a product available from Microsoft that allows for more sophisticated deployment and management of software updates. System Center Configuration Manager allows you to accomplish the following tasks that are not possible with WSUS:

- Allows updates for third-party applications to be deployed to client computers running the Windows 7 operating system.
- Allows update deployment to be scheduled to occur at a specific time rather than at the time the update is approved.
- Allows more flexible control of the distribution of updates.
- Allows use of Wake On LAN feature to wake clients at a specific time for software update deployment.

#### MORE INFO USING SYSTEM CENTER CONFIGURATION MANAGER FOR SOFTWARE UPDATES

To learn more about using SCCM for software updates, consult the following TechNet Web page: <http://technet.microsoft.com/en-us/library/bb633264.aspx>.

---

#### EXAM TIP

Remember what the prerequisites are for using WSUS with BranchCache.

---

## PRACTICE Verifying Update Deployment

---

In this set of exercises, you use different techniques to verify the deployment of updates to client computers running the Windows 7 operating system. Verifying the deployment of updates is an important step in the update deployment cycle. Although you can deploy updates from a WSUS server fairly easily, you cannot be certain that client computers have installed those updates until you perform some type of check.

## EXERCISE 1 Manually Verifying Installed Updates

You can use Windows PowerShell, which is installed by default on computers running the Windows 7 operating system, to generate a list of installed updates. It is also possible to generate a list of updates on remote computers by running this command against a remote computer that is specially configured for remote management through Windows PowerShell. To complete this exercise, perform the following steps.

1. Log on to computer WKSTN1 with the Mark Lee user account.
2. Start a Windows PowerShell session.
3. Enter the command **Get-HotFix**, and then review the results.
4. In the Search Programs And Files text box, type **View Installed Updates**, and then click the View Installed Updates item. Review the list of installed updates, as shown in Figure 8-9.

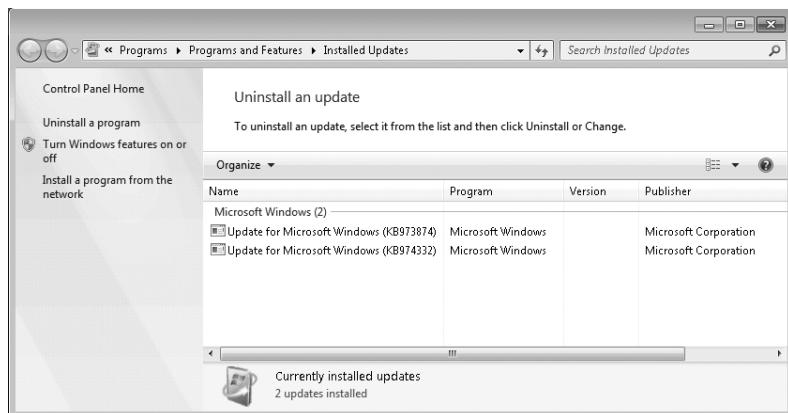


FIGURE 8-9 Installed updates

## EXERCISE 2 Installing and Using Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer allows you to scan a computer to see if it is missing any updates.

1. If you have not done so already, log on to computer WKSTN1 with the Mark Lee user account.
2. Locate the Microsoft Baseline Security Analyzer installation file. Double-click this file to begin the installation. You will receive a security warning informing you that the file has been obtained from the Internet. Click Run to start the installation process.
3. On the Microsoft Baseline Security Analyzer Setup page, click Next.
4. On the License Agreement page, select the I Accept The License Agreement option, and then click Next.

5. On the Destination Folder page, review the default location, and then click Next. On the Start Installation page, click Install. The Microsoft Baseline Security Analyzer begins to install on the computer. You will be presented with another User Account Control dialog box at which you should click Yes. Click OK when you are informed that the Microsoft Baseline Security Analyzer has installed successfully.
6. Double-click the shortcut to the Microsoft Baseline Security Analyzer that has been placed on the desktop by the installation process. At the User Account Control dialog box, click Yes.
7. On the Check Computers For Common Security Misconfigurations page, click Scan A Computer.
8. The default values allow for the local computer to be scanned. Select the Advanced Update Services Options check box and then select the Scan Using Microsoft Update Only option. Then click Start Scan.
9. Review the generated report, and then close the Microsoft Baseline Security Analyzer.

## Lesson Summary

- WSUS is a server role that you can install on a computer running Windows Server 2008 R2. It allows local control over the distribution of software updates.
- WSUS groups allow the deployment of updates to be staggered.
- BranchCache allows Windows 7 Enterprise and Ultimate clients in branch office to share locally cached copies of deployed updates, which means that you do not need to deploy a branch office WSUS server.
- The MBSA tool allows you to scan computers on a network for missing updates.
- System Center Configuration Manager allows you to perform more complex update deployment tasks, such as scheduling update deployment and using Wake On LAN functionality.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, “Designing an Update Management Strategy.” 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. Microsoft releases software updates on the second Tuesday of each month. You want to deploy updates to all computers in your organization within 21 days of the update's release except when an update conflicts with an existing configuration. Prior to general deployment, you want to deploy updates on a group of test computers to determine whether any conflicts become apparent over the course of a week of normal operation. Which of the following strategies should you pursue for update deployment at your organization? (Choose all that apply; each answer forms part of a complete solution.)

  - A. Create a WSUS computer group named TestGroup. Add the computer accounts of the test computers to this group. Deploy software updates to this group by the third Tuesday of each month.
  - B. Create a WSUS computer group named TestGroup. Add all computer accounts to this group. Deploy software updates to this group by the third Tuesday of each month.
  - C. Deploy any software update that did not cause a conflict with the test group of computers to the All Computers WSUS group on the third Tuesday of each month.
  - D. Deploy any software update that did not cause a conflict with the test group of computers to the All Computers WSUS group on the fourth Tuesday of each month.
2. Your organization currently has WSUS 3 SP1 deployed on a computer running Windows Server 2008 in its head office. This computer's name is Updates.Contoso.Internal. You have recently deployed Windows 7 Enterprise to all client computers in your organization. Clients in branch offices currently retrieve updates from the head office WSUS server. There are no Windows Server 2008 R2 servers currently deployed at your organization's branch offices. What steps should you take to take advantage of BranchCache with WSUS to minimize the amount of updates that need to be downloaded across the WAN link? (Choose all that apply; each answer forms part of a complete solution.)

  - A. Upgrade Updates.Contoso.Internal to Windows Server 2008 R2.
  - B. Enable the BranchCache feature on Updates.Contoso.Internal.
  - C. Upgrade WSUS 3 SP1 to WSUS 3 SP2.
  - D. Configure branch office clients to use BranchCache hosted cache mode.
  - E. Configure branch office clients to use BranchCache distributed cache mode.
3. You have recently deployed Windows 7 Professional to all client computers in your organization. Your organization has three branch offices. Each branch office is connected to the head office by a dedicated WAN link. Branch offices do not have a direct connection to the Internet, and all branch office Internet traffic passes through the head office. You have deployed WSUS 3.0 SP1 on a computer with the Windows Server 2008 operating system installed at the head office. You want to optimize the use of WAN link bandwidth to branch offices for software update traffic. Which of the following strategies could you employ?

- A. Upgrade the WSUS server in the head office to WSUS 3.0 SP2.
  - B. Configure clients in branch offices to use BranchCache.
  - C. Deploy WSUS replica servers in each branch office. Configure branch office clients to use the WSUS replicas for updates. Configure the WSUS replicas to download updates from the head office WSUS server.
  - D. Upgrade the WSUS server in the head office to Windows Server 2008 R2.
4. You are in the process of planning the deployment of WSUS at an industrial research organization. The research organization consists of six separate divisions, each of which has its own IT team. You want to minimize the amount of data downloaded from the Microsoft Update servers, but each division's IT team should be delegated the responsibility to approve updates. Which of the following WSUS deployments should you deploy considering the organizational requirements?
- A. Configure six replica servers.
  - B. Configure one upstream server. Configure six downstream servers as replicas of the upstream server.
  - C. Configure one upstream server. Configure six downstream servers as autonomous servers.
  - D. Configure six autonomous servers.

## Lesson 2: Deploying Updates to Clients

---

After an organization has decided on an update infrastructure, you must configure client computers running Windows 7 to access that update infrastructure. The most common way of configuring client computers running Windows 7 to retrieve and install updates in an organizational environment is through Group Policy. Policies allow you to perform many tasks, such as setting the location of the update server, specifying update installation times, and configuring the Windows Update clients to determine whether updates that require a reboot forcibly log a user off or allow a delay until the user finishes his session.

**After this lesson, you will be able to:**

- Configure the automatic updates client.
- Configure Group Policy to support automatic updates.
- Schedule updates and restarts.

**Estimated lesson time: 40 minutes**

# Managing Windows Update Clients

Managing Windows Update clients requires you to ensure that all client computers on your organizational network receive updates. As you learned in Lesson 1, only client computers that are WSUS server clients are present in a WSUS server's reports. Unless you scan all the hosts on the network with a tool like the Microsoft Baseline Security Analyzer, you might be unaware of clients on your network that need updates because they have not checked in with the WSUS server.

Another method through which you can ensure that client computers on the organizational network are receiving and installing updates is to implement Network Access Protection (NAP). When you implement NAP, you can configure the network so that clients that are not up to date with software updates are denied access to network resources. You can also configure NAP to force noncompliant clients into remediation. Remediation is a process that allows clients to access and install update files so that they become compliant with network policies.

## MORE INFO NETWORK ACCESS PROTECTION

To find out more about Network Access Protection, consult the following link on TechNet:  
<http://technet.microsoft.com/en-us/network/bb545879.aspx>.

Prior to connecting a client computer running the Windows 7 operating system to a WSUS server, you might need to update the Windows Update client to the latest version. Clients that connect to a WSUS server are automatically prompted to update to new client software, provided by the WSUS server, if they need to. Figure 8-10 shows an update to the Windows Update client.

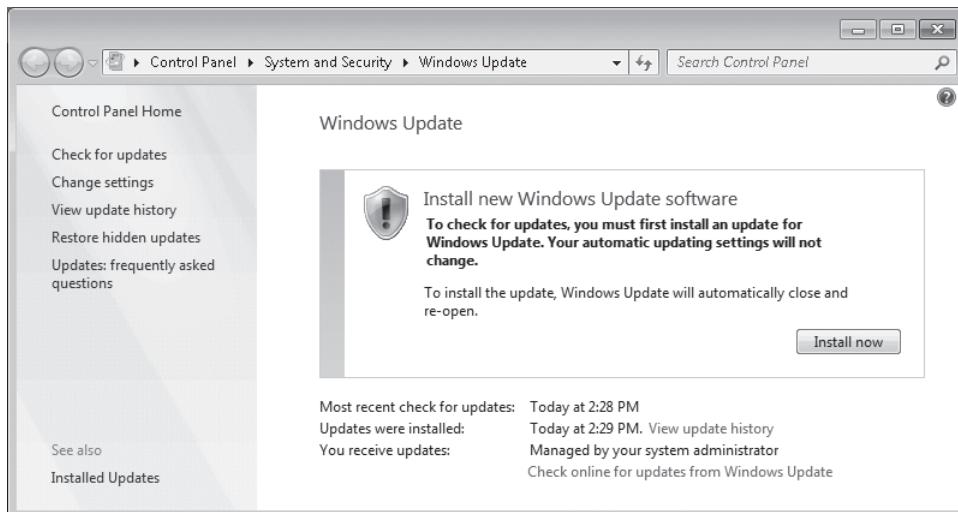


FIGURE 8-10 Updating the Windows Update client

## Configuring Update-Related Group Policy

Except for a few minor settings that can be configured through the Windows Update control panel, the majority of settings related to update deployment for computers running the Windows 7 operating system are configured through Group Policy. The majority of Windows Update-related policies are located in the Computer Configuration\Administrative Templates\Windows Update node of a standard Group Policy object. Some policies, which you learn about later, are also duplicated in the User Configuration node. The policies that are available in the Computer Configuration node are as follows:

- **Configure Automatic Updates** This policy allows you to configure update detection, download, and installation settings. You can configure the following settings using this policy:
  - **Notify for Download And Notify For Install** Logged-on user is notified that updates are available for download and installation.
  - **Auto Download And Notify For Install** Logged-on user is notified that updates have been downloaded and are available for installation.
  - **Auto Download And Schedule The Install** When configured, this setting allows the computer to download the update and then install it at a specific time. This setting is most likely to be used by enterprise desktop administrators. When you choose this setting, you must also specify an installation day and time. The options are to install every day or to install on a specific weekday. You can choose installation times only in full-hour increments.
- **Enabling Windows Update Power Management To Automatically Wake Up The System To Install Scheduled Updates** This policy allows computers with an appropriately configured BIOS to wake from hibernation to install updates. From a deployment perspective, this has the advantage of ensuring that users will not be interrupted in the performance of their work duties because the update installation can be configured to occur in the middle of the night when the computer has been set to hibernate. This policy is effective only if the Configure Automatic Updates policy is configured to schedule installation at a specific time when the target computer is in hibernation. Keep in mind that the computer will not be able to automatically wake from a fully powered-off state, only from a hibernation state.
- **Specify Intranet Microsoft Update Service Location** This policy allows you to configure the location of the local WSUS server. This policy is critically important when you are configuring client computers running Windows 7 to use WSUS rather than Windows Update. You configure this policy in the practice exercise at the end of this lesson.
- **Enable Client-Side Targeting** This policy allows administrators to assign computers to specific WSUS groups. If this policy is used to assign a computer to a WSUS group that does not exist on the WSUS server, the computer is assigned to the Unassigned Computers group.

- **No Auto-Restart With Logged On Users For Scheduled Automatic Updates**  
**Installations** When this policy is configured, Windows waits until the currently logged-on user logs off before attempting to install any updates that require the computer to be restarted. Configure this policy if you want to minimize the disruption caused by update installation when you cannot configure computers to wake from hibernation.
- **Automatic Updates Detection Frequency** This policy determines how often the Windows Update client checks the location configured in the Specify Intranet Microsoft Update Service Location policy. Unless this policy is configured, the Windows Update client checks for updates every 22 hours by default. This policy allows for more frequent checks to be made. You cannot configure update checks to occur less frequently than once every 22 hours.
- **Do Not Display 'Install Updates And Shut Down' Option In Shut Down Windows Dialog Box** When enabled, the Install Updates And Shut Down option on the Start button's Shut Down menu is disabled.
- **Do Not Adjust Default Option To 'Install Updates And Shut Down' In Shut Down Windows Dialog Box** Unless this policy is enabled, if updates are available for installation, the default shutdown option will be 'Install Updates and Shut Down'. If this policy is enabled, the user's last shutdown choice will be the default shutdown option.
- **Allow Non-Administrators To Receive Update Notifications** This policy, when enabled, allows users that are not members of the administrators local group to install updates. If this policy is not enabled, nonadministrator users who attempt to install updates will be prompted by a User Account Control dialog box.
- **Turn On Software Notifications** This policy determines whether users will be notified about the availability of optional updates. In a managed environment, the WSUS administrator controls the deployment of optional updates and this policy is not necessary.
- **Allow Automatic Updates Immediate Installation** When this policy is enabled, any update that does not require a client computer restart is installed automatically.
- **Turn On Recommended Updates Via Automatic Updates** Enabling this policy configures Windows Update to automatically install updates with the Recommended classification.
- **Re-Prompt For Restart With Scheduled Installations** This policy configures the amount of time that a user can postpone a restart when the Configure Automatic Updates policy is set to install updates at a specific time.
- **Delay Restart For Scheduled Installations** This policy determines how long Windows waits before automatically restarting after a scheduled installation.
- **Reschedule Automatic Updates Scheduled Installations** This policy allows you to configure how long a computer waits after startup before it attempts update installation if it was powered off during the scheduled update installation time.
- **Allow Signed Updates From An Internet Microsoft Update Service Location** This policy allows the installation of signed updates from third-party publishers.

Although Windows Update policies are available in both the Computer Configuration and User Configuration nodes of Group Policy, only three policies are available in the User Configuration\Administrative Templates\Windows Update node, all of which are present in the Computer Configuration node. The policies that can be applied to users are as follows:

- Do Not Display 'Install Updates And Shut Down' Option In Shut Down Windows Dialog Box
- Do Not Adjust Default Option To 'Install Updates And Shut Down' In Shut Down Windows Dialog Box
- Remote Access To Use All Windows Update Features



### Quick Check

- Which policy do you configure to have client computers automatically add themselves to WSUS groups?

### Quick Check Answer

- The client-side targeting policy allows you to automatically configure client computers to add themselves to specific WSUS groups.

## Scheduling Deployment and Restart

After you approve an update on a WSUS server, the WSUS server deploys the update to approved clients that contact the WSUS server from that time forward. You cannot use WSUS to schedule an update for deployment at a specific future time. You can configure an update deadline, but an update deadline is a time in the future by which a deployed update must be installed by a Windows Update client. Organizations that need to schedule updates to be deployed at specific times should deploy System Center Configuration Manager. System Center Configuration Manager allows updates to be deployed at specific future times and dates. System Center Configuration Manager also supports Wake On LAN functionality, which allows compatible clients to be wakened from hibernation by the update server for the deployment and installation of updates.

Although you cannot schedule update deployment with WSUS, you can schedule when the Windows Update client on each client computer installs updates. So although you cannot fine-tune when an update will be downloaded from the WSUS server to the client, you can fine-tune when the client will actually attempt to install that update. You can configure this using the Configure Automatic Updates policy and specifying a scheduled install day and install time. Windows Update then always attempts to install any available updates according to this schedule.

## Rolling Back Updates

Occasionally, even with rigorous testing, you might only find out that an update causes a conflict after it has been deployed to all computers in your organization. If the update was deployed with WSUS, you might be able to approve the update for removal, as shown in Figure 8-11. Keep in mind that not all updates support removal. If you cannot roll back the installation of an update through WSUS, you might be able to manually remove the update using a logon script or through the Installed Updates section of the Programs And Features control panel.

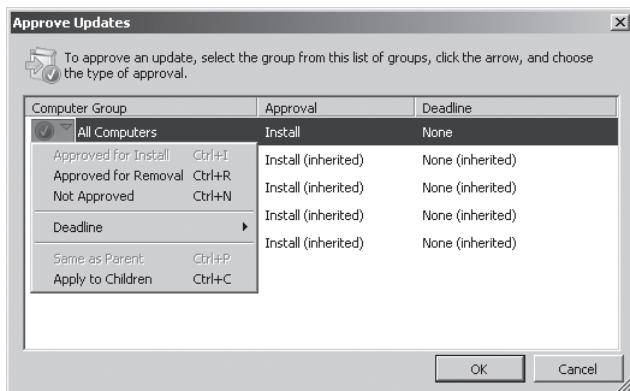


FIGURE 8-11 Update approved for removal



### EXAM TIP

Know which policy you need to configure to point a client computer running the Windows 7 operating system at a local WSUS server.

## PRACTICE Configuring Update-Related Policies

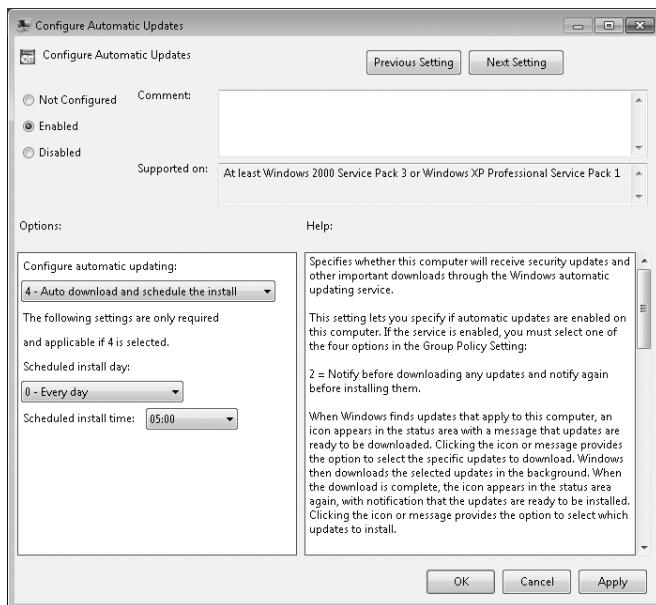
In large organizations, you configure update policy centrally through Group Policy. In this exercise, you configure some of the most common update-related Group Policy items.

### EXERCISE 1 Setting Local Update Policy

In this practice, you configure policy so that the local WSUS server is used for updates, updates are immediately installed, the computer wakes (if it is in a sleep state) to install updates, and the computer does not automatically restart to complete update installation if a user is currently logged on. To complete this practice, perform the following steps:

1. If you have not done so already, log on to computer WKSTN1 with the Mark Lee user account.

2. In the Search Programs And Files text box, type **gpedit.msc**, and then press Enter. The Local Group Policy Editor opens.
3. Navigate to the Computer Configuration\Administrative Templates\Windows Components\Windows Update node.
4. Enable the Configure Automatic Updates policy. Set the policy to Automatically Download And Schedule The Install. Set the Scheduled Install Day to Every Day at 5:00 A.M., as shown in Figure 8-12.



**FIGURE 8-12** Configuring automatic updates

5. Enable the Allow Automatic Updates Immediate Installation policy.
6. Enable the Enabling Windows Update Power Management To Automatically Wake Up The System To Install Scheduled Updates policy.
7. Enable the No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations policy.
8. Edit and enable the Specify Intranet Microsoft Update Service Location policy. Set the policy as shown in Figure 8-13.

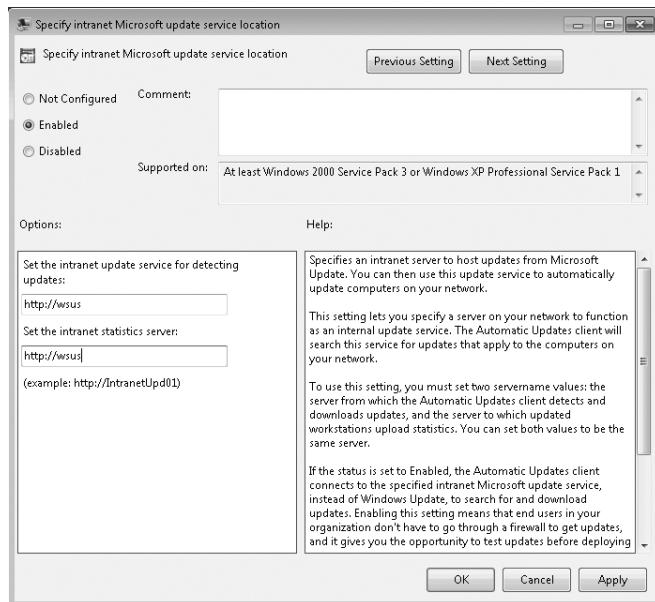


FIGURE 8-13 WSUS server location

9. Close the Local Group Policy Editor.

## Lesson Summary

- The Configure Automatic Updates policy needs to be set to Auto Download And Schedule The Install to ensure that updates are downloaded and automatically installed.
- The Specify Intranet Microsoft Update Service Location policy allows you to specify the location of the local update server.
- The Client-Side Targeting policy allows you to configure WSUS group membership.
- WSUS deployments occur when the update is approved. You can use System Center Configuration Manager to deploy an update at a specific time and date.
- You can configure the Windows Update client to install updates according to a specific schedule, although this will not control when the update is downloaded to the client computer.
- You can roll back some updates from the WSUS console by unapproving them.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Deploying Updates to Clients." 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. A server with Windows Server Update Services 3 SP2 is located on your organization’s head office network. A Group Policy Object (GPO) is applied to an organizational unit (OU) that hosts all of the computer accounts of the computers running Windows 7 in your organization. Which of the following Group Policy policies must you configure to ensure that these computers running Windows 7 receive their updates from the WSUS server rather than directly from Microsoft Update?
  - A. Automatic Updates Detection Frequency
  - B. Enable Client-Side Targeting
  - C. Turn On Recommended Updates Via Automatic Updates
  - D. Specify Intranet Microsoft Update Service Location
2. Security is configured so that only users who have accounts in the ServiceDesk and Domain Admins groups have local administrator privileges on computers running Windows 7 at Contoso. Members of the Sales team have portable computers and are regularly out of the office. Members of the Sales team should be able to install updates without being delegated unnecessary privileges. Which of the following Group Policy policies should the administrators at Contoso configure?
  - A. Configure Automatic Updates
  - B. Allow Non-Administrators To Receive Update Notifications
  - C. No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations
  - D. Allow Signed updates From An Intranet Microsoft Update Service Location
3. Members of your organization’s sales team have laptop computers. When they are on the road, they connect to your organization over the Internet either through a cellular modem card or through hotel Internet connections. You want to minimize the amount of data transmitted over the cellular modem card, but you also want to keep the computers as up to date as possible. You want to minimize the amount of configuration users must perform. Which of the following settings should you choose when configuring the Configure Automatic Updates policy in the GPO that applies to the OU that hosts the sales team’s computer accounts?
  - A. Notify For Download And Notify For Install
  - B. Auto Download And Notify For Install
  - C. Auto Download And Schedule The Install
  - D. Allow Local Admin To Choose Setting

4. Several of the portable computers in your organization use Microsoft Update as a source of operating system and application updates. Which of the following tools can you use to verify that these computers have the most recent software updates installed?
- A. Windows Server Update Services
  - B. GResult.exe
  - C. Microsoft Baseline Security Analyzer
  - D. Oclist.exe

## Chapter Review

---

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

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

## Chapter Summary

- Windows Server Update Services allows administrators to use Internet bandwidth more efficiently and allows them to control which updates are deployed to computers in the organization.
- WSUS groups can be configured so that updates can be deployed to a limited number of clients for testing before being deployed to all computers in the organization.
- BranchCache can be used to make update deployment more efficient in branch office locations.
- Windows Update clients are configured through Group Policy.

## 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.

- BranchCache
- Distributed cache mode
- Hosted cache mode
- Replica mode

## Case Scenarios

In the following case scenarios, you apply what you've learned about subjects of this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Contoso WSUS Upgrade

You are designing an upgrade of the current WSUS infrastructure at Contoso as a part of the company's client operating system migration from Windows XP to Windows 7. Contoso has a head office site and five branch office sites. The branch offices are connected to the head office through a WAN link. Branch offices do not have a direct connection to the Internet. Contoso has an enterprise licensing agreement with Microsoft. You currently manage software updates through computers running Windows Server 2003 with Software Update Services installed. Software Update Services is an earlier version of Windows Server Update Services. Each branch has its own local Software Update Services server. As a part of your update plan, you want to consolidate the existing Software Update Services server by deploying only a single Windows Server Update Services server at the head office location. With this information in mind, answer the following questions:

1. What edition of Windows 7 should you choose for branch offices to minimize update traffic across WAN links when the local branch office SUS servers are retired?
2. What steps should you take in terms of operating system selection and feature installation when deploying the WSUS server at the head office?

### Case Scenario 2: Fabrikam Software Update Policies

You are in the process of configuring policies related to software updates at Fabrikam. All WSUS servers at Fabrikam are hosted on servers running the Windows Server 2008 R2 operating system with the BranchCache feature installed. All client computers are running the Windows 7 Enterprise operating system. Fabrikam's head office is located in Melbourne, Victoria, Australia with branch offices located in the regional cities of Traralgon, Morwell, and Bairnsdale. You want to ensure that computers in the Traralgon office use the WSUS server in Traralgon rather than the Melbourne WSUS server or the Microsoft Update servers on the Internet. Clients in the Morwell and Bairnsdale offices should retrieve updates and approvals from the Melbourne WSUS server but should use WAN bandwidth in the most efficient manner possible. Your other goal is to ensure that users are not logged off when an update requires an operating system restart to complete the installation process. With this information in mind, answer the following questions:

1. Which Group Policy item should you configure for the computers in the Traralgon office?
2. Which Group Policy policies should you configure for clients in the Morwell and Bairnsdale offices?
3. Which policy item should you configure to ensure that users are not forcibly logged off when an update requires a restart to complete the update installation process?

## Suggested Practices

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

### Plan and Manage Software Updates

Perform these practice exercises if you have access to a test server with the Windows Server 2008 R2 operating system installed.

- **Practice 1** Install the WSUS 3.0 SP2 role on a server. Configure the server so that it does not host updates locally.
- **Practice 2** Create a new computer group called TestComputers. Configure WSUS 3.0 SP2 approval rules so that all updates are automatically approved for computers in the TestComputers group but not configured for computers that are not members of this group.
- **Practice 3** Configure the server to support BranchCache with WSUS. Configure local Group Policy on a computer running Windows 7 to support BranchCache distributed cache mode.

### 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 70-686 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.

# Deploying Applications

Applications are as much a part of the Windows 7 client life cycle as the operating system itself and the updates you apply to it. As with virtually all other elements of a desktop deployment, an application deployment strategy should be a part of your planning process from the very beginning. Many of the workstation configuration decisions discussed in earlier chapters must incorporate application requirements into the planning process.

## Exam objectives in this chapter:

- Design a delivery or deployment strategy.
- Manage application compatibility.

## Lessons in this chapter:

- Lesson 1: Designing an Application Deployment Strategy **356**
- Lesson 2: Managing Application Compatibility **369**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- A computer running Windows 7 or Windows Server 2008 R2 on which you have installed Microsoft SQL Server 2008 Express.



### REAL WORLD

Craig Zacker

Although the deployment of applications is treated as a separate chapter in this book, it is actually an integral part of a Windows 7 workstation deployment project. The applications you intend to use on your workstations are as important as the operating system and its updates. The Windows 7 deployment life cycle described in Chapter 1, “Preparing to Deploy Windows 7,” must consider applications throughout its Plan, Deliver, and Operate phases.

# Lesson 1: Designing an Application Deployment Strategy

Deploying Windows 7 to your desktop workstations is a complicated enough task, as you have learned in earlier chapters, but in most cases, workstations require more than the operating system to provide users with the tools they need to do their jobs. The workstations must provide users with access to applications, and administrators provide them with that access by devising an application deployment strategy.

## After this lesson, you will be able to:

- Create a list of user requirements.
- Evaluate application requirements.
- Understand the differences between server-based and client-based applications.
- Select a method for deploying applications.

Estimated lesson time: 60 minutes

## Selecting Applications

The first and most obvious step in devising an application deployment strategy is to decide what applications your users need. This is an essential part of the workstation configuration planning that you perform in the early stages of the Windows 7 deployment project. The primary factor that differentiates one workstation configuration from another is the set of applications the computer has to run. The applications dictate what hardware goes into the computer, what operating system elements you must install, and what security access the computer's users require. If you design your workstation configurations without factoring in application requirements, you are likely to find yourself doing a lot of computer upgrading and retrofitting later.

## Identifying User Requirements

Workstation configurations are based on the tasks that the computer users need to accomplish, and those tasks are made possible by the applications running on the computers. Early in the planning process, you should make a list of the tasks your users perform regularly and begin evaluating applications that are capable of performing these tasks.

Each type of user you are addressing in your deployment project probably has a different set of required tasks. However, this does not mean that you must create a separate workstation configuration and a separate set of applications for each user type. There are two main reasons why this is so:

- **Workstation configuration management** The more workstation configurations you decide to create, the more complicated your workstation deployment and maintenance process becomes. By creating configurations that can satisfy the needs of several user types, you streamline the deployment process.
- **Application bundling** It is often more economical to purchase a suite of applications than to buy individual copies of each application you need. For example, many organizations install an office suite on all of their workstations, even though few if any of their users regularly need all of the applications contained in the suite.

When you have created the initial workstation configurations you plan to deploy, you can compile a list of tasks that each workstation is expected to perform and begin evaluating applications that can perform these tasks. As part of your evaluation process, you of course consider the tasks that each application is capable of performing, but you should also consider the following additional elements:

- **Deployment versatility** Is it possible to deploy the application in various ways? You can install it locally on each workstation, but can you run it from a server? Can you package the application for automated deployment? Can you deploy it using Remote Desktop Services? Can you deploy it virtually using App-V? If you have not yet settled on an application deployment strategy for your workstations, applications with this type of versatility can provide you with valuable options.
- **Compatibility** Is the application capable of running on Windows 7? Are there any known compatibility problems with any of the workstation's other hardware and software components?

#### **MORE INFO COMPATIBILITY TESTING**

For more information on compatibility testing, see Lesson 2, "Managing Application Compatibility," later in this chapter.

- **Interoperability** Are the document files the application produces compatible with the other applications that will run on the workstation?
- **Dependencies** Does the application require any other applications, operating system updates, hardware, or software components to run?
- **Bundling** Is the application available with additional capabilities that could be useful to your users? Is there a choice between a stand-alone version of the application or one bundled with a suite?
- **Economy** What is the cost of the application? Are there discounts available for multiple licenses or site licensing?

## Determining Application Requirements

Virtually all application developers publish the basic system requirements for their products. However, to fully realize the ramifications of adopting a particular application, you must consider all of the other hardware and software components in your workstations.

For example, a developer might recommend that you install a particular application on a computer with one gigabyte of memory, but this recommendation does not account for the various operating system features that you might have enabled on the computer, nor does it account for other applications that the computer might be running at the same time. For example, the manufacturer of an office suite might recommend one gigabyte of memory, but does that mean that one gig is enough to run the word processor, the spreadsheet, and the presentation graphics program all at the same time, or just one of those three?

Manufacturer recommendations also tend not to distinguish between an application that is running comfortably and one that is barely functional. The only way to be sure that an application can run well on a particular workstation configuration is to test it under as realistic conditions as possible, and that means building a test workstation with all of the applications a particular user type needs and running it as that type of user would.

### HARDWARE REQUIREMENTS

When studying the hardware requirements for the applications you are evaluating, consider the following elements:

- **Memory** Always the most important hardware specification, as far as performance is concerned, a workstation configuration should call for sufficient memory to run all of the applications the user typically has open, with representative document files loaded as well.
- **Processor** Processor speed can have a lesser, though still palpable, effect on performance than memory. Certain specialized applications can realize a greater benefit from a faster processor, but in most cases, the processor requirements for Windows 7 are sufficient for most applications.
- **Graphics** In a typical business setting, the standard graphics adapter integrated into most workstation motherboards is sufficient to run most applications. However, there are graphic-intensive applications, such as image and video editing programs, that can benefit from a more specialized graphics adapter.
- **Storage** Many enterprises use network servers for their primary storage, and they configure workstations to store even their user profile data there. However, applications installed locally still require some storage space for their program files and often need additional space for temporary files as well. In most cases, the storage supplied in the average computer is sufficient for a basic workstation configuration. However, if the users routinely work with extremely large files, additional local storage space might be warranted.
- **Network** For most commercially marketed applications, network speed is not a stated requirement. However, in an enterprise workstation deployment, running applications from a server drive is sometimes an option, and the speed of the network can affect the application's performance.

## SOFTWARE PREREQUISITES

Apart from the hardware, the other application requirements you might have to consider are software prerequisites on the workstation. Some applications require specific versions of the Microsoft .NET Framework, and some Web-based applications require specific versions of Windows Internet Explorer.

## Auditing Clients for Application Requirements

After you have finalized your workstation configurations, including the applications you intend to deploy and their requirements, you must make certain that your workstations meet those requirements. For a new computer deployment, this is a matter of purchasing appropriate hardware and properly configuring the operating system installation. However, when deploying Windows 7 to existing workstations, you must ensure that they all have the hardware and software necessary to run the applications you intend to deploy on them.

In Chapter 1, you learned about the various methods for gathering a workstation hardware inventory. If you have Microsoft System Center Configuration Manager (SCCM) 2007 on your network, you can use that to gather hardware inventory information from your workstations. Workstations with the SCCM client installed have a Hardware Inventory Client Agent and Software Inventory Client Agent that report extensive information back to the SCCM server. Administrators can then view the inventory information using the Resource Explorer application, as shown in Figure 9-1.

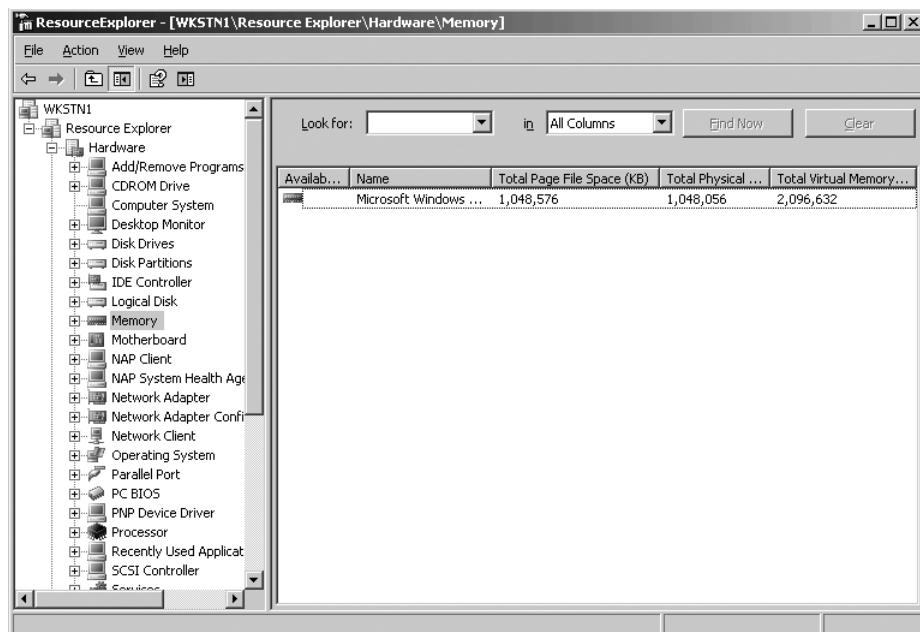


FIGURE 9-1 The SCCM 2007 Resource Explorer

SCCM also enables administrators to generate reports based on specific hardware and software contents. The Asset Intelligence tool can provide detailed reports of critical workstation elements pertinent to software distribution, such as memory installed and available disk space, as shown in Figure 9-2.

(Number of Records: 1)												
Resource ID	Computer Name	Domain/Workgroup	SMS Site Name	Top Console User	Operating System	Service Pack Level	Serial Number	Asset Tag	Memory (KBytes)	Processor (GHz)	Disk Space (MB)	Free Disk Space (MB)
5	WKSTN1	SYSTEMCENTER99	System Center	Unknown	Microsoft Windows 7 Enterprise		None	No Asset Tag	1048056	2660	40643	29335

**FIGURE 9-2** An SCCM 2007 Asset Intelligence report

For enterprises that do not use SCCM 2007, the Microsoft Assessment And Planning Toolkit 5.0 provides a more limited hardware inventory solution, but it has the benefits of requiring no client agent and of being a free download.

#### **MORE INFO USING MAP TOOLKIT**

For more information on the Microsoft Assessment And Planning (MAP) Toolkit 5.0, see Lesson 2, "Gathering Upgrade Information," in Chapter 1.

Without SCCM 2007, auditing software prerequisites is somewhat more problematic. The next best way to ensure that your workstations all receive specific updates is to use Windows Server Update Services (WSUS) and the Windows Update client to deploy specific updates to all of your workstations.

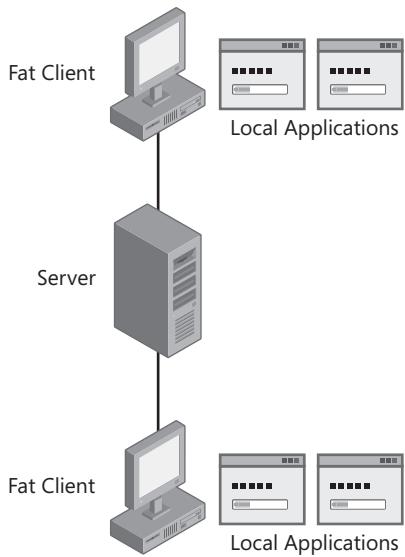
#### **MORE INFO USING WSUS**

For more information on deploying Windows Server Update Services, see Chapter 8, "Planning a Windows 7 Client Update Strategy."

## Deploying Applications

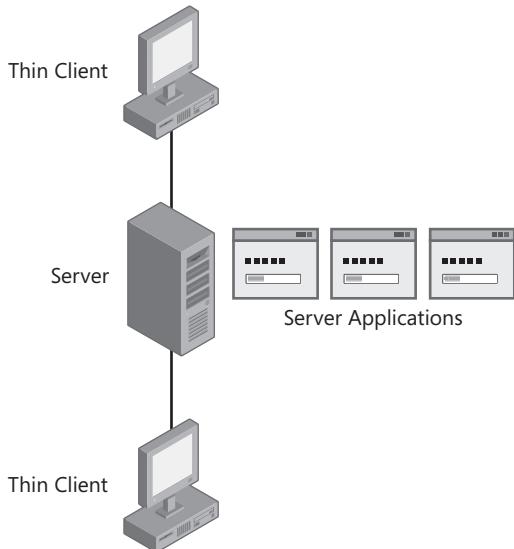
The area with the most flexibility in the planning of your application deployment is the method by which you are going to install and run your workstation applications. Windows 7 and Windows Server 2008 R2 provide a variety of application deployment options, and selecting one is in most cases not a decision you want to leave to the end of the workstation deployment project. How you deploy applications to your workstations and how the workstations run those applications is all part of the fundamental philosophy you want to apply to your network.

To illustrate with widely opposed examples, one enterprise might decide to deploy powerful, fat-client workstations with a lot of memory and large hard disks, so they can deploy all of their applications locally, as shown in Figure 9-3. In this case, the administrators must decide what method they want to use to install the applications on each computer.



**FIGURE 9-3** Fat clients with locally installed applications

In contrast, another enterprise might choose to purchase relatively minimal, thin-client workstations and run the applications on their servers, as shown in Figure 9-4.



**FIGURE 9-4** Thin clients with server-based applications

These opposing scenarios have ramifications that extend far beyond the application deployment process. The fat-client model requires workstations with greater hardware requirements, which makes them more expensive to purchase. The administrators must install all of the applications on each computer individually and maintain them individually as well. By making the clients do most of the work, the servers can be relatively small.

The thin-client model enables the organization to purchase smaller, less expensive workstations, but at the same time, they must provide much larger servers with enough power to run all of the applications for all of the workstation users. The server hardware is much more expensive in this case, but the administrators have to install and maintain only one copy of the applications on each server.

As you can see, virtually every phase of the workstation deployment process is affected by this decision. Workstation hardware, client configuration, server hardware, and software maintenance procedures are just a few of the elements that enterprise administrators must plan with the application deployment process in mind. The following sections describe the application deployment options available to the Windows 7 desktop administrator and the circumstances in which it is most appropriate to use each one.

## Scaling the Application Deployment Process

As with the operating system deployment process, the size of the project is the first element that planners should consider when planning an application deployment. Installing applications on 10 computers is a lot different from installing them on 100, and 100 is very different from 1000. For the most part, the same rule applies to applications as to operating systems: the more workstations you have to install, the more you want to automate the process.

## Using Server-Based Versus Client-Based Applications

The two basic options for deploying applications on Windows 7 workstations are to install them on a server or on the individual workstations. As mentioned earlier, the ramifications of this decision extend throughout the deployment process. To install applications on the clients, you must have workstations with sufficient hardware to run the applications, and you must perform an installation of each application on each computer. In a server-based deployment, you install a single copy of each application on a server and deploy it to the clients using a technology such as Remote Desktop Services.

### INSTALLING APPLICATIONS ON CLIENTS

Client-based deployments require greater workstation hardware expenditures and have more complicated administrative life cycles, but they have distinct advantages as well. Because each workstation has its own copy of the applications, a certain level of performance is guaranteed, based on the local hardware available to run them. A server or network failure might be a temporary inconvenience to the users, but their work can usually continue.

A client-based deployment requires the administrators to run an installation process for each application on each workstation, which can be a complicated undertaking. Maintenance is also complicated because each workstation must receive all updates and configuration changes individually. The amount of trouble this causes depends on the application itself. Microsoft Office, for example, requires frequent updates, but Microsoft Update enables administrators to deploy them along with the regular operating system updates.

Other applications might require administrators to download and evaluate updates and then deploy them to each workstation. This is the type of situation in which a network

management application such as SCCM 2007 can be extremely beneficial. You can use SCCM not only to deploy the applications themselves, but also deliver updates to the workstations automatically, on a schedule determined by the administrators.

### INSTALLING APPLICATIONS ON SERVERS

Server-based application deployments might seem like a much simpler solution than client installations at first, but they too have both advantages and disadvantages. In a server-based deployment, you install the applications on a Windows Server 2008 R2 server with the Remote Desktop Services (RDS) role installed. Client workstations then access the application from the server, using the Remote Desktop client supplied with Windows 7.

Because the application runs on the server, the workstation needs sufficient hardware only to run the client program, which is minimal. Because the server has only one copy of the application that services multiple clients, only one installation is required, and the administrators have to apply updates only once. The deployment process is therefore greatly simplified.

Although convenient for the administrator, deploying applications using RDS increases the burden on the server substantially. A single server might have to maintain application sessions for dozens or hundreds of users at once, which means that the computer needs more and faster processor cores and a lot more memory. Administrators also have to consider the amount of network traffic generated by this application sharing process. The RDS client/server traffic generated by one session is not that much, but when you multiply that by hundreds of clients, the additional strain on the network can be significant.

Running applications on servers also provides a single point of failure. If an RDS server goes down, all of its clients are cut off from their applications. The same is true if a network outage prevents the clients from accessing the servers. There is an economic factor to consider as well. RDS clients require an additional license, which adds to the cost of the operating system.

### MIXING APPLICATIONS

The decision of whether to use server-based or client-based applications is more of a philosophical than a practical one. Both methods are viable solutions, and both have advantages and disadvantages. If you are deploying new workstations into an existing enterprise, you must consider whether your servers and your network are up to the task before you decide on server-based applications. If you are deploying Windows 7 and new applications onto existing workstations, you must determine whether they have the hardware to support the configuration.

There is, of course, no need to deploy all of your applications using one method or the other. You can install some applications locally, while running others from servers. There are frequently economic and licensing issues that affect this decision. For example, you might want to install Microsoft Office on each workstation locally because all of your users need it and automating the deployment of the applications and their subsequent updates is relatively easy. You might also have an application that various users need only occasionally. Rather than installing the application on every workstation and purchasing licenses for everyone, you can deploy it on a server and purchase only enough licenses to support the maximum number of users at any one time.

## Selecting an Application Deployment Method

All of the factors discussed in this lesson so far should contribute to the final decision of how you are going to deploy your selected applications to your workstations. The following sections discuss the options that Windows 7 and Windows Server 2008 R2 make available to you.

### PERFORMING MANUAL INSTALLATIONS

A local—or client-based—installation is one in which you install the application on the workstation’s hard disk. The simplest way to do this is the manual installation method, in which an installer starts the application’s setup program from a CD or DVD or a network drive. As with a manual operating system installation, this is generally the slowest method and the one that requires the most interaction from the installer. For small deployments, however, manual installations might require less time and effort than designing and implementing an elaborate automated deployment.

Another element to consider when evaluating the manual deployment option is how many applications you have to install on each workstation and how complex those installations are. Deploying an office suite that uses one setup program to install five different applications is quicker and easier than installing five separate products, each with its own installation procedure.

For most desktop administrators, the manual installation option is not a practical solution for applications, just as it is not practical for the operating system. There are other ways to deploy applications locally, however.

### USING THICK IMAGES

Chapter 3, “Creating and Managing System Images,” describes three basic types of system images you can create from your reference computers. One of these, the thick image, incorporates all of the applications that you plan to deploy in a particular workstation configuration. By installing and configuring all of the applications on the reference computer prior to capturing an image of it, you eliminate the need for an application deployment process after the operating system deployment.

### USING PACKAGE-BASED DEPLOYMENTS

Package-based deployment methods enable administrators to install applications on workstations with a minimum of interaction. A package is essentially a database file with an .msi extension that contains everything a computer needs to install and run a particular application. Packages contain the application files themselves, as well as registry settings, installation instructions, and other application components. Windows Installer, the installation engine incorporated into Windows 7 and all other Windows versions since Windows 2000, reads the instructions from the package and installs the application on the computer without needing an interactive setup program.

Windows 7 associates the .msi file extension with Windows Installer, so you can simply execute an MSI package manually to begin the installation process. However, you also can automate the deployment of package files, using Group Policy or SCCM 2007.

## **DEPLOYING PACKAGES USING GROUP POLICY**

By creating software installation policies in a Group Policy object and associating them with Active Directory Domain Services (AD DS) domains, sites, or organizational units, you can deploy packages to users or computers throughout the enterprise. Group Policy is a part of AD DS, so this deployment method is free and relatively simple to configure. The primary complication is that, in most cases, applications do not come packaged as .msi files, and administrators must use a third-party product to create the packages. For more information on deploying package files using Group Policy, see Chapter 10, “Using Application Deployment Tools.”

## **DEPLOYING PACKAGES USING SCCM 2007**

Deploying packages to computers throughout an enterprise is the primary function of System Center Configuration Manager. However, although you can use SCCM to deploy the same MSI packages as Group Policy, and with greater flexibility, it has other capabilities as well.

SCCM uses the term “package” to describe a software element that it distributes to clients on the network, but the definition is not the same as the Windows Installer package described earlier. Using SCCM’s Configuration Manager console, you create your own packages that can consist of virtually any materials needed to install software on a client computer. If you have a Windows Installer package in MSI format, you can use SCCM to deploy it, but you can also install an application using the source files, without a third-party packaging utility. For more details on creating and deploying packages using SCCM, see Chapter 10.

As with an operating system deployment, if you already have SCCM on your network, you should definitely use it to perform your local application deployments. The same corollary also holds true: if you do not have SCCM, it is probably not worth installing it just for application deployments. However, when you consider that SCCM can deploy your operating systems, your applications, and the updates for both, many administrators might begin to see it as a viable solution.

## **USING SERVER-BASED RDS DEPLOYMENTS**

If you opt for server-based applications, you have several ways of configuring Remote Desktop Services (RDS), known as Terminal Services in Windows Server 2008 and earlier, is a collection of services that enables administrators to publish individual applications or entire desktops to workstations on the network. By electing to deploy your applications using RDS, you are committing to much greater hardware requirements for your servers, but you eliminate the need for a complex application installation process on the workstations.

The Remote Desktop Connection client is built into all Windows versions, including Windows 7, but the license needed to access an RDS server is not. By selecting this deployment method, you are also committing to the additional expense of an RDS client access license (CAL) for each user that accesses applications from your servers.

Compared to a local workstation deployment, deploying applications on your RDS servers is a relatively simple process. After installing the Remote Desktop Services role, you simply install the application—just once—in the usual manner. The application does not need any special capabilities or configuration; RDS is responsible for the client sharing. If you have a large number of clients and plan to use multiple RDS servers, you can automate the installation of the applications, just as you would for client workstations.

With RDS, the application runs on the server; the only information transmitted to and from the client is that needed for the interface: keystrokes, mouse movements, and display data. The network traffic generated by a single client is therefore minimal, although scale is critical, as with any network application. The traffic for hundreds of clients can conceivably flood a network, just as with any other client/server application.

### USING MICROSOFT APPLICATION VIRTUALIZATION

Microsoft Application Virtualization—also known as App-V—is a technology that enables Windows servers to virtualize applications, much in the way that Hyper-V virtualizes operating systems. With App-V, servers supply applications to a client running on the workstation, and the client executes them locally. However, the client does not install the application first; instead, it runs the application in a virtual environment that is completely isolated from the client operating system.

App-V can cache applications on a workstation for improved performance, but App-V never writes application files to the workstation’s file system, nor does it add settings to the workstation’s registry. The environment in which the application runs is sometimes known as a sandbox because it is isolated from all other applications running on the workstation.

Because App-V runs applications in a virtualized environment, there are no compatibility issues with operating systems or between applications. You can use App-V to deploy applications directly to workstations or to RDS servers, the latter of which makes it possible for a single server to run multiple versions of a single application.

When App-V deploys applications directly to the workstation, the applications run using workstation, not App-V server, resources. When you deploy the applications to RDS, the applications run on the RDS server, which in turn serves them to the Remote Desktop Connection clients on the network.

### PRACTICE Gathering Asset Intelligence with SCCM 2007

---

Because a self-taught student cannot be expected to have access to a System Center Configuration Manager server, the practice for this lesson consists of SCCM videos produced by Microsoft.

#### EXERCISE 1 Viewing a “Using Asset Intelligence” Video

On a Windows computer with Internet access, you can view a video demonstration of the SCCM Asset Intelligence feature.

1. Launch Internet Explorer.

2. In the address box, type <http://go.microsoft.com/fwlink/?LinkId=196897> and press Enter.
3. Click the Play button in the video window to start the clip.

## **EXERCISE 2 Viewing an “Inventory Reporting” Video**

On a Windows computer with Internet access, you can view a video demonstrating how to view the information gathered by the Asset Intelligence feature in SCCM.

1. Launch Internet Explorer.
2. In the address box, type <http://go.microsoft.com/fwlink/?LinkId=196898> and press Enter.
3. Click the Play button in the video window to start the clip.

## **Lesson Summary**

- The primary factor that differentiates one workstation configuration from another is the applications the computer must run. The applications dictate what hardware goes into the computer, what operating system elements you must install, and what security access the computer’s users require.
- When deploying Windows 7 to existing workstations, you must ensure that they all have the hardware and software necessary to run the applications you intend to deploy on them.
- The two basic options for deploying applications on Windows 7 workstations are to install them on a server or on the workstations. To install applications on the clients, you must have workstations with sufficient hardware. In a server-based deployment, you install a single copy of each application on a server, and deploy it using RDS.
- Client-based deployments require greater workstation hardware expenditures and have more complicated administrative life cycles, but because each workstation has its own copy of the applications, a certain level of post-deployment performance is guaranteed.
- In a server-based deployment, you install the applications on a Windows Server 2008 R2 server with the RDS role installed. Client workstations then access the application from the server, using the Remote Desktop client supplied with Windows 7.
- Package-based deployment methods enable administrators to install applications on workstations with a minimum of interaction. A package is a database file that contains everything a computer needs to install and run an application. Windows Installer, the installation engine in Windows 7, reads the instructions from the package and installs the application.

- RDS, known as Terminal Services in Windows Server 2008 and earlier, is a collection of services that enables administrators to publish individual applications or entire desktops to workstations on the network.
- Microsoft Application Virtualization is a technology that enables Windows servers to virtualize applications, much in the way that Hyper-V virtualizes operating systems.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. Which of the following tools can you use to perform an inventory of the applications running on your workstations without having to install a client on each one?
  - A. System Center Configuration Manager
  - B. Application Compatibility Toolkit
  - C. Microsoft Assessment And Planning Toolkit
  - D. Microsoft Application Virtualization
2. Which of the following application deployment methods does not result in an application that runs using workstation hardware resources?
  - A. Remote Desktop Services
  - B. System Center Configuration Manager
  - C. Microsoft Application Virtualization
  - D. Group Policy
3. Which of the following application deployment methods requires the least amount of installation time and interaction at the target workstation?
  - A. Manual installation
  - B. Thick images
  - C. System Center Configuration Manager
  - D. Group Policy
4. Which of the following statements is not true about Microsoft Application Virtualization?
  - A. Microsoft Application Virtualization can deliver applications to desktop workstations or to RDS servers.

- B. Microsoft Application Virtualization requires that a client be installed on each workstation that is to receive applications.
- C. Microsoft Application Virtualization executes applications using workstation hardware resources.
- D. Microsoft Application Virtualization installs applications on the workstation with no interaction from the user.

## Lesson 2: Managing Application Compatibility

One of the largest barriers to the effective deployment of applications in an enterprise is compatibility. Applications must be compatible with the operating systems on which they run, and with each other, to function effectively. When deploying Windows 7—especially onto existing computers—you might discover that applications that ran effectively in the past are not compatible with the new operating system. You might also want to confirm that new applications you are evaluating can run on Windows 7. Microsoft provides a variety of tools that the enterprise administrator can use to screen applications for compatibility problems and locate solutions to those problems.

**After this lesson, you will be able to:**

- Understand the possible causes of application compatibility problems.
- Create an application inventory.
- Remediate compatibility problems.

**Estimated lesson time: 60 minutes**

## Understanding Application Incompatibilities

As part of the planning for a Windows 7 deployment project, you must make sure that the applications your users rely on continue to run on the new operating system. Windows 7 includes some new features that can affect the performance of applications, including the following:

- **User Account Control (UAC)** Although UAC is less intrusive in Windows 7 than it was in Windows Vista, it still affects the way in which applications access administrator privileges, even when using an administrator account. Legacy applications not designed for this behavior can therefore fail to obtain the privileges they need.
- **Data execution prevention (DEP)** DEP is a security mechanism that prevents the computer from executing code stored in a memory region that is flagged as nonexecutable. This is a feature designed to protect against attacks that deliberately attempt to store code in a buffer overflow.

- **Mandatory integrity control (MIC)** MIC is a system security feature (also known as Protected Mode in Internet Explorer) that defines four possible integrity levels for running processes. The integrity level assigned to a process determines what access the process receives to system resources.
- **Session 0 isolation** In Windows versions prior to Windows Vista, system services and the applications launched by the first logged-on user all share the same session, called session 0. Starting in Windows Vista, session 0 is dedicated exclusively to system services; all applications and other user-mode processes run in session 1 or higher. This can prevent legacy applications from communicating with system services in the way they were intended.
- **Folder names** Windows 7 uses different names than Windows XP for some of its default folders. For example, the user profiles that are stored in the Documents And Settings folder in Windows XP are now found in the Users folder in Windows 7. A nonstandard application that calls for specific Windows XP folder names during its installation might fail when it cannot find those folders.

These are just a few of the design changes that can affect the application execution and performance. Because of features like these, legacy applications—especially those designed for Windows XP or earlier—might not run properly on Windows 7. To address these issues, Microsoft provides a number of solutions, some of which are intended for end users and others for enterprise administrators.

## Creating an Application Inventory

In an enterprise environment, the most important compatibility issue is identifying the applications that have problems long before the workstation deployment occurs. In some cases, the only viable solution to a compatibility problem is upgrading the application or selecting an entirely different product. These are not solutions you want to be forced to pursue after you have evaluated, purchased, and deployed an application. Therefore, one of the early steps in your deployment planning process should be to create an inventory of all the applications running on your workstations, so you can test them for compatibility issues with Windows 7.

As with the hardware inventory discussed in Lesson 1 of this chapter, you can choose from a variety of tools to perform an application inventory of your existing workstations, including the following:

- **SCCM 2007** Using its Software Inventory Client Agent and Software Metering Client Agent, SCCM can gather software inventory information from clients, compare the workstation configuration to a database of application hardware requirements, and create extensive, customized reports, as shown in Figure 9-5. As noted elsewhere, SCCM requires an extensive infrastructure, possibly including additional servers for a multisite enterprise.

Copy || Export || Print || Add to Favorites || E-mail

**Report Name:** Software 01A - Summary of installed software in a specific collection

**Category:** Asset Intelligence

**Comment:** This report provides a summary of installed software ordered by the number of instances found from inventory.

Parameters:	Collection	SMS00001
	Specify the number of rows to return.	100
	Publisher (Optional)	

5/24/2010 10:44:04 PM					(Number of Records: 3)
	Product Name	Publisher	Version	Family Name	Category Name
<input checked="" type="checkbox"/>	Microsoft Windows Imaging Application Platform Interface 1.0	Microsoft	1.0.0.0	Operating Environment	Frameworks and S
<input checked="" type="checkbox"/>	Configuration Manager Client	Microsoft Corporation	4.00.6221.1000	Unidentified	Unidentified
<input checked="" type="checkbox"/>	Microsoft Windows 7 Enterprise	Microsoft Corporation	6.1.7600	Unidentified	Unidentified

**FIGURE 9-5** Software reporting in SCCM

- **Asset Inventory Service (AIS)** Available as part of the Microsoft Desktop Optimization Pack (MDOP), AIS uses a Web-based database hosted in the Microsoft datacenters. Client agents installed on each workstation, anywhere in the enterprise, send their software inventory information to the database at scheduled times using their Internet connections. The Microsoft servers then compare the incoming data with a dynamic software catalog and store the resulting information in a SQL Server database. AIS administrators can then access the database as needed to generate reports on software usage.
- **MAP Toolkit 5.0** As part of its agentless inventory process, the MAP Toolkit can identify up to 60,000 applications running on a network's computers and list their version numbers and the number of installed copies it has detected, as shown in Figure 9-6.

The screenshot shows an Excel spreadsheet titled "AppVirtAssessment-07-16-2009-10h13m45s.xlsx - Microsoft Excel". The first sheet is named "Discovered Applications". The data starts with a header row:

Application	Software Version	Number of Installed Copies
Microsoft SQL Server 2008 Database Engine Services	10.0.1600.22	46
Microsoft SQL Server 2008 Common Files	10.0.1600.22	38
Microsoft SQL Server 2008 Database Engine Shared	10.0.1600.22	34
Microsoft SQL Server 2008 Management Studio	10.0.1600.22	32
Microsoft Office Proofing (English) 2007	12.0.4518.1014	29
Microsoft SQL Server 2008 Client Tools	10.0.1600.22	26
Microsoft .NET Framework 3.5 SP1	3.5.30729	25
Microsoft Save as PDF or XPS Add-in for 2007 Microsoft Office programs	12.0.4518.1014	24
Microsoft Office Shared Setup	12.0.4518.1014	19
Metadata MUI (English) 2007		

**FIGURE 9-6** Software reporting in the MAP Toolkit 5.0

These three options are listed in descending order of their cost and their infrastructure requirements. Each one, however, is capable of compiling an inventory of applications running on your workstations. To this inventory, you must then add any new applications that you are planning to deploy on your Windows 7 computers.



### Quick Check

- For a desktop administrator seeking to inventory a fleet of workstations, what is the primary advantage of using the MAP Toolkit, other than the fact that it is free?

### Quick Check Answer

- The primary advantage is that you do not have to install an agent program on each client computer.

## Detecting Incompatibilities

After you have compiled an inventory of the applications that you plan to use on your Windows 7 workstations, you can choose from two basic methods for determining whether they are compatible with the operating system and the workstation configuration. You can consult a list or database of known incompatibilities, or you can test the applications yourself.

### Consulting Internet Resources

For a large enterprise deployment, this should not be an either/or decision; you should do both. It is always a good idea to check outside resources, to reap the benefit of other peoples' experiences. Microsoft maintains an extensive database of compatibility issues, based on their own product testing and on information supplied by other users. The Microsoft Application Compatibility Toolkit (ACT) enables you to collect your own information and compare it with this database. There are also third-party resources available, including the application manufacturers and peer forums.

### Testing for Incompatibilities

The job does not end with Internet research, however. The workstation testing that is part of the deployment's Build stage, both in the lab and in a production deployment, must include all of the applications that the users need, configured and ready for use. The testers must then simulate actual working conditions as closely as possible and perform all of the tasks that the users need to perform. If they encounter any probability problems, they must document the circumstances carefully so that you can reproduce the problem later when you are evaluating solutions.

The Application Compatibility Toolkit contains a variety of tools that can help you in the process of testing for application incompatibilities. For more information, see "Using the Application Compatibility Toolkit," later in this lesson.

# Evaluating Application Incompatibility Solutions

When you discover a compatibility issue between an application and Windows 7 or between applications, you can choose from a number of ways to address the problem. The most obvious solution is simply not to use the application. You can try to obtain a patch or an updated version from the manufacturer, or you can seek out a competing application from another manufacturer. However, before you switch products, you might want to try some of the solutions in the following sections.

## Using Compatibility Modes

It is not unusual for older, legacy applications to have difficulty running on Windows 7. This is especially true for applications designed for Windows XP and earlier versions. To address these incompatibilities in a manner that is understandable to nearly all end users, Windows 7 provides a series of compatibility modes. A compatibility mode is a set of routines that enables Windows 7 to emulate an earlier Windows version.

For example, if you install an application that was designed for the original Windows XP release and it does not run in Windows 7, you can open the Properties sheet for the application's executable file and select the Compatibility tab, as shown in Figure 9-7.

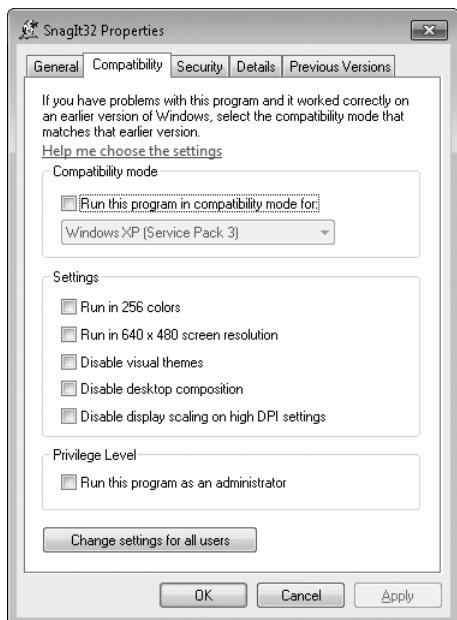


FIGURE 9-7 The Compatibility tab of an executable's Properties sheet

On the Compatibility tab, selecting the Run The Program In Compatibility Mode check box enables you to select one of the following compatibility modes, corresponding to the various Windows and service pack releases:

- Windows 95
- Windows 98 / Windows Me
- Windows NT 4.0 (Service Pack 5)
- Windows 2000
- Windows XP (Service Pack 2)
- Windows XP (Service Pack 3)
- Windows Server 2003 (Service Pack 1)
- Windows Server 2008 (Service Pack 1)
- Windows Vista
- Windows Vista (Service Pack 1)
- Windows Vista (Service Pack 2)

**CAUTION EMULATED, NOT IMITATED**

Configuring an executable file with a compatibility mode does not guarantee that the application will run. Compatibility modes provide some of the fundamental characteristics of the earlier operating systems, but they do not emulate them in every way.

In addition to the operating system emulations, the compatibility tab also enables you to configure the following settings:

- **Run In 256 Colors** Configures the program to run with a limited color depth
- **Run In 640 x 480 Screen Resolution** Configures the program to run with a limited screen resolution
- **Disable Visual Themes** Disables display modes that can interfere with the program's interface
- **Disable Desktop Composition** Disables window transparency and other Aero display features while the application is running
- **Disable Display Scaling On High DPI Images** Disables application resizing because of large font sizes
- **Run This Program As An Administrator** Executes the program with elevated privileges

After you select settings on the Compatibility tab, the system retains them for the current user. If you also click the Change Settings For All Users button, the system applies the same settings to all users logging on to the computer.

## USING THE PROGRAM COMPATIBILITY TROUBLESHOOTER

For end users that are not conversant with compatibility and emulation issues, Windows 7 includes the Program Compatibility Troubleshooter, which is a wizard-based tool that steps users through the process of identifying the compatibility problems affecting an application. When you right-click an executable and select Troubleshoot Compatibility from the context menu, the Program Compatibility troubleshooter appears, as shown in Figure 9-8.

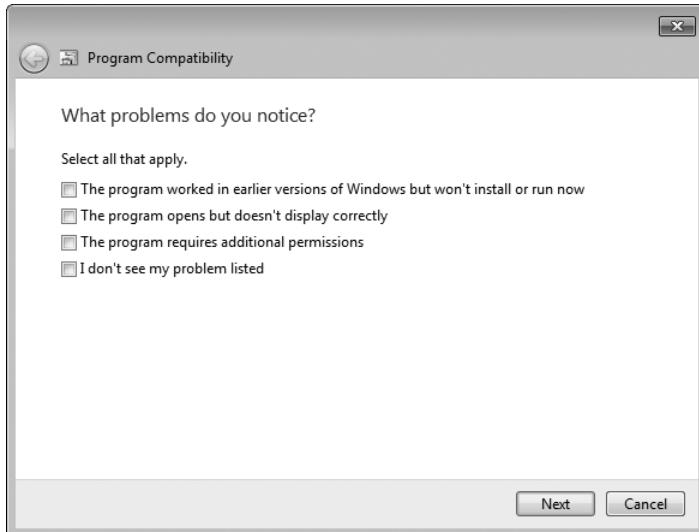


FIGURE 9-8 The Program Compatibility troubleshooter

By prompting the user to answer a series of questions, the troubleshooter isolates the problem and suggests compatibility mode settings that might solve the problem.

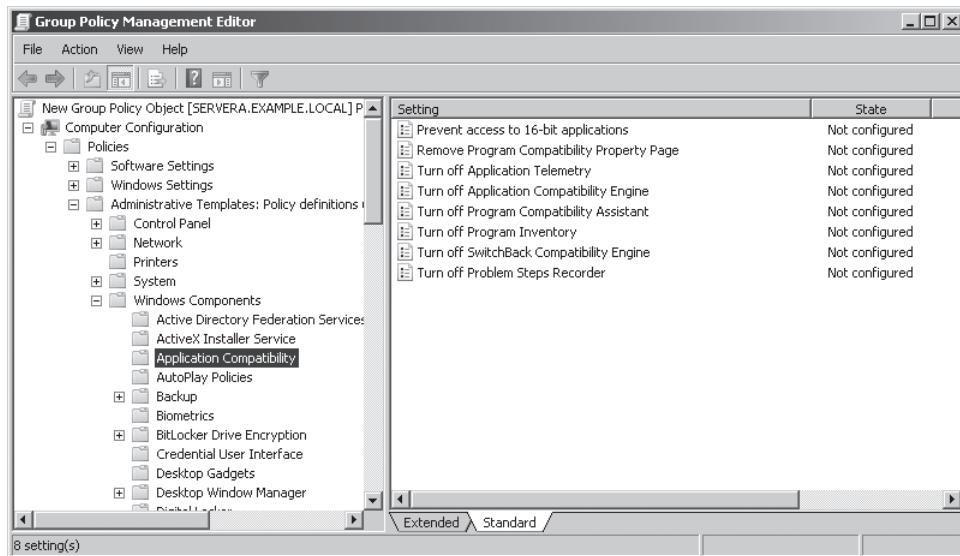
## SUPPRESSING COMPATIBILITY CONTROLS USING GROUP POLICY

In an enterprise environment, administrators often take charge of compatibility issues themselves and do not want or need end users modifying the Windows 7 compatibility settings. In that case, administrators can suppress the appearance of the compatibility controls in Windows 7 using Group Policy settings.

In the Computer Configuration\Policies\Administrative Templates\Windows Components\Application Compatibility folder of a Group Policy object, as shown in Figure 9-9, the following policy settings limit access to the Windows 7 compatibility controls:

- **Remove Program Compatibility Property Page** When enabled, removes the Compatibility tab from the Properties sheets of executables and shortcuts
- **Turn off Program Compatibility Assistant** When enabled, disables the Program Compatibility Assistant, preventing the computer from displaying compatibility warnings during application installations and start-ups

- **Turn off Application Compatibility Engine** When enabled, prevents the computer from looking up applications in the compatibility database, boosting system performance but possibly affecting the execution of legacy applications



**FIGURE 9-9** Application Compatibility Group Policy settings

These policy settings can effectively disable the end user's ability to resolve compatibility problems, so administrators must be sure that they have already addressed all such problems in the workstation configuration before enabling them.



#### EXAM TIP

When studying Windows 7 configuration settings, be sure to familiarize yourself with their Group Policy equivalents.

## Using Compatibility Fixes

Although Windows 7 includes a collection of generic compatibility modes for older Windows versions, they cannot address all possible application compatibility problems. What's more, many administrators do not want to leave end users to resolve compatibility problems or be forced to configure compatibility modes on individual workstations.

However, some incompatible applications require a solution that is customized for that particular piece of software. A compatibility mode is a collection of compatibility fixes. A compatibility fix—also called a shim—is a software routine that rests between an application and the operating system. For example, when a Windows XP application makes a function call to the operating system—that is, when it asks the operating system to provide a service, such as access to the file system—the compatibility fix translates the call, making it appear to the application that it is running on a Windows XP system.

To locate known compatibility fixes for specific applications or create new ones, you use the Microsoft Application Compatibility Toolkit, as discussed later in this lesson. The ACT is a collection of tools that enables administrators to take full control of workstation compatibility issues.

## Using Remote Desktop Services

When you deploy an application to a Windows 7 computer using RDS, the application is not really running on Windows 7; it is running on the RDS server. Therefore, if the application has a compatibility issue with Windows 7, but it runs properly on the server operating system, you can avoid the problem by deploying the application with RDS.

Using RDS can also prevent you from having to configure a compatibility mode or install a compatibility fix on all of your workstations. You can patch the application after it's on the server, and all of the RDS client sessions will run the patched version.

## Virtualizing Applications

Virtualizing applications using Microsoft Application Virtualization (App-V) also can eliminate compatibility problems. Because App-V isolates each application in its own sandbox, there is no way that applications can conflict with each other. Virtualization even makes it possible to run two different versions of the same application, something you typically cannot do in a standard environment.

One of the longstanding problems with RDS (and Terminal Services before it) occurs when a network has workstations running different versions of Windows, and therefore needs to provide clients with different versions of an application. A single RDS server cannot, in most cases, have two versions of the same application installed at the same time, so it has always been that the only way to serve two versions of the application to clients was to run them on separate RDS servers. Now, however, App-V can run the two versions on the same server in virtualized sandboxes, enabling RDS to serve the application to all of the clients.

For more information on virtualizing desktops and applications using RDS, see Chapter 10.

## Using Windows XP Mode

The ultimate solution for a Windows XP application that absolutely will not run on Windows 7 is to use Windows XP Mode, a Windows 7 feature that creates a virtual Windows XP system on a workstation. Because the application is running in a true Windows XP environment, not in an emulation, there can be no incompatibilities with Windows 7.

Windows XP is essentially a virtual machine running in the Microsoft Virtual PC environment. You must download and install Virtual PC, as well as the Windows XP Mode files, available at <http://www.microsoft.com/windows/virtual-pc/download.aspx>. Because it is a virtual machine implementation, Windows XP Mode requires a processor and BIOS that support hardware virtualization, as well as additional memory. The workstation is also likely to experience some performance degradation as a result of the additional overhead. You should consider Windows XP Mode to be a last resort and use it for applications you can't run any other way.

## Using the Application Compatibility Toolkit

Application Compatibility Toolkit 5.6 is a collection of programs that enable administrators to gather information about the applications and devices on a network and assess their compatibility with Windows 7 and other components. The product is available as a free download from Microsoft at <http://www.microsoft.com/downloads/details.aspx?familyid=24DA89E9-B581-47B0-B45E-492DD6DA2971&displaylang=en>. You can install ACT on a Windows server or workstation, but the toolkit requires access to a SQL Server database, where it stores its data.

### **NOTE USING SQL SERVER**

ACT 5.6 can use SQL Server 2008 or SQL Server 2005 (with the latest service pack), in either a commercial edition or the Express edition, which is available as a free download. SQL Server 2008 Express Edition is available at <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=01af61e6-2f63-4291-bcad-fd500f6027ff>.

The ACT package includes the following components:

- Application Compatibility Manager
- Compatibility Administrator
- Internet Explorer Compatibility Test Tool
- Setup Analysis Tool
- Standard User Analyzer

These components are described in the following sections.

### Application Compatibility Manager

Application Compatibility Manager, shown in Figure 9-10, is the primary tool for enterprise administrators planning a large-scale deployment. This application enables you to gather information from your workstations and research potential compatibility issues, using Microsoft online resources. The workflow for this process proceeds as described in the following sections.

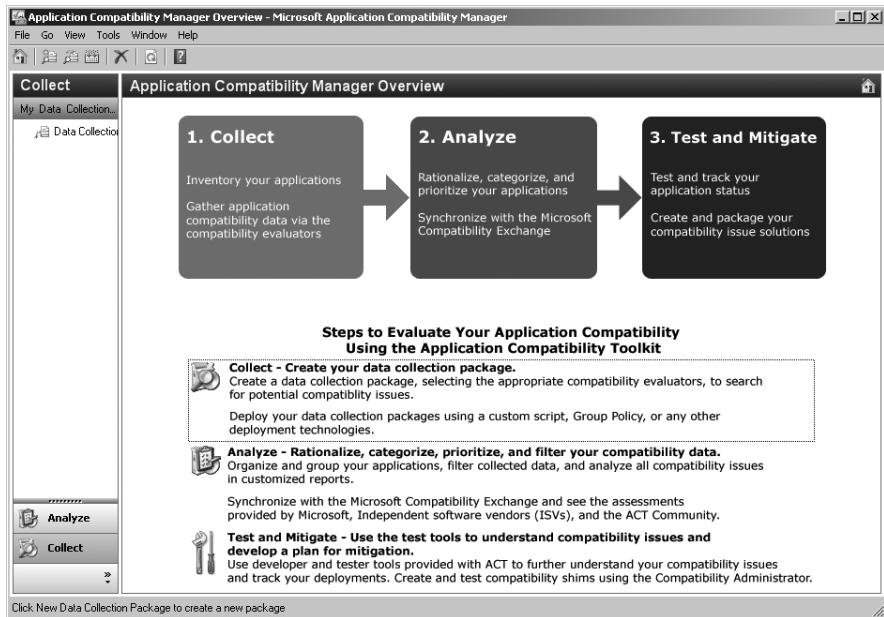


FIGURE 9-10 Application Compatibility Manager

## COLLECT

The collection phase requires that you use Application Compatibility Manager to create data collection packages (DCPs). DCPs are agents that you deploy to your workstations as Windows Installer (MSI) files. A DCP can contain any of the following components, called compatibility evaluators:

- **Inventory Collector** Gathers general information about the system and all of the applications installed on it. It's included in all DCPs.
- **User Account Control Compatibility Evaluator** Checks the workstation for compatibility issues because of the limited access provided by User Account Control.
- **Windows Compatibility Evaluator** Checks the workstation for compatibility issues because of session 0 isolation, authentication problems, and deprecated operating system components.
- **Update Compatibility Evaluator** Registers the effect of installing Windows updates on the workstation.

The compatibility evaluators, running on your workstations, compile information in log files, which they upload to an ACT Log Processing Share. The ACT Log Processing Service then processes the client log files and adds the information to the ACT database. Depending on the size of the network, you can place the Application Compatibility Manager application, the Log Processing Share, the Log Processing Service, and the SQL Server database on different computers, or you can run them all on the same system.

### **ANALYZE**

After you have the data you collected in the ACT database, you can begin to analyze it, a process that typically starts with organizing the applications into categories and establishing deployment priorities, based on your organization's needs. You can then compare your collected data with that in the Microsoft Compatibility Exchange. This provides you with access to information about compatibility issues experienced by other people, including Microsoft testers, application developers, and other enterprise administrators. You can then use Application Compatibility Manager to create detailed reports containing the data you have compiled.

### **TEST AND MITIGATE**

With the information gathering and analysis phases completed, you can begin the process of testing your applications to determine whether any of the compatibility problems you have discovered exist on your network. ACT provides a variety of tools and documentation that you can use to construct a compatibility lab and establish a testing regimen.

The final phase of the process, assuming that you have identified any application compatibility issues on your network, is to mitigate them. You do this by using the Compatibility Administrator program to locate appropriate compatibility fixes or compatibility modes, or even create your own fixes or modes.

## **Compatibility Administrator**

The Microsoft Compatibility Exchange is a source for information on application compatibility problems and their possible solutions, which Microsoft maintains and updates on a regular basis. To access this resource, you use the Compatibility Administrator application, which is included in the ACT in 32-bit and 64-bit versions. When you open the application, as shown in Figure 9-11, you can browse through a list of hundreds of applications in the left pane, and see the available compatibility fixes for the selected application on the right.

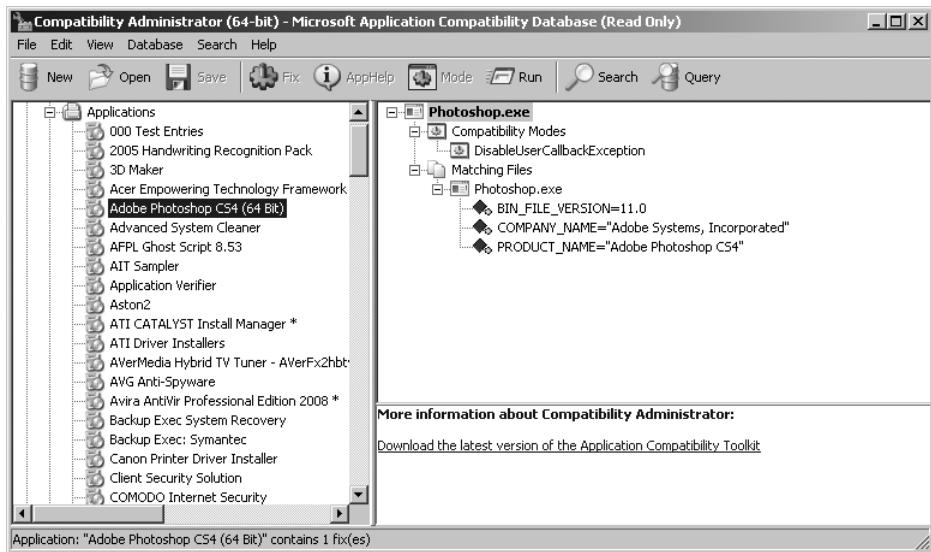


FIGURE 9-11 Compatibility Administrator

## Internet Explorer Compatibility Test Tool

As Web-based applications become increasingly more complicated, they also become increasingly likely to experience compatibility issues. To isolate these issues, it is not enough to test the browser application itself; you must also test the specific Web sites that your users need to access. ACT includes a program called the Internet Explorer Compatibility Test Tool that enables you to scan Web pages and applications in real time.

When you run the program and click the Enable button, the tool begins to monitor all of your browser activities, as you access the sites you want to test. By performing all of the functions the Web application offers, you can gather a complete debugging log in the tool's Live Data window, as shown in Figure 9-12.

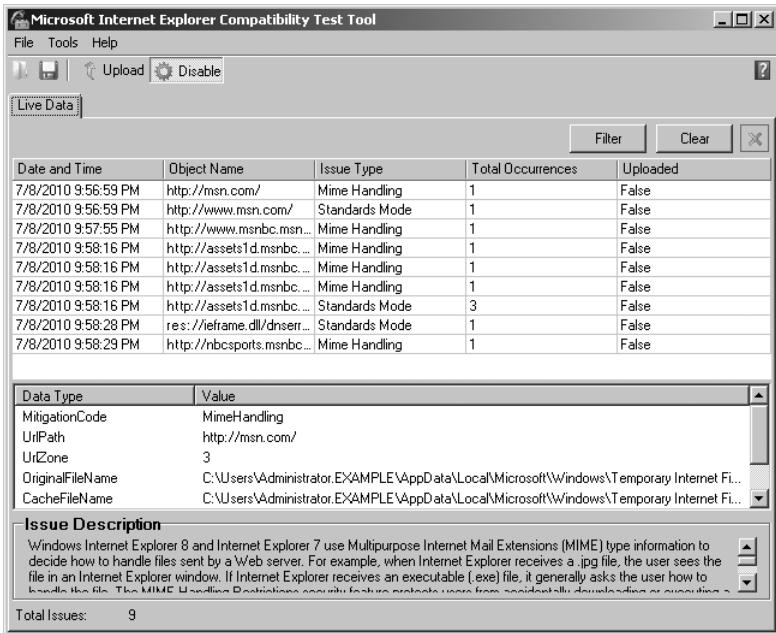


FIGURE 9-12 Internet Explorer Compatibility Test Tool

## Standard User Analyzer

As mentioned earlier in this chapter, UAC is a common source of compatibility issues because applications designed for previous versions of Windows might not receive the access they require to run. ACT includes a tool, primarily intended for application developers, that tests for these issues, much in the same way that the Internet Explorer Compatibility Test Tools examine Web-based applications.

The Standard User Analyzer, using a wizard-based or manual format, executes an application you select, and as you access the application's various functions, the analyzer displays its activities in real time, as shown in Figure 9-13, and stores them in a log.

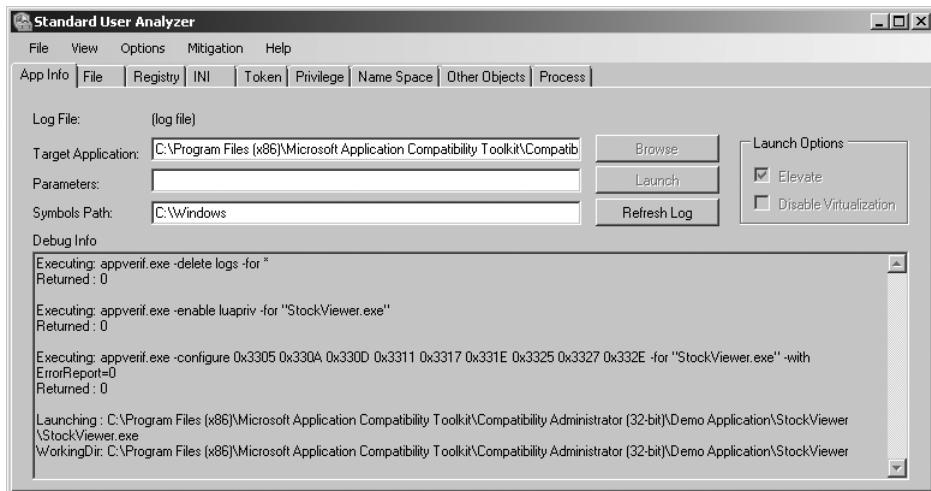


FIGURE 9-13 Standard User Analyzer

## Setup Analysis Tool

Also designed primarily for application developers, the Setup Analysis Tool in the ACT can detect potential compatibility issues in setup programs, including the following:

- Installation of kernel mode drivers
- Installation of 16-bit components
- Installation of Graphical Identification and Authentication (GINA) DLLs
- Changes of files or registry keys that are under Windows Resource Protection (WRP)

### PRACTICE Installing and Configuring the Application Compatibility Toolkit

ACT is the primary tool for administrators seeking to research compatibility problems in preparation for a large-scale Windows 7 workstation deployment. Version 5.6 of the package now includes a sample Stock Viewer application that you can use to test some of the included tools.

## **EXERCISE 1** Installing ACT 5.6

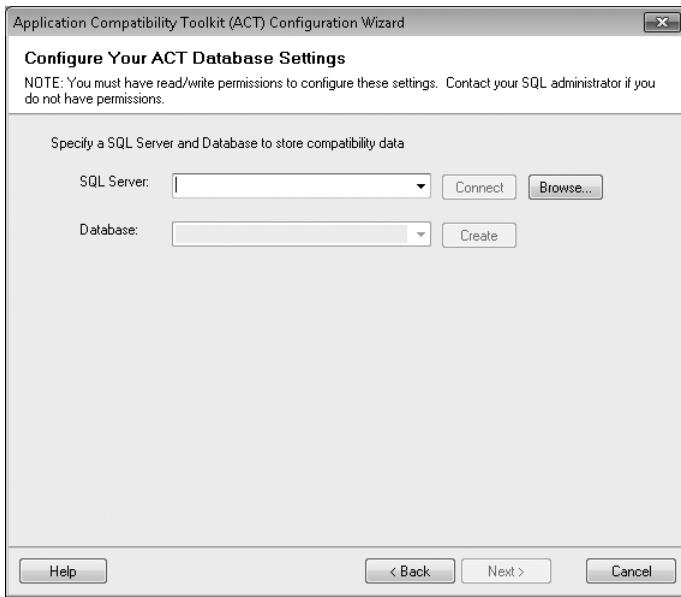
ACT is available as a free download from Microsoft Download Center.

1. Launch Internet Explorer.
2. In a browser window, in the address box, type the following URL and press Enter:  
<http://www.microsoft.com/downloads/details.aspx?familyid=24DA89E9-B581-47B0-B45E-492DD6DA2971&displaylang=en>.
3. Download the ApplicationCompatibilityToolkitSetup.exe file and save it to a folder on your computer.
4. Double-click the ApplicationCompatibilityToolkitSetup.exe file to execute it. The Microsoft Application Compatibility Toolkit 5.6 Setup Wizard appears, displaying the Welcome page.
5. Click Next. The End-User License Agreement page appears.
6. Select the I Accept The Terms In The License Agreement check box and click Next. The Destination Folder page appears.
7. Click Next to accept the default folder name. The Ready To Install Microsoft Application Compatibility Toolkit 5.6 page appears.
8. Click Install. The wizard installs the toolkit and displays the Completed page.
9. Click Finish. The wizard closes.

## **EXERCISE 2** Configuring ACT 5.6

Before you can use the Application Compatibility Manager application, you must configure it to use a SQL Server database.

1. Click Start. Then click All Programs | Microsoft Application Compatibility Toolkit | Application Compatibility Manager. The Microsoft Application Compatibility Manager window appears and launches the Microsoft Application Compatibility Toolkit (ACT) Configuration Wizard.
2. Click Next to bypass the Welcome page. The Select The Configuration Option page appears.
3. Leave the Enterprise Configuration option selected and click Next. The Configure Your ACT Database Settings page appears, as shown in Figure 9-14.



**FIGURE 9-14** The Configure Your ACT Database Settings page

4. In the SQL Server drop-down list, select your computer and click Connect.
5. In the Database text box, type **ACT** and click Create. The wizard creates a new database instance.
6. Click Next. The Configure Your Log File Location page appears.
7. In the Path text box, browse to a folder on your computer. Click Next to accept the default Share As value. The Configure Your ACT Log Processing Service Account page appears.
8. Click Next to accept the default Local System option. The Congratulations page appears.
9. Click Finish. The Microsoft Application Compatibility Monitor console appears.

## Lesson Summary

- Windows 7 includes some new features that can affect the performance of applications, including User Account Control (UAC), data execution prevention (DEP), mandatory integrity control (MIC), and session 0 isolation.
- One of the early steps in your deployment planning process should be to create an inventory of all the applications running on your workstations, so you can test them for compatibility issues with Windows 7.
- There are two basic methods for determining whether applications are compatible with Windows 7. You can consult a list or database of known incompatibilities, or you can test the applications yourself.
- Some incompatible applications require a solution that is customized for that particular piece of software. A compatibility fix—also called a shim—is a software routine that rests between an application and the operating system.
- Virtualizing applications using Microsoft Application Virtualization also can eliminate compatibility problems. Because App-V isolates each application in its own sandbox, there is no way that applications can conflict with each other.
- Application Compatibility Toolkit 5.6 is a collection of programs that enable administrators to gather information about the applications and devices on a network and assess their compatibility with Windows 7 and other components.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. Which of the following compatibility solutions is intended for use by end users?
  - A. Internet Explorer Compatibility Test Tool
  - B. App-V
  - C. Program Compatibility Troubleshooter
  - D. Shims

2. Which of the following tools in the Application Compatibility Toolkit do you use to create data-collection packages?
  - A. Compatibility Administrator
  - B. Application Compatibility Manager
  - C. Standard User Analyzer
  - D. Setup Analysis Tool
3. Which of the following application inventory tools is part of the Microsoft Desktop Optimization Pack?
  - A. Software Metering Client Agent
  - B. Microsoft Assessment And Planning Toolkit
  - C. Software Inventory Client Agent
  - D. Asset Inventory Service

## Chapter Review

---

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

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

## Chapter Summary

- An application deployment strategy specifies what applications users need, what system requirements the applications need, and how you plan to provide users with access to those applications.
- Windows 7 includes features that can affect the performance of applications, including User Account Control (UAC), data execution prevention (DEP), mandatory integrity control (MIC), and session 0 isolation. One of the early steps in your deployment planning process should be to create an inventory of all the applications running on your workstations, so you can test them for compatibility issues with Windows 7.

## 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.

- App-V
- compatibility fix
- compatibility mode
- Microsoft Application Virtualization
- package (Windows Installer)
- package (System Center Configuration Manager)
- Remote Desktop Services (RDS)
- sandbox
- shim
- Windows Installer

## Case Scenarios

In the following case scenario, you will apply what you've learned about subjects of this chapter. You can find answers to the scenario questions in the "Answers" section at the end of this book.

### Case Scenario 1: Planning an Application Deployment

Howard is in the planning stage of a deployment project in which he will install Windows 7 on 100 workstations in the Customer Service department of his company. The workstations are currently running Windows XP, with a customized call tracking database application. The workstations, as they are currently configured, just barely meet the Windows 7 hardware requirements, and Howard does not want to have to perform hardware upgrades. The database application has its own requirements, which call for more memory and a faster processor than the workstations currently have. Which of the application deployment strategies discussed in this chapter yields the best performance from the workstations? Explain your answer.

### Case Scenario 2: Deploying Packages

Richard wants to deploy an application to the workstations on his company network by distributing a package file using Group Policy. However, the application disk does not contain a Windows Installer package (MSI) file. After doing some research on the Internet, Richard discovers that he must use a third-party product to create a package file containing his application.

Taking his application disk with him, along with a laptop that has the application installed on it, Richard travels across town to his friend Ben's office. Ben has System Center Configuration Manager 2007 installed on his network, which Richard has learned can create packages.

Ben is busy elsewhere in the office so using the SCCM Configuration Manager console and its help files, Richard follows the procedure for creating a package containing his application. However, when he looks at the folder that he designated as the destination for the package, he cannot find an MSI file. Why has SCCM Configuration Manager failed to create an MSI file, and what can Richard do to create a file he can deploy using Group Policy?

## Suggested Practices

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

### Designing an Application Deployment Strategy

- **Practice 1** Using Internet Explorer, browse to the home page for Microsoft Application Virtualization at <http://www.microsoft.com/systemcenter/appv/default.mspx> and examine the capabilities of this technology.
- **Practice 2** Using a search engine, locate three third-party products that can create Windows Installer package (MSI) files and examine their capabilities.

### Maintaining Application Compatibility

- **Practice 1** Using the Windows 7 computer where you have installed ACT, run the Internet Explorer Compatibility Test Tool, click Enable, and use Internet Explorer to visit some of your favorite Web sites. Then examine the information captured by the tool.
- **Practice 2** Using the Windows 7 computer where you have installed ACT, run the Standard User Analyzer and use it to launch the StockViewer.exe demonstration application provided with ACT. Test all of the application's functions and examine the information captured by the tool.

## 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 70-686 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.



# Using Application Deployment Tools

In Chapter 9, “Deploying Applications,” you learned about the various application deployment technologies that Windows 7 and Windows Server 2008 R2 provide. In this chapter, you learn more about the actual process of deploying applications using these technologies.

## Exam objectives in this chapter:

- Design a delivery or deployment strategy.

## Lessons in this chapter:

- Lesson 1: Deploying Applications Using Group Policy and SCCM 2007 **392**
- Lesson 2: Deploying Applications Using RDS **416**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- A computer running Windows Server 2008 R2, which you have configured as an Active Directory Domain Services (AD DS) domain controller, and on which you have installed the Remote Desktop Services (RDS) role with the Remote Desktop Session Host and Remote Desktop Web Access role services.
- The Microsoft Deployment Toolkit 2010 installation file (MicrosoftDeploymentToolkit2010\_x64.msi or MicrosoftDeploymentToolkit2010\_x86.msi) that you downloaded in the practice for Chapter 3, “Creating and Managing System Images,” or any Windows Installer package file with an MSI extension.



## REAL WORLD

Craig Zacker

Economic factors are often the decisive element in network design decisions, and when it comes to application deployment for large enterprises, Group Policy is the tool that nearly everyone already owns. System Center Configuration Manager (SCCM) 2007 requires a substantial investment of time and effort as well as money. The required server infrastructure, coupled with the client license fees, can often be far too expensive to justify the product's usefulness.

The Remote Desktop Services software, client and server, is included with the Windows operating systems, but RDS also requires a license for each client computer. However, the most difficult part of the economic equation is comparing the workstation hardware requirements for a local application deployment with the server hardware you need to use RDS for your applications.

## Lesson 1: Deploying Applications Using Group Policy and SCCM 2007

Deploying Windows 7 to your desktop workstations is a complicated enough task, as you have learned in earlier chapters, but in most cases, workstations require more than the operating system to provide users with the tools they need to do their jobs. The workstations must provide users with access to applications, and administrators provide them with that access by devising an application deployment strategy.

**After this lesson, you will be able to:**

- Deploy applications using Group Policy Software Installation.
- Deploy applications using SCCM 2007.

**Estimated lesson time: 60 minutes**

# Deploying Applications Using Group Policy

Deploying applications using Group Policy has the advantage of requiring no special infrastructure beyond that of AD DS, which most enterprise networks already have. When compared to a manual installation of an application on a workstation, Group Policy deployment provides users with quick access to the software they need, with a minimum of interaction. Administrators might not trust end users to perform a manual installation of a complex application unaided, but end users can usually complete a Group Policy installation with no special assistance.

## Creating Packages

As discussed in Chapter 9, Group Policy application deployment is package-based. To deploy an application in this manner, the application must be in the form of a Windows Installer package file with an .msi extension. Some application developers—and particularly Microsoft—supply their products as package files or provide package files on the application installation disks.

For applications that do not include package files, your only recourse if you want to deploy them using Group Policy is to create the packages yourself. This requires an external utility because Microsoft does not include any package creation tools with Windows or with its applications. A variety of third-party tools are available, with varying capabilities, some of which are free and some commercial. A few of these package creation tools are listed in Table 10-1.

**TABLE 10-1** Windows Installer Package Creation Utilities

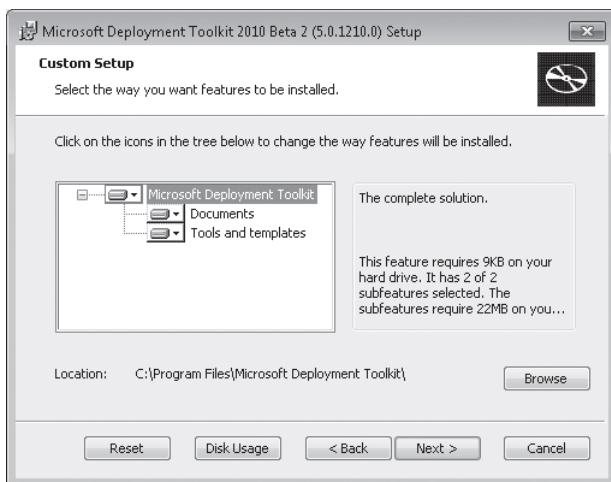
PRODUCT	COMPANY	URL
Visual Studio 2010	Microsoft	<a href="http://www.microsoft.com/visualstudio/en-us/">http://www.microsoft.com/visualstudio/en-us/</a>
Advanced Installer	Caphyon, Ltd.	<a href="http://www.advancedinstaller.com">http://www.advancedinstaller.com</a>
InstallShield	Flexera Software	<a href="http://www.flexerasoftware.com/products/installshield.htm">http://www.flexerasoftware.com/products/installshield.htm</a>
Wise Package Studio	Altiris/Symantec	<a href="http://www.symantec.com/business/package-studio">http://www.symantec.com/business/package-studio</a>
WIX Toolset	Microsoft	<a href="http://wix.codeplex.com/">http://wix.codeplex.com/</a>
MSI Package Builder	Emco Software	<a href="http://www.emco.is/products/msi-package-builder/features.php">http://www.emco.is/products/msi-package-builder/features.php</a>



#### EXAM TIP

When preparing for the 70-686 exam, you should be aware that the exam covers the process of deploying packages by using Group Policy, but not the process of creating those packages.

A Windows Installer package file is a relational database that contains one or more products, with each product consisting of a number of features and one or more components. The component is the smallest unit that the Windows Installer engine can install. For example, a single .msi file might contain two products: an application in 32-bit and 64-bit versions. Each product might contain several features, which are the different programs that make up the application, with each feature having multiple components. The Windows Installer wizard interface typically displays the various features, as shown in Figure 10-1, enabling the user to select which ones to install.



**FIGURE 10-1** The Windows Installer wizard interface

Windows Installer packages contain instructions that dictate how the installation process proceeds on the target computer. A package can include an interactive preinstallation phase, in which the end user can select a location for the application and the features to be installed, among other options. Packages can also be configured to install the application with no interaction, either because the optional parameters are specified on a command line—a method called quiet mode—or because the default installation parameters are preconfigured in the package itself.

#### **NOTE DEPLOYING OTHER FILE TYPES**

In addition to MSI packages, there are other file types you can deploy using Group Policy Software Installation, such as patch files (with an MSP extension) that contain updates or service packs and modification files (with an MST extension), which alter the installation process of an existing MSI file. For example, if you have an MSI package supplied by the manufacturer, you can use a third-party tool to create an MST file that changes the installation defaults, rather than modify the MSI file.

## **Understanding Group Policy Deployment Components**

The process of deploying applications to Windows 7 workstations using Group Policy involves the following three main components:

- **Software Installation extension** Software Installation is an extension to the Group Policy Management Editor snap-in, which appears by default whenever you edit a Group Policy object. Administrators use the extension to create Software Installation policies, which specify the packages to be deployed and contain settings that dictate how the workstations install the applications.
- **Windows Installer** The Windows installation engine that reads the contents of Windows Installer MSI files and follows the instructions contained therein to install, maintain, or remove applications. All Windows server and workstation versions since Windows 2000 include Windows Installer, and associate the engine with the .msi file name extension.
- **Get Programs control panel** The Windows 7 and Windows Server 2008 R2 component on which applications published using Group Policy appear. Users can install applications deployed to this control panel as needed. In Windows versions prior to Windows Server 2008 and Windows Vista, this component was called the Add Or Remove Programs control panel.

## **Understanding Group Policy Deployment Types**

The Software Installation extension is a component that uses Group Policy to associate packages with specific AD DS objects. AD DS then functions as a delivery service that deploys advertisements for the packages to specific computers and users on the network. After it's there, the Windows Installer engine on the receiving computer processes the MSI package, executing the instructions it contains to install the application.

Every Group Policy object has two Software Installation policies, one under Computer Configuration and one under User Configuration, as shown in Figure 10-2. Computers in the AD DS domain apply Computer Configuration policies when they start up, and User Configuration policies when a user logs on to the domain.

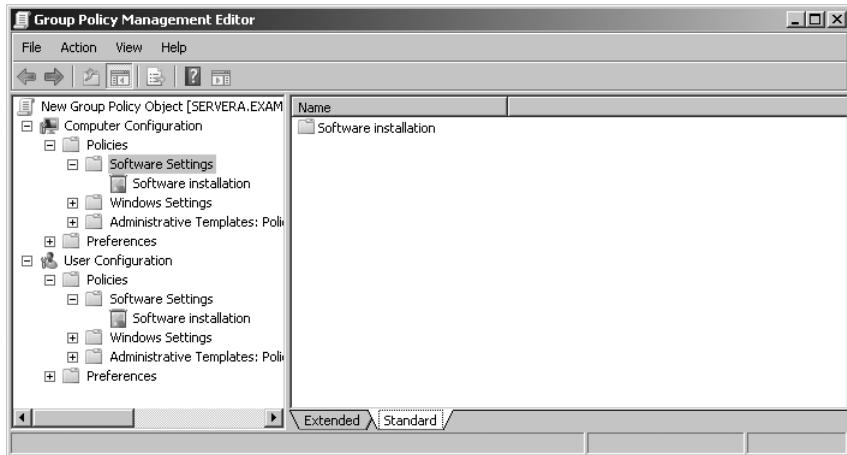


FIGURE 10-2 Software Installation policies in a GPO

The Software Installation extension supports two types of package deployment, as follows:

- **Assign** The Software Installation policy creates an advertisement that, in the case of a user policy, adds the application to the target computer's start menu, and can also associate specific file name extensions with the application. When the user launches the application for the first time or opens a file associated with it, the system accesses the MSI file from the network and uses Windows Installer to perform the installation. The package advertisement follows the user to whichever computer she uses to log on. You can also assign packages to computers, in which case the installation occurs automatically when the system starts.
- **Publish** The Software Installation policy creates an advertisement, which it stores in AD DS, and which adds the application to the Get Programs control panel in Windows 7 or Windows Server 2008 R2 (or the Add Or Remove Programs control panel in earlier versions). This enables the user to select the program for installation or removal at any time. You can publish a package only to users; the Computer Configuration policy does not support the publish option.

Table 10-2 lists some of the questions you should ask when deciding the type of deployment you should use.

**TABLE 10-2** Software Installation Deployment Options

	PUBLISH (USER)	ASSIGN (USER)	ASSIGN (COMPUTER)
After the deployment, when is the software available for installation?	After the next logon	After the next logon	The next time the computer starts.
How does the user install the software?	By using the Get Programs control panel	By accessing the application from the Start menu or a shortcut	The software is installed automatically when the computer reboots.
If the software is not installed and the user opens a file associated with the software, does the software install?	Yes (if auto-install is turned on)	Yes	Not applicable; the software is already installed.
Can the user remove the software by using the Get Programs control panel?	Yes, and the user can choose to install it again	Yes, and the software is available for reinstallation	No. Only an administrator can remove the software.

## Creating Software Installation Policies

The steps involved in creating Group Policy Software Installation policies are as follows:

1. Plan an AD DS strategy.
2. Create a software distribution point.
3. Configure Software Installation defaults.
4. Create Software Installation package policies.
5. Configure Software Installation package properties.

### PLANNING AN AD DS STRATEGY

When planning a Group Policy application deployment, you must review your organization's software requirements and compare them to your AD DS organizational structure and your available Group Policy Objects (GPOs). With this information, you can determine how you want to deploy your applications. Then create a test environment to determine exactly how you want to assign or publish software to your users or computers.

Some of the basic strategies for Group Policy software deployment that you should consider are as follows:

- Create organizational units (OUs) based on software management, rather than security, needs. This strategy enables you to target applications to the appropriate users.
- Deploy software close to the root of your AD DS domain. Deploying software high in the domain hierarchy makes it easier to provide all of the users in an organization with access to an application. This reduces administration because you can deploy the package using a single GPO rather than having to re-create the object in multiple containers deeper in the AD DS hierarchy.
- Deploy multiple applications with a single GPO. In organizations where users share the same core set of applications, this practice reduces administration overhead by enabling you to create and manage a single GPO rather than multiple GPOs. Also, the user logon process is faster because a single GPO deploying multiple applications processes faster than multiple GPOs each deploying one application.
- Publish or assign applications only once to a given group of users or computers. Deploying the same application in multiple configurations is sometimes necessary to support different types of users. However, you should avoid deploying multiple copies of the same application in such a way that users are forced to decide which version they need. Instead, adjust your deployment strategy wherever possible so that each configuration is delivered only to the users and computers that need it.

### **CREATING A SOFTWARE DISTRIBUTION POINT**

A software distribution point is a location on a shared network drive on which you store the packages you intend to deploy using Group Policy. When you create a Software Installation policy, the package you specify is not actually stored in the AD DS database. The GPO contains only a pointer to the package's location. Therefore, the package must be accessible, not only to the computer where you are running the Group Policy Management Editor, but also to the computers and users who are to receive it.

You can create multiple distribution points or a single distribution one for all of your packages as long as you create separate folders for each application and each version. Configure the share and NTFS permissions so that administrators have Read and Write access to the distribution point. Users need only Read access.

### **CONFIGURING SOFTWARE INSTALLATION DEFAULTS**

The Properties sheets for the Software Installation folders in Group Policy Management Editor contain configuration settings that apply to all of the package policies you create in that folder. Some of the settings establish defaults for parameters you can customize on individual policies, as shown in Figure 10-3, while others enable multiple applications deployed by the same GPO to coexist.

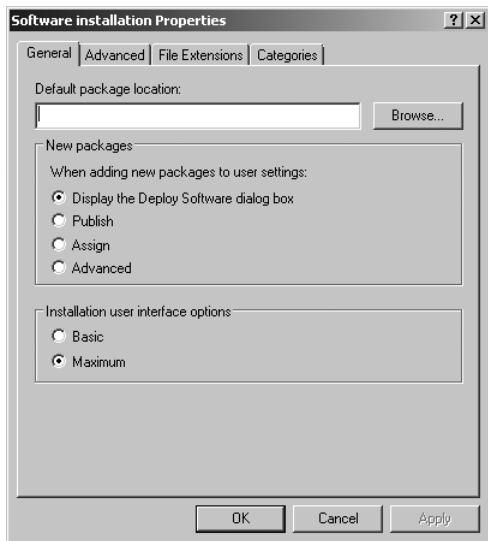


FIGURE 10-3 The General tab of the Software Installation Properties sheet

For example, the File Extensions tab, shown in Figure 10-4, enables you to establish priorities for the file associations created by the deployed applications. If you install two applications that both create associations for the same file extension, you can specify which one of the applications should launch when a user opens a file with that extension.

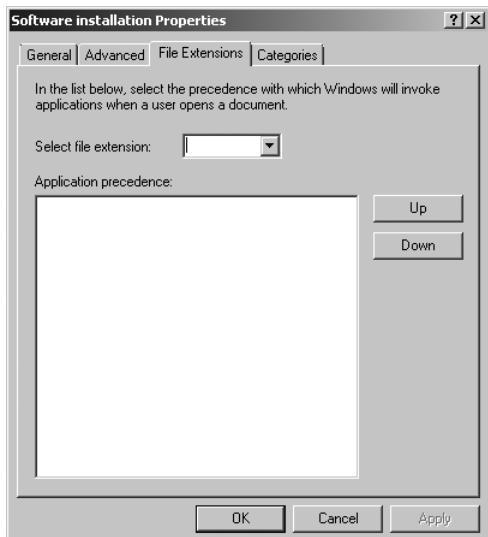


FIGURE 10-4 The File Extensions tab of the Software Installation Properties sheet

## CREATING SOFTWARE INSTALLATION PACKAGE POLICIES

When you browse to the Software Installation folder under Computer Configuration or User Configuration, right-click it, and select New | Package from the context menu, you must first browse to the software distribution point you created and select the package file you want to deploy. After you do this, the Deploy Software dialog box appears, as shown in Figure 10-5, in which you can specify whether you want to assign or publish the package. When you deploy a package to computers (as opposed to users), the Published option is unavailable, and if you select the Advanced option, the package's Properties sheet appears.

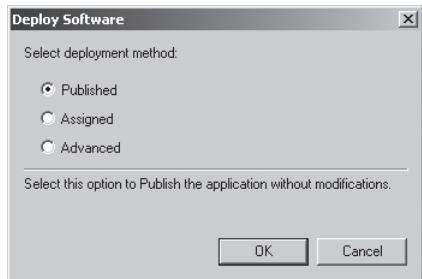


FIGURE 10-5 The Deploy Software dialog box

### CAUTION MAINTAINING LICENSES

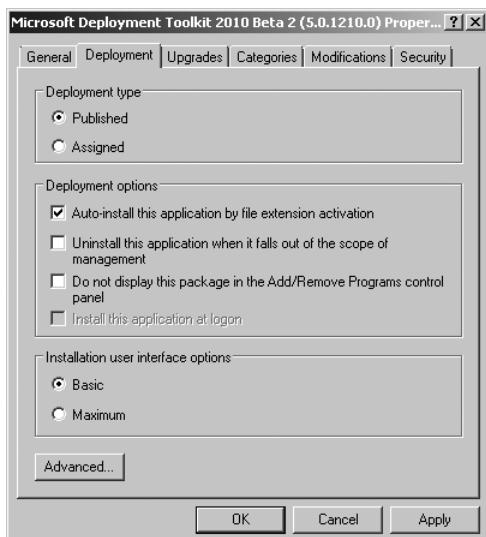
You must have the appropriate software licenses for applications written by independent software vendors that you distribute using Group Policy policies. It is your responsibility to match the number of users who can access and use the software to the number of licenses you have on hand. It is also your responsibility to verify that you are working within the license agreement included by each independent software vendor.

## CONFIGURING SOFTWARE INSTALLATION PACKAGE PROPERTIES

Double-click a policy package (or select the Advanced option in the Deploy Software dialog box) to open its Properties sheet, as shown in Figure 10-6. On the Deployment tab, you can switch between Assign and Publish, as well as configure the following parameters:

- **Auto-Install This Application By File Extension Activation** Select this check box to use the application precedence for file name extensions as determined on the File Extensions page of the Software Installation Properties sheet. When you deploy the package to computers, the check box is selected and grayed out because the application is installed automatically by default.

- **Uninstall This Application When It Falls Out Of The Scope Of Management** Select this check box to remove the application at logon (for users) or startup (for computers) if they move to a site, domain, or OU for which the application is not deployed in a GPO.
- **Do Not Display This Package In The Add/Remove Programs Control Panel** Select this check box to specify that this package should not be displayed in the Get Programs control panel (in Windows 7 or Windows Server 2008 R2) or the Add Or Remove Programs control panel.
- **Basic** Select this option to provide only a basic display to users during the installation process.
- **Maximum** Select this option to display all installation messages and screens to users during the package installation.



**FIGURE 10-6** The Deployment tab of a package policy's Properties sheet

The Properties sheet also includes the following additional tabs:

- **Upgrades** Enables you to designate packages as upgrades to other packages already deployed
- **Categories** Enables you to specify the category under which the package is listed in the Get Programs or Add Or Remove Programs control panel
- **Modifications** Enables you to add MST package files containing installation modifications to an existing package deployment
- **Security** Enables you to specify permissions that control access to the package you are creating

**NOTE CHOOSING A LOCAL DEPLOYMENT METHOD**

It is up to each organization to decide which local application deployment method is best suited to its skills and its needs. With Group Policy, the deployment process is free and relatively simple, but the package creation process can be quite complex. With SCCM 2007, creating packages is a relatively straightforward process, but installing the SCCM infrastructure is complicated and expensive.

## Deploying Applications Using SCCM 2007

Chapter 9 discussed how you can use SCCM 2007, in cooperation with Microsoft Deployment Toolkit (MDT) 2010, to deploy Windows 7 workstations on an enterprise network. You can incorporate applications into that operating system deployment in several ways: by installing them on your reference computers before capturing images of them, creating thick images, or by executing the application installation as part of a task sequence.

The basic process of deploying applications—or any software—using SCCM 2007 is the same as that for an operating system: you create a package containing the software and advertise it to a collection of computers. The computers receive the advertisement, through the SCCM client, and execute the instructions in the package.

The difference between an SCCM package and a Windows Installer package was also discussed in Chapter 9. SCCM does not require a special format for its packages or a third-party utility to create them. You use the Configuration Manager console to create packages that contain the software you want to deploy and programs that execute on the target computers.

"Program" (in SCCM) is a technical term that refers to a command that executes on the client computer. For example, if you have a standard application with source files and a Setup.exe file that you want to deploy using SCCM, you create a package that contains the source files and a program that contains a command line executing Setup.exe with appropriate parameters. When the designated clients receive the advertisement indicating that the package is available, they download the program and execute it, causing the installation to commence.

SCCM is essentially a delivery service that provides software to clients in a predetermined manner. It is up to the SCCM administrator to create programs that can execute properly on the client computers. If, for example, you create a program that contains an improperly formatted Setup.exe command line, the client computers generate an error, just as if you typed the command incorrectly in person.

## Understanding the SCCM Software Deployment Process

The process of deploying an application using SCCM 2007 consists of the following basic steps:

1. Create distribution points
2. Create a collection
3. Create a package
4. Select distribution points
5. Create a program
6. Advertise the program to the collection

These steps are discussed in the following sections.

### CREATING DISTRIBUTION POINTS

SCCM is a highly scalable product, designed to support the largest enterprises. When deploying an application to clients at multiple physical sites, you can create multiple distribution points to prevent each client from having to access the source files over a slow wide area network (WAN) connection. After creating a package, you copy it to the distribution points so that each client can then access it from a local server.

Creating distribution points is typically a part of the SCCM 2007 infrastructure design, so they should already be in place by the time you are ready to create packages. To add a distribution point in Configuration Manager, you browse to the Site Management\<site>\Site Settings\Site Systems folder and launch the New Site System Server Wizard, as shown in Figure 10-7.

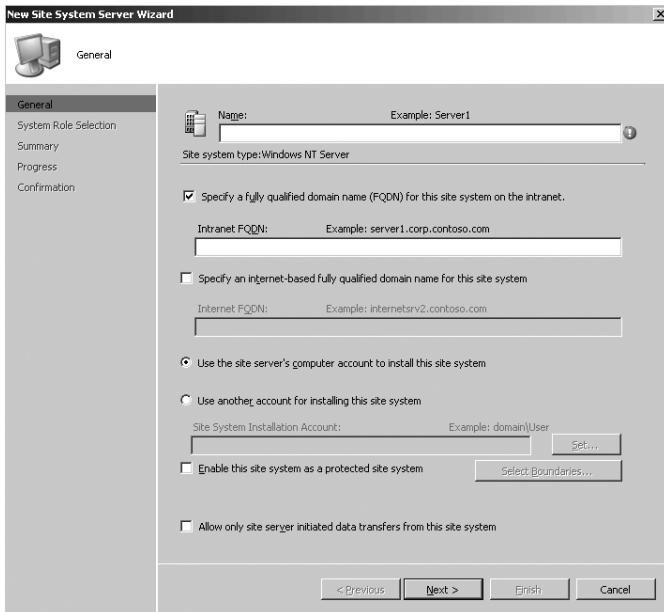


FIGURE 10-7 The New Site System Server Wizard

After specifying the name of the server on your network you want to add, the wizard displays the System Role Selection page, as shown in Figure 10-8, which enables you to choose Distribution Point as the SCCM role you want that server to perform.

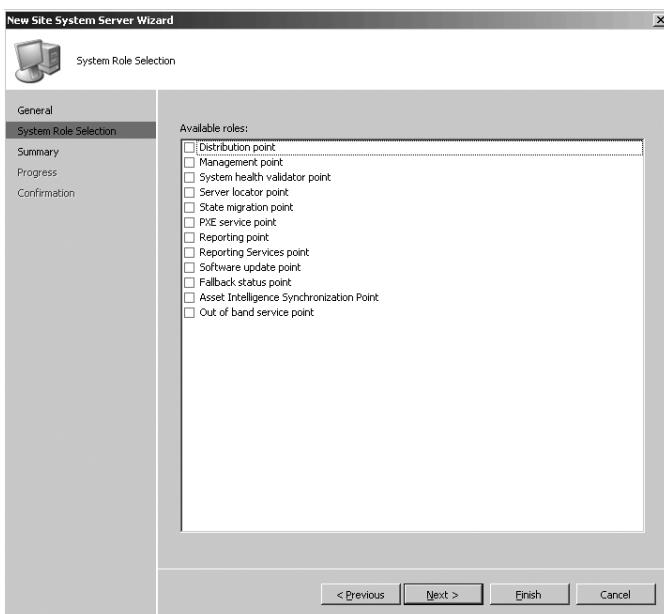


FIGURE 10-8 The System Role Selection page in the New Site System Server Wizard

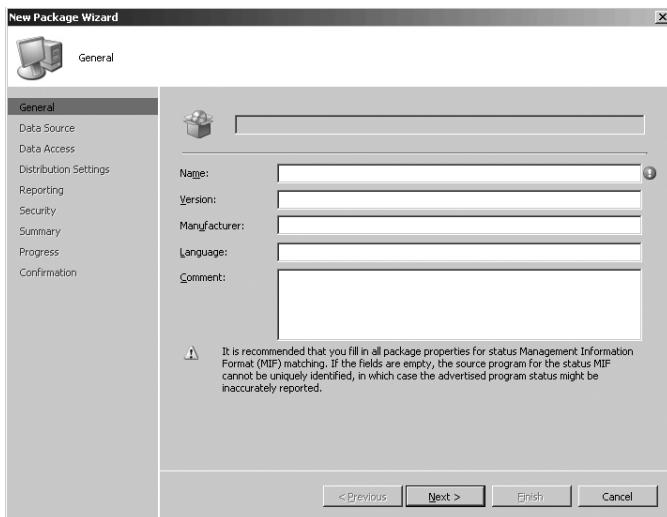
## CREATING A COLLECTION

In SCCM, you use collections to specify which computers or users are to receive deliveries from the SCCM servers. This makes it easy to deploy applications to selected computers with great precision. When you are deploying applications to computers that already have the SCCM client installed, you can use the Configuration Manager console to discover clients and add them to collections as needed. For more information on creating collections, see the section "Creating Collections" in Chapter 7, "Designing Lite-Touch and Zero-Touch Deployments."

## CREATING A PACKAGE

Creating a package in Configuration Manager is essentially a matter of assembling the materials you need SCCM to deliver to the target computers so that the computers can install your application. To create a package using SCCM 2007, use the following procedure:

1. On your SCCM site server, launch the Configuration Manager console.
2. Browse to the Computer Management\Software Distribution\Packages folder.
3. Right-click the Packages folder and select New | Package from the context menu. The New Package Wizard appears, displaying the General page, as shown in Figure 10-9.



**FIGURE 10-9** The General page of the New Package Wizard

4. Type a name for the package in the Name text box, as well as other identifying information, if you want. Then click Next. The Data Source page appears, as shown in Figure 10-10.

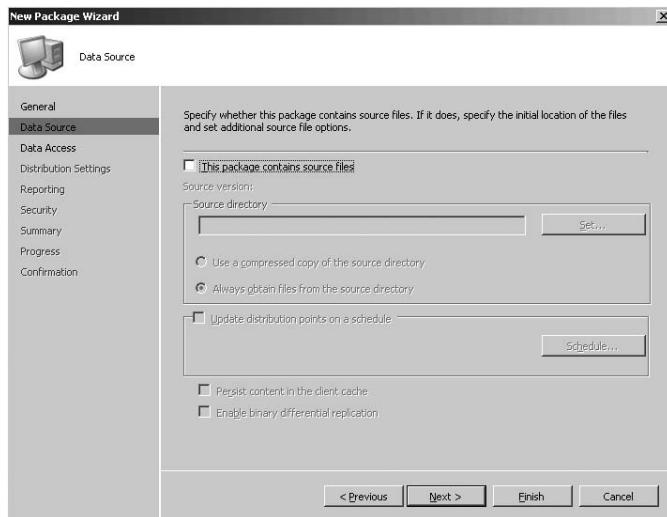


FIGURE 10-10 The Data Source page of the New Package Wizard

5. Select the check box for The Package Contains Source Files and then the Use A Compressed Copy Of The Source Directory option.
6. Click Set. The Set Source Directory dialog box appears, as shown in Figure 10-11.

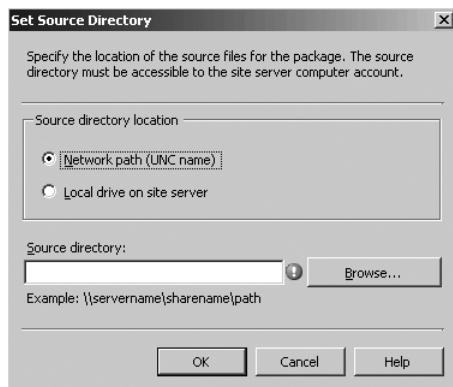
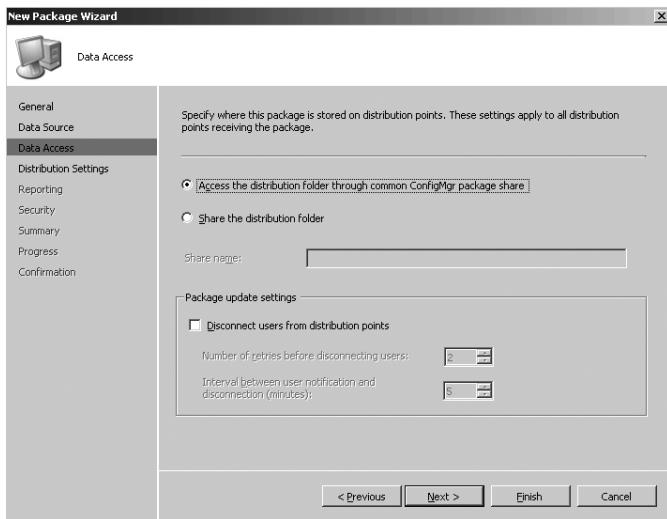


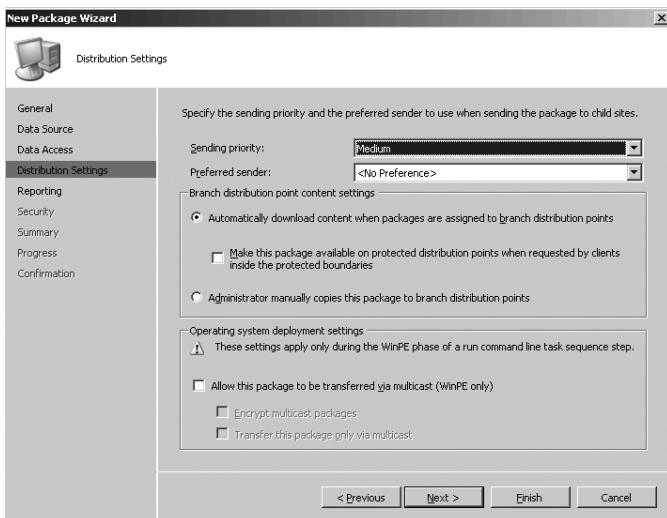
FIGURE 10-11 The Set Source Directory dialog box

7. In the Source Directory text box, type or browse to the location of the application source files. Then select the appropriate Source Directory Location option, and click OK.
8. Click Next. The Data Access page appears, as shown in Figure 10-12.



**FIGURE 10-12** The Data Access page of the New Package Wizard

9. Click Next to accept the default settings. The Distribution Settings page appears, as shown in Figure 10-13.



**FIGURE 10-13** The Distribution Settings page of the New Package Wizard

10. Click Next to accept the default settings. The Reporting page appears, as shown in Figure 10-14.

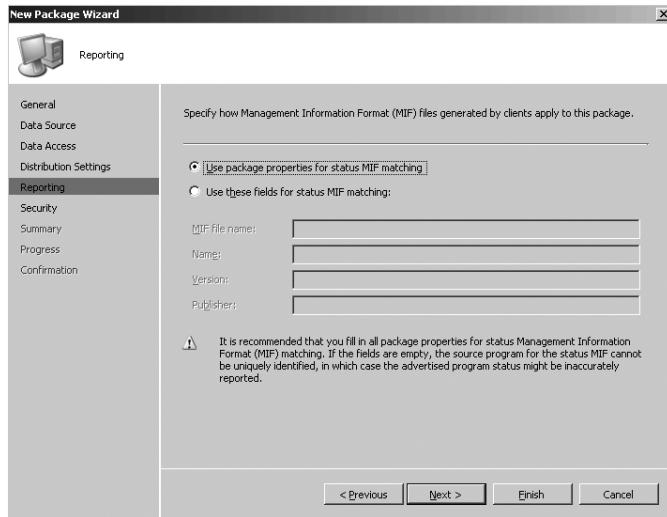


FIGURE 10-14 The Reporting page of the New Package Wizard

11. Click Next to accept the default settings. The Security page appears, as shown in Figure 10-15.

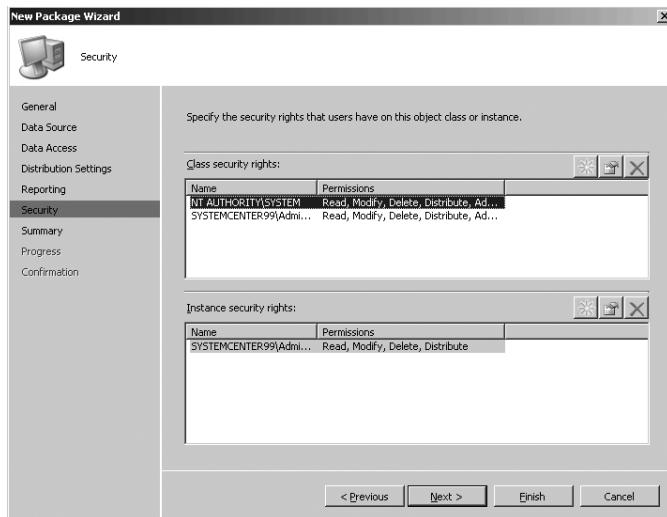
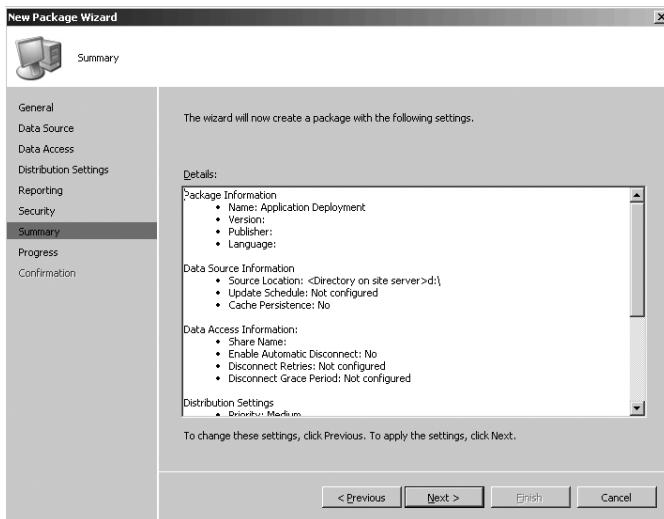


FIGURE 10-15 The Security page of the New Package Wizard

12. Click Next to accept the default settings. The Summary page appears, as shown in Figure 10-16.



**FIGURE 10-16** The Summary page of the New Package Wizard

13. Click Next. The wizard creates the package.
14. Click Close.

When you expand the package you have just created, you see the following four subheadings:

- **Access Accounts** Specifies who can access the source files in the package
- **Distribution Points** Specifies which distribution points SCCM uses to deploy the package
- **Programs** Enables you to create the programs that execute on the target computers
- **Package Status** Displays information about the package's activities

#### SELECTING DISTRIBUTION POINTS

For the package you created to be accessible to clients, you must copy it to at least one distribution point. The computer on which you have SCCM installed is a distribution point by default, and you can add the package to any other distribution points you have added using the New Site System Server Wizard.

To add a package to distribution points, use the following procedure:

1. In Configuration Manager, browse to the Computer Management\Software Distribution\Packages folder and expand the package you want to distribute.
2. Right-click the Distribution Points heading and select New Distribution Points from the context menu. The New Distribution Points Wizard appears.
3. Click Next to bypass the Welcome page. The Copy Package page appears, as shown in Figure 10-17.

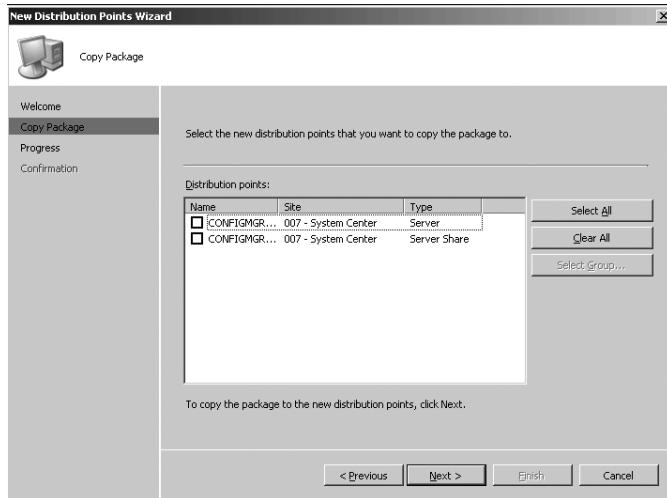


FIGURE 10-17 The Copy Package page of the New Distribution Points Wizard

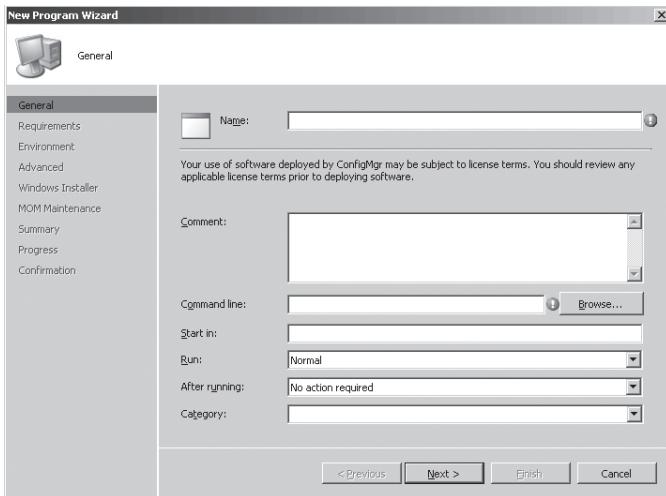
4. Select the check boxes for the distribution points you want to use to deploy the package and click Next. The Wizard Completed page appears.
5. Click Close.

#### CREATING A PROGRAM

In SCCM 2007, a program contains the command that the target computers execute to install the application in a package. You must create at least one program for every package. You can create multiple programs to support different installation options. For example, if an application's setup program provides you with installation options such as Typical, Complete, and Custom to choose from, you must create three separate programs to support all of those options.

To create a program, use the following procedure:

1. In Configuration Manager, browse to the Computer Management\Software Distribution\Packages folder and expand the package you want to distribute.
2. Right-click the Programs heading and select New | Program from the context menu. The New Program Wizard appears, displaying the General page, as shown in Figure 10-18.



**FIGURE 10-18** The General page of the New Program Wizard

3. In the Name text box, type a descriptive for the program.
4. In the Command Line text box, type the command line to execute on the target computers, including any required parameters.

#### **CAUTION CONFIGURING COMMAND LINE PARAMETERS**

SCCM 2007 has no way of checking whether the command line you specify in a program is correctly formatted or includes the proper parameters. The only way to know for sure is to execute the command on a target computer.

5. You can specify in the Start In text box the folder in which you want the command line to execute. The default is the folder in which the source files are stored.
6. In the Run drop-down list, specify whether you want the program to be visible as it runs.
7. In the After Running drop-down list, specify whether the client system should restart after the installation is completed.
8. Click Next. The Requirements page appears, as shown in Figure 10-19.

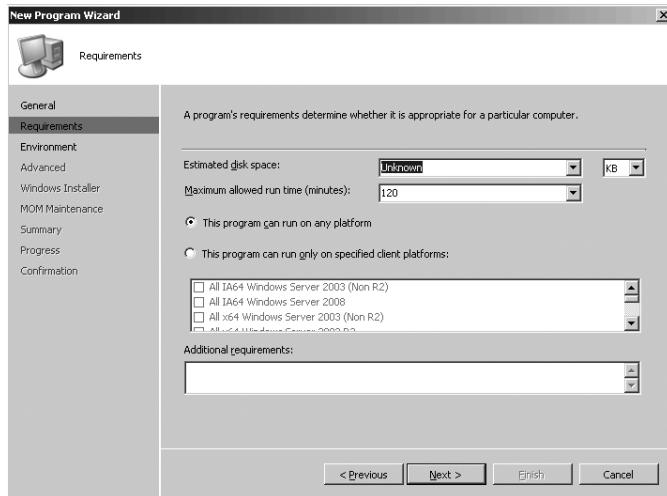


FIGURE 10-19 The Requirements page of the New Program Wizard

9. Configure any properties a client must meet before it is permitted to run the program. Then click Next. The Environment page appears, as shown in Figure 10-20.

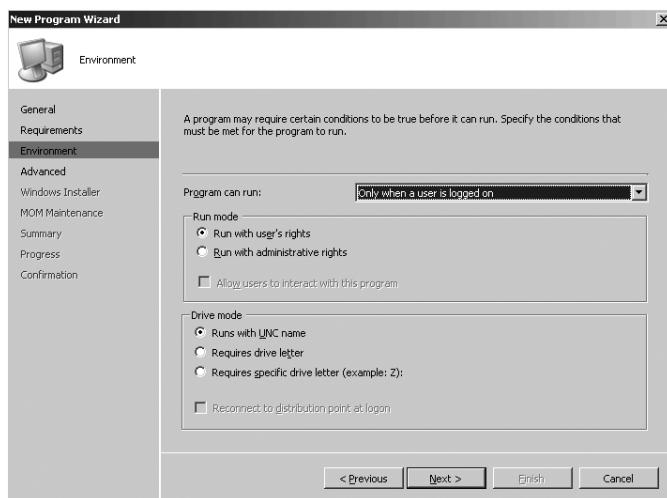
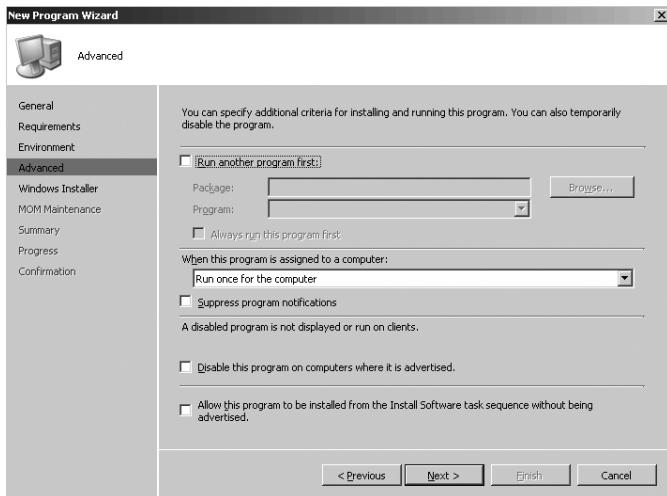


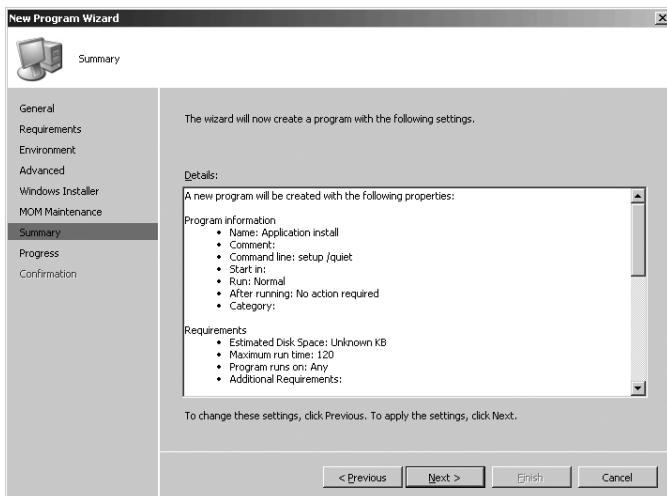
FIGURE 10-20 The Environment page of the New Program Wizard

10. Configure the environment in which the client will run the program. Then click Next. The Advanced page appears, as shown in Figure 10-21.



**FIGURE 10-21** The Advanced page of the New Program Wizard

11. Configure any special requirements the application requires and click Next. The Windows Installer page appears.
12. Click Next. The MOM Maintenance Mode page appears.
13. Click Next. The Summary page appears, as shown in Figure 10-22.



**FIGURE 10-22** The Summary page of the New Program Wizard

14. Click Next. The Wizard Completed page appears.
15. Click Close.

## ADVERTISING A PROGRAM

After you have created the package and all of its constituent parts, you are ready to create an advertisement that notifies the clients of the package's existence. Using SCCM's scheduling capabilities, you can control when the advertisement is available to clients, thus regulating the amount of network traffic generated by the application deployment process.

For more information on creating advertisements in SCCM 2007, see "Creating Advertisements" in Chapter 7.

## PRACTICE Deploying Packages with Group Policy Software Installation

---

In this practice, you create a Group Policy Object (GPO) and configure it to distribute a software package, but to avoid accidental distribution, you do not link the GPO to an AD DS object.

### EXERCISE 1 Creating a Group Policy Object

To distribute software by using Group Policy, the best approach is to create a new GPO specifically for that purpose.

1. Click Start. Then click Administrative Tools | Group Policy Management. The Group Policy Management console appears.
2. Expand your forest and your domain.
3. Under your domain, right-click the Group Policy Objects heading and select New from the context menu. The New GPO dialog box appears.
4. In the Name text box, type **Software Distribution Test** and click OK. The Software Distribution Test GPO appears in the console.

### EXERCISE 2 Configuring Software Installation Policies

To create Software Installation policies, you must open the GPO you created in the Group Policy Management Editor.

1. In the Group Policy Management console, right-click the Software Distribution Test GPO you created and select Edit from the context menu. The Group Policy Management Editor console appears and loads the GPO.
2. Under User Configuration, browse to the Policies\Software Settings\Software Installation folder.
3. Right-click the Software Installation folder and select New | Package from the context menu. An Open combo box appears.

4. Browse to the location of the MicrosoftDeploymentToolkit2010\_x64.msi or MicrosoftDeploymentToolkit2010\_x86.msi file, select the file, and click Open. The Deploy Software dialog box appears.
5. Select the Advanced option and click OK. The Microsoft Deployment Toolkit 2010 Properties sheet appears.
6. Click the Deployment tab.
7. Leave the Published option selected and clear the Auto-Install This Application By File Extension Activation check box.
8. Click OK. The policy appears in the Software Installation folder.

## Lesson Summary

- To deploy an application by using Group Policy, the application must be in the form of a Windows Installer package file with an .msi extension. For applications that do not include package files, your only recourse if you want to deploy them using Group Policy is to create the packages yourself, which requires an external utility.
- Software Installation is an extension to the Group Policy Management Editor snap-in that administrators use to create Software Installation policies, which specify the packages to be deployed and contain settings that dictate how the workstations install the applications.
- The Software Installation extension supports two types of package deployment: assign, which adds the application to the target computer's Start menu, and publish, which adds the application to the Get Programs control panel in Windows 7.
- The steps involved in creating Group Policy Software Installation policies are these: plan an AD DS strategy, create a software distribution point, configure Software Installation defaults, create Software Installation package policies, and configure Software Installation package properties.
- The basic process of deploying applications by using SCCM 2007 is the same as that for an operating system: you create a package containing the software and advertise it to a collection of computers. The computers receive the advertisement, through the SCCM client, and execute the instructions in the package.
- The process of deploying an application by using SCCM 2007 consists of the following steps: create distribution points, create a collection, create a package, select distribution points, create a program, and advertise the program to the collection.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Deploying Applications Using Group Policy and SCCM 2007." The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE ANSWERS**

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

1. Which of the following statements about Group Policy Software Installation policies is true?
  - A. You can publish a package to users, but not to computers.
  - B. You can publish a package to computers, but not to users.
  - C. You can publish a package to both computers and users.
  - D. You can publish a package to neither computers nor users.
2. Which of the following tabs appears in the Software Installation Properties sheet, but not in a package policy's Properties sheet?
  - A. Categories
  - B. File Extensions
  - C. Upgrades
  - D. Modifications
3. Which of the following subheadings beneath an SCCM 2007 package must you configure for a software distribution to occur successfully? (Choose all correct answers.)
  - A. Access Accounts
  - B. Distribution Points
  - C. Programs
  - D. Package Status

## Lesson 2: Deploying Applications Using RDS

Group Policy Software Installation and SCCM 2007 are both methods for delivering an application's installation files to a workstation. After the application installation is completed, Group Policy and SCCM are no longer involved; the application runs locally, just as if you installed it manually. Remote Desktop Services (RDS), by contrast, is a server-based deployment mechanism that requires the continued participation of the server as the applications are running.

**After this lesson, you will be able to:**

- Understand the RDS architecture.
- Deploy desktops and applications using RDS.
- Create RemoteApp packages.

**Estimated lesson time: 60 minutes**

## Overview of RDS Deployment

In its most basic form, RDS works by running applications on a Windows Server 2008 R2 server and enabling workstations to access those applications. The workstation runs a client application, which establishes a connection to the server, creating a session for that client's exclusive use. The session can provide the client with a complete Windows desktop, including a full range of applications, a desktop dedicated to one application, or an application in an individual window.

An RDS server with a single copy of an application installed on it can provide multiple users with access to that application. The number of users is functionally limited by the hardware resources in the server. Each user has its own copy of the application, enabling it to function independently of the other users, but RDS uses special memory management techniques to avoid loading multiple copies of every application file for each user.

An RDS session consists of the following three basic components:

- **Remote Desktop Session Host** The core service running on the server, hosting individual applications and full desktops. Remote Desktop Session Host is a role service that is part of the Remote Desktop Services role on Windows Server 2008 R2 servers.
- **Remote Desktop Connection** The client program running on the workstation. Remote Desktop Connection is included with all of the current versions of Windows.
- **Remote Desktop Protocol (RDP)** The communications protocol that connects the Remote Desktop Connection client to the Remote Desktop Session Host service on the RDS server. RDP carries only interface traffic, such as keystrokes and mouse movements from client to server and display data from server to client.

### **NOTE SERVICE RENAMED**

Prior to Windows Server 2008 R2, Remote Desktop Services was known as Terminal Services, and the Remote Desktop Session Host role service was called Terminal Server. The technologies are essentially the same and are fully compatible. Only the names of the various server components have changed.

## Understanding RDS Deployment Options

Some administrators use RDS as a complete client desktop solution. They install all of the applications their users need on the RDS server and, after the users connect with the Remote Desktop Connection client, they spend all of their time working in the RDS session. Supporting large numbers of users and users with different requirements can complicate this arrangement enormously, however.

Other administrators prefer to employ RDS as a partial solution, using it to provide only certain applications to clients. A standard RDS session can contain just a few applications, or even one, and clients can switch back and forth between local applications and those provided by RDS.

Combining two desktops on a single workstation can be confusing to some users, however. People who spend all their time in an RDS desktop might not even realize that they are connecting to a server for their applications. Having to switch from one desktop to another might be asking too much of them.

A feature called RemoteApp, introduced in Windows Server 2008, addresses this issue by delivering individual applications to clients in separate windows. There is no RDS desktop involved; the windows appear to the user just as they would if they were running the application locally. Users do not run the Remote Desktop Connection client to access RemoteApp applications; instead, they use a desktop icon provided by an administrator, or they click an icon on an intranet Web page.

Users can open multiple RemoteApp programs at the same time, and as long as all of the programs are hosted by the same RDS server, the applications all run in a single session. RemoteApp is therefore no less efficient than a full remote desktop, when it comes to the hardware resources it consumes on the RDS server.

## Deploying RemoteApp Applications

Deploying a full RDS desktop is basically a matter of installing the Remote Desktop Services role on a Windows Server 2008 R2 computer with the Remote Desktop Session Host role service, and then installing the applications you want to share. When you grant users access to the RDS server, they can connect using the Remote Desktop Connection client and run the applications you installed.

Unless you are planning to deploy a full workstation application configuration using RDS, you are probably better off using RemoteApp to deploy individual applications. Deploying applications using RemoteApp involves the following tasks:

- Add RemoteApp programs
- Package RemoteApp applications
- Access RemoteApp through the Web

To provide users with access to applications by using RemoteApp, you must install the applications in the normal manner, and then use the RemoteApp Manager console, as shown in Figure 10-23, to designate them as RemoteApp programs.

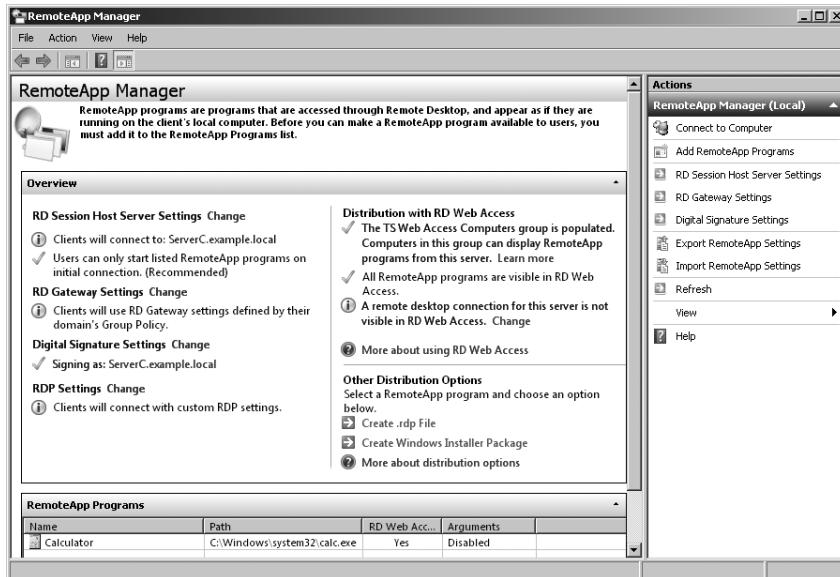
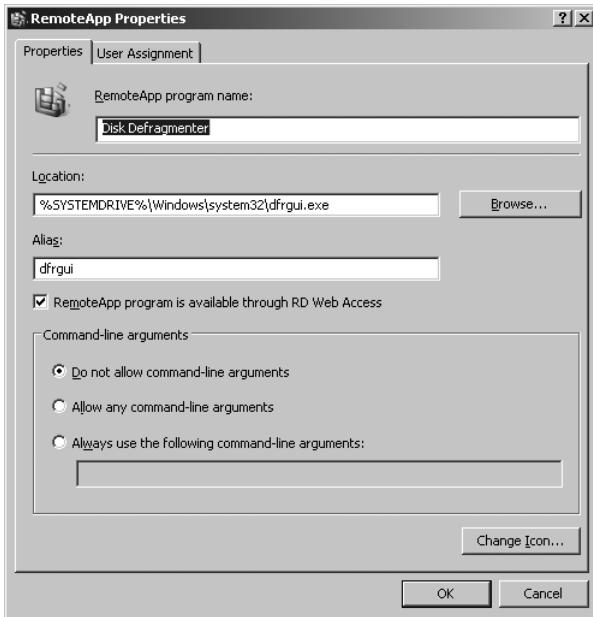


FIGURE 10-23 The RemoteApp Manager console

When you launch the RemoteApp Wizard, you can select any of the applications currently installed on the server. The Properties sheet for each application, as shown in Figure 10-24, enables you to modify the parameters that RDS uses to share the application. For example, you can add arguments to the command line that launches the application, enable users to supply their own command line arguments, and even change the name that appears with the application icon on your client computers.



**FIGURE 10-24** The RemoteApp Properties sheet

When you complete the wizard, the application appears in the console in the RemoteApp Programs list.

## Packaging RemoteApp Applications

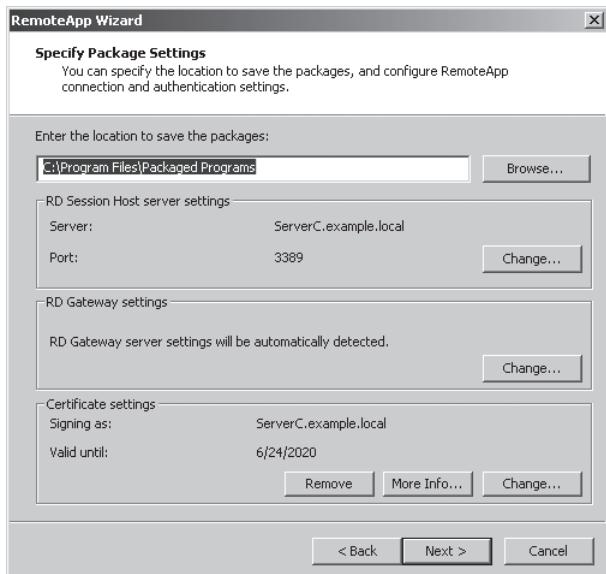
After you have designated your applications as RemoteApp programs, you can package them for deployment to your clients. The Remote Desktop Connection client program can provide workstations with an RDS desktop, but not with individual RemoteApp applications. To deploy RemoteApp applications to your workstations, you can use any one of the following three methods:

- Package the program as an RDP file
- Package the program as an MSI file
- Add the program to an intranet Web page

The following sections discuss these methods.

### Creating RDP Files

A Remote Desktop Protocol package is a file with an .rdp extension, which contains all of the settings needed for the client computer to connect to a specific RemoteApp program on a specific RDS server. Creating an .rdp file is simply a matter of selecting one of the entries in the RemoteApp Programs list in the RemoteApp Manager console and choosing Create .rdp File from the Action menu. This launches the RemoteApp Wizard, in which you can configure the package settings shown in Figure 10-25.



**FIGURE 10-25** The Specify Package Settings page in the RemoteApp Wizard

By default, the wizard creates RDP files in the C:\Program Files\Packaged Programs folder, but you can modify the path to create them anywhere. After you have created the file, you can use any method to get it to your client computers. You can copy the file to a shared network drive to which your users have access, copy it to a workstation's local drive, send it via e-mail to a user, or deploy it using a software distribution product such as SCCM 2007. All the user has to do is execute the file, and the process of connecting to the RDS server begins. After the user authenticates, the computer establishes a connection to the server, and the application appears on the user's desktop in a standard window.



### Quick Check

- When you create an RDP file on Workstation A that launches the Event Viewer console and send it via e-mail to a user on Workstation B, which computer's events appear in the console when the user on Workstation B runs the file?

### Quick Check Answer

- The events from Workstation A appear in the console, because it is Workstation A that is actually running the program.

## Creating Windows Installer Packages

The RemoteApp Manager console is also capable of packaging RemoteApp program information as a Windows Installer (MSI) package. Selecting a RemoteApp program and clicking Create Windows Installer file launches the same RemoteApp Wizard, which creates an RDP file in the same way. The only difference here is that the wizard then packages the RDP file in a Windows Installer (MSI) file. This enables you to deploy the file—and therefore the application—to your client workstations using Group Policy Software Installation settings, as covered earlier in this chapter.

## Using RD Web Access

The other method for deploying RemoteApp programs, and RDS desktops as well, is Remote Desktop Web Access (RD Web Access), an RDS role service that uses Internet Information Services (IIS) to provide users with client access to RDS servers. When you install the Remote Desktop Web Access role service, the Add Role Services Wizard also installs the Web Services (IIS) role and creates a secured intranet Web site for RDS.

Users connecting to the intranet site must first authenticate themselves, after which an RD Web Access page appears, as shown in Figure 10-26.

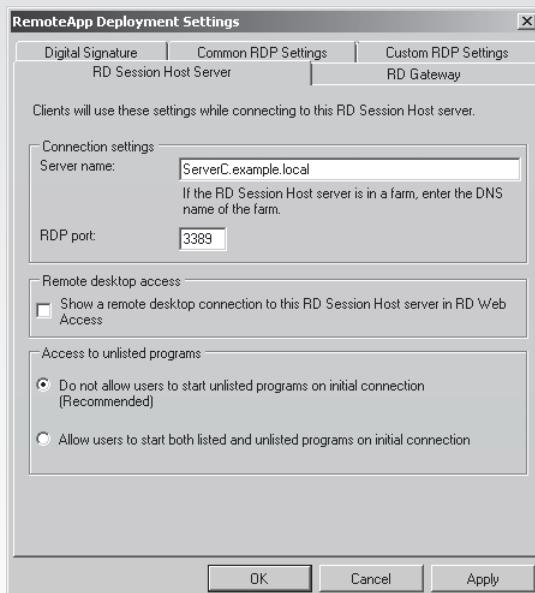


FIGURE 10-26 The RD Web Access page

For a RemoteApp program to appear on the RD Web Access site, you must select the RemoteApp Program Is Available Through RD Web Access check box on the program's Properties sheet. You can also select an entry in the RemoteApp Programs list and click Show in RD Web Access in the Action pane.

#### **NOTE PUBLISHING A DESKTOP IN RD WEB ACCESS**

In addition to publishing RemoteApp programs in the RD Web Access intranet site, you can also provide users with access to a full RDS desktop. Clicking RD Session Host Server Settings in the Action pane opens the RemoteApp Deployment Settings dialog box, as shown in Figure 10-27.



**FIGURE 10-27** The RemoteApp Deployment Settings dialog box

When you select the Show A Remote Desktop Connection To This RD Session Host Server In RD Web Access check box, a Remote Desktop icon appears on the Web page as well. This provides users with the same access as the Remote Desktop Connection client, without the need to configure that client and establish a connection manually.

#### **PRACTICE Deploying Applications Using RemoteApp**

To deploy server-based applications to network workstations, the RDS RemoteApp feature requires a minimum of setup and little or no end user reeducation.

##### **EXERCISE 1 Creating RemoteApp Programs**

RemoteApp itself requires only the RDS Remote Desktop Session Host role service.

1. Click Start. Then click Administrative Tools | Remote Desktop Services | RemoteApp Manager. The RemoteApp Manager console appears.
2. In the Actions pane, click Add RemoteApp Programs. The RemoteApp Wizard appears.

3. Click Next to bypass the Welcome page. The Choose Programs To Add To The RemoteApp Programs List page appears, as shown in Figure 10-28.



**FIGURE 10-28** The Choose Programs To Add To The RemoteApp Programs List page

4. Select the check boxes for the Calculator, Paint, and WordPad programs.
5. With the WordPad program selected, click Properties. The RemoteApp Properties sheet for the WordPad program appears.
6. Select the Allow Any Command-Line Arguments option and click OK. A message box appears, warning of the danger of allowing command line arguments.
7. Click Yes to close the message box.
8. Click Next. The Review Settings page appears.
9. Click Finish. The three programs you selected appear in the RemoteApp Programs list.

## EXERCISE 2 Connecting to the RD Web Access Site

After you have selected programs for RemoteApp, you can access them using your intranet Web site.

1. Open Server Manager. Click Configure IE ESC, and in the Internet Explorer Enhanced Security configuration dialog box, click the Off option for Administrators. Then click OK.
2. Click Start. Then click Internet Explorer. The Windows Internet Explorer window appears.

3. In the address box, type **https://127.0.0.1/rdweb**. If a Certificate error page appears, click Continue To This Website. An RD Web Access page appears.
4. If an information bar appears, prompting you to run an add-on, click the bar and select Run Add-on. A Security Warning message box appears.
5. Click Run.
6. In the Domain\User Name and Password text boxes, type the credentials for an administrative account and click Sign In. A page appears with icons for the three programs you selected.
7. Double-click the Calculator icon. A dialog box appears, confirming that you want to connect to a program from an unknown publisher.
8. Click Connect. A Windows Security dialog box appears.
9. Enter your credentials again and click Connect. A Calculator window appears.

## Lesson Summary

- RDS works by running applications on a Windows Server 2008 R2 server and enabling workstations to access those applications. The workstation runs a client application, which establishes a connection to the server, creating a session for that client's exclusive use.
- An RDS session consists of the following three basic components: Remote Desktop Session Host, the core service running on the server; Remote Desktop Connection, the client program running on the workstation; and Remote Desktop Protocol, the communications protocol that connects the Remote Desktop Connection client to the Remote Desktop Session Host service on the RDS server.
- RemoteApp delivers individual applications to clients in separate windows. There is no RDS desktop involved; the windows appear to the user just as they would if they were running the application locally.
- Deploying a full RDS desktop is basically a matter of installing the Remote Desktop Services role on a Windows Server 2008 R2 computer with the Remote Desktop Session Host role service, and then installing the applications you want to share.
- After you have designated your applications as RemoteApp programs, you can package them for deployment to your clients, using any one of the following three methods: package the program as an RDP file, package the program as an MSI file, or add the program to an intranet Web page.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Deploying Applications Using RDS." 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. The Remote Desktop Session Host role service provides the core functionality of Remote Desktop Services. Which of the following RDS features requires you to install an additional role service for the Remote Desktop Services role?
  - A. Remote Desktop Protocol
  - B. Remote Desktop Connection
  - C. Remote Desktop Web Access
  - D. RemoteApp
2. Which of the following methods can you not use to deploy an RDP file?
  - A. Send the file to users in an e-mail.
  - B. Place the file on a shared network drive.
  - C. Create a Group Policy Software Installation policy.
  - D. Create an SCCM software distribution package.
3. Which of the following statements about the Remote Desktop Services RemoteApp feature is true?
  - A. Running multiple RemoteApp applications on a workstation requires no more memory than running them all in a single RDS desktop.
  - B. Each RemoteApp application requires its own session on the RDS server.
  - C. To use RemoteApp, you must have an Internet Information Services Web server.
  - D. You can run only one RemoteApp application on any single workstation.

## Chapter Review

---

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

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

## Chapter Summary

- Deploying applications by using Group Policy has the advantage of requiring no special infrastructure beyond that of Active Directory Domain Services, which most enterprise networks already have. When compared to a manual installation of an application on a workstation, Group Policy deployment provides users with quick access to the software they need, with a minimum of interaction.
- In its most basic form, Remote Desktop Services works by running applications on a Windows Server 2008 R2 server, and enabling workstations to access those applications. The workstation runs a client application, which establishes a connection to the server, creating a session for that client's exclusive use. The session can provide the client with a complete Windows desktop, including a full range of applications, a desktop dedicated to one application, or an application in an individual window.

## 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.

- program
- quiet mode
- RemoteApp
- Remote Desktop Connection
- Remote Desktop Protocol (RDP)
- Remote Desktop Session Host

## Case Scenario

In the following case scenario, you will apply what you've learned about subjects of this chapter. You can find answers to the scenario questions in the "Answers" section at the end of this book.

### Case Scenario 1: Performing an SCCM Software Distribution

Alice has been assigned the task of deploying an application to all of the workstations in the Sales department by using System Center Configuration Manager 2007. The workstations all have the SCCM client installed on them and, using the computer on which SCCM is installed, Alice has created a collection that contains those workstations. After inserting the installation disk for the application into the computer's DVD drive, she creates a package and, on the Data Source page, selects the Always Obtain Files From The Source Directory option and specifies the drive letter of the DVD as the location for the source files. Then she selects the SCCM server as the distribution point for the application. When Alice attempts to create an advertisement, the Select A Package dialog box does not contain her package.

What are two possible reasons why the package does not appear?

## Suggested Practices

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

### Assigning and Publishing Software Installation Policies

- **Practice 1** In your AD DS domain, create an organizational unit containing only a Windows 7 test computer and link the Software Distribution Test GPO you created to it. Restart the test computer and note the availability of the package you deployed in the Get Programs control panel.
- **Practice 2** In the Software Distribution Test GPO you created, change the Software Installation policy from Publish to Assign. Then restart the test computer and note the availability of the package you deployed in the Start menu.

### Using the Remote Desktop Connection Client

- **Practice 1** On a Windows 7 workstation, use the Remote Desktop Connection client to connect to your RDS server.
- **Practice 2** Install the Remote Desktop Gateway role service on your RDS server and configure the Remote Desktop Connection client to access your RDS server from the Internet.

## 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 70-686 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.



# Troubleshooting Internet Explorer and Group Policy Issues

Troubleshooting is a primary skill for every IT professional. After you learn it, you can apply the basic techniques for isolating and identifying a technical problem to almost any situation. In this chapter and the next one, you learn some general principles of troubleshooting and apply them to some of the most common issues facing Windows 7 desktop administrators.

## Exam objectives in this chapter:

- Identify and resolve Internet Explorer issues.
- Identify and resolve Group Policy issues.

## Lessons in this chapter:

- Lesson 1: Troubleshooting Internet Explorer Issues **432**
- Lesson 2: Troubleshooting Group Policy Issues **452**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- A computer running Windows 7 with access to the Internet

# Lesson 1: Troubleshooting Internet Explorer Issues

Many users spend a great deal of their time running Windows Internet Explorer—whether or not they are supposed to—so it tends to be a frequent source of help-desk calls and technical support requests. There are very few types of applications that have as many potential problem sources as a Web browser. Failures can be caused by the browser itself, by the Internet Web server the user is trying to access, or by any one of the many systems in between. There are also a number of infrastructure services indirectly related to the client/server communication that cause problems.

**After this lesson, you will be able to:**

- Understand basic troubleshooting steps.
- Identify the primary causes of Internet Explorer problems.
- Understand the causes of Internet Explorer performance issues.

**Estimated lesson time: 60 minutes**

## Understanding General Troubleshooting Procedures

The process of troubleshooting Internet Explorer problems is fundamentally the same as that for any IT problem. The procedure can be broken down into the following basic steps:

1. Identify the symptoms.
2. Determine the scope of the problem.
3. Isolate the location of the problem.
4. List possible causes.
5. Apply a solution.
6. Test the results.

These steps are described in the following sections.

### Identifying the Symptoms

Talking to the user and ascertaining what problematic behavior the user is experiencing can be the most important part of the troubleshooting process. If you cannot recreate the problem at will, you cannot test possible solutions. This part of the process can be simple or quite complex. The problem could be that Internet Explorer won't run at all, or there could be highly specific circumstances in which the problem occurs.

Obtaining reliable information from users can often be difficult. They can frequently be vague about the circumstances in which a problem occurred or neglect to write down the error messages they receive. Learning to ask the right questions and develop an unintimidating demeanor with less experienced users is all part of the troubleshooter's job.

## Determining the Scope

After you understand the nature of the problem and can repeat it, the next step is to determine how widespread it is. The more situations the problem affects, the more serious it is, and prioritizing is one of the main reasons for this step in the process.

First, you might determine how much of the user's experience is affected by the problem. If a user calls the help desk because he cannot access a particular Internet Web site, one of your first questions should be whether other Internet sites are affected as well. A problem accessing only one site is probably caused by user error or an issue with the site itself. If he can't access the Internet at all, it might well be due to an internal issue.

The next step would be to expand the scope laterally, and find out whether other users on the network are experiencing the same problem. You can sometimes do this by comparing notes with other support personnel, to see whether they are receiving the same type of call from other users. Otherwise you might have to call other users, access other computers remotely, or travel to other sites.

The scope of a problem is often a critical part of ascertaining its priority. Help desks and technical support organizations often receive more requests for help than they can handle at one time, and, as in a hospital's Emergency department, triage is crucial. Triage is the process of determining which conditions are the most serious and require immediate attention, and which can wait. It's not always a matter of the first in line being the first served.

Obviously, issues that affect multiple users usually receive a higher priority than those affecting a single user, and network issues take precedence over departmental issues. The jobs performed by the users can also make a difference. A technical problem that prevents users in the Sales department from taking orders—and generating revenue—merits more immediate attention than a problem in the Research & Development department.

Another aspect of problem scope is the precedence of issues affecting entire systems, as compared to those affecting just one application. If users can do their jobs without Internet Explorer, a Web browsing problem is not an immediate priority.



### REAL WORLD

Craig Zacker

**P**olitical considerations are always a factor in technical support prioritization, and IT personnel just have to get used to it. When a vice president's computer has a minor issue, it should not be surprising to see it at the head of the priority list, even if half the company is sitting idle because of a more critical issue and has to wait.

## **Isolating the Location**

In part, the process of determining the scope of the problem can also help you to determine where the cause of the problem is located. If an issue is limited to one computer, the problem is usually not caused by a network or infrastructure failure. However, if multiple computers are affected, you must determine how many and which ones, so you can list the components that could be causing the problem.

After you have determined that a problem exists outside a single computer, the isolation process gets more complicated. If some, but not all, of the computers at the site are affected, there is likely to be some issue with the internal infrastructure of a particular subnet, segment, or switch. If all of the computers in the site are experiencing the same problem, the list of possible causes is limited to components that serve the entire network.

## **Listing Possible Causes**

After you have isolated the problem to a specific location, or to a list of possible locations, you can begin to think about possible causes. Virtually any problem can have multiple causes, and at this point, the troubleshooting process frequently becomes a matter of trial and error.

## **Applying a Solution**

After you select the most likely cause for the problem, the next step is to try resolving it. In some cases, the process of isolating the problem leads naturally to a cause and a solution. For example, in the case of a hardware problem, the typical solution is to replace a questionable device with one that you are sure works. By doing so, you confirm the location of the problem, specify its cause, and implement a solution, all at the same time.

## **Testing the Results**

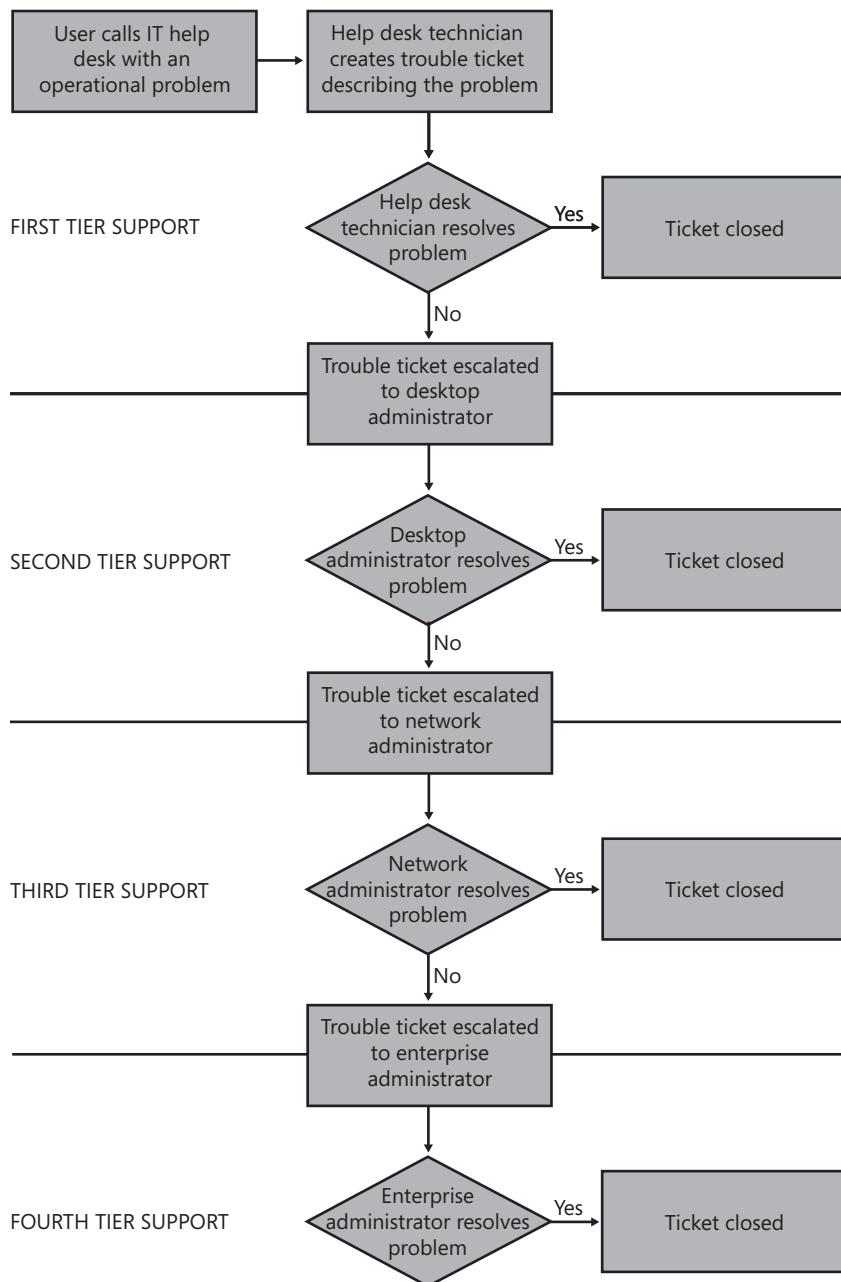
The final step of the troubleshooting process is to try once again to recreate the problem, to see if your solution has had the effect you want. If the problem appears to be solved, further testing might be in order to confirm that your fix has not broken something else. If your solution does not resolve the problem, you must go back to your list of possible causes and try something else.

## **Understanding Your Role in the Troubleshooting Process**

Depending on how the IT department of your organization is organized and what technical support policies are in place, the role of the Windows 7 desktop administrator in the troubleshooting process might vary. In smaller organizations, you might be responsible for fielding end-user problems and following them wherever they lead. However, in larger organizations, you might find yourself somewhere in the middle of a technical support hierarchy, above the entry-level help desk, for example, but below the network and enterprise administrators.

End users report their problems to the help desk, where the troubleshooting process begins. If the help-desk representatives are unable to resolve the issue, they might pass it to

you, and if necessary, you might escalate it to another level in turn. Most large organizations maintain a database of trouble calls—or “tickets”—that functions as the institutional memory of the troubleshooting process. This enables the troubleshooting process to be split among several tiers of support technicians, as shown in Figure 11-1.



**FIGURE 11-1** An example of a tiered technical support operation

As a desktop administrator in a large enterprise, you should in most cases be spared the tasks usually performed by first-tier help-desk support. Many of the support calls in a typical enterprise are the result of user error or of circumstances beyond the control of the organization. The primary job of the first tier is to field these calls and help the users with their operational procedures. If the problem does seem to be a desktop issue, the help desk might escalate the call to you. In the same way, however, you might determine that the problem falls outside of your area. If you determine that many users are affected and that the problem appears to be a network issue, it might be appropriate for you to escalate the call to a tier above you that is responsible for that area.

## Troubleshooting Web Site Access Issues

There are any number of reasons why a specific Web site might be inaccessible to a user, many of which fall outside the purview of the enterprise. The Web server itself might be down, or there might be some sort of service interruption on the Internet between that server and your network. In many cases, simply waiting a few minutes and trying again resolves the issue.

However, when the circumstances begin to indicate that there might be an internal problem causing the failure, an escalation to a desktop administrator becomes appropriate. For example, any of the following scenarios could be sufficient cause for escalation:

- Multiple users are unable to access a Web site.
- A user experiences recurring issues with Web site access.
- Multiple users complain that a site doesn't work as expected.

In these cases, the focus turns away from end-user procedures, as the desktop administrator attempts to identify technical issues that might be causing the problem.

## Gathering Information

The first step in troubleshooting a problem like this is to find out exactly what the users' experiences have been. Consider asking questions such as the following:

- **What sites have the users been unable to access?** If users are having trouble accessing particular Web sites, you might be able to find something that all of the inaccessible sites have in common. For example, if all of the sites in a particular domain are inaccessible, a name resolution issue could be involved. If all of the problematic sites use a particular programming language, there could be a compatibility problem.
- **Can the users access other sites successfully?** If users are able to access intranet, but not Internet, sites, a network infrastructure problem might be blocking Internet access. If users are able to access some Internet sites, but not others, you can rule out these network infrastructure problems.
- **Are the sites completely or only partially inaccessible?** If users are able to see some elements of a site, while others do not appear, there is likely to be an issue with a plug-in or a particular Web programming language.

- **Have the sites ever been accessible?** Sites that were accessible at one time and now are not indicate that a change in the condition of the computer, the network, or the destination server has occurred.
- **How many users have been experiencing the problem?** A single user experiencing a problem is frequently caused by a workstation issue. When multiple users experience the same problem, they might have an issue with the workstation configuration they all use. Another possibility is that the users with the problem are all connected to the same subnet or segment or share some other networking resource that is malfunctioning.
- **How long have they been unable to access the sites?** Some problems can clear up by themselves in minutes, but a continuing or recurring problem can indicate a transient condition that is difficult to troubleshoot.

## Locating the Problem

When a user cannot access a Web site using Internet Explorer, and you have reason to believe that the cause might be something other than a transient Internet condition, and you have obtained all the information you can from the user, it is time to begin investigating the issue yourself.

### REPEATING THE CONDITIONS

The first thing to do, obviously, is to try accessing the same Web site yourself. If you can access the site, and other users still cannot, that tells you there is an issue on those other users' computers or on the network that is preventing them from connecting to the site. For whatever reason that issue is not affecting you means you have to begin looking for network issues that can affect multiple users.

### LOOKING FOR NETWORK PROBLEMS

The next step is to try accessing the Web site from other network segments or subnets. You are attempting to discover whether there is an infrastructure issue affecting part, but not all, of the network. For example, there could be a routing or switching problem that is preventing a specific subnet from accessing the Internet. There could be a cabling problem that has disconnected a subnet from the rest of the network. There could also be a Group Policy configuration issue that is affecting some of the computers on the network, but not all of them.

For a troubleshooter, this type of testing requires a familiarity with the underlying infrastructure of the network. You can try to access a site from various other computers, but unless you know how the network is laid out, you can't draw any conclusions other than the existence of a problem beyond the individual workstation. An enterprise network that has been properly designed and constructed should also be properly diagrammed and documented, so even a technician new to the organization should be able to consult these records to determine what the computers experiencing a problem have in common.

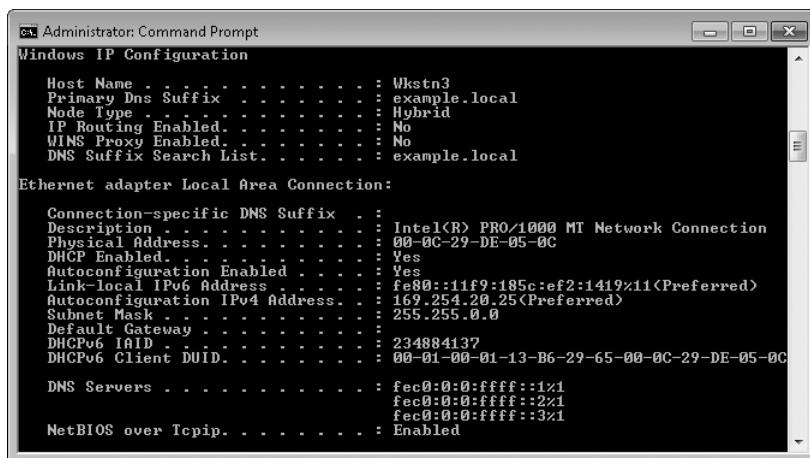
## Testing Possible Causes

Experienced administrators are aware of the problems that are most likely to cause access failures in Internet Explorer, and they can often shortcut the troubleshooting process by checking for those problems first. Some of the most common causes of those type of failure are discussed in the following sections.

### LOOKING FOR DHCP PROBLEMS

A problem with a Dynamic Host Configuration Protocol (DHCP) server can prevent just the computers on a specific subnet from obtaining the IP addresses they need to access the Internet. When a computer running Windows fails to locate a DHCP server, or if the server is unable to supply it with an address, Windows automatically assigns itself an address, using a technique called Automatic Private IP Addressing (APIPA).

APIPA assigns addresses in the 169.254.0.0/16 subnet, as shown in Figure 11-2, which enable the computers to communicate with other APIPA systems, but which are not routable, usually, to the network's Internet interface. This is one possible reason why some computers might be able to access an Internet site, while others cannot. To check for a problem like this, you can look for computers with 169.254.0.0/16 addresses, and if you find them, check the functionality of the DHCP servers on the network.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The title bar also includes "Windows IP Configuration". The content of the window is a text-based output of network configuration details:

```
Administrator: Command Prompt
Windows IP Configuration

Host Name . . . . . : Wkstn3
Primary Dns Suffix . . . . . : example.local
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List. . . . . : example.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address . . . . . : 00-0C-29-DE-05-0C
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::11f9:185c:ef2:1419%11<Preferred>
Autoconfiguration IPv4 Address . . . . . : 169.254.20.25<Preferred>
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID . . . . . : 00-01-00-01-13-B6-29-65-00-0C-29-DE-05-0C

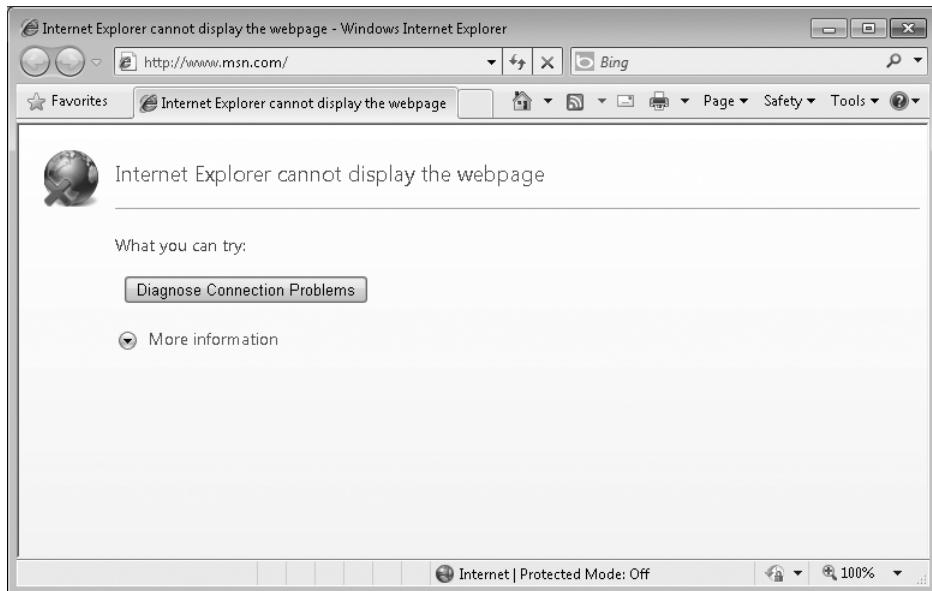
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                         fec0:0:0:ffff::2%1
                         fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

FIGURE 11-2 APIPA addressing

For many desktop administrators, DHCP servers are outside their area of responsibility, and the discovery of an issue like this means that the problem has to be escalated to another team.

## LOOKING FOR DNS PROBLEMS

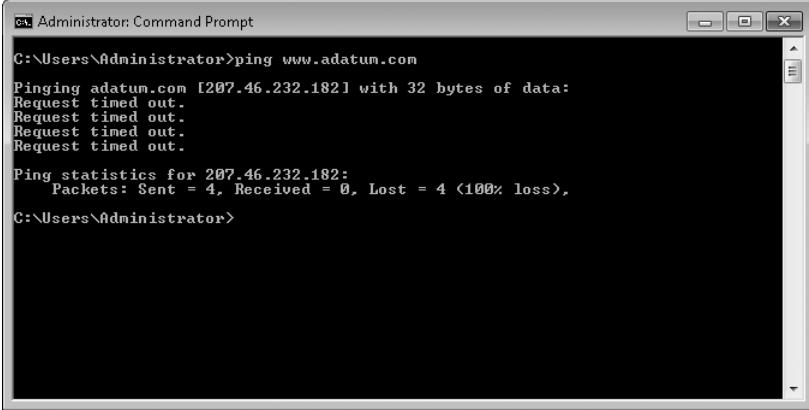
The Domain Name System (DNS) provides computers with the name resolution services they need to access Active Directory Domain Services (AD DS) and Internet resources. When you connect to a Web site using Internet Explorer, the first thing the browser does is resolve the Web server name into an IP address using DNS. If the DNS servers the computer is configured to use are not available, this name resolution process fails, and you see the familiar Internet Explorer Cannot Display The Webpage error message, shown in Figure 11-3.



**FIGURE 11-3** Internet Explorer's primary error message

If a DNS failure is the cause of a computer's inability to access a Web site, it should still be able to access the site using an IP address. Therefore, you can test for a DNS problem by replacing the server name in the URL with the server's IP address.

For example, if a computer cannot access the <http://www.adatum.com> site, but it can access <http://207.46.232.182>, DNS is almost certainly the problem. The 207.46.232.182 IP address is the equivalent of the [www.adatum.com](http://www.adatum.com) server name. You can find the IP address for any Internet domain or server name by pinging the name from a command prompt on another computer. As with Internet Explorer, the Ping.exe program resolves the name into an address before it actually attempts to connect to the server, as shown in Figure 11-4. Even if the Ping test fails, the name resolution process should succeed if the computer's DNS server is operational.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is "ping www.adatum.com". The output shows several "Request timed out." messages followed by a summary line: "Ping statistics for 207.46.232.182: Packets: Sent = 4, Received = 0, Lost = 4 <100% loss>."

```
C:\Users\Administrator>ping www.adatum.com
Pinging adatum.com [207.46.232.182] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.232.182:
    Packets: Sent = 4, Received = 0, Lost = 4 <100% loss>.

C:\Users\Administrator>
```

FIGURE 11-4 The Ping.exe program resolving a DNS name

Every computer has the addresses of one or more DNS servers as part of the TCP/IP configuration. DHCP clients retrieve the DNS server addresses along with their IP addresses and other settings. In a manually configured computer, you must supply at least one DNS address with the other TCP/IP settings, as shown in Figure 11-5.

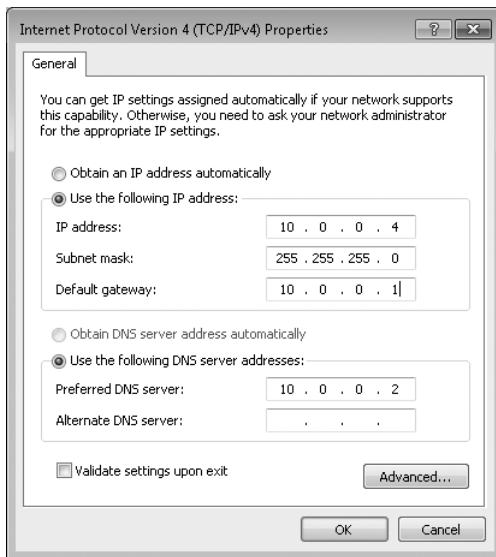


FIGURE 11-5 TCP/IP configuration parameters in a manually configured Windows computer

As with DHCP, DNS problems often fall outside of the desktop administrator's purview, and might require further escalation to another team.

## LOOKING FOR FIREWALL PROBLEMS

Firewalls block network traffic by design, and an improperly configured firewall could prevent users from accessing Internet Web sites. The possibility of unsecured Web sites being blocked by a firewall is minimal, however. Firewalls typically work by blocking port numbers, and virtually all firewall products are configured to permit traffic using the well-known port number 80—the port that Web traffic uses. However, protected Web sites, such as those using Secure Sockets Layer (SSL) encryption, use different port numbers, which are not as well known. The possibility that someone might configure a firewall to block these port numbers is much more likely.

Windows 7 has its own firewall, which the operating system enables by default. Most organizations also have another firewall, to protect the network from intruders on the Internet. Web servers are prime targets for intrusion, so the computers at the other end of the Web connection tend to be behind firewalls as well. Therefore, when a user on your network accesses a Web site on the Internet, the traffic running between Internet Explorer on the client computer and the Web server might have to pass through several firewalls, any one of which can block traffic required for the user to connect to the site.

Each Windows computer has its own individually configurable Windows Firewall service, but on an enterprise network, administrators typically exercise control over all of the firewalls at once using Group Policy, as shown in Figure 11-6. When this is the case, testing for and resolving the problem is a matter of modifying the Group Policy settings that control Windows Firewall.

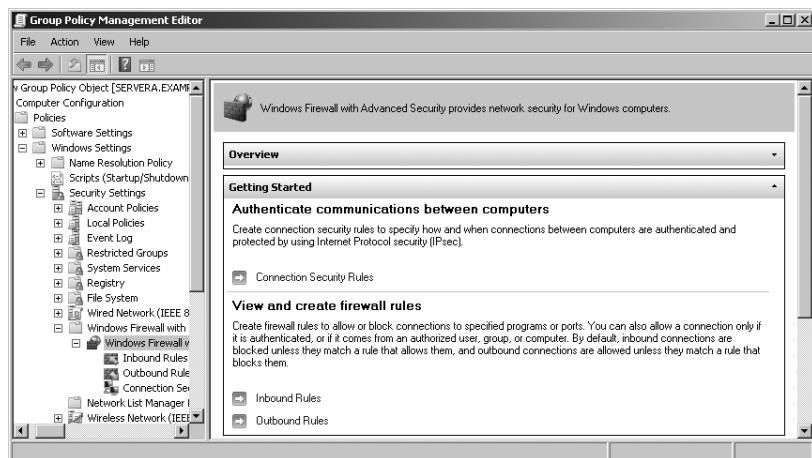


FIGURE 11-6 Group Policy settings that control Windows Firewall



## REAL WORLD

Craig Zacker

Inexperienced network users can typically be said to fall into two camps: those who are afraid to touch anything and those that are utterly fearless. For desktop administrators, the latter type is most dangerous. If you leave control of Windows Firewall up to individual users, most of them leave it alone. In fact, most of them probably do not know it's there. However, there are always those dangerous few with a desire to experiment, and one of the chief benefits of Group Policy is the ability to constrain those instincts.

The easiest way to test whether a firewall is causing a connection problem between a Web browser like Internet Explorer and a Web server is to simply turn it off, temporarily. To do this, in the Group Policy object (GPO) controlling Windows Firewall, you open the Windows Firewall With Advanced Security dialog box, as shown in Figure 11-7. For each of the available profiles, you can set the Firewall State setting to Off, which disables Windows Firewall on each computer to which you apply the GPO.

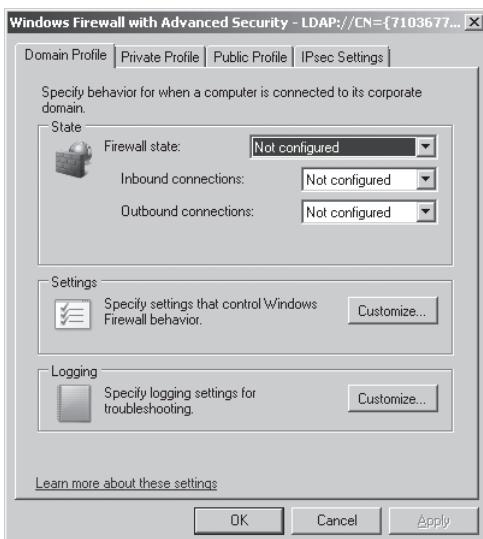


FIGURE 11-7 The Windows Firewall with Advanced Security dialog box in a Group Policy object

To apply the modified GPO settings, you can restart the client computers or execute the following command from a command prompt on each one:

```
gpupdate /force
```

If turning the firewall off resolves the problem, you know that the firewall is configured to block some traffic that is essential to the Web connection. However, leaving the firewall turned off is not a practical option, so it is time to examine the firewall rules, to determine which one is blocking the required traffic. As with other network infrastructure issues, this is usually not the responsibility of a desktop administrator.

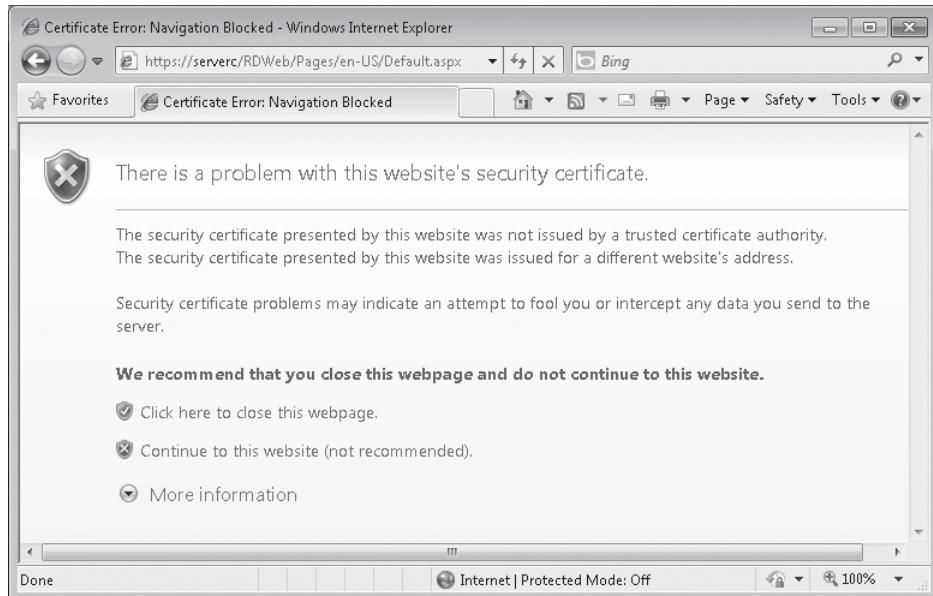
#### **NOTE ADDITIONAL FIREWALLS**

If Windows Firewall on the workstations is not the source of the problem, an enterprise or corporate firewall still might be blocking essential traffic. This firewall could be a third-party product, and this too falls outside of a desktop administrator's jurisdiction.

#### **LOOKING FOR CERTIFICATE PROBLEMS**

The servers hosting secured Web sites typically require digital certificates to confirm their authenticity to clients. The certificates must be issued by an authority that the clients trust so that they know they are actually connecting to the server they expect, and not a bogus system set up by an imposter. For Internet Web servers, the usual procedure is to purchase a certificate from a commercial authority with an established reputation.

If the client trusts the authority, it must also trust any system presenting a certificate issued by the authority. However, if the server is missing the required certificate, or the certificate has expired, or the certificate was issued by an authority the client does not trust, Internet Explorer generates an error message like the one shown in Figure 11-8.



**FIGURE 11-8** An Internet Explorer error caused by a missing or incorrect certificate

In a case like this, administrators can explain the cause of the users' problem, but there is nothing they can do about it, except inform the server administrator of the issue. However, the same certificate issues can pertain to intranet servers as well. Intranet Web servers don't have to use a commercial certification authority (although they can). Because the clients and the server are both part of the same organization, a certificate issued by an internal authority is trusted by both parties. Here again, if the certificate is missing or expired, an error appears, but in this case, the team responsible for the server can resolve the problem by obtaining a new certificate.



### Quick Check

- True or False: When securing its own intranet Web sites, an organization can issue its own digital certificates.

### Quick Check Answer

- True. The organization can issue its own certificates for intranet Web sites because both the client and the server trust the issuing certificate authority.

## Troubleshooting Browser Performance Issues

Internet Explorer is also susceptible to problems that do not result in complete Web site access failures. In some cases, Web sites load partially, or extremely slowly, or even generate permission errors, without the cause being on the server side of the connection.

### Compatibility Problems

Each version of Internet Explorer contains support for new Web programming features and deprecates a number of other features from old browser versions. Many Web sites on the Internet were designed to conform to browser standards that were current at the time, but which now are outdated. As a result, some of these sites do not display properly in the latest browsers, including the Internet Explorer version supplied in Windows 7. Some Web pages might display partially, with certain elements replaced by placeholders, whereas in others the layout of the elements on the page might be incorrect.

Internet Explorer includes a feature called Compatibility View, which enables the browser to emulate older development standards. When the browser displays a Web page that is designed to an older standard, a broken window icon appears, as shown in Figure 11-9. Clicking that icon switches the browser into Compatibility View mode, which can sometimes improve the appearance of the page.



FIGURE 11-9 Internet Explorer, displaying the Compatibility View icon

Users can also create their own lists of sites that Internet Explorer should display using Compatibility View. To do this, select Tools | Compatibility View Settings to display the Compatibility View Settings dialog box, as shown in Figure 11-10.

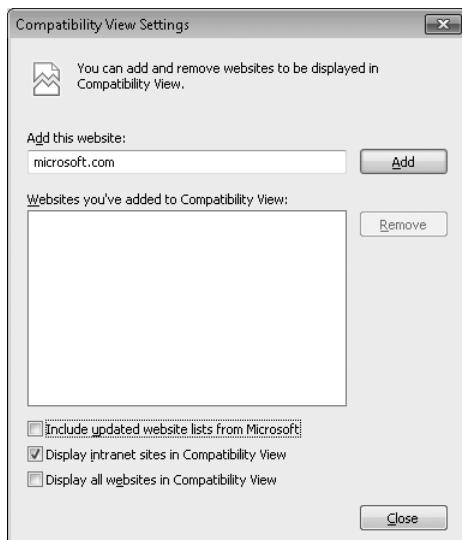


FIGURE 11-10 The Compatibility View Settings dialog box

Advising users to click the Compatibility View icon is clearly more of a usability issue than a technical support one, but it is also possible to configure Compatibility View using Group Policy, to prevent users from experiencing known problems in the first place. For example, you can add known problem sites to a list and distribute it to all of your users as part of a policy setting.

The policy settings for Compatibility View are located in the Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Compatibility View folder of every GPO, as shown in Figure 11-11.

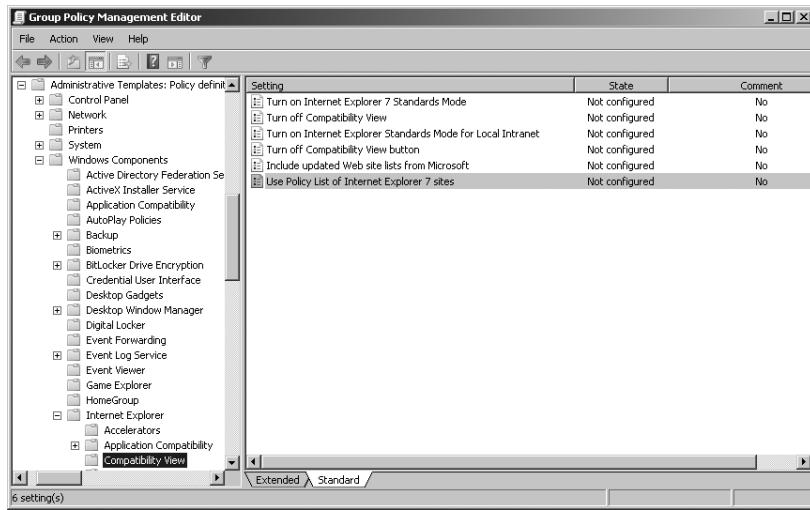


FIGURE 11-11 Compatibility View settings in a Group Policy object

The functions of the Compatibility View policies are as follows:

- **Turn on Internet Explorer 7 Standards Mode** Configures Internet Explorer to display all Web pages using the standard from the previous version of the browser. This enables older Web sites to display normally, but it can cause sites designed to the current standard to display improperly.
- **Turn off Compatibility View** Disables the Compatibility View feature in Internet Explorer, preventing the broken window icon from appearing and disabling the Compatibility View settings.
- **Turn on Internet Explorer Standards Mode for Local Intranet** Configures Internet Explorer to display all intranet content using the standard from the previous version of the browser. Users cannot modify this behavior.

- **Turn off Compatibility View button** Suppresses the appearance of the broken window icon on the Internet Explorer toolbar.
- **Include updated Web site lists from Microsoft** Configures Internet Explorer to use the Microsoft site compatibility lists when displaying Web pages. These lists identify known Internet sites that the browser should display using Compatibility View.
- **Use Policy list of Internet Explorer 7 sites** Enables administrators to create a list of sites that Internet Explorer should display using Compatibility View.

## Security Zone Problems

In addition to providing access to Internet resources, Internet Explorer can also function as the client side of a client/server application. Web-based applications are capable of doing nearly anything that conventionally designed applications can do, as long as they have access to the appropriate system resources. When users require access to Web-based applications, network administrators often use Internet Explorer security zones to regulate the access that the browser provides to system resources.

For example, an intranet application might require the browser to run plug-ins and other components. However, granting Internet sites that kind of access could be dangerous. By adding the intranet site to a security zone with greater access to the system, you can provide it with the resources it needs without endangering the computer.

Internet Explorer defines four security zones, as follows:

- Internet
- Local intranet
- Trusted sites
- Restricted sites

By modifying the settings on the Security tab of the Internet Options dialog box, as shown in Figure 11-12, administrators can specify what level of access the sites in each zone should have. Of course, as with nearly every setting in Windows 7, an enterprise environment complicates the configuration process.

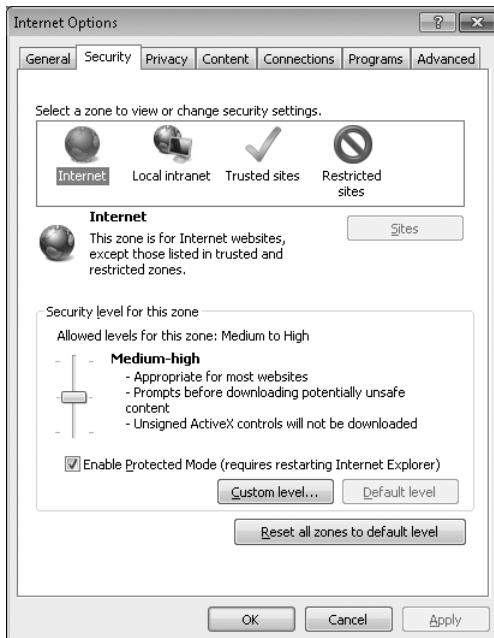


FIGURE 11-12 The Security tab of the Internet Options dialog box

To deploy a Web-based application to a large group of users, you might need to customize the security zone settings and add the site hosting the application to the correct zone. No desktop administrator wants to configure zone settings on hundreds of individual computers, however, so the natural course of action is to configure the zone settings using Group Policy.

When the client side of a Web-based application does not receive access to the resources it needs, it can generate an error message or fail to run entirely, resulting in trouble calls from users. In an enterprise setting, the problem could have any of the following causes:

- The Group Policy settings for the security zones were configured improperly.
- The workstation failed to receive the Group Policy settings from AD DS.
- A user at the workstation modified the security zone settings.
- The site hosting the application was added to the incorrect security zone.

Internet Explorer places sites in the Internet security zone by default, and unfortunately, some support personnel find that the most expedient way to resolve a problem like this is to lower the security level for the Internet zone. This relaxes the security for all of the sites in that zone, which might enable the application to run, but which also opens the system up to attacks from the Internet.

If everyone attempting to access a particular Web-based application experiences a problem, the proper course of action is to make sure that the security level for one of the other zones is set to accommodate the application and that the site hosting the application is added to that zone.

If some users can access the application and others cannot, a Group Policy issue might be preventing the security zone configuration settings from reaching the computers experiencing the problem.

## Add-on Problems

In the course of its development over the years, Internet Explorer has grown from being merely a Web browser to a versatile platform for application deployment. One of the features that facilitates this development is the ability to expand the browser's capability using add-ons. Add-ons are software components—created by Microsoft or by third-party developers—that interact with Internet Explorer by means of an application programming interface (API). This means that an add-on can interact with the internal functions of the browser, enabling Internet Explorer to function as the interface to a software product running on the computer or an application on an Internet site.

If users report that they are unable to access a site or application that requires a special add-on, this should be one of the first things you check in your troubleshooting process. Depending on how the add-on is deployed, the problem might be caused by user error, such as a failure to allow the browser to install the add-on, or there might be a Group Policy issue preventing the computer from installing the add-on.

### PRACTICE Configuring Internet Explorer Settings

---

In this practice, you configure Internet Explorer to use Compatibility View for certain Web sites and modify the default security zone settings.

#### EXERCISE 1 Configuring Compatibility View Settings

The Compatibility View Settings dialog box enables you to specify sites that you want to display in Compatibility View mode.

1. Click the Internet Explorer icon on the taskbar. The Internet Explorer windows appears.
2. In the address box, type **microsoft.com** and press Enter. The Microsoft home page appears.
3. In the address box, type **technet.microsoft.com** and press Enter. The TechNet home page appears, along with the Compatibility View icon.
4. Click Tools | Compatibility View Settings. The Compatibility View settings dialog box appears.
5. In the Add This Website text box, type **http://technet.microsoft.com** and click Add.
6. Click Close.
7. Close Internet Explorer and then launch it again.
8. In the address box, type **technet.microsoft.com** again and press Enter. The TechNet home page appears, this time in Compatibility View mode.
9. Close Internet Explorer.

## **EXERCISE 2 Configuring Security Zone Settings**

To allow trusted sites full access to Internet Explorer functions, reconfigure the Security zone settings as follows.

1. Click the Internet Explorer icon on the taskbar. The Internet Explorer window appears.
2. Click Tools | Internet Options. The Internet Options dialog box appears.
3. Click the Security tab.
4. Select the Local intranet icon.
5. Adjust the Security level slider to Medium.
6. Select the Trusted sites icon.
7. Adjust the Security level slider to Low.
8. Click OK.

## **Lesson Summary**

- The process of troubleshooting Internet Explorer problems is fundamentally the same as that for any IT problem. The procedure can be broken down into the following basic steps: identify the symptoms, determine the scope of the problem, isolate the location of the problem, list possible causes, apply a solution, and test the results.
- Depending on how the IT department of your organization is organized, the role of the Windows 7 desktop administrator in the troubleshooting process might vary. In smaller organizations, you might be responsible for fielding end-user problems and following them wherever they lead. However, in larger organizations, you might find yourself somewhere in the middle of a technical support hierarchy.
- Try accessing the Web site from other network segments or subnets. You are attempting to discover whether there is an infrastructure issue affecting part, but not all, of the network.
- A problem with a Dynamic Host Configuration Protocol (DHCP) server can prevent just the computers on a specific subnet from obtaining the IP addresses they need to access the Internet. When a computer running Windows fails to locate a DHCP server, or if the server is unable to supply it with an address, Windows automatically assigns itself an address, using a technique called Automatic Private IP Addressing (APIPA).
- If a computer cannot access the <http://www.adatum.com> site, but it can access <http://207.46.232.182>, DNS is almost certainly the problem.

- Firewalls block network traffic by design, and an improperly configured firewall could prevent users from accessing Internet Web sites.
- Internet Explorer includes a feature called Compatibility View, which enables the browser to emulate older development standards.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Troubleshooting Internet Explorer Issues." 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. What kind of problem is indicated when Internet Explorer fails to access any sites on the Internet and the computer has an IP address on the 169.254.0.0/16 network?
  - A DNS failure
  - A DHCP failure
  - A Windows Firewall configuration error
  - A missing certificate
2. Which of the following is not a possible cause of a problem that enables Internet Explorer to access standard Web sites using port 80 but not Web sites protected with SSL?
  - A Windows Firewall configuration problem
  - A DNS failure
  - A missing certificate
  - A security zone problem
3. Which of the following methods should you use to test whether a DNS problem is preventing access to an Internet Web site?
  - Modify the security zone settings for the Internet zone.
  - Connect to the site using an *https://* prefix.
  - Check to see if the computer is using a 169.254.0.0/16 address for the DNS server.
  - Use an IP address in the URL rather than a server name.

## Lesson 2: Troubleshooting Group Policy Issues

Group Policy is an essential tool for Windows administrators at all levels. For desktop administrators, Group Policy eliminates the need to manually configure dozens, if not hundreds, of individual Windows 7 settings. For troubleshooters, Group Policy might seem to present a large number of potential problem sources, but compared to checking individual configuration settings on every workstation, troubleshooting Group Policy is a pleasure.

**After this lesson, you will be able to:**

- Recognize problems caused by Group Policy.
- Understand the various ways that workstations can fail to receive Group Policy settings.
- Use Group Policy troubleshooting tools.

**Estimated lesson time: 60 minutes**

### Recognizing Group Policy Issues

Group Policy is simply a mechanism for deploying registry settings to Windows computers on a network. When a user reports that a computer is not functioning properly, in many cases the cause can be traced to an improperly configured registry setting, but that does not necessarily mean that it is a Group Policy issue. The Windows Control Panel and the Registry Editor are also capable of modifying registry settings, and it is the troubleshooter's job to determine how and why the registry was configured incorrectly. For example, you might trace a particular problem to a specific registry setting, but manually altering that setting does no good if there is a Group Policy object that restores the incorrect setting each time the computer restarts.

Therefore, one of the first things a successful Group Policy troubleshooter should know is how your particular organization uses Group Policy. Familiarity with the Group Policy objects deployed to the network and the settings they contain is the best way to determine whether a computer problem is the result of a Group Policy issue and where in the Group Policy infrastructure the cause of the problem is located.

When faced with a problem report that involves Group Policy, one of the first questions the troubleshooter should ask is whether the behavior the user is experiencing is intended or not. For example, administrators can use Group Policy to suppress certain operating system features and interface elements that they do not want users to see. Some users, noting that the interface in their work computers look different from that of their home systems, might think that something is wrong, when in fact the interface is limited by design. Situations like these are simply a matter of educating the user.

However, after you have determined that a computer is malfunctioning because a particular setting is not configured, or not configured correctly, you must then determine how the setting is supposed to be configured. In a properly planned and documented Windows 7 deployment, this information should be part of the workstation configuration, as discussed in Chapter 4, "Configuring Clients."

## Troubleshooting Group Policy Delivery

One of the most fundamental Group Policy issues that can affect Windows 7 performance is the failure of the Group Policy settings to reach the workstation. Administrators can configure settings correctly in a Group Policy object, but if they fail to deploy the GPO correctly, the workstations might not receive that GPO and the settings it contains.

After you determine that a workstation is experiencing a problem because a setting that should be configured using Group Policy has not been configured, you should be able to consult the documentation for your network to determine how the missing setting should have been deployed. In other words, there should be a record somewhere of which GPO should contain the setting and how that GPO should be deployed in AD DS. If no such record exists, you might have to begin the more arduous process of examining the GPOs in your domain and locating the one that contains—or should contain—that specific setting.

### **NOTE CREATING REDUNDANT GPOS**

Many organizations have Group Policy infrastructures that are both complicated and undocumented, usually as a result of being developed as needs arise. An administrator realizes the need to deploy a particular Group Policy setting and, rather than determine how that setting should fit into a carefully planned strategy, the administrator simply creates a new GPO containing that setting and links it to an AD DS object. This method can be effective, but also highly inefficient. The eventual result can be overburdened domain controllers managing dozens of unnecessary GPOs and decreased workstation performance as they apply all of those GPOs.

There are many possible reasons why Windows 7 workstations might not be receiving the Group Policy settings they need. Some of the most common reasons are discussed in the following sections.

## Checking Link Status

After creating a GPO, you deploy it by linking the GPO to an AD DS domain, site, or organizational unit (OU) object using the Group Policy Management console. When you create a link between a GPO and an AD DS object, the console enables the link by default, as you can see by looking at the Link Enabled column, as shown in Figure 11-13.

Link...	GPO	Enforced	Link Enabled	GPO Status	VMI Filter
1	Default Domain Policy	No	Yes	Enabled	None
2	New Group Policy Object	No	Yes	Enabled	None
3	Windows 7 Workstations	No	Yes	Enabled	None

FIGURE 11-13 Enabled links between GPOs and AD DS objects

However, you can also disable a link by right-clicking the GPO and, from the context menu, toggling the Link Enabled indicator. This prevents the computers on the network from applying the settings in the GPO. One of the first things you should check when you are troubleshooting Group Policy issues is whether all of the GPOs are linked to appropriate AD DS objects and whether the links are enabled. You might find, for example, that another administrator disabled a link while working on the GPO and forgot to enable it again.

## Checking Object Location

When you link a GPO to an AD DS domain, site, or OU, all of the objects in that container receive the settings in the GPO. If a workstation fails to receive the Group Policy settings it is supposed to have, it may well be because the computer or user object is not located in the correct container. If, for example, you create a monolithic GPO for workstations in the Sales department and link it to the Sales OU, a computer mistakenly placed in the Marketing OU instead of the Sales OU does not receive those settings. In the same way, if you create a large number of functional GPOs and you mistakenly link one of those to the Marketing OU instead of the Sales OU, the Sales computers do not receive all of the settings they need.

## Checking Computer vs. User Assignments

Group Policy objects have both Computer Configuration and User Configuration settings, and in some cases, there are identical settings that you can assign to either computers or users. When you are troubleshooting a Group Policy issue, you must be conscious of whether the settings a workstation is missing are assigned to the computer itself or the user operating it.

For example, a problem might appear on a workstation not because the GPOs are improperly configured, but rather because the user who is logged on is not a member of the proper security group. Testing this theory might be as simple as logging on with a different user account and trying to re-create the error.

## Checking for Updates

When workstations fail to exhibit the correct Group Policy settings, one possible explanation could be that the system has not yet received a recently configured GPO. To make sure that a computer is up to date in its Group Policy settings, you can restart the system or open a command prompt window and type the following command:

```
gpupdate /force
```

## Checking Policy Inheritance

Checking GPO links and object placement is relatively easy when you are dealing with a simple, flat domain. However, when you have an AD DS hierarchy with multiple layers of OUs, inheritance becomes a critical part of Group Policy deployment and troubleshooting. By default, when you link a GPO to an AD DS object, the settings in that GPO are inherited by all objects subordinate to the linked object.

Most enterprise administrators design their AD DS hierarchies with this tendency in mind. By linking GPOs with more general settings to objects higher up in the AD DS hierarchy, they can then link GPOs farther down that contain only the settings needed by specific workstation types. This makes it easier to maintain and troubleshoot Group Policy because the more general settings are located in only one, or a few, domain-level GPOs, rather than in a dozen or more OU-level GPOs.

For this arrangement to function properly, however, the OUs farther down in the hierarchy must inherit the settings from those farther up. This inheritance, as mentioned earlier, is the default behavior, but there are several mechanisms that can interfere with it, as discussed in the following sections.

## CHECKING FOR BLOCKED INHERITANCE

When you right-click an AD DS object in the Group Policy Management console, and in the context menu, activate the Block Inheritance toggle, the object appears with an exclamation point icon, as shown in Figure 11-14. With this feature activated, the object does not inherit any GPO settings from the parent objects above it. Only the GPOs linked directly to the object that has the block take effect.

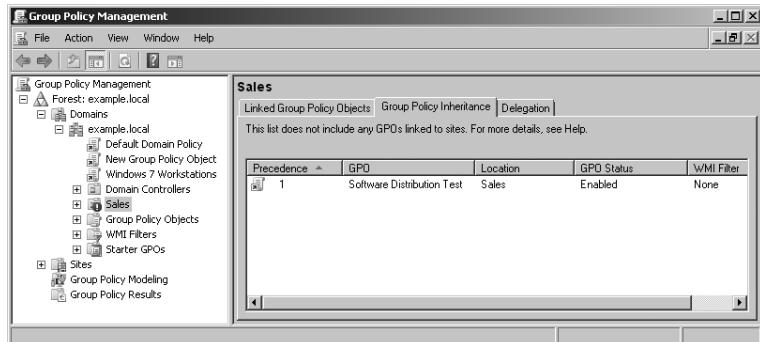


FIGURE 11-14 Blocked inheritance in the AD DS hierarchy

The use of inheritance blocks as a permanent architectural feature of an AD DS hierarchy is generally not recommended because it complicates the administration process and often leads to redundant GPOs and other components. However, troubleshooters should check for existence of blocks, whether temporary or permanent, as a possible cause for workstation Group Policy failures.

## CHECKING PRECEDENCE

As a result of AD DS inheritance, a single object can receive settings from multiple GPOs, and those settings might conflict. Therefore, it is part of the troubleshooter's job to understand how the settings from multiple GPOs interact.

The basic rules for GPO application are as follows:

- GPOs linked to AD DS objects take precedence over local GPOs.
- GPOs linked to OUs take precedence over GPOs linked to domains and sites.
- GPOs linked to domains take precedence over GPOs linked to sites.
- GPOs linked to lower-level OUs take precedence over those linked to higher-level OUs.
- When multiple GPOs are linked to a single object, the GPO linked first takes precedence.

Windows computers apply GPOs with lower precedence first so that their settings can be overwritten by the GPOs with higher precedence. In the Group Policy Management console, when you select an AD DS object, the Linked Group Policy Objects tab displays the GPOs linked directly to that object, as shown in Figure 11-15. The GPO at the top of the list—that is, the one with the lowest number—has the highest precedence and is applied last. Administrators can modify the precedence of the links using the arrow buttons to the left of the list.

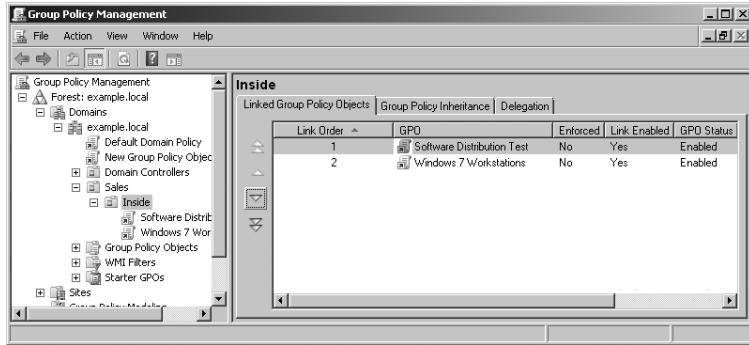


FIGURE 11-15 The Linked Group Policy Objects list in the Group Policy Management console

The Group Policy Inheritance tab, shown in Figure 11-16, lists all of the GPOs applied to the object, including those inherited from parent objects.

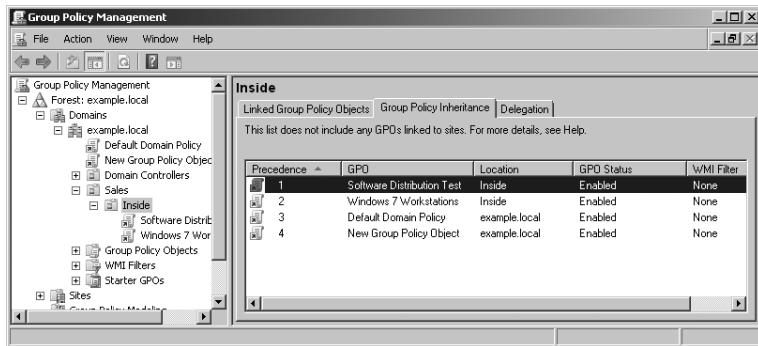


FIGURE 11-16 The Group Policy Inheritance tab in the Group Policy Management console

## CHECKING FOR ENFORCEMENT

Enforcing a GPO, by right-clicking it and selecting Enforced from the context menu, moves it to the top of the precedence list, as shown in Figure 11-17, and prevents any other settings from blocking it.

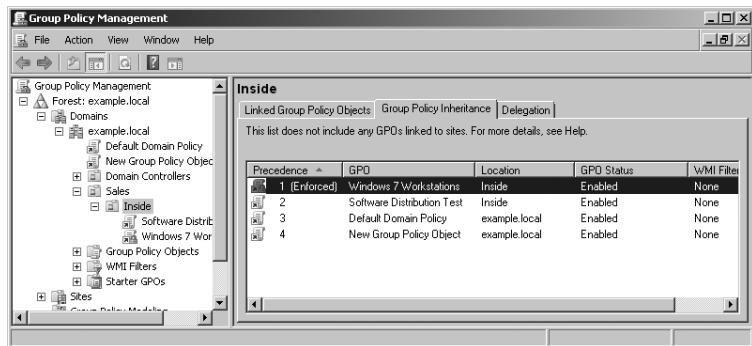


FIGURE 11-17 An Enforced GPO in the Group Policy Management console

## CHECKING SECURITY FILTERING

By default, Windows applies the settings in a GPO to the Authenticated Users special identity, but administrators can use Group Policy's security filtering feature to modify this behavior and limit the settings to specific users, groups, and computers. If workstations are not receiving the settings they need, be sure to check the security filtering feature in each GPO, as shown in Figure 11-18.

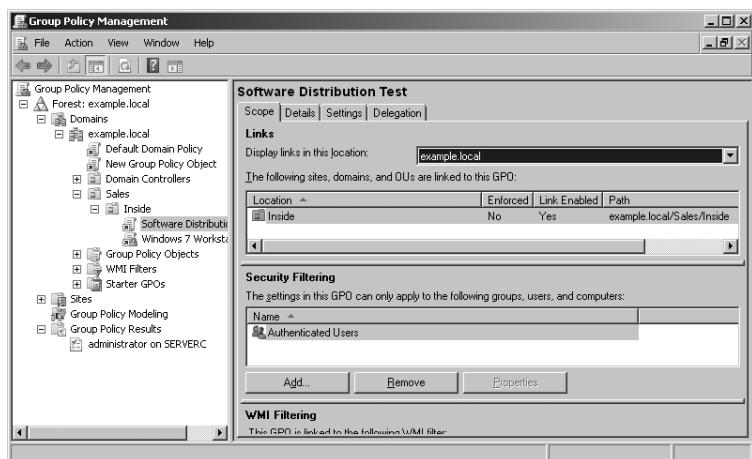
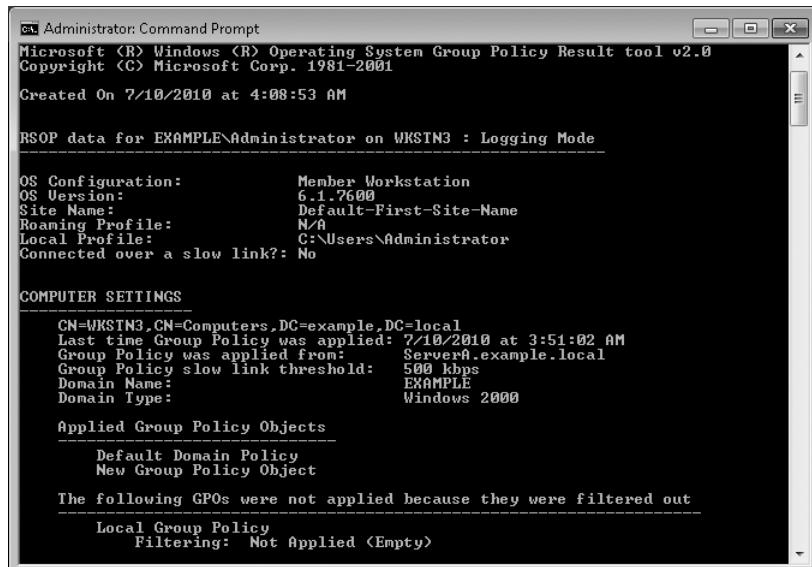


FIGURE 11-18 Security filtering in a GPO

## VIEWING GROUP POLICY RESULTS

As you have seen, many factors can interfere with Group Policy distribution, and examining individual GPOs and their links to AD DS objects for each of these factors can be a laborious task. Fortunately, Windows includes tools that enable you to work backwards from the client instead. Gpresult.exe is a command-line program that enables you to view information about the Group Policy settings that apply to a particular client workstation. In other words, you can use this tool to see which GPOs are operating for that computer.

In its simplest form, you can run Gpresult.exe with the /r parameter from the command prompt on any Windows 7 computer. This produces a display that lists the GPOs supplying the computer and user settings to the system, part of which is shown in Figure 11-19.



The screenshot shows a Command Prompt window titled "Administrator: Command Prompt". The title bar also displays the path "Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0" and the copyright notice "Copyright (C) Microsoft Corp. 1981-2001". The window content is as follows:

```
Created On 7/10/2010 at 4:08:53 AM

RSOP data for EXAMPLE\Administrator on WKSTN3 : Logging Mode

OS Configuration: Member Workstation
OS Version: 6.1.7600
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\Administrator
Connected over a slow link?: No

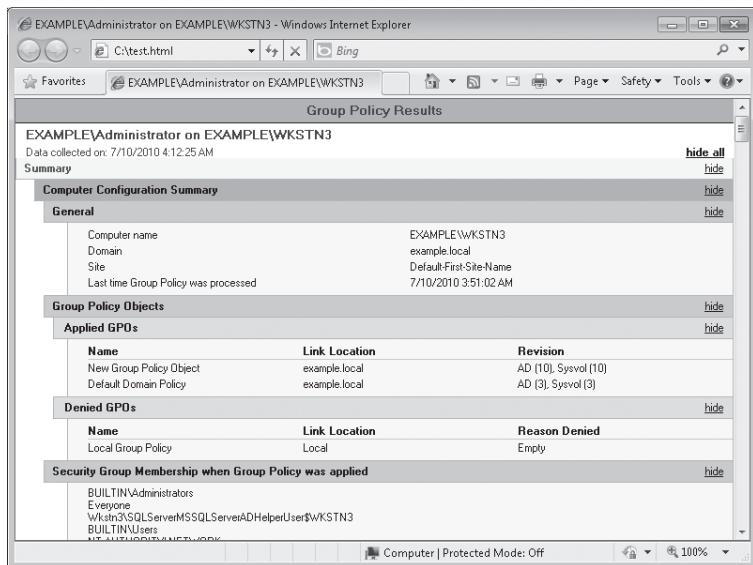
COMPUTER SETTINGS
CN=WKSTN3,CN=Computers,DC=example,DC=local
Last time Group Policy was applied: 7/10/2010 at 3:51:02 AM
Group Policy was applied from: ServerA.example.local
Group Policy slow link threshold: 500 kbps
Domain Name: EXAMPLE
Domain Type: Windows 2000

Applied Group Policy Objects
Default Domain Policy
New Group Policy Object

The following GPOs were not applied because they were filtered out
Local Group Policy
Filtering: Not Applied (Empty)
```

FIGURE 11-19 Using Gpresult.exe at the command prompt

In addition, the program is capable of generating a report in HTML format, which lists all of the policy settings applied to the computer and the user, as shown in Figure 11-20.



**FIGURE 11-20** Using Gpresult.exe to generate an HTML report

Finally, Gpresult.exe is also capable of generating reports for remote systems on the network. You can run the program with the /s parameter from the command prompt, or you can launch the Group Policy Results Wizard from the Group Policy Management console.

#### **NOTE RESULTANT SET OF POLICY**

Gpresult.exe is the latest incarnation of a tool that used to be known as Resultant Set of Policy (RSoP). In fact, RSoP still exists as a snap-in for Microsoft Management Console. If you run Rsop.msc from a computer's Run dialog box or a command prompt, the snap-in appears in a new MMC console. The interface looks almost exactly like that of the Group Policy Management Editor, except that the console contains only the settings applied to the computer. However, for computers running Windows Vista or later, Rsop.msc cannot display all of the settings the system receives through GPOs. For Windows Vista and Windows 7, you must use Gpresult.exe instead.

## Checking Permissions

As with nearly every other element in Windows, users and computers need permissions to access a GPO. By default, GPOs grant the Allow Read permission to the Authenticated Users special identity, which is sufficient for normal circumstances. However, modifying the permissions on a GPO could prevent workstations from receiving settings from it. To check the permissions on a GPO, open it in the Group Policy Management Editor console, right-click the GPO at the root of the console, open its Properties sheet, and click the Security tab.

## Checking for Loopback Processing

Loopback processing is a Group Policy feature designed for kiosks and other public terminals that enables Windows to apply User Configuration settings based on the computer's identity instead of the user's. On a public terminal, you might have user settings you want to apply for all users, not just specific ones, and this option makes that possible.

To use loopback processing, browse to the Computer Configuration\Administrative Templates\System\Group Policy folder and enable the User Group Policy Loopback Processing Mode setting, as shown in Figure 11-21.

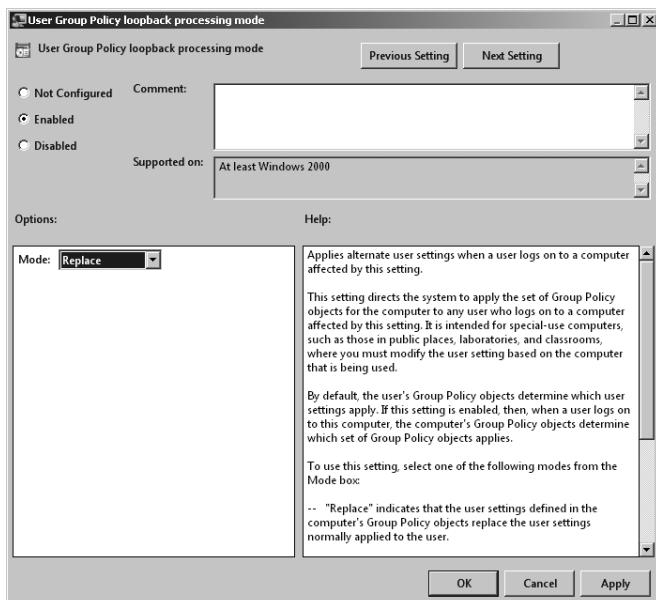


FIGURE 11-21 Enabling loopback processing



---

**EXAM TIP**

When preparing for the 70-686 exam, be sure that you know how to use the Group Policy tools included with Windows 7, including Gpresult.exe and Upupdate.exe.

---

**PRACTICE    Using Gpresult.exe**

---

To display information about the Group Policy objects applied to a workstation, you can use Gpresult.exe.

**EXERCISE 1    Running Gpresult.exe from the Command Prompt**

To run Gpresult.exe from the command line, use the following procedure.

1. Click Start. Then click All Programs | Accessories | Command Prompt. A Command Prompt window appears.
2. At the command prompt, type **gpresult /r > gpresult.txt** and press Enter.
3. Type **notepad gpresult.txt** and press Enter. A Notepad window appears, displaying the output from the Gpresult.exe program.
4. Close the Notepad and Command Prompt windows.

**EXERCISE 2    Creating HTML Reports with Gpresult.exe**

To create an HTML report using Gpresult.exe, use the following procedure.

1. Click Start. Then click All Programs | Accessories | Command Prompt. A Command Prompt window appears.
2. At the command prompt, type **gpresult /h gpresult.htm** and press Enter.
3. Type **gpresult.htm** and press Enter. An Internet Explorer window appears, displaying the output from the Gpresult.exe program in HTML format.
4. Close the Internet Explorer and Command Prompt windows.

## Lesson Summary

- Becoming familiar with the Group Policy objects deployed to the network and the settings they contain is the best way to determine whether a computer problem is the result of a Group Policy issue and where in the Group Policy infrastructure the cause of the problem is located.
- One of the most fundamental Group Policy issues that can affect Windows 7 performance is the failure of the Group Policy settings to reach the workstation.
- After creating a GPO, you deploy it by linking the GPO to an AD DS domain, site, or organizational unit (OU) object using the Group Policy Management console.
- When you right-click an AD DS object in the Group Policy Management console and, in the context menu, activate the Block Inheritance toggle, the object appears with an exclamation point icon. With this feature activated, the object does not inherit any GPO settings from the parent objects above it.
- The basic rules for GPO application are as follows: GPOs linked to AD DS objects take precedence over local GPOs. GPOs linked to OUs take precedence over GPOs linked to domains and sites. GPOs linked to domains take precedence over GPOs linked to sites. GPOs linked to lower-level OUs take precedence over those linked to higher-level OUs. When multiple GPOs are linked to a single object, the GPO linked first takes precedence.
- Gpresult.exe is a command-line program that enables you to view information about the Group Policy settings that apply to a particular client workstation. In other words, you can use this tool to see which GPOs are operating for that computer.

## Lesson Review

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

### **NOTE** ANSWERS

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

1. Which of the following statements about GPO precedence is true?
  - A. GPOs linked to sites take precedence over GPOs linked to domains.
  - B. GPOs linked to higher-level OUs take precedence over those linked to lower-level OUs.
  - C. Local GPOs take precedence over Active Directory Domain Services GPOs.
  - D. GPOs linked to OUs take precedence over GPOs linked to domains.
2. When workstations are failing to receive the Group Policy settings they need, it could be because security filtering has limited GPO distribution to specific \_\_\_\_\_.
  - A. Domains
  - B. Security groups
  - C. Sites
  - D. Organizational units
3. Which of the following tools can you use to make sure that a workstation has received all of the latest GPO modifications?
  - A. Gpresult.exe
  - B. Gpupdate.exe
  - C. Group Policy Management Console
  - D. Resultant Set of Policy

## Chapter Review

---

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

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

## Chapter Summary

- Internet Explorer tends to be a frequent source of help desk calls and technical support requests. Failures can be caused by the browser itself, by the Internet Web server the user is trying to access, or by any one of the many systems in between. There are also a number of infrastructure services indirectly related to the client/server communication that cause problems.
- Group Policy is an essential tool for Windows administrators at all levels. For desktop administrators, Group Policy eliminates the need to manually configure dozens, if not hundreds, of individual Windows 7 settings. For troubleshooters, Group Policy might seem to present a large number of potential problem sources, but compared to checking individual configuration settings on every workstation, troubleshooting Group Policy is a pleasure.

## 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.

- Automatic Private IP Addressing (APIPA)
- Compatibility View
- Gpresult.exe
- Resultant Set of Policy (RSoP)

## Case Scenarios

In the following case scenario, you will apply what you've learned about subjects of this chapter. You can find answers to the scenario questions in the "Answers" section at the end of this book.

### Case Scenario 1: Troubleshooting a Web-Based Application

Adrian is a desktop administrator for Contoso, Corp. He has recently completed a large deployment project in which he upgraded 200 Windows XP workstations to Windows 7. Unfortunately, Adrian has just discovered that a cloud-based application those workstations require was not tested during the deployment. The users access the application by loading a Web-based client hosted by a Web site at <https://www.adatum.info>. When the users load the client using the version of Internet Explorer in Windows 7, several vital page components fail to run.

After performing his own tests, Adrian has determined that the client runs properly in Compatibility View mode, but he wants to implement a fix using Group Policy so that users don't have to correct the condition themselves. He also does not want to modify the display of any sites other than the client. Which of the following combinations of Group Policy settings must Adrian deploy to the workstations? Explain your answer.

A.

Turn on Internet Explorer 7 Standards Mode	Enabled
Turn off Compatibility View	Enabled
Turn on Internet Explorer Standards Mode for Local Intranet	Not configured
Turn off Compatibility View button	Not configured
Include updated Web site lists from Microsoft	Not configured
Use Policy list of Internet Explorer 7 sites	Not configured

B.

Turn on Internet Explorer 7 Standards Mode	Not configured
Turn off Compatibility View	Disabled
Turn on Internet Explorer Standards Mode for Local Intranet	Not configured
Turn off Compatibility View button	Disabled
Include updated Web site lists from Microsoft	Enabled
Use Policy list of Internet Explorer 7 sites	Not configured

**C.**

Turn on Internet Explorer 7 Standards Mode	Enabled
Turn off Compatibility View	Not configured
Turn on Internet Explorer Standards Mode for Local Intranet	Enabled
Turn off Compatibility View button	Not configured
Include updated Web site lists from Microsoft	Not configured
Use Policy list of Internet Explorer 7 sites	Not configured

**D.**

Turn on Internet Explorer 7 Standards Mode	Not configured
Turn off Compatibility View	Not configured
Turn on Internet Explorer Standards Mode for Local Intranet	Not configured
Turn off Compatibility View button	Not configured
Include updated Web site lists from Microsoft	Not configured
Use Policy list of Internet Explorer 7 sites	Enabled

## Case Scenario 2: Deploying a GPO

Richard has a collection of Group Policy settings that he must deploy to the workstations of the company department heads, so they can run a timesheet application for the hourly employees. He has created a GPO containing those settings and has named it TimesheetApp. After linking the GPO to the domain object in Active Directory Domain Services, Richard quickly received a number of problem calls from salaried employees, complaining that the application they use to file their expenses has stopped working. Testing has established that it is the settings in the TimesheetApp GPO that are causing the expense voucher application to malfunction. How can Richard deploy the TimesheetApp GPO to the department heads only, without interfering with the other application?

## Suggested Practices

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

### Troubleshooting Internet Explorer Issues

- **Practice 1** Draw a diagram of the technical support hierarchy in your organization, specifying the nature of the tiers and the circumstances under which incidents are escalated.
- **Practice 2** Examine the Windows Firewall rules on your computer and determine what rules would block the secured sites you regularly access.

### Troubleshooting Group Policy Issues

- **Practice 1** Study the Gpresult.exe report for your computer and examine the settings applied to it with Group Policy.
- **Practice 2** Install the Group Policy Management console on your computer and, based on a Gpresult.exe report, examine the settings in the GPOs applied to your workstation.

## 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 70-686 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.

# Troubleshooting Networking and Authentication-Authorization Issues

**A**t one time in the business world, the data network was a convenience, enabling users to access shared printers and files. If a workstation experienced a problem with its network connectivity, the user could continue to work on most tasks. Today, however, users often rely on the network for their applications and their communications, as well as storage and resource sharing. Without the Web, without e-mail, without network applications, productivity stops, so network configuration troubleshooting is one of the most important skills for the desktop administrator.

## Exam objectives in this chapter:

- Identify and resolve networking issues.
- Identify and resolve authentication and authorization issues.

## Lessons in this chapter:

- Lesson 1: Troubleshooting Network Issues **470**
- Lesson 2: Troubleshooting Authentication and Authorization Issues **488**

## Before You Begin

---

To complete the practice exercises in this chapter, you must have the following:

- For the Lesson 1 practice, a computer running Windows 7 with access to the Internet
- For the Lesson 2 practice, a computer running Windows 7 that is a member of an Active Directory Domain Services (AD DS) domain

## Lesson 1: Troubleshooting Network Issues

---

When a workstation fails to connect to the network, there are literally dozens of possible reasons for the failure. For this reason, a thorough understanding of the basic troubleshooting procedures described in Chapter 11, “Troubleshooting Internet Explorer and Group Policy Issues” is critical. In a medium to large enterprise, it is relatively rare for one person to handle all of the technologies that are required to provide network connectivity, so it is important for the troubleshooter to isolate the location of the problem as soon as possible and, if necessary, escalate the issue to the appropriate team.

Although there are some common factors that can affect all network connections, the first thing a troubleshooter typically wants to know is which of the three basic connection types the person experiencing the problem is using: wired, wireless, or remote. Each of these network types has a different set of faults that they experience most frequently. These faults, and the techniques for troubleshooting them, are discussed in the following sections.

**After this lesson, you will be able to:**

- Troubleshoot wired network connections.
- Troubleshoot wireless network connections.
- Troubleshoot remote network connections.

**Estimated lesson time: 60 minutes**

### Troubleshooting Wired Network Connections

The same infrastructure problems that can prevent Windows Internet Explorer from accessing Web sites, as discussed in Chapter 11, can also apply to general networking failures. A network configuration problem often affects all network communications, so if a user reports an issue with one task or application, one of a troubleshooter’s first priorities should be to determine whether the problem is a general networking failure or one that is specific to an application or resource.

When a workstation on a wired network has no network connectivity at all, the next step for the troubleshooter is to determine if other computers are similarly afflicted. This can help to determine whether the problem is in the workstation itself or caused by an external infrastructure failure.

## Checking TCP/IP Configuration Settings

Every workstation on a Windows network must be configured with TCP/IP settings that provide it with an identity and the information needed to communicate with other computers. Checking the TCP/IP configuration is a basic troubleshooting step because misconfigured settings can manifest themselves as several different types of networking failures.

The primary Windows tool for examining TCP/IP configuration settings is `Ipconfig.exe`, a command-line program that displays all of the computer's network configuration settings. When you run `Ipconfig.exe` with the `/all` parameter, you see a display like that shown in Figure 12-1.

```
C:\Users\Administrator>ipconfig /all
Windows IP Configuration

Host Name . . . . . : Wkstn3
Primary Dns Suffix . . . . . : example.local
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : example.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . : example.local
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address . . . . . : 00-0C-29-DE-05-0C
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::11f9:185c:ef2:1419%11<Preferred>
    IPv4 Address . . . . . : 10.0.0.51<Preferred>
        Subnet Mask . . . . . : 255.255.255.0
        Lease Obtained . . . . . : Thursday, July 08, 2010 7:43:27 PM
        Lease Expires . . . . . : Friday, July 16, 2010 7:43:24 PM
        Default Gateway . . . . . : 10.0.0.1
        DHCP Server . . . . . : 10.0.0.3
        DHCPv6 IAID . . . . . : 234884137
        DHCPv6 Client DUID . . . . . : 00-01-00-01-13-B6-29-65-00-0C-29-DE-05-0C
    DNS Servers . . . . . : 10.0.0.2
    NetBIOS over Tcpip. . . . . : Enabled
```

FIGURE 12-1 The `Ipconfig.exe` output display

As you can see, `Ipconfig.exe` displays the computer's IP addresses, both version 4 and version 6, as well as its subnet mask and all of the other required configuration parameters. One of the most important advantages of using `Ipconfig.exe` is that it displays settings obtained from Dynamic Host Configuration Protocol (DHCP) servers. The Internet Protocol Version 4 (TCP/IPv4) Properties sheet, shown in Figure 12-2, displays some of the same information, but only when you have manually configured the settings; DHCP settings do not appear in this interface.

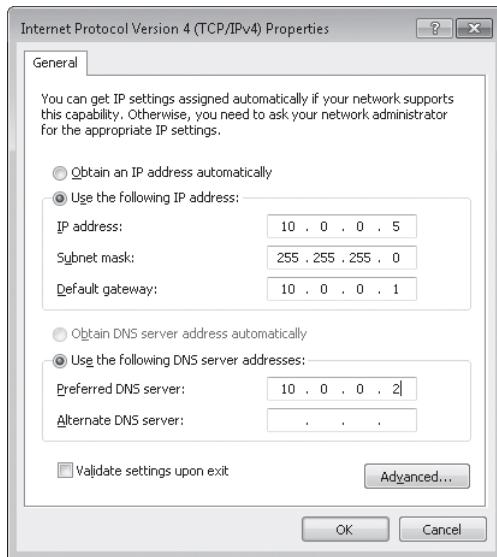


FIGURE 12-2 The Internet Protocol Version 4 (TCP/IPv4) Properties sheet

Some of the most important settings that appear in the `Ipconfig.exe` display, as well as their potential implications in network troubleshooting, are as follows:

- **DHCP Enabled** Indicates whether the computer obtained its TCP/IP configuration settings from a DHCP server.



#### EXAM TIP

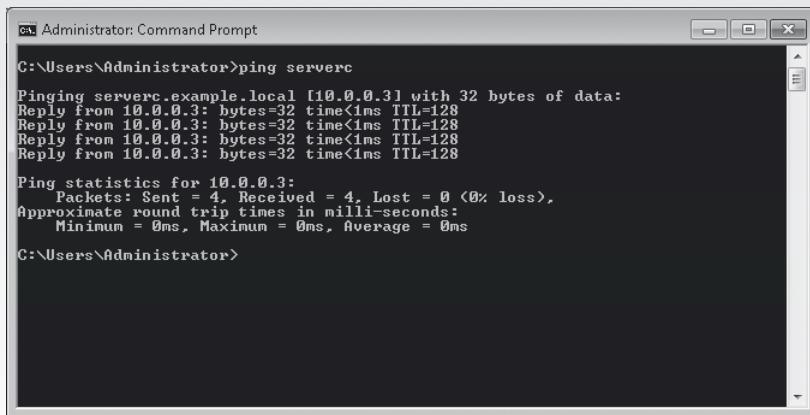
When you prepare for the 70-686 exam, be aware that when DHCP is enabled, any problems with the other settings should affect other computers on the network as well. If the DHCP Enabled value is Yes and the computer's IP address is on the 169.254.0.0/16 subnet, the computer was unable to access a DHCP server and assigned itself an address.

- **IPv4 Address** Every computer on a TCP/IP network must have a unique IP address. If the computer's address is assigned by DHCP, duplicate addresses are almost never a problem, but systems manually configured with duplicate addresses generate error messages to the user. A manually configured IP address on the wrong network prevents all network communications from occurring.
- **Subnet Mask** Specifies which bits of the IP address identify the network and which bits identify the host on the network. If the computer is configured by DHCP, problems with this setting are unlikely. On a manually configured computer, an incorrect value prevents all network communications from occurring.

- **Default Gateway** Specifies the IP address of a router that provides access to other networks. If this address is missing or incorrect, the computer can access resources on the local network but cannot communicate with other networks. If the address is correct but the router is malfunctioning, the other computers on the local network experience the same problem.
- **DNS Servers** Specifies the IP address of at least one Domain Name System (DNS) server on the network. If the address is missing or incorrect, the computer cannot connect to Internet servers by name because it cannot resolve the names into IP addresses.

**TIP USING PING.EXE**

Ping.exe is the Windows version of a standard TCP/IP network testing tool. When you run Ping.exe from the command prompt with the name or IP address of another TCP/IP computer, the program transmits a series of Echo Request messages using a protocol called Internet Control Message Protocol (ICMP). The computer receiving those messages then replies with a series of Echo Reply messages, which Ping.exe displays to the original user, as shown in Figure 12-3.



A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the output of a "ping" command. The command was run from the path "C:\Users\Administrator>" and targeted the IP address "10.0.0.3". The output shows four successful echo replies, each with 32 bytes of data and a time less than 1ms. It also provides statistics for the ping, indicating 4 packets sent, 0 lost, and a round-trip time of 0ms.

```
C:\Users\Administrator>ping serverc

Pinging serverc.example.local [10.0.0.3] with 32 bytes of data:
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

FIGURE 12-3 A successful Ping.exe test

A successful Ping.exe test indicates that the other computer is up and running, and has a functional TCP/IP networking stack. Failure of a Ping.exe test can indicate that the destination computer is turned off, is disconnected from the network, or has a firewall configured to block ICMP traffic.

### Quick Check

- If a DHCP server is configured to supply clients on a particular subnet with the wrong Subnet Mask value, will the computers still be able to communicate?

### Quick Check Answer

- Yes. As long as the computers on the subnet have the same Subnet Mask value, they will be able to communicate.

## Checking for Hardware Problems

At one time, networking was an optional feature on computers, and administrators had to manually install network interface adapters and the device drivers they need to function. Today, virtually all new computers have a network adapter integrated into the motherboard, and in most cases, Windows 7 is capable of automatically detecting, configuring, and installing drivers for that adapter.

This does not mean that troubleshooters can discount hardware as a possible source of networking problems, however. There are still a variety of hardware malfunctions that can inhibit network communications at many levels.

Manual driver configuration is largely a thing of the past, but a missing network adapter driver or a driver conflict with another device can cause all network communication to cease. The first place to check for driver issues is the Device Manager tool. When Windows fails to locate a required driver, the device appears with a warning icon in Device Manager, as shown in Figure 12-4.

The networking capabilities of a workstation can be affected by hardware problems outside the computer too, of course. An unplugged or damaged cable can cause permanent or transient interruptions, as can a malfunctioning switch or hub. Network interface adapters typically have a light emitting diode (LED) next to the cable jack called a link pulse indicator. When the adapter on a computer is properly connected to a switch or hub, the two devices exchange link pulse signals, causing the indicator to light. If the indicator on a workstation's network adapter is unlit, the cable could be broken or disconnected, or the device at the other end of the cable could be malfunctioning.

#### **NOTE** NETWORK ADAPTER LINK PULSE SIGNALS

Network interfaces exchange link pulse signals even when the computer is turned off.

As long as the power supply is connected to an AC source, the network adapter receives current and exchanges signals with the device at the other end of the cable.

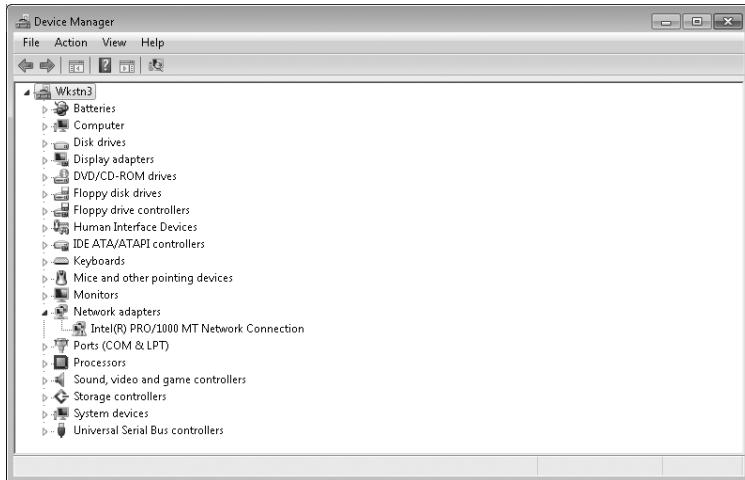


FIGURE 12-4 The Device Manager with a missing driver

## Checking for Infrastructure Problems

As mentioned in Chapter 11, infrastructure issues can also affect network communications in a variety of ways. The first step in determining whether a network communications problem is caused by an infrastructure failure is to see if other computers on the network are experiencing the same problem. For example, a DHCP problem almost always affects other computers because if a DHCP server is configured to provide incorrect TCP/IP settings, all of the computers on the network receive those same settings. The same is true of a DNS problem. If a DNS server fails, all of the computers that rely on it for name resolution suffer the same problem.

### DETECTING ROUTING ISSUES

A router is a device that connects one network to another, passing traffic between the two as needed. Enterprise networks can have dozens of routers, and the Internet has thousands. When a user accesses a Web site on the Internet, the traffic might pass through 20 or more routers on its way from the source to the destination. Each one of the routers along the way is referred to as a hop.

When a router malfunctions, the computers on each side are isolated from each other. Depending on the design of the networks, the effect of a router failure can be minimal or catastrophic. If the router that connects an enterprise network to the Internet should fail, internal systems are cut off from Internet resources. For a user in the enterprise, this can mean an annoying delay in accessing a Web site, but for a company, this can also mean that customers on the Internet are unable to place orders, which makes it a much more critical failing.

Some enterprise networks have redundant internal routers so that if one fails, traffic can simply take another route to its destination. On networks with no such redundancy, however, a router failure can mean that users are able to access some network resources, but not others. On the Internet, router failures typically cause minor delays, but on rare occasions, a critical router can fail, isolating large parts of the Internet from each other. For the troubleshooter, the difficult question can be to determine which router is malfunctioning. In the case of an internal router failure, the appropriate support team must address the problem as soon as possible. If a router on the Internet has failed, typically there is nothing to do but wait.

#### **TIP USING TRACERT.EXE**

Tracert.exe is the Windows version of a command-line tool originally called traceroute, which can help administrators locate a malfunctioning router. Tracert.exe works by transmitting groups of ICMP Echo Request messages, with each group configured to go one hop beyond the previous one. The program then resolves the address of the router at each hop into a name and displays a trace listing the routers between the source and the destination systems, like the following:

```
Tracing route to www.adatum.co.uk [10.146.1.1]
over a maximum of 30 hops:
  1 <10 ms  1 ms  <10 ms  192.168.2.99
  2 105 ms  92 ms  98 ms  qrvl-67terminal01.epoch.net [172.24.67.3]
  3 101 ms  110 ms  98 ms  qrvl.epoch.net [172.24.67.1]
  4 123 ms  109 ms  118 ms  svcr03-7b.epoch.net [172.24.103.125]
  5 123 ms  112 ms  114 ms  clsm02-2.epoch.net [172.24.88.26]
  6 136 ms  130 ms  133 ms  sl1-0-T3.fabrikam.net [10.228.116.5]
  7 143 ms  126 ms  138 ms  sl1-3.fabrikam.net [192.168.5.117]
  8 146 ms  129 ms  133 ms  sl1-12-0.fabrikam.net [192.168.5.1]
  9 131 ms  128 ms  139 ms  sl1-13-0.fabrikam.net [192.168.18.38]
 10 130 ms  134 ms  134 ms  sl1-8-0.fabrikam.net [192.168.7.94]
 11 147 ms  149 ms  152 ms  sl1-0.fabrikam.net [192.168.173.10]
 12 154 ms  146 ms  145 ms  ny2-ge021.router.demon.net [172.21.173.121]
 13 230 ms  225 ms  226 ms  tele-ge023.router.demon.net [172.21.173.12]
 14 233 ms  220 ms  226 ms  tele-fxp1.router.demon.net [10.159.252.56]
 15 223 ms  224 ms  224 ms  tele-14.router.demon.net [10.159.254.245]
 16 236 ms  221 ms  226 ms  tele-165.router.demon.net [10.159.36.149]
 17 220 ms  224 ms  210 ms  www.adatum.co.uk [10.146.1.1]

Trace complete.
```

By running a trace between a source computer and a selected destination, you can determine how far the traffic gets before it encounters a nonfunctioning router. In the case of computers experiencing problems connecting to Internet sites, this is a way for the troubleshooter to confirm that the problem is located outside the enterprise. Pathping.exe, another tool included with Windows 7, combines the functionality of Ping.exe and Tracert.exe.

## DETECTING FIREWALL ISSUES

Firewall problems can be complicated. Whereas at one time, a network would be likely to have only a single firewall, today almost every computer has one, and enterprise networks typically have a corporate firewall as well. The combination of filters in these firewalls can have a cumulative effect on network traffic that can make it difficult to locate the real source of a problem.

Turning firewalls off is a good way to determine whether they are the cause of a problem, but after that, the troubleshooter must figure out what essential traffic is being blocked and which firewall is blocking it. Only then is it possible to propose a modification to the firewall configuration.

## Using Network Monitor

**N**etwork Monitor is a protocol analyzer, a graphical tool that captures samples of the data packets transmitted over a network and examines their contents.

Looking inside a packet, you can see which protocols the computers are using at each layer of the networking stack, as shown in Figure 12-5. You can also examine the traffic patterns on the network, to see which protocols are getting through and which are being stopped by firewalls.

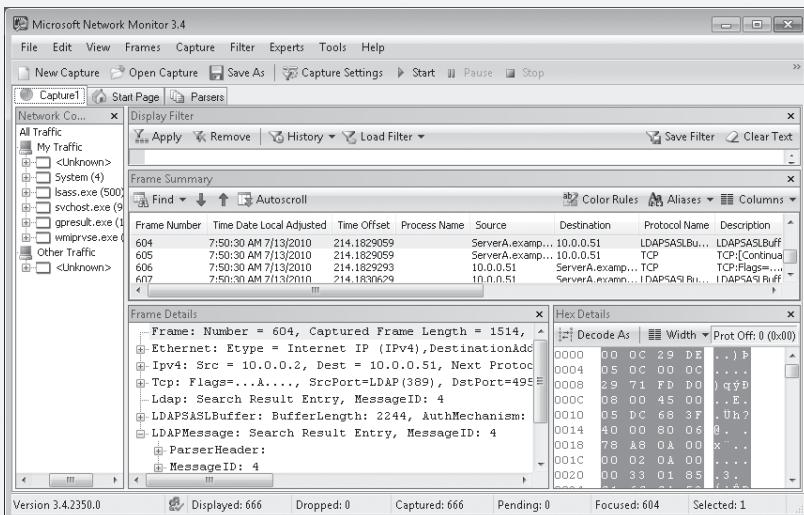


FIGURE 12-5 A packet captured in Network Monitor

Network Monitor 3.4 is a free download from the Microsoft Download Center at <http://go.microsoft.com/fwlink/?LinkId=198217>. Administrators should note, however, that Network Monitor is not only a difficult tool to use effectively, requiring knowledge of TCP/IP and Windows networking, it is also a potentially dangerous tool. Using Network Monitor, an individual can examine the data inside network packets, possibly including passwords and other unprotected information. Unauthorized personnel should be prohibited from using the tool.

## NETWORKING AND BRANCHCACHE

Troubleshooting is not always a matter of solving user problems, such as service outages and connection failures. Network conditions can also have subtle or transient effects on the performance of various applications and services. In these cases, just detecting the problem can be difficult, and resolving it can require extensive knowledge both of networking and of the application or service in question.

BranchCache is a peer caching technology that is designed to conserve bandwidth between remote sites connected by relatively slow and expensive wide area network (WAN) links. The effectiveness of BranchCache is based on the performance of those links. BranchCache clients save data to their local caches only when the time it takes to transmit data between the client and the remote server—called the latency interval—exceeds a certain threshold. If administrators find that the clients are not caching data as expected, it is possible that the actual latency of the network connection is not exceeding the threshold. In other words, the WAN connection is too fast.

The solution is either to slow down the WAN, which is probably not desirable, or adjust the threshold. The Group Policy setting that controls the threshold is Configure BranchCache For Network Files, as shown in Figure 12-6, which is located in the Computer Configuration\Policies\Administrative Templates\Network\BranchCache folder of a Group Policy object (GPO). The default value for the setting is 80 ms. Decreasing the value causes the client to cache more files; increasing the value causes it to cache fewer files.

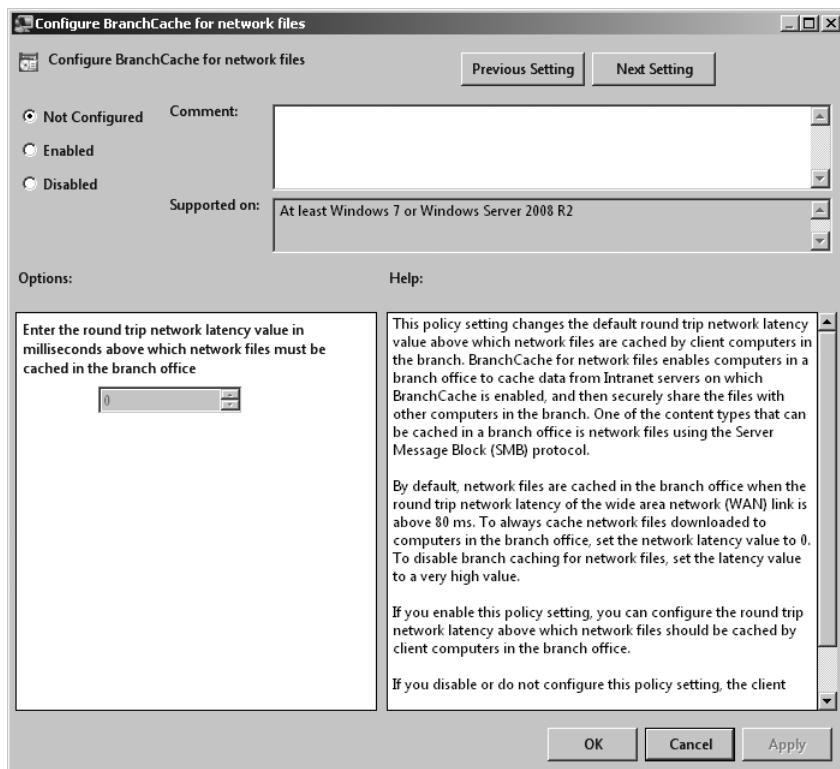


FIGURE 12-6 The Configure BranchCache For Network Files policy setting

# Troubleshooting Wireless Network Connections

Wireless networks are susceptible to many of the same faults as wired networks. Wireless computers use much of the same infrastructure, so DHCP, DNS, routing, and firewall problems can have the same effect as they would on wired systems. However, wireless networks are also subject to other types of problems that generally occur more frequently. Troubleshooters must be conscious of the types of issues that are most common for the platforms they're working on, so they don't waste time on areas that are unlikely to be the cause of the problem they are trying to resolve.



## REAL WORLD

Craig Zacker

**M**edical students learn about hundreds of diseases, and it is typical for them to find the uncommon, peculiar ones to be more interesting than the familiar and mundane. As a result, their superiors often have to remind them that when they hear hoof beats, they should think horses, not zebras, meaning that when diagnosing an ailment, they should start with the obvious first. The same is true in computer troubleshooting. For example, if a wired computer fails to connect to the network, do not start by checking the configuration of the network adapter driver; check the simple things first, such as whether the network cable is plugged in.

## Checking for Transmission Issues

The inherent uncertainty of radio transmissions is the single biggest difference between wireless and wired networks. Therefore, in the case of a networking problem involving wireless computers, you should consider transmission issues as possible causes before you proceed on to the TCP/IP configuration and infrastructure issues discussed earlier.

The single most common cause of networking failures on wireless networks, whether permanent or intermittent, is the inability of the computer to acquire a signal from a wireless access point. There are many possible reasons for a signal acquisition failure, including excessive distance, intervening walls and structures, antenna configuration, and electromagnetic interference.

It is often the case with wireless networking that conditions that were favorable for a connection on one day are unfavorable on the next, and it is difficult, if not impossible, for an administrator with the usual tools and skills to determine why. However, because wireless computers are frequently mobile, the easiest way to test for a transmission issue can often be to move the computer closer to the wireless access point.

If network connectivity improves, you must consider some way to make that adjustment more permanent. You can install additional wireless access points on the network; install a more effective antenna on the computer; remove sources of interference, such as microwaves and cordless phones; or just keep the computer closer to the access point.

## Detecting Encryption Issues

Another extremely common source of wireless networking failures is the incompatibility or misconfiguration of wireless security protocols. As in any communications system, both parties must speak the same language. When they do not, no communication is possible.

Wired networks are vulnerable to attacks facilitated by signal interception, but the attacker must have physical access to the network, in the form of a computer with a network cable connection. Wireless networks are also vulnerable, but access to them is much easier to achieve. In many cases, attackers can covertly access a wireless network from a mobile computer in a building's parking lot.

To protect a wireless network, security protocols are essential, and all of the wireless equipment on the network must support the same one. Most of the early wireless LAN systems supported the Wired Equivalent Privacy (WEP) protocol, but this was found to have some serious shortcomings. Today, most wireless LAN implementations support Wi-Fi Protected Access (WPA and WPA2).

Wireless security protocols do not have automatic negotiation capabilities, as many other communication protocols do. For example, when two wireless devices based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards attempt to connect, they negotiate the fastest common standard they possess, falling back on the slower standards to maintain compatibility. By contrast, administrators must configure the devices to use a specific security protocol in a specific mode. If the two devices do not use the same protocol, they cannot communicate.

Wireless LAN devices typically have some means of displaying the other wireless devices they detect in the area, as shown in Figure 12-7, so troubleshooters can easily distinguish between transmission issues and encryption issues. If a computer is receiving a reasonably strong signal from an access point to which it cannot connect, the security protocol or its configuration are most likely the reason for the failure.

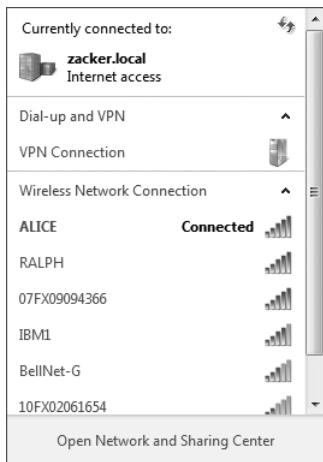


FIGURE 12-7 Detected wireless devices

In addition to using the correct security protocol, wireless devices must also have that protocol configured identically. For example, devices configured to use WPA or WPA2 must have the same encryption option setting, which specifies the algorithm they use to encrypt data, and more important, the same passphrase. A passphrase is an alphanumeric string that you select, which the devices use to encrypt data. If you don't configure all of the devices on the network with the same passphrase, they cannot communicate.

Determining whether a wireless communication problem is being caused by an encryption issue is relatively simple. If you temporarily turn off the encryption on both devices and they are able to communicate, encryption is definitely the problem. Troubleshooting security protocol settings can be problematic, however, because computers and access points use different interfaces for security configuration. Sometimes options for the same setting or feature have different names, and the process of getting devices to communicate can be a matter of trial and error.

For example, the Windows 7 Wireless Network Properties sheet, shown in Figure 12-8, refers to the encryption protocol as the Security type.

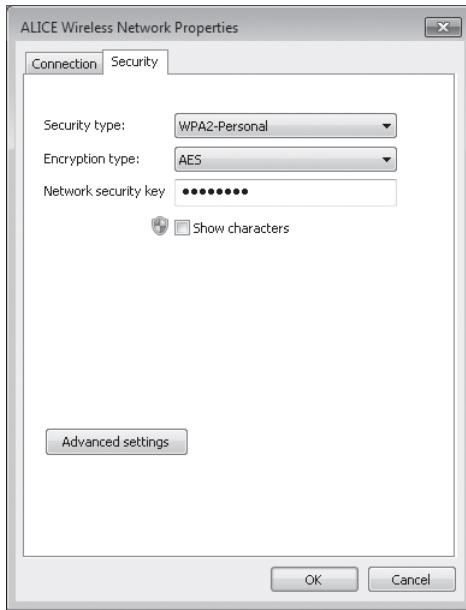


FIGURE 12-8 The Wireless Network Properties sheet

**NOTE WIRELESS CONFIGURATION INTERFACES**

Mobile computers nearly always have a Wi-Fi network interface adapter, but desktop computers almost never do. In both cases, the adapter might be an added component, which might or might not include its own configuration program. Windows 7 has a built-in wireless network configuration interface, but in many cases, third-party wireless adapters use a configuration program supplied by the manufacturer.

## Troubleshooting Remote Network Connections

As with wireless networks, remote network connections have extra elements that can complicate the troubleshooting process. Remote networking problems typically involve enterprise users that are unable to access the network from home or while traveling. The first step in troubleshooting this type of problem is to find out what remote access technology the individual is using. Users can connect to the network with either of the following remote access technologies:

- Remote Desktop
- Virtual private network (VPN)

The following sections discuss each of these technologies.

## Troubleshooting Remote Desktop Connections

Remote Desktop enables client users on the enterprise network or on the Internet to access a Windows desktop or Windows applications on a Remote Desktop Services (RDS) server. Administrators often use the unlicensed version of Remote Desktop included with all versions of Windows to access systems elsewhere on the network, but by purchasing client access licenses, an organization can provide users with network applications and services hosted by an RDS server running Windows Server 2008 R2.

As discussed in Chapter 10, “Using Application Deployment Tools,” a Remote Desktop (or Terminal Services) connection consists of client and server applications as well as the Remote Desktop Protocol (RDP), which enables the two to communicate. When users fail to connect to the network from a remote location using RDS, the desktop administrator should begin the troubleshooting process by asking how far the user got in the connection process.

If the remote user’s Remote Desktop Connection client is unable to communicate with the RDS server in any way, the first thing to check is whether the RDS server is functioning properly. You can do this by trying to connect from inside the network or by examining the server itself. The second most likely cause for a connection failure involves access to the network using the RDP protocol. RDP uses port number 3389 to connect a client to a server, which most firewalls tend to block by default. Therefore, the troubleshooter must make sure that all of the firewalls between the client and server systems have that port open.

### **NOTE USING REMOTE DESKTOP GATEWAY**

RDS connections between clients on the Internet and servers on an enterprise network are quite dangerous, from a security standpoint because they open an avenue for attack that provides full access to the server. To provide Remote Desktop access to Internet clients, Windows Server 2008 R2 includes a Remote Desktop Gateway role service, which takes the RDP traffic and encapsulates it within standard Secure Sockets Layer (SSL) packets. This enables administrators to provide remote users with RDS access to the network without opening port 3389 in the corporate firewall; instead, the packets enter using SSL port 443, which is already open in most firewalls.

If the user gets to the point of logging on to the network, the RDS server is operational and there is no firewall problem, but there could be an issue with the user’s credentials or some other authentication problem. For more information on troubleshooting authentication and authorization issues, see Lesson 2, “Troubleshooting Authentication and Authorization Issues,” later in this chapter.

## Troubleshooting VPN Connections

Virtual private network (VPN) connections are a more traditional method of providing remote users with access to a network. The basic architecture is similar to that of Remote Desktop: a remote client uses the Internet to connect to a server on the enterprise network, which then provides the client with access to network resources. However, VPNs are capable of using a variety of different protocols, which complicates the potential for firewall difficulties.

As noted earlier with wireless networks, two computers must be using the same protocols to communicate. However, VPNs are able to automatically negotiate their communication parameters. By default, a Windows 7 VPN connection is set to Automatic, as shown in Figure 12-9 so that it can negotiate a connection with the server. VPNs also negotiate the use of a common authentication protocol, based on the capabilities of the client and the server.

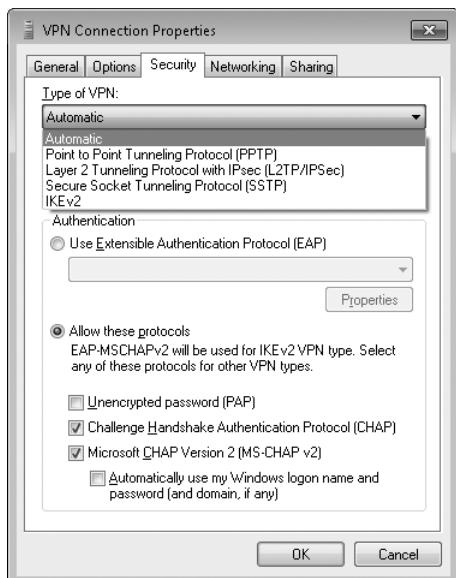


FIGURE 12-9 The Properties sheet for a Windows 7 VPN connection

If the user configures the client to use one specific protocol, however, autonegotiation is effectively disabled, and the server must be able to support the selected protocol. Therefore, if the client fails to establish a connection with the server, the troubleshooter should make sure that the client and the server have at least one protocol in common and that they are configured to use it. In addition, all of the firewalls between the client and the server must be configured to allow VPN traffic using that protocol through.

Another possible reason for VPN connection failures is that the client is not properly equipped to access the network. Network Access Protection (NAP) is a Windows Server technology that enforces policies specifying who can connect to the server. The policies can require clients to belong to certain groups, use certain authentication methods, and maintain a certain level of health by installing the latest updates.

## PRACTICE Using Network Troubleshooting Tools

---

In this practice, you use some of the Windows 7 networking tools to observe Internet traffic.

### EXERCISE 1 Using Ping.exe

The Ping.exe tool tests one computer's connectivity with another.

1. Using Internet Explorer, locate a Web site with a domain in the country where you live and one in a country on the other side of the world.
2. Click Start. Then click All Programs | Accessories | Command Prompt. The Command Prompt window appears.
3. At the command prompt, type **ping** and the local domain name, and press Enter. The Ping.exe test results appear.
4. At the command prompt, type **ping** and the distant domain name, and press Enter. The Ping.exe test results appear.
5. Note the difference in the time values for the two tests because of the distant locations of the two servers.

### EXERCISE 2 Using Tracert.exe

The Tracert.exe tool displays the traffic's path through the Internet routers to the destination.

1. Click Start. Then click All Programs | Accessories | Command Prompt. The Command Prompt window appears.
2. At the command prompt, type **tracert** and the distant domain name, and press Enter. The Tracert.exe test results appear.
3. Note the jump in the time values as the trace begins connecting to the routers across the oceans.

## Lesson Summary

- A network configuration problem often affects all network communications, so if a user reports an issue with one task or application, one of a troubleshooter's first priorities should be to determine whether the problem is a general networking failure or one that is specific to an application or resource.
- When a workstation on a wired network has no network connectivity at all, the next step for the troubleshooter is to determine whether other computers are similarly afflicted.
- Every workstation on a Windows network must be configured with TCP/IP settings that provide it with an identity and the information needed to communicate with other computers. Checking the TCP/IP configuration is a basic troubleshooting step because misconfigured settings can manifest themselves as several different types of networking failures.
- A missing network adapter driver or a driver conflict with another device can cause all network communication to cease. The first place to check for driver issues is the Device Manager tool.
- The first step in determining whether a network communications problem is caused by an infrastructure failure is to see whether other computers on the network are experiencing the same problem.
- BranchCache clients save data to their local caches only when the network's latency interval exceeds a certain threshold. If administrators find that the clients are not caching data as expected, it might be that the actual latency of the network connection is not exceeding the threshold.
- The single most common cause of networking failures on wireless networks, whether permanent or intermittent, is the inability of the computer to acquire a signal from a wireless access point. There are many possible reasons for a signal acquisition failure, including excessive distance, intervening walls and structures, antenna configuration, and electromagnetic interference.
- Another extremely common source of wireless networking failures is the incompatibility or misconfiguration of wireless security protocols. As in any communications system, both parties must speak the same language. When they do not, no communication is possible.
- If the remote user's Remote Desktop Connection client is unable to communicate with the RDS server in any way, the first thing to check is that the RDS server is functioning properly.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. Which of the following network troubleshooting tools is not included with the Windows 7 operating system?
  - A. Ping.exe
  - B. Network Monitor
  - C. Pathping.exe
  - D. Tracert.exe
2. Which of the following network communication technologies is not capable of automatically negotiating the use of a common protocol for client/server communications?
  - A. Wireless security protocols
  - B. Wireless communication protocols
  - C. Virtual private networking protocols
  - D. Virtual private networking authentication protocols
3. Which of the following TCP/IP configuration settings, when incorrectly configured, completely prevents the computer from communicating on the network? (Choose all correct answers.)
  - A. IPv4 Address
  - B. Subnet Mask
  - C. Default Gateway
  - D. DNS Servers

## Lesson 2: Troubleshooting Authentication and Authorization Issues

Even with network connectivity confirmed, users still might be unable to access the network resources they need. In nearly all cases, users must authenticate themselves to confirm their identities before they can gain significant access to network resources. After the authentication, the system must authorize the users, to provide them with a specific degree of access to selected resources. If either one of these two processes fails, users cannot access the network.

**After this lesson, you will be able to:**

- Recognize account problems affecting authentication and authorization.
- Recognize workstation problems affecting authentication and authorization.
- Recognize Kerberos problems affecting authentication and authorization.

**Estimated lesson time: 60 minutes**

### Troubleshooting Logon Failures

When a user reports an inability to log on to an Active Directory Domain Services (AD DS) network, the troubleshooter is faced with a list of potential problems that range from mundane usability issues to extremely complex directory service matters. The first step in troubleshooting an authentication failure is to make sure that it really is an authentication failure. All of the net-working issues discussed in Lesson 1 of this chapter can prevent a user from logging on, but a true authentication problem assumes that network connectivity is intact. Therefore, troubleshooters should begin by confirming that the computer experiencing the logon problem is not affected by one of the standard permanent or transient network communication issues.

The next step—as usual—is to determine the scope of the problem. If one user cannot log on to the AD DS domain from a particular workstation, can a different user log on from that workstation? Can the first user log on from a different workstation? Answering questions like these enable you to determine whether the problem lies in the user’s account, in the workstation, or in the AD DS domain itself.

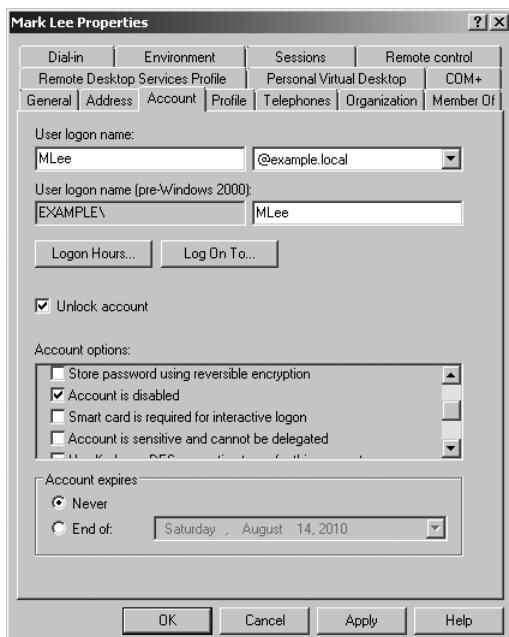
## Checking for Account Problems

Inability to log on to an AD DS domain could be the result of account problems, caused either accidentally or deliberately. This is particularly likely if only one computer or user is affected. You can make sure that the computer account for the workstation is not disabled in the AD DS domain and that the user account attempting to log on is not disabled. When the computer account is disabled, a message like the one shown in Figure 12-10 appears as the system starts. When the user account is disabled, the logon fails because the domain controller does not accept the credentials.



**FIGURE 12-10** Results of a disabled computer account

You might find that another administrator has disabled one or the other of these accounts for some reason, or that the user has been locked out due to an excessive number of failed logon attempts. These are the simplest things to check, using the Active Directory Users And Computers console, as shown in Figure 12-11, and the simplest problems to remedy.



**FIGURE 12-11** A disabled account in Active Directory Users And Computers

However, if you find that an account is disabled, you should also seek to determine why. On a network with relatively secure account lockout policies, a locked user account could indicate that the user mistyped his or her password a few times. However, on a network where the account lockout policies are relatively lax, this could indicate that someone attempted a brute force attack on the account, only to lock it after a large number of attempts.

Another account-level issue that could prevent a successful logon is that of user rights. A user account must have the Allow Log On Locally user right to be able to log on. By default, users receive this right through Local Security Policy on the workstation, which assigns it to the local Users group, as shown in Figure 12-12.

Because the AD DS Domain Users group is a member of the workstation's local Users group, all domain accounts receive this user right. However, if someone changes the default user rights assignments, either in Local Security Policy or in Group Policy (which overrides local settings), a user account might fail to receive that right, causing the logon to fail. In addition to user rights, there are other security options in Local Security Policy, such as Network Security: LAN Manager Authentication Level, which can inhibit domain logons when altered from their default values.

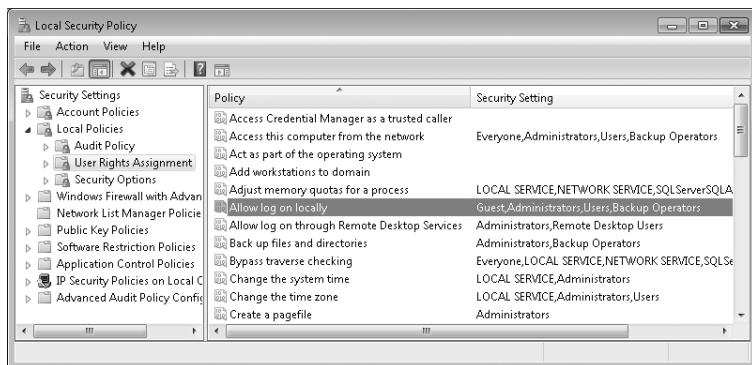


FIGURE 12-12 User rights assignments in Local Security Policy

## Checking for Workstation Problems

Apart from the Local Security Policy settings and typical networking issues, there are some other workstation settings that can interfere with the authentication process. The typical symptoms of a workstation problem are that all domain logons from that workstation fail, regardless of user, while at the same time, those users can successfully log on from other workstations.

One of the workstation issues that can prevent successful authentications is time synchronization failure between the workstation and the domain controller. For various reasons, but chiefly to prevent replay attacks, it is important that all of the computers in an AD DS domain have their clocks synchronized to within five minutes of each other.

Every Windows computer in an AD DS domain runs the Windows Time service, which functions as a time client, using an AD DS domain controller as its source. Normally, a Windows workstation synchronizes its clock with that of the AD DS domain controller, a process that is automatic, invisible, and requires no maintenance. If for any reason, a workstation's clock time should vary significantly from the authoritative value for the domain and be unable to synchronize with a domain controller, all domain logons will fail. Typically, this occurs only when the Windows Time service is not running properly on the domain controller or when network conditions prevent the computers from exchanging Network Time Protocol messages.

The simplest and most obvious way to make sure that an authentication failure is not the result of a time synchronization problem is to check that the workstation's clock and the domain controller's clock are showing the same time. You should also make sure that the Windows Time service is running on both the workstation and the domain controllers.

In most cases, time synchronization problems are the result of attempts to modify the default configuration of the Windows Time service. You can use the W32tm.exe utility to display the current configuration of the service on the local computer, as shown in Figure 12-13, or to modify the current configuration settings.

```
C:\> Administrator: Command Prompt
C:\Users\Administrator>w32tm /query /configuration
[Configuration]
EventLogFlags: 2 <Local>
AnnounceFlags: 10 <Local>
TimeJumpAuditOffset: 28800 <Local>
MinPollInterval: 10 <Local>
MaxPollInterval: 15 <Local>
MaxNegPhaseCorrection: 4294967295 <Local>
MaxPosPhaseCorrection: 4294967295 <Local>
MaxAllowedPhaseOffset: 300 <Local>

FrequencyCorrectRate: 4 <Local>
PollReadjustFactor: 5 <Local>
LargePhaseOffset: 50000000 <Local>
SpikeWatchPeriod: 900 <Local>
LocalClockDispersion: 10 <Local>
HoldPeriod: 5 <Local>
PhaseCorrectRate: 1 <Local>
UpdateInterval: 30000 <Local>

[TimeProviders]
NtpClient <Local>
  DllName: C:\Windows\system32\w32time.dll <Local>
  Enabled: 1 <Local>
  InputProvider: 1 <Local>
  CrossSiteSyncFlags: 2 <Local>
  AllowNonstandardModeCombinations: 1 <Local>
  ResolvePeerBackoffMinutes: 15 <Local>
  ResolvePeerBackoffMaxTimes: 7 <Local>
  CompatibilityFlags: 2147483648 <Local>
  EventLogFlags: 1 <Local>
  LargeSampleSkew: 3 <Local>
  SpecialPollInterval: 3600 <Local>
  Type: NT5DS <Local>

UmiCTimeProvider <Local>
  DllName: C:\Windows\System32\vmictimeprovider.dll <Local>
  Enabled: 1 <Local>
  InputProvider: 1 <Local>
  NtpServer <Local>
  DllName: C:\Windows\system32\w32time.dll <Local>
  Enabled: 0 <Local>
  InputProvider: 0 <Local>
```

FIGURE 12-13 Windows Time configuration settings, displayed by W32tm.exe

## Checking for Kerberos Problems

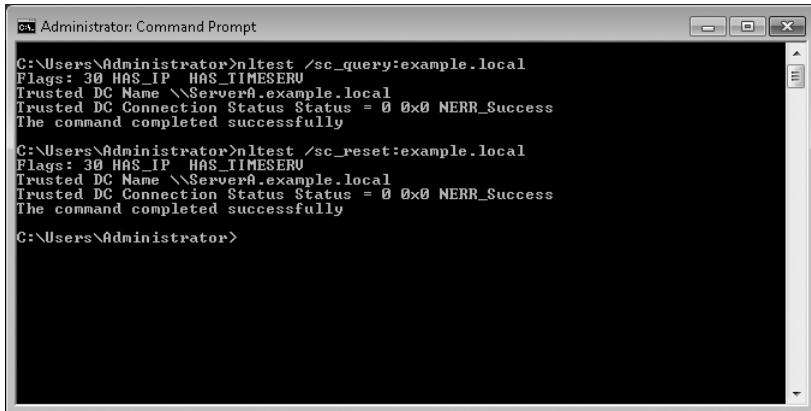
The process of logging on to an AD DS domain is a complicated one, with a number of different services and technologies involved. Chief among these is Kerberos, an authentication protocol that enables users to log on without transmitting passwords and other sensitive information over unsecured channels. If you are experiencing logon failures, and you find errors in the System event log of either the workstation or the domain controller that cite services such as Kerberos, Netlogon, LsaSrv, or Key Distribution Service (KDC), you are probably experiencing a Kerberos problem.

### **NOTE** INTRODUCING KERBEROS

Kerberos is the name of the three-headed dog guarding the gates to Hades in Greek mythology. The name is appropriate because the Kerberos authentication process requires three computers: the client requesting access to a secured resource, the server hosting the secured resource, and a third system, trusted by both of the other two, that functions as an authentication provider. On an AD DS network, that third system is the domain controller.

In most large enterprises, desktop administrators are not responsible for troubleshooting Kerberos and other high-end AD DS functions, but there are a number of tools they can use to display information about possible causes of the authentication failure, including the following:

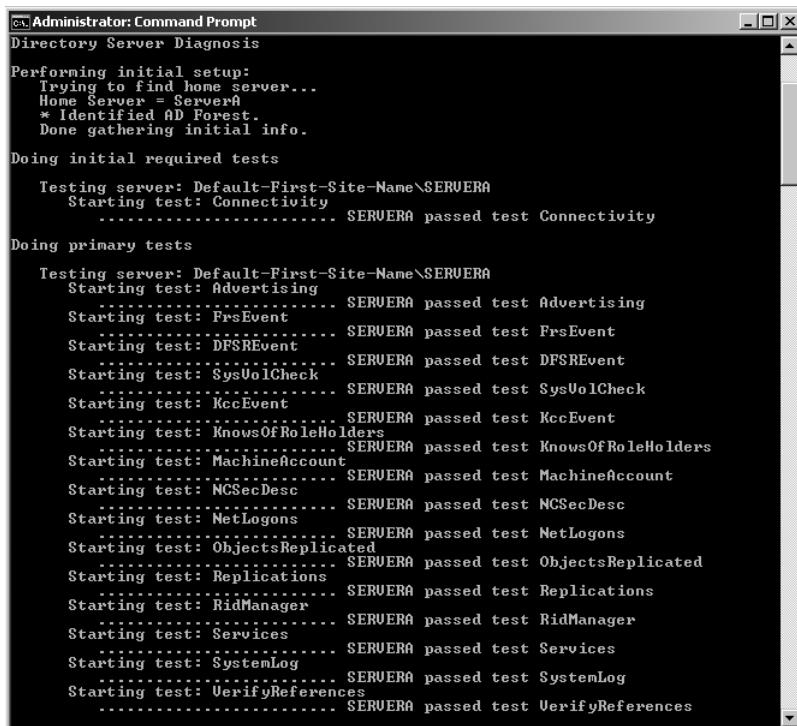
- **Nltest.exe** AD DS workstations have a secure channel to the domain controller, created by the Netlogon service and protected by a password stored on the domain controller. The password changes every 30 days, by default, and if the password on the workstation and the domain controller become unsynchronized for any reason, Netlogon errors begin appearing in the event log. To reset the secure channel, you can rejoin the workstation to the domain or use the Nltest.exe utility at an elevated workstation command prompt. Running Nltest.exe with the /sc\_query:<domainname> parameter reports on the state of the secure channel, and running it with the /sc\_reset:<domainname> parameter removes and then rebuilds the secure channel, as shown in Figure 12-14.



```
C:\>Administrator: Command Prompt  
C:\>nltest /sc_query:example.local  
Flags: 30 HAS_IP HAS_TIMESERV  
Trusted DC Name \\\\ServerA.example.local  
Trusted DC Connection Status Status = 0 0x0 NERR_Success  
The command completed successfully  
  
C:\>nltest /sc_reset:example.local  
Flags: 30 HAS_IP HAS_TIMESERV  
Trusted DC Name \\\\ServerA.example.local  
Trusted DC Connection Status Status = 0 0x0 NERR_Success  
The command completed successfully  
  
C:\>Administrator>
```

FIGURE 12-14 Nltest.exe output

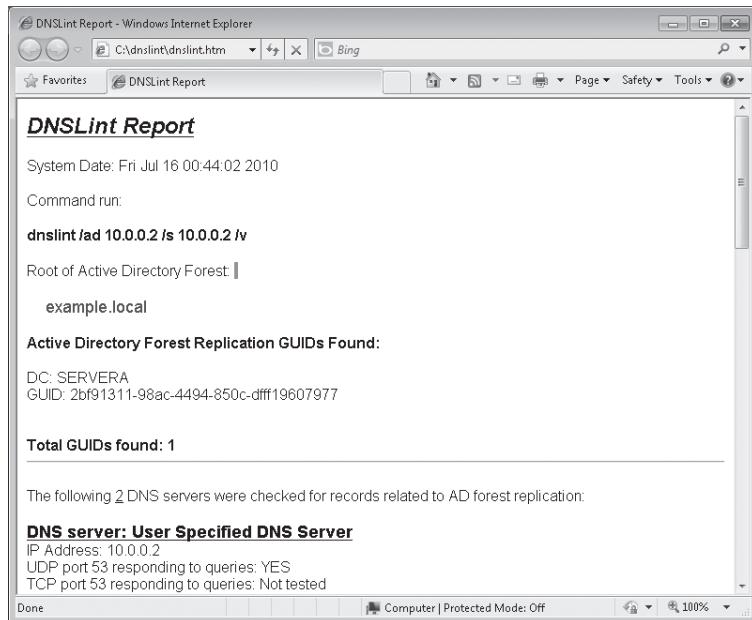
- **Domain Controller Diagnostics (Dcdiag.exe)** A command-line program that executes a series of diagnostic tests on a domain controller, as shown in Figure 12-15, and displays information about possible problem areas. Among other things, the program can list System events generated by AD DS processes, name resolution failures, and service stoppages.



```
C:\>Administrator: Command Prompt  
Directory Server Diagnosis  
  
Performing initial setup:  
    Trying to find home server...  
    Home Server = ServerA  
    * Identified AD Forest.  
    Done gathering initial info.  
  
Doing initial required tests  
  
    Testing server: Default-First-Site-Name\\SERVERA  
        Starting test: Connectivity  
            ..... SERVERA passed test Connectivity  
  
Doing primary tests  
  
    Testing server: Default-First-Site-Name\\SERVERA  
        Starting test: Advertising  
            ..... SERVERA passed test Advertising  
        Starting test: FrsEvent  
            ..... SERVERA passed test FrsEvent  
        Starting test: DFSREvent  
            ..... SERVERA passed test DFSREvent  
        Starting test: SysVolCheck  
            ..... SERVERA passed test SysVolCheck  
        Starting test: KccEvent  
            ..... SERVERA passed test KccEvent  
        Starting test: KnowsOfRoleHolders  
            ..... SERVERA passed test KnowsOfRoleHolders  
        Starting test: MachineAccount  
            ..... SERVERA passed test MachineAccount  
        Starting test: NCSSecDesc  
            ..... SERVERA passed test NCSSecDesc  
        Starting test: NetLogons  
            ..... SERVERA passed test NetLogons  
        Starting test: ObjectsReplicated  
            ..... SERVERA passed test ObjectsReplicated  
        Starting test: Replications  
            ..... SERVERA passed test Replications  
        Starting test: RidManager  
            ..... SERVERA passed test RidManager  
        Starting test: Services  
            ..... SERVERA passed test Services  
        Starting test: SystemLog  
            ..... SERVERA passed test SystemLog  
        Starting test: VerifyReferences  
            ..... SERVERA passed test VerifyReferences
```

FIGURE 12-15 Domain Controller Diagnostics output

- **DNSLint.exe** A command-line utility that can verify the Lightweight Directory Access Protocol (LDAP) functionality of a domain controller and check that the appropriate records exist on a specified DNS server, as shown in Figure 12-16.



The screenshot shows a Windows Internet Explorer window displaying the 'DNSLint Report'. The title bar reads 'DNSLint Report - Windows Internet Explorer'. The address bar shows 'C:\dnslint\dnslint.htm'. The page content includes:

- System Date: Fri Jul 16 00:44:02 2010
- Command run:  
`dnslint /ad 10.0.0.2 /s 10.0.0.2 /v`
- Root of Active Directory Forest: example.local
- Active Directory Forest Replication GUIDs Found:**
  - DC: SERVERA  
GUID: 2bf91311-98ac-4494-850c-dfff19607977
- Total GUIDs found: 1**
- The following 2 DNS servers were checked for records related to AD forest replication:
  - DNS server: User Specified DNS Server**
    - IP Address: 10.0.0.2
    - UDP port 53 responding to queries: YES
    - TCP port 53 responding to queries: Not tested

FIGURE 12-16 DNSLint.exe output

#### **NOTE OBTAINING DNSLINT.EXE**

DNSLint.exe is not included with the Windows operating systems. You must download it from the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=198218>.

- **Kerbtray.exe** Kerberos authentication and authorization is based on specialized packets called tickets. The Kerberos Key Distribution Service (KDS), running on an AD DS domain controller, issues tickets to users, and the users present the tickets to gain access to network resources. Because the tickets are valid only for a specific user, at a specific time, and for a specific purpose, they are inherently more secure than passwords. Kerbtray.exe is a utility that displays information about all of the tickets issued to the current user and enables you to purge those tickets as well. Running Kerbtray.exe on a workstation adds a ticket icon to the notification area, and double-clicking that icon opens the Kerberos Tickets dialog box shown in Figure 12-17. The various tickets issued to the Client Principal, who is the logged-on user, appear. Selecting a ticket enables you to display detailed information about it on the various tabs of the dialog box. If errors referring to Kerberos tickets appear in the event log, you can right-click the Kerbtray.exe icon and select Purge Tickets from the context menu.

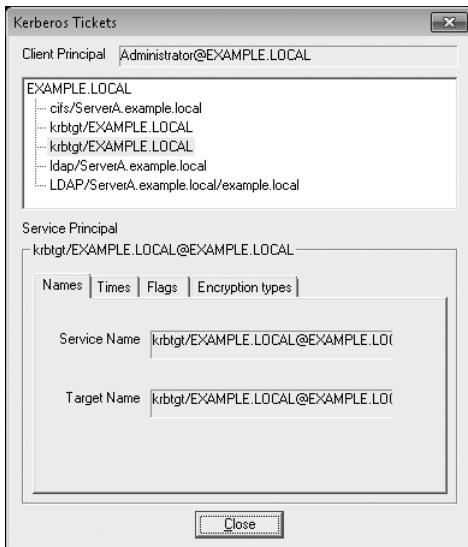


FIGURE 12-17 The Kerberos Tickets dialog box

- **Kerberos List (Klist.exe)** A command-line program that provides roughly the same functions as Kerbtray.exe. The command **klist tickets** lists the tickets cached by the system, as shown in Figure 12-18, and **klist tgt** displays information about the Kerberos ticket-granting ticket. To purge all tickets from the system, use **klist purge**.

```
C:\> Administrator: Command Prompt
C:\> klist tickets
Cached Tickets: <7>
Server: krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 14:58:25
Renew Time: 7/23/2010 4:58:25

Server: krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 14:58:25
Renew Time: 7/23/2010 4:58:25

Server: cifs/ServerA.example.local@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 14:58:25
Renew Time: 7/23/2010 4:58:25

Server: ldap/ServerA.example.local@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 14:58:25
Renew Time: 7/23/2010 4:58:25

Server: LDAPS/ServerA.example.local@example.local@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 14:58:25
Renew Time: 7/23/2010 4:58:25

Server: cifs/serverc.example.local@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 4:49:17
Renew Time: 7/22/2010 18:49:17

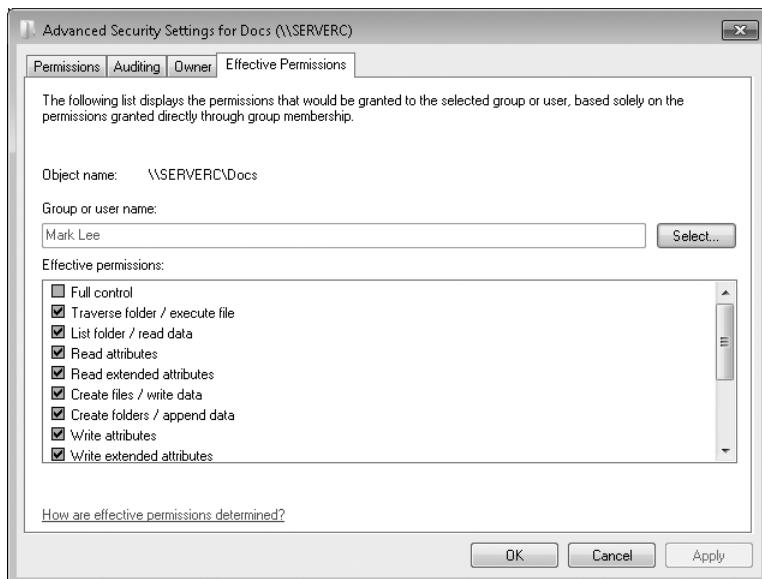
Server: HOST/serverc@EXAMPLE.LOCAL
KerbTicket Encryption Type: Unknown <18>
End Time: 7/16/2010 4:49:17
Renew Time: 7/22/2010 18:49:17
```

FIGURE 12-18 Output from the Klist.exe program

## Troubleshooting Authorization Failures

Authorization failures prevent users from accessing network resources, even after they have successfully authenticated. In an AD DS environment, Kerberos issues can affect authorization as well as authentication. If a user attempts to access a network resource and fails, you can try deleting the ticket and reconnecting. If the problem persists, there might be an AD DS issue that goes beyond the responsibility of the desktop administrator and requires escalation.

For most authentication failures, however, Kerberos problems qualify as zebras, not horses. The far more common reason for post-authentication access failures is a lack of permissions. For file system access, the issue could be share permissions, NTFS permissions, or a combination of both. To test for share permission access, the troubleshooter can try accessing the files from the console (remotely or locally), rather than through a share. For NTFS permissions, which can originate from a variety of sources, including explicit assignments, inheritance from parent folders, and group memberships, you can use the Effective Permissions tab in the Advanced Security Settings dialog box, as shown in Figure 12-19, to display the accumulated result of permissions from all sources.



**FIGURE 12-19** The Effective Permissions tab in the Advanced Security Settings dialog box

## PRACTICE Using Kerberos Troubleshooting Tools

---

In this practice, you use a variety of tools to display information about the Kerberos authentication and authorization processes.

### EXERCISE 1 Using Nltest.exe

On a Windows 7 workstation that is connected to an AD DS domain, use the following procedure to check the state of the secure channel between the computer and the domain controller.

1. Click Start. Then click All Programs | Accessories | Command Prompt. A Command Prompt window appears.
2. At the command prompt, type **nltest /sc\_query:<domainname>**, where *<domainname>* is the name of your AD DS domain.
3. Close the Command Prompt window.

### EXERCISE 2 Using Kerbtray.exe

On a Windows 7 workstation that is connected to an AD DS domain, use the following procedure to examine the Kerberos tickets issued to the user logged on to the workstation.

1. Click Start. Then click All Programs | Accessories | Command Prompt. A Command Prompt window appears.
2. At the command prompt, type **kerbtray** and press Enter. The Kerbtray icon appears in the notification area.
3. Double-click the Kerbtray icon. The Kerberos Tickets dialog box appears.
4. Examine the properties of the tickets issued to the user.
5. Close the Kerberos Tickets dialog box and the Command Prompt window.

## Lesson Summary

- The first step in troubleshooting an authentication failure is to make sure that it really is an authentication failure. Networking issues can prevent a user from logging on, but a true authentication problem assumes that network connectivity is intact. Troubleshooters should begin by confirming that the computer experiencing the logon problem is not affected by one of the standard permanent or transient network communication issues.
- Inability to log on to an AD DS domain could be the result of account problems, caused either accidentally or deliberately. This is particularly likely if only one computer or user is affected. You can make sure that the computer account for the workstation is not disabled in the AD DS domain and that the user account attempting to log on is not disabled.
- The typical symptoms of a workstation problem are that all domain logons from that workstation fail, regardless of user, while at the same time, those users can successfully log on from another workstation.
- One of the workstation issues that can prevent successful authentications is time synchronization failure between the workstation and the domain controller. For various reasons, but chiefly to prevent replay attacks, it is important that all of the computers in an AD DS domain have their clocks synchronized to within five minutes of each other.
- The process of logging on to an AD DS domain is a complicated one, with a number of different services and technologies involved. Chief among these is Kerberos, an authentication protocol that enables users to log on without transmitting passwords and other sensitive information over unsecured channels.
- One common reason for post-authentication access failures is a lack of permissions. For file system access, the issue could be share permissions, NTFS permissions, or a combination of both.

## Lesson Review

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

**NOTE ANSWERS**

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

1. Which of the following tools must be run on an Active Directory Domain Services domain controller?
  - A. Nltest.exe
  - B. DNSLint.exe
  - C. Dcdiag.exe
  - D. Kerbtray.exe
2. For a workstation to successfully authenticate to a domain, its clock time must be within \_\_\_\_\_ of the domain controller's click time.
  - A. 5 seconds
  - B. 5 minutes
  - C. 15 minutes
  - D. 1 hour
3. When a user is able to log on to the domain and access network resources from one workstation, but not from another, which of the following could not be the problem?
  - A. The second computer's account is disabled in Active Directory Domain Services.
  - B. The Domain Users group is not a member of one workstation's local Users group.
  - C. The second workstation is disconnected from the network.
  - D. The domain controller is disconnected from the network.

## Chapter Review

---

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

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

## Chapter Summary

- Although there are some common factors that can affect all network connections, the first thing a troubleshooter typically wants to know is which of the three basic connection types the person experiencing the problem is using: wired, wireless, or remote. Each of these network types experiences a different set of faults most frequently.
- Even with network connectivity confirmed, it is still possible for users to be unable to access the network resources they need. In nearly all cases, users must authenticate themselves to confirm their identities before they can gain significant access to network resources. After the authentication, the system must authorize the users to provide them with a specific degree of access to selected resources. If either of these two processes fail, users cannot access the network.

## 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.

- Ping.exe
- Tracert.exe
- Network Monitor
- latency interval
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA and WPA2)
- Kerberos

## Case Scenarios

In the following case scenario, you will apply what you've learned about subjects of this chapter. You can find answers to the scenario questions in the "Answers" section at the end of this book.

### Case Scenario 1: Troubleshooting TCP/IP Configuration Settings

Lupe is working the IT help desk and her first call of the morning is from a user that cannot access the Internet in any way. Because she is nearby, Lupe goes to the user's cubicle and examines her computer. Running `Ipconfig.exe` with the `/all` parameter, Lupe sees the following:

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : example.local
Description . . . . . : Intel(R) PRO/1000 PL Network Connection
Physical Address. . . . . : 00-1A-5B-3D-BC-1F
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.2.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.2.1
DNS Servers . . . . . : 192.168.2.1
Primary WINS Server . . . . : 192.168.2.1
Lease Obtained. . . . . : Thursday, July 15, 2010 4:16:02 AM
Lease Expires . . . . . : Friday, July 23, 2010 4:16:02 AM
```

Why is the user unable to access the Internet, and what must Lupe do to resolve the problem?

### Case Scenario 2: Troubleshooting an Authentication Problem

Elsie, a user at Contoso, Ltd., calls the help desk early one morning and reports that she is unable to log on to her Windows 7 workstation. After confirming that Elsie is using the correct account name and password, you ask her whether the other users around her have been able to log on this morning. She answers yes, no one seems to be having trouble except her. Then you ask Elsie to try logging on from another nearby workstation. After a few minutes, she reports back that her logon attempts fail from the other workstation also. Based on the information you have so far, which of the following conclusions can you make about Elsie's problem? Explain why each option is or is not correct.

- a. Elsie's workstation is the source of the problem.
- b. The domain controller is malfunctioning.
- c. The problem is located in Elsie's user account.

## Suggested Practices

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

### Troubleshooting Networking Issues

- **Practice 1** Download and install Network Monitor and use it to capture and analyze a sample of traffic from your network.
- **Practice 2** Experiment with the Pathping.exe utility and consider how it differs from Tracert.exe.

### Troubleshooting Authentication and Authorization Issues

- **Practice 1** Run the Dcdiag.exe program on your network's domain controller and examine the results of the various tests.
- **Practice 2** Install and use the Dlist.exe program to display and purge the Kerberos tickets on your workstation.

## 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 70-686 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.



# Answers

## Chapter 1: Lesson Review Answers

---

### Lesson 1

**1. Correct Answer: B**

- A. Incorrect:** The Plan phase contains stages that can run concurrently, and even recur during later phases of the project.
- B. Correct:** The stages of the Deliver phase must occur sequentially. Each stage must be completed (or nearly completed) before the next stage can begin.
- C. Incorrect:** The Operate phase contains stages defining services that must run concurrently.
- D. Incorrect:** The Manage level is part of the Plan, Deliver, and Operate phases, enabling its stages to run throughout the project.

**2. Correct Answer: C**

- A. Incorrect:** The primary function of the Governance, Risk, and Compliance SMF is to establish policies that delegate authority, accountability, and responsibility for the outcome of IT projects.
- B. Incorrect:** The primary function of the Business/IT Alignment SMF is to recognize the needs of the organization and define a portfolio of IT services that address those needs.
- C. Correct:** The primary function of the Policy SMF is to define a set of policies for IT services that meet the organization's requirements in matters of security, privacy, and appropriate use.
- D. Incorrect:** The primary function of the change and Configuration SMF is to manage project and service changes in a predictable and repeatable manner, while minimizing the risks inherent in those changes.

**3. Correct Answer: B**

- A. Incorrect:** The Plan phase defines processes that largely occur before the beginning of the MDT 2010 deployment process.
- B. Correct:** The tasks involved in the MDT 2010 deployment process roughly correspond to the stages of the Deliver phase in the MOF 4.0 life cycle model.
- C. Incorrect:** The Operate phase defines processes that occur after the MDT 2010 deployment is completed.
- D. Incorrect:** The Manage level defines processes that might occur during the MDT 2010 deployment but that operate outside its purview.

## Lesson 2

1. **Correct Answer: B**
  - A. **Incorrect:** The Performance Monitor application is included with all versions of Windows.
  - B. **Correct:** The MAP Toolkit 4.0 is available from the Microsoft Download center without charge.
  - C. **Incorrect:** System Center Configuration Manager 2007 is a product that you must purchase from Microsoft.
  - D. **Incorrect:** System Information is an application included with all versions of Windows.
2. **Correct Answer: B**
  - A. **Incorrect:** One of the advantages of MAP Toolkit is that it does not require any special agents or other software on the clients.
  - B. **Incorrect:** MAP Toolkit is available free of charge, whereas SCCM is a retail product.
  - C. **Incorrect:** MAP Toolkit is capable of using the free SQL Server Express product from Microsoft.
  - D. **Correct:** SCCM is capable of performing ZTI deployments; MAP Toolkit is not.
3. **Correct Answers: A, C, and D**
  - A. **Correct:** Windows 7 has specific memory requirements that a workstation must meet if the operating system is to run properly.
  - B. **Incorrect:** The number and type of network adapters is not necessary to determine whether a workstation can run Windows 7.
  - C. **Correct:** Windows 7 requires a certain amount of free disk space to install properly.
  - D. **Correct:** Windows 7 requires a specific type and speed of processor to run effectively.

## Chapter 1: Case Scenario Answers

---

### Case Scenario 1: Making a Windows 7 Deployment Decision

1. SCCM 2007 is an expensive product and complicated to install, and for Bob's purposes, it is not likely to yield hardware inventory information that is any more useful than MAP Toolkit 4.0. However, SCCM 2007 can be a valuable tool, both for Bob's proposed Windows 7 deployment project and for managing the workstations afterwards. If he had been planning to implement SCCM anyway, now might be a good time to do it.

2. Although MAP Toolkit 4.0 states that all of Bob's workstations are capable of running Windows 7, their performance might not be exemplary, especially when running resource-intensive applications. Bob should not proceed with the deployment without more testing.
3. Because Windows 7 requires more memory than Windows XP, Bob might be assuming that the XP workstations will yield better performance with a memory upgrade. Because the memory requirements for Windows Vista and Windows 7 are more similar, no such upgrade should be necessary for those workstations. These are reasonable assumptions, but Bob's proposal would look better if he were to conduct some tests and generate some factual performance data before recommending a substantial hardware and software expenditure.
4. Benchmarking the performance of the workstations both before and after a Windows 7 upgrade is the best way to determine whether the computers will function adequately with the new operating system. The cost of the testing will be minimal, and Bob will be able to insert facts into his proposal rather than suppositions.

## Case Scenario 2: Preparing for Windows 7 Deployment

1. No, handing off control of the project to the Operate team would be premature. The Operate team takes over only when the Deploy stage is completely finished.
2. Yes, Carol should perform at least one pilot deployment to test the performance of the workstation builds under conditions as close to a production environment as possible.
3. Yes, according to the MOF, there must be a release readiness management review before the actual deployment process begins. This review ensures that the workstation builds are stable and that the team has addressed all issues that arose during the testing process.

## Chapter 2: Lesson Review Answers

---

### Lesson 1

1. **Correct Answer: B**
  - A. **Incorrect:** You cannot use a retail key with Windows 7 Enterprise. You can use only a volume license key with this edition of Windows 7.
  - B. **Correct:** You can use a MAK key with Windows 7 Enterprise. You can activate MAK keys by using MAK proxies when you are dealing with computers on an isolated network.
  - C. **Incorrect:** You cannot use an OEM key in this situation because OEM keys are provided to vendors, and your 10 computers are from different vendors.
  - D. **Incorrect:** You cannot use a KMS server because you do not have a sufficient number of clients on the network. You need 25 clients on the network before a KMS server can be used.

**2. Correct Answer: C**

- A. Incorrect:** The KMS client activation threshold is 25 clients. The KMS server activation threshold is 5 clients.
- B. Incorrect:** The KMS client activation threshold is 25 KMS clients.
- C. Correct:** The KMS client operating system activation threshold is 25 KMS clients. Because the server uses KMS, you need 24 more clients to reach the client activation threshold.
- D. Incorrect:** The KMS client activation threshold is 25 clients.

**3. Correct Answers: B and D**

- A. Incorrect:** MAK Independent Activation requires that the computer have a direct connection to the Internet.
- B. Correct:** MAK Proxy Activation allows you to activate multiple computers that use MAK keys.
- C. Incorrect:** There are only 15 clients. KMS requires a minimum of 25 clients.
- D. Correct:** You can use telephone activation to activate clients that are on networks isolated from the Internet, even when those clients use MAK keys.

**4. Correct Answer: C**

- A. Incorrect:** You do not specify a MAK key during the auditUser pass of Sysprep. You use the auditUser pass to process user-related Windows setup settings in audit mode.
- B. Incorrect:** You do not specify a MAK key during the generalize pass of Sysprep. You use the generalize pass to remove system-specific settings.
- C. Correct:** You can specify a MAK key during the Sysprep specialize configuration pass.
- D. Incorrect:** You do not specify a MAK key during the auditSystem pass of Sysprep. You use the auditSystem pass to process unattended Windows setup settings in audit mode.

**5. Correct Answers: A and C**

- A. Correct:** The Enterprise edition of Windows 7 supports volume licensing.
- B. Incorrect:** The Ultimate edition of Windows 7 does not support volume licensing.
- C. Correct:** The Professional edition of Windows 7 supports volume licensing.
- D. Incorrect:** The Home Premium edition of Windows 7 does not support volume licensing.

## Lesson 2

**1. Correct Answer: B**

- A. Incorrect:** Windows 7 Home Premium does not support deployment to a VHD file. This edition also does not support activation through KMS.
- B. Correct:** Windows 7 Enterprise supports deployment to a VHD file on a physical host and also supports KMS activation.
- C. Incorrect:** Although Windows 7 Ultimate supports deployment to a VHD, this edition of Windows does not support KMS activation.
- D. Incorrect:** Windows 7 Professional does not support deployment to a VHD. You can use Windows 7 Professional with KMS activation.

**2. Correct Answer: C**

- A. Incorrect:** Windows 7 Enterprise includes licenses to allow four instances rather than two instances.
- B. Incorrect:** Windows 7 Enterprise includes licenses to allow four instances rather than three instances.
- C. Correct:** Windows 7 Enterprise includes licenses to allow four instances of the product to be run virtually without requiring additional licenses.
- D. Incorrect:** Windows 7 Enterprise includes licenses to allow four instances rather than five instances.

**3. Correct Answer: A**

- A. Correct:** Only the Enterprise and Ultimate editions of Windows 7 support BranchCache. Only an x64 version supports 16 GB of RAM.
- B. Incorrect:** Only the Enterprise and Ultimate editions of Windows 7 support BranchCache. The x86 version does not support 16 GB of RAM.
- C. Incorrect:** Only the Enterprise and Ultimate editions of Windows 7 support BranchCache. The Professional edition of Windows 7 does not.
- D. Incorrect:** Only the Enterprise and Ultimate editions of Windows 7 support BranchCache. The Professional edition of Windows 7 does not. The x86 versions do not support 16 GB of RAM.

**4. Correct Answers: A and C**

- A. Correct:** Hyper-V supports hosting x64 versions of Windows 7 Enterprise, which is required if 8 GB of memory is to be allocated to the client.
- B. Incorrect:** Virtual PC 2007 does not support x64 clients, so it is unable to support a virtual client assigned 8 GB of memory.
- C. Correct:** Virtual Server 2005 R2 supports hosting x64 operating systems, so it can support hosting the x64 version of Windows 7 Enterprise.
- D. Incorrect:** Windows Virtual PC does not support hosting x64 versions of Windows 7 Enterprise.

## Lesson 3

### 1. Correct Answers: A, B, and C

- A. **Correct:** Windows 7 supports offline migration by using USMT.
- B. **Correct:** Windows XP Professional supports offline migration by using USMT.
- C. **Correct:** Windows Vista supports offline migration by using USMT.
- D. **Incorrect:** Windows 2000 Professional does not support an offline migration by using USMT.

### 2. Correct Answer: D

- A. **Incorrect:** MigApp.xml contains rules about the migration of application settings.
- B. **Incorrect:** Config.xml contains information about what should be excluded from migration.
- C. **Incorrect:** MigUser.xml contains information about migrating user profiles and user data.
- D. **Correct:** MigDocs.xml allows you to configure rules that specify the location of custom user documents folders.

### 3. Correct Answer: C

- A. **Incorrect:** Hard-link migration stores use the original files, so you cannot encrypt a hard-link migration by using Scanstate.exe.
- B. **Incorrect:** You cannot encrypt uncompressed migration stores by using Scanstate.exe.
- C. **Correct:** You can encrypt compressed stores, both remote and local, by using the Scanstate.exe utility.
- D. **Incorrect:** You cannot encrypt uncompressed migration stores by using Scanstate.exe.

### 4. Correct Answer: C

- A. **Incorrect:** Using a remote store violates the condition that the data not be transferred from the computer.
- B. **Incorrect:** An uncompressed local store requires more space than a hard-link migration store.
- C. **Correct:** Hard-link migration stores keep the data on the computer during a wipe-and-load migration but do not require that the data be copied, which would consume more space on the volume.
- D. **Incorrect:** A compressed local store requires more space than a hard-link migration store.

## **Chapter 2: Case Scenario Answers**

---

### **Case Scenario 1: Branch Office and Head Office Activation**

- 1.** The Professional and Ultimate editions of Windows 7 can be used with volume licenses.
- 2.** You should use KMS at the head office location because this strategy minimizes the amount of administrative effort required. You need to activate only the one KMS server.
- 3.** You should use MAK Proxy Activation at each location. You cannot use KMS because you do not have a sufficient number of clients on the isolated network to allow the use of KMS. You must have at least 25 clients on a network before you can use a KMS solution. MAK Proxy Activation minimizes the amount of effort required for activating clients on isolated networks.

### **Case Scenario 2: Migrating Users to Virtual Machines**

- 1.** You should choose Windows 7 Enterprise edition because this edition allows the use of AppLocker and can be activated by using KMS.
- 2.** You can use a compressed remote store. This meets your goal of using a Scanstate-encrypted store. You cannot use a local store because you are moving files to new computers.
- 3.** The Loadstate.exe utility is used to import data from an encrypted migration store to a client virtual machine when you are using the User State Migration Tool.

## **Chapter 3: Lesson Review Answers**

---

### **Lesson 1**

- 1. Correct Answer: A**
  - A. Correct:** Deployment Workbench is a tool included with MDT 2010, not Windows AIK.
  - B. Incorrect:** Windows System Image Manager (SIM) is included in the Windows 7 AIK.
  - C. Incorrect:** Sysprep.exe is included in the Windows 7 AIK.
  - D. Incorrect:** ImageX.exe is included in the Windows 7 AIK.

**2. Correct Answer: D**

- A. Incorrect:** Manual image creation is the least complex method, but Microsoft Deployment Toolkit 2010 is for more complex deployments than Windows 7 Automated Installation Kit.
- B. Incorrect:** Microsoft Deployment Toolkit 2010 is for more complex deployments than Windows 7 Automated Installation Kit, and manual image creation is the least complex.
- C. Incorrect:** Windows 7 Automated Installation Kit is for more complex deployments than manual image creation, and Microsoft Deployment Toolkit 2010 is the most complex.
- D. Correct:** Manual image creation is the least complex method, Windows 7 Automated Installation Kit is for more complex deployments, and Microsoft Deployment Toolkit 2010 is the most complex.

**3. Correct Answer: C**

- A. Incorrect:** The first step in a typical Windows 7 AIK image creation is to create an answer file, which is an XML script file named Unattend.xml or Autounattend.xml by default.
- B. Incorrect:** The second step in a typical Windows 7 AIK image creation is to start the reference computer and use the answer file you created to install the operating system.
- C. Correct:** After installing the operating system on the reference computer, you must prepare it for imaging by running the Sysprep.exe utility, not the Oscdimg.exe utility. You use the Oscdimg.exe utility to generate a sector-based image (with an .iso extension) of the Windows PE boot disk.
- D. Incorrect:** The final step of a typical Windows 7 AIK image creation is to start the reference computer with a Windows PE disk and use the ImageX.exe utility to create an image file.

**4. Correct Answer: B**

- A. Incorrect:** You can create the deployment share in a stand-alone Distributed File System (DFS) namespace.
- B. Correct:** You should not create the deployment share in a domain-based DFS namespace because Windows PE will not be able to access it.
- C. Incorrect:** You can create the deployment share on a local disk.
- D. Incorrect:** You can create the deployment share on a network share.

**5. Correct Answer: A**

- A. Correct:** Although a domain controller is recommended if you are deploying computers in an Active Directory Domain Services environment, it is not a required component in the image creation lab.
- B. Incorrect:** A Windows 7 AIK or MDT 2010 image creation lab requires a build computer to run the image creation and deployment tools.

- C. **Incorrect:** A Windows 7 AIK or MDT 2010 image creation lab requires a reference computer to serve as a model for the workstation images.
- D. **Incorrect:** A Windows 7 AIK or MDT 2010 image creation lab requires at least one test workstation, which you use to make sure your images function properly.

## Lesson 2

- 1. **Correct Answer: B**
  - A. **Incorrect:** You can add cabinet (.cab) files to an offline image by using DISM.exe.
  - B. **Correct:** You cannot add Microsoft System Installer (.msi) packages to an offline image by using DISM.exe.
  - C. **Incorrect:** You can add device drivers that have a Windows Information (.inf) file to an offline image by using DISM.exe.
  - D. **Incorrect:** You can add Windows Update Stand-alone Installer (.msu) packages to an offline image by using DISM.exe.
- 2. **Correct Answers: B and C**
  - A. **Incorrect:** You cannot use DISM.exe to add a device driver to an image that is currently online.
  - B. **Correct:** You can use DISM.exe to add a language pack to an online image.
  - C. **Correct:** DISM.exe enables you to enable and disable operating system features while the image is online.
  - D. **Incorrect:** Although you can add a language pack file to an online image, you cannot change the currently active user interface language while the image is online.
- 3. **Correct Answer: C**
  - A. **Incorrect:** DISM.exe enables you to install device drivers to an offline image file, including drivers required to boot the workstation.
  - B. **Incorrect:** DISM.exe enables you to activate and deactivate specific operating system features.
  - C. **Correct:** DISM.exe enables you to install Windows Update Stand-alone Installer (.msu) packages, but after you have installed them, you cannot remove them.
  - D. **Incorrect:** DISM.exe enables you to apply an answer file containing application installation instructions to an offline image file.

## Chapter 3: Case Scenario Answers

---

### Case Scenario 1: Capturing an Image by Using ImageX.exe

Ralph's first mistake was to install the Windows 7 AIK on the computer he wanted to image. He should have installed Windows AIK on another computer. Ralph also neglected to run Sysprep.exe with the /generalize parameter on the Windows 7 computer before attempting to image it. Finally, ImageX.exe generated an error because the program cannot capture an image of a system disk while the operating system is running. To perform a successful image capture, Ralph must create a Windows PE boot disk on the computer running the Windows 7 AIK and use that to boot the new Windows 7 workstation. Then he can run ImageX.exe and successfully capture an image.

### Case Scenario 2: Modifying the User Interface Language

- h.** Before he can make any modifications to the image, Harold must mount it to a folder.
- i.** Windows 7 is a language-neutral operating system, so Harold must install a language pack to provide the image with support for the French user interface.
- b.** After installing the language pack, Harold must reset the default user interface from English to French.
- d.** After modifying the mounted image files, Harold must commit the changes he has made to the Windows Imaging file.
- e.** Having modified the image and committed the changes, Harold must dismount the image before he can deploy it to the workstations.

## Chapter 4: Lesson Review Answers

---

### Lesson 1

#### 1. Correct Answer: B

- A. Incorrect:** Group Policy Management Console is a tool administrators use to deploy configuration settings. You use GPMC to create Group Policy objects, which are Active Directory Domain Services (AD DS) objects containing configuration settings, which administrators can apply to users or computers and can associate with domains, sites, or organizational units (OUs).
- B. Correct:** The Local Group Policy Editor is an MMC snap-in that you can use to apply Group Policy settings to the local computer only, not to large numbers of computers.

- C.** **Incorrect:** Administrators use logon/logoff script files to deploy configuration settings that execute when a user logs on.
- D.** **Incorrect:** Administrators use startup/shutdown script files to deploy configuration settings that execute when the system starts, and they apply to all users.
- 2. Correct Answers: A and B**
- A.** **Correct:** Logon/logoff scripts run under the account with which the user logs on, and they are relatively limited in the types of tasks they can perform.
- B.** **Correct:** Startup/shutdown scripts use the credentials of the computer object and have System privileges on the local computer. This makes it possible for startup/shutdown scripts to access the entire local file system and the registry.
- C.** **Incorrect:** Logon/logoff scripts run under the account with which the user logged on and they are relatively limited in the types of tasks they can perform. The Startup/shutdown scripts use the credentials of the computer object and have System privileges on the local computer, making it possible for startup/shutdown scripts to access the entire local file system and the registry.
- D.** **Incorrect:** Startup/shutdown scripts use the credentials of the computer object and have System privileges on the local computer. This makes it possible for startup/shutdown scripts to access the entire local file system and the registry. The Logon/logoff scripts run under the account with which the user logs on and are relatively limited in the types of tasks they can perform.
- 3. Correct Answers: A, C, and D**
- A.** **Correct:** Startup/shutdown and logon/logoff scripts can be simple batch files.
- B.** **Incorrect:** WSH is a script hosting engine, not a scripting language in itself.
- C.** **Correct:** VBScript is a limited variation of the Visual Basic programming language that administrators can use to create startup/shutdown and logon/logoff scripts.
- D.** **Correct:** Startup/shutdown and logon/logoff scripts can consist of Windows PowerShell commands.
- 4. Correct Answer: D**
- A.** **Incorrect:** Background processing skips certain resource-intensive policies, such as Folder Redirection, which makes it faster than foreground processing.
- B.** **Incorrect:** Under some conditions, functional GPOs can process faster than monolithic GPOs.
- C.** **Incorrect:** GPO processing is highly dependent on whether the GPO has changed since it was last processed. GPOs that are unchanged load much faster than those that have changed.
- D.** **Correct:** Asynchronous processing is faster than synchronous processing because it uses background rather than foreground processing.

**5. Correct Answer: D**

- A. Incorrect:** It is true that functional GPOs are numerous and contain relatively few settings.
- B. Incorrect:** It is true that functional GPOs are dedicated to a specific area or type of setting.
- C. Incorrect:** It is true that functional GPOs enable you to organize related settings into separate GPOs so that you can delegate responsibility for them to specific administrators.
- D. Correct:** Monolithic GPOs contain all of the settings a workstation needs, including Computer Configuration and User Configuration settings, Policies and Preferences settings, and Administrative Templates settings.

## Lesson 2

**1. Correct Answers: A, B, and D**

- A. Correct:** By selecting the Follow The Documents Folder setting, you can make Videos a subdirectory of the Documents folder.
- B. Correct:** By selecting the Follow The Documents Folder setting, you can make Music a subdirectory of the Documents folder.
- C. Incorrect:** The Saved Games folder redirection policy does not have a Follow The Documents Folder setting, so you cannot make it a subdirectory of the Documents folder.
- D. Correct:** By selecting the Follow The Documents Folder setting, you can make Pictures a subdirectory of the Documents folder.

**2. Correct Answer: D**

- A. Incorrect:** Local user profiles are stored on the workstation and do not require network access.
- B. Incorrect:** Roaming profiles are stored on network servers, but if the network is not available, the computer uses a local profile instead.
- C. Incorrect:** Mandatory profiles are read-only profiles stored on network servers, but if the network is not available, the computer uses a local profile instead.
- D. Correct:** Super-mandatory profiles are read-only profiles stored on network servers. If the network is not available, the user logon process fails.

## Chapter 4: Case Scenario Answers

---

### Case Scenario 1: Deploying GPOs

- a. Linking the Sales and Order Entry GPOs to the domain object does not achieve the configuration you want because all of the workstations in the Sales and Order Entry OUs receive settings from whatever OU has the highest precedence.
- b. Linking the Sales GPO to the Sales OU and the Order Entry GPO to the Order Entry OU is the simplest way to achieve the required configuration because the policy values in the Order Entry GPO overwrite the values from the Sales GPO on the Order Entry workstations.
- c. Blocking inheritance would prevent the computers in the Order Entry OU from receiving the baseline settings applied to the domain object.
- d. Although creating Sales and Order Entry groups and using security filters can create the required configuration, it is far from being the easiest way.

### Case Scenario 2: Configuring Audit Policies

To deploy the GPO so that only Windows 7 workstations receive the settings, Alice can link the GPO to the domain object and then create a WMI filter that queries each workstation for its operating system.

## Chapter 5: Lesson Review Answers

---

### Lesson 1

1. Correct Answers: A and D
  - A. **Correct:** AppLocker policies can be used to restrict the execution of applications only on computers running Windows 7 Enterprise or Ultimate. Software Restriction Policies must be used to restrict the execution of applications on clients running Windows 7 Professional.
  - B. **Incorrect:** AppLocker policies can be hosted on Windows Server 2003 and Windows Server 2008 domain controllers as long as the Active Directory Schema has been extended to support AppLocker.
  - C. **Incorrect:** AppLocker policies can be used to restrict the execution of applications that are not digitally signed.
  - D. **Correct:** AppLocker policies can be used to restrict the execution of applications only on computers running Windows 7 Enterprise and Ultimate. Software Restriction Policies must be used to restrict the execution of applications on clients running Windows Vista Enterprise.

**2. Correct Answer: A**

- A. Correct:** You need to configure the User Account Control: Behavior Of The Elevation Prompt For Standard Users policy so that when a user who is not a member of the local administrators group performs a task that requires elevated privileges, an administrator connected through remote assistance is able to provide the appropriate credentials for elevation.
- B. Incorrect:** You do not need User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode because users who are receiving remote assistance are logged on with accounts that have standard permissions.
- C. Incorrect:** You should not configure the User Account Control: Detect Application Installations And Prompt For Elevation policy because this policy relates to elevation for a specific activity and does not allow an administrator connected through a remote assistance session to a standard user's desktop to be able to enter her credentials.
- D. Incorrect:** You should not configure the User Account Control: Run All Administrators In Admin Approval Mode because you need to configure a policy for standard users. Configuring this policy does not allow an administrator connected through a remote assistance session to a standard user's desktop to be able to enter his credentials.

**3. Correct Answers: A, C, E, and F**

- A. Correct:** You need to configure the Account Lockout Duration policy to ensure that user lockout occurs for 15 minutes if a user enters an incorrect password sequentially three times.
- B. Incorrect:** You do not need to configure the Enforce Password History policy. This policy is used to ensure that users do not use the same password after it is changed. The question makes no mention of this requirement.
- C. Correct:** You need to configure the Maximum Password Age policy to ensure that users change their passwords every 21 days.
- D. Incorrect:** You do not need to configure the Minimum Password Age policy because the question makes no mention of minimum password ages.
- E. Correct:** You must configure the Account Lockout Threshold policy so that you can specify how many invalid passwords entered in succession trigger an account lockout.
- F. Correct:** You must set the Reset Account Lockout Counter After policy to ensure that sequential failed logins are tracked over a 30-minute period.

**4. Correct Answers: B, C, and D**

- A. Incorrect:** You do not need to set the Configure Use Of Passwords For Removable Data Drives policy to meet your goals. This policy determines how passwords are used with BitLocker To Go-protected devices, but it does not restrict the use of USB flash devices to those that are specifically protected by BitLocker configured with a particular organizational ID.

- B.** **Correct:** You need to configure the Deny Write Access To Removable Drives Not Protected By BitLocker policy to ensure that users are unable to write data to USB flash devices not protected by BitLocker.
- C.** **Correct:** You need to configure the Provide The Unique Identifiers For Your Organization policy to ensure that users are able to use only BitLocker-encrypted USB flash devices that are tied to your organization's identifier.
- D.** **Correct:** You need to set the Control Use Of BitLocker On Removable Drives policy so that BitLocker can be used and so that ordinary users are restricted from encrypting their own USB flash storage devices.

**5. Correct Answer: D**

- A. Incorrect:** Although BitLocker can be used to encrypt the hard disk drives of computers that do not have TPM chips, this requires that a USB flash device be connected at startup, which violates the conditions imposed in the question.
- B. Incorrect:** BitLocker To Go can be used only with removable storage devices. You cannot use BitLocker To Go to encrypt files and folders from a volume hosted on an internal hard disk.
- C. Incorrect:** IPSec allows only for the encryption of network transmissions. It cannot be used to encrypt files and folders.
- D. Correct:** Encrypting File System allows you to encrypt files and folders on a local volume without requiring the use of BitLocker.

## Lesson 2

**1. Correct Answer: C**

- A. Incorrect:** You should not configure the Security Zones: Use Only Machine Settings policy because this option means that the Computer policy rather than the User policy applies. You need to configure the Security Zones: Do Not Allow Users To Add/Delete Sites policy to accomplish your goal.
- B. Incorrect:** You should not configure the Security Zones: Do Not Allow Users To Change Policies option because this policy controls the security level assigned to the zone, not which sites are actually assigned to the zone.
- C. Correct:** You should configure and enable the Security Zones: Do Not Allow Users To Add/Delete Sites option because this policy blocks users from modifying the contents of the Trusted Sites and Restricted Sites zones.
- D. Incorrect:** You should not configure the Restrict Search Providers To A Specific List Of Providers page because this policy configures restrictions on the use of search providers rather than the Trusted Sites and Restricted Sites zones.

**2. Correct Answer: D**

- A. Incorrect:** The Deploy Non-Default Accelerators policy does not limit which accelerators are deployed but is used to deploy nondefault accelerators.
- B. Incorrect:** The Deploy Default Accelerators policy does not limit which accelerators are deployed but is used to specify accelerator defaults.
- C. Incorrect:** The Turn Off Accelerators policy turns off accelerators. You want to limit the accelerators available and not turn them off.
- D. Correct:** Using the Use Policy Accelerators policy limits accelerators to those deployed through Group Policy.

**3. Correct Answer: D**

- A. Incorrect:** Using local Group Policy would require that settings be configured manually on each of the 60 portable computers. This requires substantially more effort than using Internet Explorer Administration Kit to configure settings prior to application deployment.
- B. Incorrect:** Windows Internet Explorer settings are not contained within the area of Group Policy that can be managed through Security Policy. The Windows Internet Explorer policies are located in the Administrative Templates area of a Group Policy object.
- C. Incorrect:** You cannot use domain level Group Policy because the portable computers are not a part of the organization's Active Directory environment.
- D. Correct:** You should use the Internet Explorer Administration Kit because this allows you to create a configuration of Windows Internet Explorer that includes the organizational settings, and you can then deploy this application to the 60 stand-alone portable computers.

**4. Correct Answer: D**

- A. Incorrect:** Configuring the Prevent Deleting Passwords policy prevents users from deleting stored passwords but does not prevent the deletion of temporary Internet files and cookies.
- B. Incorrect:** Configuring the Prevent Deleting InPrivate Filtering Data policy prevents the deletion of InPrivate filtering data but does not prevent the deletion of temporary Internet files and cookies.
- C. Incorrect:** Configuring the Prevent Deleting Favorites Site Data policy blocks users from deleting favorites site data but does not prevent the deletion of temporary Internet files and cookies.
- D. Correct:** You should configure the Prevent The Deletion Of Temporary Internet Files And Cookies policy because this policy allows you to block users from deleting these items.

**5. Correct Answer: B**

- A. Incorrect:** InPrivate Filtering restricts the ability of third-party Web sites to track activity across a browsing session. It is not related to blocking the browser from storing cookie and browsing history data.
- B. Correct:** InPrivate browsing stops the browser from storing cookie and browsing history data beyond the length of the browsing session. You should use this policy to disable this feature as a method of accomplishing your goal.
- C. Incorrect:** You should not configure this policy because it relates to InPrivate Filtering rather than InPrivate Browsing.
- D. Incorrect:** You should not configure this policy because it relates to InPrivate Filtering rather than InPrivate Browsing.

## Chapter 5: Case Scenario Answers

---

### Case Scenario 1: Client Security at Contoso

1. You should configure the netbook computers to use Encrypting File System because they do not have a TPM chip that would allow the deployment of BitLocker without reconfiguring policy to require a USB startup key.
2. You can use AppLocker policies to restrict the execution of applications so that only applications signed by an approved vendor can be run on the computers running Windows 7 at Contoso.
3. You can ensure that computers accept inbound communication only from computers that are members of the Contoso domain by configuring a connection security rule by using Windows Firewall with Advanced Security.

### Case Scenario 2: Internet Explorer Configuration

1. You should configure InPrivate filtering through Group Policy.
2. Configure Group Policy to block the installation of unapproved add-ons and accelerators.
3. You should add the address of the Fabrikam Web site to the Trusted Sites zone.

# Chapter 6: Lesson Review Answers

---

## Lesson 1

### 1. Correct Answer: B

- A. **Incorrect:** Booting a workstation by using WDS eliminates the need for a local boot device, such as a Windows 7 installation disk.
- B. **Correct:** The Local Group Policy Editor is an MMC snap-in that you can use to apply Group Policy settings to the local computer only, not to large numbers of computers.
- C. **Incorrect:** Booting a workstation by using WDS eliminates the need for a local boot device, such as a USB flash drive.
- D. **Incorrect:** Booting a workstation by using WDS eliminates the need for a local boot device, such as a Windows PE boot disk.

### 2. Correct Answers: A and C

- A. **Correct:** Task sequences contain answer files and can therefore do anything that answer files can do, but they can also perform other actions before and after answer file processing.
- B. **Incorrect:** Creating a task sequence in Deployment Workbench automatically creates an answer file, not the other way around.
- C. **Correct:** You can configure a task sequence to automatically capture an image of an installed workstation and upload it to the MDT deployment share.
- D. **Incorrect:** You can use a task sequence to install a reference computer or a target computer.

### 3. Correct Answer: D

- A. **Incorrect:** The /oobe parameter configures a workstation to display the Windows Welcome user interface pages on startup.
- B. **Incorrect:** The /generalize parameter prepares a workstation for image capture by removing all user-specific and computer-specific settings.
- C. **Incorrect:** The /shutdown parameter causes the workstation to shut down after processing the other parameters.
- D. **Correct:** The /audit parameter enables you to start the workstation without completing the Windows Welcome user interface pages. You can then configure operating system settings or install applications on the target computer to create a customized configuration.

### 4. Correct Answer: A

- A. **Correct:** Deployment Workbench is included in Microsoft Deployment Toolkit 2010, not Windows 7 AIK.
- B. **Incorrect:** ImageX.exe is included in Windows 7 AIK.
- C. **Incorrect:** Deployment Image Servicing and Management is included in Windows 7 AIK.
- D. **Incorrect:** Windows System Image Manager is included in Windows 7 AIK.

## Lesson 2

**1. Correct Answer: B**

- A. Incorrect:** The new computer scenario is supported in a ZTI deployment.
- B. Correct:** The upgrade computer scenario is not supported in a ZTI deployment.
- C. Incorrect:** The refresh computer scenario is supported in a ZTI deployment.
- D. Incorrect:** The replace computer scenario is supported in a ZTI deployment.

**2. Correct Answer: A**

- A. Correct:** The ZTI method supports only network-based deployments.
- B. Incorrect:** ZTI deployments are completely automated and require no interaction at the workstation site.
- C. Incorrect:** ZTI deployments use RPC communications. Therefore, firewalls between the servers and workstations must permit RPC traffic to pass.
- D. Incorrect:** Because they perform more tasks, ZTI deployments are more difficult to configure than LTI deployments.

**3. Correct Answer: C**

- A. Incorrect:** In the new computer scenario, there is no user state data to capture or restore.
- B. Incorrect:** In the upgrade computer scenario, there is no need to capture or restore user state data because the upgrade process leaves the existing user state in place.
- C. Correct:** In the refresh computer scenario, a single task sequence captures the user state data, installs Windows 7, and then restores the user state data.
- D. Incorrect:** The replace computer scenario uses two separate task sequences to capture and restore the user state data.

**4. Correct Answers: A, B, and C**

- A. Correct:** WDS is included in Windows Server 2008 R2 and Windows Server 2008. You must therefore have a server on your network running one of these operating systems to deploy MDT 2010 boot images by using WDS.
- B. Correct:** Deploying boot images over the network by using WDS requires workstations with PXE-compliant network adapters.
- C. Correct:** To deploy images over the network by using WDS, you must have persistent, high-speed network connections.
- D. Incorrect:** Although WDS supports multicasting and requires routers that support it to service workstations on other networks, you can deploy boot images without multicasting, in which case multicast routing capabilities are not required.

## Chapter 6: Case Scenario Answers

---

### Case Scenario 1: Capturing an Image by Using WDS

1. On the server running Windows Server 2008 R2, install the Windows Deployment Services role by using Server Manager.
2. Using the Windows Deployment Services console, configure WDS.
3. Add the Boot.wim image file from a Windows 7 installation disk to the Boot Images container in the Windows Deployment Services console.
4. Convert the Boot.wim image to a capture image and add it to the Boot Images node.
5. On the newly installed workstation, run the Sysprep.exe utility from the command line with the /generalize and /oobe parameters.
6. Reboot the workstation, pressing F12 to bypass the local drive and perform a network boot.
7. From the boot menu, select the capture image you created and added on the WDS server.
8. Using the Image Capture Wizard, capture an image of the workstation, name it, and upload it to the WDS server.

### Case Scenario 2: Refreshing Workstations

The workstations are not downloading the install image by using multicast transmissions because they are using the Windows Deployment Wizard to download the images from the MDT deployment share, not from the WDS server. To conserve bandwidth, Alice must either deploy the install image by using WDS, or use another method, such as staggering deployments or moving the workstations to a dedicated deployment network.

## Chapter 7: Lesson Review Answers

---

### Lesson 1

1. **Correct Answer: B**
  - A. **Incorrect:** In a New Computer installation, there is no user state data to save.
  - B. **Correct:** In a Refresh Computer installation, a task sequence saves the user state data from the target computer, installs Windows 7, and then restores the user state data.
  - C. **Incorrect:** In a Replace Computer installation, a task sequence saves the user state data from an existing workstation, not from the target computer.
  - D. **Incorrect:** An Upgrade Computer installation preserves the user state data on the target computer, so there is no need to save it to another location.

**2. Correct Answer: C**

- A. Incorrect:** To suppress the Select A Task Sequence To Execute On This Computer page, you must add the SkipTaskSequence command to the CustomSettings.ini file.
- B. Incorrect:** To suppress the Join The Computer To A Domain Or Workgroup page, you must add the SkipDomainMembership command to the CustomSettings.ini file.
- C. Correct:** Adding the UserID, UserDomain, and UserPassword commands to the CustomSettings.ini file prevents the Specify Credentials For Connecting To Network Shares page from appearing. There is no need for a Skip command.
- D. Incorrect:** To suppress the Operating System Deployment Completed Successfully page, you must add the SkipFinalSummary command to the CustomSettings.ini file.

**3. Correct Answers: B and D**

- A. Incorrect:** The UserID command specifies the account that the wizard uses to access the deployment share on the build server. This value does not have to be unique.
- B. Correct:** The ProductKey command specifies an individual product key value for the Windows installation, and it therefore must be unique. MAK product keys use a different command.
- C. Incorrect:** The TaskSequenceID command specifies which task sequence the Windows Deployment Wizard should run on the target computer. This value does not have to be unique.
- D. Correct:** The OSDComputerName command specifies the name to be assigned to the target computer. The value must be unique on the network.

**4. Correct Answer: A**

- A. Correct:** By running the Litetouch.vbs script from an existing Windows installation, the task sequence can access the user state data on the computer.
- B. Incorrect:** Booting the target computer by using a WIM image deployed by Windows Deployment Services does not enable the task sequence to access the existing Windows operating system files on the computer.
- C. Incorrect:** Booting the target computer by using a disk created from an ISO image does not enable the task sequence to access the existing Windows operating system files on the computer.
- D. Incorrect:** Booting the target computer by using a disk created from an ISO image does not enable the task sequence to access the existing Windows operating system files on the computer.

## Lesson 2

**1. Correct Answer: B**

- A. Incorrect:** The MDT Files package enables the target computer to access MDT functions through the SCCM server. This package does not provide access to user state data.
- B. Correct:** The USMT package contains the User State Migration Tools programs, which enable the target computer to save and restore user state settings.
- C. Incorrect:** The Client package enables administrators to manage the target computer after the Windows 7 installation. This package does not provide access to user state data.
- D. Incorrect:** The Settings package contains the CustomSettings.ini and Unattend.txt files used to perform the target computer installation. This package does not provide access to user state data.

**2. Correct Answer: A**

- A. Correct:** A new computer with no operating system has no client that enables it to be discovered by SCCM. Therefore, you must add it to the site database manually.
- B. Incorrect:** In the Refresh Computer scenario, the computer already has an operating system and an SCCM client installed. This enables the SCCM server to discover the target computer automatically, eliminating the need to add it to the site database.
- C. Incorrect:** In the Replace Computer scenario, the computer already has an operating system and an SCCM client installed. This enables the SCCM server to discover the target computer automatically, eliminating the need to add it to the site database.
- D. Incorrect:** In the Upgrade Computer scenario, the computer already has an operating system and an SCCM client installed. This enables the SCCM server to discover the target computer automatically, eliminating the need to add it to the site database.

**3. Correct Answer: D**

- A. Incorrect:** The Site databases contain information about the client computers located at a particular site, but they do not themselves enable deployments across sites.
- B. Incorrect:** Collections are sets of computers, users, or groups that you can designate as the recipients of advertisements. They do not themselves enable deployments across sites.
- C. Incorrect:** Advertisements make software packages available to collections of computers, users, or groups. They do not themselves enable deployments across sites.
- D. Correct:** Distribution points are servers located at various sites that contain copies of the packages and images used to deploy Windows 7 to target computers. By replicating data to remote distribution points, SCCM enables you to deploy Windows 7 to target computers anywhere in the enterprise.

## Chapter 7: Case Scenario Answers

---

### Case Scenario 1: Multitasking an LTI Deployment

The reason the build server is not multicasting is because Ed created his deployment share by using the default share name, which is DeploymentShare\$. To support multicasting, he must create a deployment share by using the share name LTI\$ and repeat the process of populating it, updating it, and publishing the boot images by using WDS.

## Chapter 8: Lesson Review Answers

---

### Lesson 1

#### 1. Correct Answers: A and D

- A. **Correct:** You should create a WSUS group for the test computers and deploy the updates to that test group by the third Tuesday of each month.
- B. **Incorrect:** You should not add all computer accounts to the TestGroup group because deploying updates to this group means that all computers receive updates without their being adequately tested against the current configuration.
- C. **Incorrect:** You should not deploy updates to the All Computers WSUS group on the third Tuesday of each month because this plan does not ensure adequate time to test whether updates cause conflicts with existing configurations.
- D. **Correct:** You should deploy updates to the All Computers WSUS group on the fourth Tuesday of each month to ensure adequate testing and to meet your update rollout objective.

#### 2. Correct Answers: A, B, C, and E

- A. **Correct:** You need to upgrade updates.contoso.internal to Windows Server 2008 R2 to take advantage of the BranchCache feature.
- B. **Correct:** You must enable the BranchCache feature on the WSUS server before clients can cache content by using BranchCache at branch office locations.
- C. **Correct:** You must upgrade to WSUS 3 SP2 because previous versions of WSUS do not function on the Windows Server 2008 R2 platform, and Windows Server 2008 R2 is required if you want to implement BranchCache.
- D. **Incorrect:** You should not configure branch office clients to use BranchCache hosted cache mode because hosted cache mode requires that a Windows Server 2008 R2 server be present on the local branch office network.
- E. **Correct:** You should configure branch office clients to use BranchCache distributed cache mode because distributed cache mode allows BranchCache to function on a branch office network when a Windows Server 2008 R2 server is not located on the branch office LAN.

**3. Correct Answer: C**

- A.** **Incorrect:** Although you should run the most recent version of WSUS, you do not need to upgrade the head office WSUS server to WSUS 3.0 SP2.
- B.** **Incorrect:** BranchCache is available only on Windows 7 Enterprise and Ultimate.
- C.** **Correct:** Because BranchCache is not an option, you should deploy local WSUS servers to each branch office, have the clients in the branch office use the WSUS servers, and then configure the WSUS servers to pull updates off the head office server. This reduces WAN update traffic.
- D.** **Incorrect:** Upgrading the WSUS server in the head office to Windows Server 2008 R2 does not accomplish your goal because BranchCache cannot be implemented when clients have the Windows 7 Professional operating system installed.

**4. Correct Answer: C**

- A.** **Incorrect:** You should not configure six replica servers. Replica servers use approvals from an upstream server. In this scenario, each IT team should approve updates.
- B.** **Incorrect:** You should not configure an upstream server and six replica servers. Replica servers use approvals from an upstream server. In this scenario, each IT team should approve updates.
- C.** **Correct:** You should configure an upstream server that downloads updates from Microsoft Update. You should configure autonomous servers that obtain updates from the upstream server, but allow each department's IT team to approve updates for their specific department.
- D.** **Incorrect:** You should not configure six autonomous servers because you want each department's servers to retrieve updates, but not approvals, from a location on the organizational network.

## Lesson 2

**1. Correct Answer: D**

- A.** **Incorrect:** The Automatic Updates Detection Frequency policy specifies the period of time the computer waits before checking for updates.
- B.** **Incorrect:** The Enable Client-Side Targeting policy allows computers to be placed in groups on the WSUS server but does not ensure that the WSUS server will be used for updates.
- C.** **Incorrect:** The Turn On Recommended Updates Via Automatic Updates policy specifies whether Automatic Updates deliver both Important and Recommended updates.
- D.** **Correct:** The Specify Intranet Microsoft Update Service Location policy is used to specify the location of a local WSUS server.

**2. Correct Answer: B**

- A. Incorrect:** The Configure Automatic Updates policy specifies when the computer receives updates; it does not allow nonadministrative users to install updates.
- B. Correct:** When configured, the Allow Non-Administrators To Receive Update Notifications policy allows nonadministrative users to receive update notifications and to install updates.
- C. Incorrect:** The No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations policy allows users to continue working after an update that requires a restart has been installed, rather than forcing them to log off and restart the computer.
- D. Incorrect:** The Allow Signed Updates From An Intranet Microsoft Update Service Location policy allows you to deploy updates from vendors other than Microsoft.

**3. Correct Answer: A**

- A. Correct:** You should choose the Notify For Download And Notify For Install option because this option provides a notification that allows the locally logged-on user to choose when to download and install the update.
- B. Incorrect:** You should not choose the Auto Download And Notify For Install option because this option automatically downloads any newly detected updates.
- C. Incorrect:** You should not choose the Auto Download And Schedule The Install option because this option automatically downloads any newly detected updates.
- D. Incorrect:** You should not choose the Allow Local Admin To Choose Setting as this option requires users to make their own selection rather than ensuring that they are notified that updates are available.

**4. Correct Answer: C**

- A. Incorrect:** You cannot use Windows Server Update Services to check whether computers that use Microsoft Update have the most recent updates installed.
- B. Incorrect:** Gpresult.exe is used to determine the resultant Group Policy configuration. You cannot use it to determine the status of updates.
- C. Correct:** The Microsoft Baseline Security Analyzer can be used to check whether computers that receive their updates from Microsoft Updates have the most recent updates installed.
- D. Incorrect:** Ocplist.exe is used to install components on a computer running Windows Server 2008 Server Core. You cannot use it to determine the status of software updates.

## Chapter 8: Case Scenario Answers

---

### Case Scenario 1: Contoso WSUS upgrade

1. Replace all the branch office computers with computers running Windows 7 Enterprise edition.
2. Ensure that WSUS 3.0 SP2 is installed at the head office on a computer running Windows Server 2008 R2. Enable the BranchCache feature on this server.

### Case Scenario 2: Fabrikam software update policies

1. Configure the Specify Intranet Microsoft Update Service Location policy to ensure that clients use the local WSUS server.
2. You need to configure the Specify Intranet Microsoft Update Service Location policy to point to the head office WSUS server. You also need to configure the Turn On BranchCache and Set BranchCache Hosted Cache Mode policies to ensure that clients use BranchCache in Hosted Mode for updates.
3. You should configure the No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations policy.

## Chapter 9: Lesson Review Answers

---

### Lesson 1

1. **Correct Answer: C**
  - A. **Incorrect:** System Center Configuration Manager can perform an application inventory, but it requires a client on every workstation.
  - B. **Incorrect:** Application Compatibility Toolkit can gather information about the applications on your workstations, but it requires each one to be running a client.
  - C. **Correct:** The Microsoft Assessment and Planning Toolkit can perform an application inventory and does not require an agent on the network workstations.
  - D. **Incorrect:** Microsoft Application Virtualization is a tool for deploying virtualized applications; it cannot perform an application inventory.
2. **Correct Answer: A**
  - A. **Correct:** Remote Desktop Services executes applications on a server and enables client workstations to access them. The application does not use workstation resources to run.
  - B. **Incorrect:** System Center Configuration Manager can deploy applications to workstations, but after the deployment is complete, the applications run by using workstation resources, and SCCM is no longer involved.

- C. **Incorrect:** Microsoft Application Virtualization delivers virtualized applications to workstations, but the applications run by using workstation resources.
  - D. **Incorrect:** You can use Group Policy to deliver Windows Installer packages to workstations, but the installation and the execution of the application use workstation resources.
3. **Correct Answer: B**
- A. **Incorrect:** A manual installation requires the greatest amount of time and interaction of all the proposed methods.
  - B. **Correct:** Thick images require no installation time or interaction at all because the images are included in the image file deployed to the target workstation.
  - C. **Incorrect:** An SCCM application deployment might not require any interaction at the workstation, but it does require some time for the installation.
  - D. **Incorrect:** The Group Policy deployment might require some interaction, depending on the configuration of the .msi file and the policy settings, and it definitely requires some time to perform the installation.
4. **Correct Answer: D**
- A. **Incorrect:** It is true that Microsoft Application Virtualization can deliver applications to desktop workstations or to RDS servers.
  - B. **Incorrect:** It is true that Microsoft Application Virtualization requires that a client be installed on each workstation that is to receive applications.
  - C. **Incorrect:** It is true that Microsoft Application Virtualization executes applications by using workstation hardware resources.
  - D. **Correct:** Microsoft Application Virtualization does not install applications on the client workstations.

## Lesson 2

1. **Correct Answer: C**
- A. **Incorrect:** The Internet Explorer Compatibility Test Tool is designed for use by administrators and developers seeking to discover Web site compatibility issues, not end users.
  - B. **Incorrect:** The App-V is a tool that administrators use to deploy virtualized applications to workstations. It is not intended for end users.
  - C. **Correct:** The Program Compatibility Troubleshooter is an end-user tool that uses a wizard-based interface to help users select an appropriate compatibility mode.
  - D. **Incorrect:** Shims, or compatibility fixes, are application-specific patches that administrators apply to workstations.

**2. Correct Answer: B**

- A. Incorrect:** Compatibility Administrator provides access to the Microsoft Compatibility Exchange, a central clearing house for known compatibility problems. You do not use it to create data-collection packages.
- B. Correct:** Application Compatibility Manager is a tool that enables you to gather information from your workstations and add it to a database. To do this, you must first create data-collection packages and distribute them to your workstations.
- C. Incorrect:** The Standard User Analyzer examines applications for compatibility issues caused by User Account Control. You cannot use it to create data-collection packages.
- D. Incorrect:** The Setup Analysis Tool is a logging program that analyzes application setup programs for compatibility issues. You cannot use it to create data-collection packages.

**3. Correct Answer: D**

- A. Incorrect:** Software Metering Client Agent, part of the System Center Configuration Manager product, is a component of the SCCM client that tracks application use on workstations.
- B. Incorrect:** Microsoft Assessment and Planning Toolkit is an inventory tool, but it is not part of the Microsoft Desktop Optimization Pack.
- C. Incorrect:** Software Inventory Client Agent, part of the System Center Configuration Manager product, is a component of the SCCM client that gathers information about applications installed on workstations.
- D. Correct:** Available as part of the Microsoft Desktop Optimization Pack (MDOP), AIS uses a Web-based database hosted in Microsoft's datacenters to store inventory information gathered from client workstations.

## Chapter 9: Case Scenario Answers

---

### Case Scenario 1: Planning an Application Deployment

The workstations achieve the best performance if Howard deploys the call tracking application to them by using Remote Desktop Services because RDS runs the application by using server resources, not the resources on the workstation. The workstation therefore has to run only the operating system and the Remote Desktop Connection client.

### Case Scenario 2: Deploying Packages

Although SCCM can create packages, the packages it creates are not the same as Windows Installer packages. When SCCM creates a package, it does not place all of the source files for an application into a single database file with an .msi extension. To create a Windows Installer package file, Richard has to use another utility.

## Chapter 10: Lesson Review Answers

---

### Lesson 1

- 1. Correct Answer: A**
  - A. Correct:** Group Policy Software Installation can publish a package only to users; the Computer Configuration policy does not support the publish option.
  - B. Incorrect:** Group Policy Software Installation cannot publish a package to computers.
  - C. Incorrect:** Group Policy Software Installation cannot publish a package to computers.
  - D. Incorrect:** Group Policy Software Installation can publish a package to users.
- 2. Correct Answer: B**
  - A. Incorrect:** The Categories tab appears in both the Software Installation Properties sheet and a package policy's Properties sheet.
  - B. Correct:** The File Extensions tab appears in the Software Installation Properties sheet but not in a package policy's Properties sheet.
  - C. Incorrect:** The Upgrades tab does not appear in the Software Installation Properties sheet.
  - D. Incorrect:** The Modifications tab does not appear in the Software Installation Properties sheet.
- 3. Correct Answers: B and C**
  - A. Incorrect:** The Access Accounts subheading does not require configuration to complete a software distribution.
  - B. Correct:** To successfully complete a software distribution, you must specify at least one distribution point for a package.
  - C. Correct:** To successfully complete a software distribution, you must create at least one program for a package.
  - D. Incorrect:** The Package Status subheading does not require configuration to complete a software distribution.

### Lesson 2

- 1. Correct Answer: C**
  - A. Incorrect:** Remote Desktop Protocol functionality is provided by the Remote Desktop Session Host role service.
  - B. Incorrect:** Remote Desktop Connection is a client program that does not require any role services.
  - C. Correct:** To use the RD Web Access feature, you must install the Remote Desktop Web Access role service.
  - D. Incorrect:** RemoteApp functionality is provided by the Remote Desktop Session Host role service.

- 2. Correct Answer: C**
  - A. Incorrect:** You can deploy an RDP file by sending it to users in an e-mail.
  - B. Incorrect:** You can deploy an RDP file by placing it on a shared network drive.
  - C. Correct:** You cannot use Group Policy to deploy an RDP file because Group Policy can deploy only Windows Installer (MST) packages.
  - D. Incorrect:** You can deploy an RDP file by creating a software distribution package in SCCM.
- 3. Correct Answer: A**
  - A. Correct:** RemoteApp uses one server session for multiple applications.
  - B. Incorrect:** RemoteApp uses one server session for multiple applications.
  - C. Incorrect:** RemoteApp does not require an IIS server; you can deploy applications as RDP files or Windows Installer packages instead.
  - D. Incorrect:** A workstation can run multiple RemoteApp applications.

## Chapter 10: Case Scenario Answers

---

### Case Scenario 1: Performing an SCCM Software Distribution

The package might not appear in the Select A Package dialog box because the distribution point has not yet been successfully updated with the source files. However, the more likely reason is that Alice has not created a program for the package.

## Chapter 11: Lesson Review Answers

---

### Lesson 1

- 1. Correct Answer: B**
  - A. Incorrect:** A DNS failure would not cause the computer to have an IP address on the 169.254.0.0/16 network.
  - B. Correct:** A DHCP failure would prevent access to the Internet and cause the computer to self-assign an IP address on the 169.254.0.0/16 network by using APIPA.
  - C. Incorrect:** A firewall configuration error would not cause the computer to have an IP address on the 169.254.0.0/16 network.
  - D. Incorrect:** A missing certificate would not cause the computer to have an IP address on the 169.254.0.0/16 network.

- 2. Correct Answer: B**
- A.** **Incorrect:** An incorrectly configured firewall might block the port required to access a Web site protected with SSL.
  - B.** **Correct:** A DNS failure would prevent access to all Web sites, not just those protected with SSL.
  - C.** **Incorrect:** A missing certificate could prevent Internet Explorer from accessing an SSL-protected Web site.
  - D.** **Incorrect:** A security zone problem could prevent Internet Explorer from accessing an SSL-protected Web site.
- 3. Correct Answer: D**
- A.** **Incorrect:** Modifying security zone settings has no effect because a DNS failure prevents the browser from reaching the Web server.
  - B.** **Incorrect:** The *https://* prefix is for connecting to a secured Web site and has no effect on a DNS problem.
  - C.** **Incorrect:** The 169.254.0.0/16 address is assigned by APIPA when there is a DHCP failure, not a DNS failure.
  - D.** **Correct:** A DNS failure prevents workstations from resolving names into addresses, so substituting an IP address in the URL bypasses the problem.

## Lesson 2

- 1. Correct Answer: D**
- A.** **Incorrect:** GPOs linked to domains take precedence over GPOs linked to sites.
  - B.** **Incorrect:** GPOs linked to lower-level OUs take precedence over those linked to higher-level OUs.
  - C.** **Incorrect:** GPOs linked to AD DS objects take precedence over local GPOs.
  - D.** **Correct:** GPOs linked to OUs take precedence over GPOs linked to domains and sites.
- 2. Correct Answer: B**
- A.** **Incorrect:** Security filtering cannot limit GPO distribution to domains.
  - B.** **Correct:** Security filtering can limit GPO distribution to security groups.
  - C.** **Incorrect:** Security filtering cannot limit GPO distribution to sites.
  - D.** **Incorrect:** Security filtering cannot limit GPO distribution to OUs.

**3. Correct Answer: B**

- A. Incorrect:** Gpresult.exe cannot make sure that a workstation has received all of the latest GPO modifications.
- B. Correct:** Gpupdate.exe retrieves the latest GPOs and applies them to a workstation.
- C. Incorrect:** Group Policy Management Console cannot make sure that a workstation has received all of the latest GPO modifications.
- D. Incorrect:** Resultant Set of Policy cannot make sure that a workstation has received all of the latest GPO modifications.

## Chapter 11: Case Scenario Answers

---

### Case Scenario 1: Troubleshooting a Web-based Application

Answer D is correct because you can add the URL of the client Web site to the list in the Use Policy list of Internet Explorer 7 sites policy. Answer A is incorrect because it turns off Compatibility View. Answer B is incorrect because the client Web site might not be included in the lists obtained from Microsoft. Answer C is incorrect because turning on Standards Mode would affect all sites, not just the one experiencing a problem.

### Case Scenario 2: Deploying a GPO

Richard can still link the TimesheetApp GPO to the domain object, as long as he uses Security Filtering to deploy the settings to members of a security group that contains only the department heads.

## Chapter 12: Lesson Review Answers

---

### Lesson 1

**1. Correct Answer: B**

- A. Incorrect:** Ping.exe is included with Windows 7.
- B. Correct:** Network Monitor is available as a free download from Microsoft, but it is not included with Windows 7.
- C. Incorrect:** Pathping.exe is included with Windows 7.
- D. Incorrect:** Tracert.exe is included with Windows 7.

- 2. Correct Answer: A**
- A.** **Correct:** Wireless devices must be configured to use the same security protocol with the same configuration. They are not capable of negotiating the use of a common protocol.
  - B.** **Incorrect:** Wireless devices can automatically negotiate the use of the fastest communication protocol they have in common.
  - C.** **Incorrect:** By default, VPN servers are capable of handling clients by using any one of the supported protocols.
  - D.** **Incorrect:** The VPN clients and servers are capable of negotiating the use of the strongest authentication protocol they have in common.
- 3. Correct Answers: A and B**
- A.** **Correct:** A computer with an incorrectly configured IP address cannot communicate with the other computers on the network.
  - B.** **Correct:** A computer with an incorrectly configured subnet mask cannot communicate with the other computers on the network.
  - C.** **Incorrect:** A computer with an incorrectly configured Default gateway address can communicate with computers on the local network, but not with computers on other networks.
  - D.** **Incorrect:** A computer with incorrectly configured DNS server addresses cannot communicate with the other computers by using their DNS names, but they can communicate by using IP addresses.

## Lesson 2

- 1. Correct Answer: C**
- A.** **Incorrect:** Nltest.exe can run on any Windows 7 workstation.
  - B.** **Incorrect:** DNSLint.exe can run on any Windows computer.
  - C.** **Correct:** Dcdiag.exe tests domain controller functions and therefore must run on a domain controller.
  - D.** **Incorrect:** Kerbtray.exe can run on any AD DS domain member.
- 2. Correct Answer: B**
- A.** **Incorrect:** The workstation's clock time must be within 5 minutes of the domain controller's clock time, not 5 seconds.
  - B.** **Correct:** The workstation's clock time must be within 5 minutes of the domain controller's clock time.
  - C.** **Incorrect:** The workstation's clock time must be within 5 minutes of the domain controller's clock time, not 15 minutes.
  - D.** **Incorrect:** The workstation's clock time must be within 5 minutes of the domain controller's clock time, not 1 hour.

**3. Correct Answer: D**

- A. Incorrect:** A disabled computer account would prevent the user from logging on.
- B. Incorrect:** If the Domain Users group is not a member of a workstation's local Users group, the domain user account would not receive the Allow Log On Locally user right and would not be able to log on.
- C. Incorrect:** If the second workstation was disconnected, the user would not be able to log on to the domain.
- D. Correct:** A disconnected domain controller could not be the problem because the user would not be able to access network resources from either workstation.

## Chapter 12: Case Scenario Answers

---

### Case Scenario 1: Troubleshooting TCP/IP Configuration Settings

The user is unable to access the Internet because the computer has no Default Gateway address. Because the computer is receiving its TCP/IP configuration settings through DHCP, the problem is in the DHCP server configuration. To correct the problem, Lupe must either configure the computer's TCP/IP configuration manually or troubleshoot the DHCP server.

### Case Scenario 2: Troubleshooting an Authentication Problem

The only conclusion you can make about Elsie's problem is (C), that it is located in her user account. A problem with the account would prevent her from logging on at any workstation and would not affect other users. Her workstation can't be the source of the problem because her logon attempts failed from a different workstation. The domain controller can't be malfunctioning because other users are able to log on.

# Glossary

## A

**Activation** Process in which the product key and machine ID are registered with Microsoft.

**advertisement** In Microsoft System Center Configuration Manager, the mechanism by which the server makes software packages available to collections of computers, users, or groups.

**AppLocker** A technology that allows you to restrict the execution of applications by publisher, file hash, or location.

**App-V** See *Microsoft Application Virtualization*.

**asynchronous processing** A type of Group Policy processing in which the Windows workstations display the logged-on user's desktop before it has finished downloading and processing the Group Policy objects from the domain controller.

**Automatic Private IP Addressing (APIPA)** A Windows feature that enables a computer to assign itself an IP address when it fails to obtain one from a DHCP server.

## B

**BitLocker** A technology that allows full volume encryption.

**BranchCache** A networking technology that allows computers running Windows 7 in branch offices to share files that have been retrieved across the wide area network link from a specially configured head office Windows Server 2008 R2 server.

**build computer** A computer running Microsoft Deployment Toolkit and/or Windows Automated Installation Kit, which administrators use to create and deploy Windows Imaging files.

**build-to-order (BTO)** A type of image deployment, supported by Windows 7 Automated Installation Kit, in which administrators use an answer file to build the reference computer, deploy the resulting image on the target computers, and then boot the computers in audit mode to make further customizations.

**build-to-plan (BTP)** A type of image deployment, supported by Windows 7 Automated Installation Kit, in which administrators build the reference computer by using an answer file and create an image, which they deploy to the target workstations unaltered.

## C

**capture image** A type of Windows Deployment Services (WDS) image file that enables a computer to boot, capture an image of the local disk, and upload the image to a WDS server on the network.

**collection** In System Center Configuration Manager, an organizational tool that enables administrators to perform tasks on a specific set of computers, users, or groups.

**compatibility fix** A software routine that rests between an application and an operating system, translating function calls to emulate compatible versions of both entities. Also called a *shim*.

**compatibility mode** A collection of compatibility fixes.

**Compatibility View** A feature in Windows Internet Explorer that enables the browser to emulate older development standards.

**CustomSettings.ini** The main configuration file for Microsoft Deployment Toolkit 2010. Target computers read the file when they load the Windows Deployment Wizard, and the settings inside control the behavior of the wizard and the deployment process.

## D

**Deployment Image Servicing and Management (DISM.exe)**

A command-line tool, included with Windows 7 and Windows 7 Automated Installation Kit, that you can use to mount, view, and modify Windows Imaging files in their online or offline state.

**discover image** A type of Windows Deployment Services (WDS) image file that enables computers without Pre-Boot Execution Environment-compliant network adapters to boot from a removable medium and access the WDS server over the network.

**Distributed cache mode** A BranchCache mode in which clients do not use a local server to store cached updates.

**distribution point** In System Center Configuration Manager (SCCM), a computer on the network that is designated as a storehouse for SCCM packages and images.

## F

**file-based image** A type of archive file that contains a complete image of a disk, application, or operating system, in which the smallest data storage unit is the file, not the sector. File-based images provide a number of advantages over traditional sector-based image files, including hardware independence and editability.

**functional GPO** A type of Group Policy object (GPO) that contains only a fraction of the settings needed for a complete workstation configuration. As a result, administrators typically have to apply multiple GPOs to realize a full configuration.

## G

**GPO Accelerator** A Microsoft program that automatically creates the organizational units and Group Policy objects needed to implement the Enterprise Client and Specialized Security Limited Functionality environments defined in the Windows Security Guide documents.

**Gpresult.exe** A command-line program that displays information about the Group Policy settings that apply to a particular client workstation.

## H

**Hard-link** Migration technique in which files remain in place during their migration to a new operating system.

**Hosted cache mode** A BranchCache mode in which clients use a local server to store cached updates.

**hybrid image** A Windows Imaging file that installs all of the applications and other software components the workstation needs, but does not include all of those other components as part of the image file. Instead, the system accesses the additional components from a share on the network.

## I

**ImageX.exe** A command-line tool, included in the Windows 7 Automated Installation Kit, that enables administrators to capture and service Windows Imaging files.

**InPrivate Browsing** An Internet Explorer browsing mode that blocks the application from recording browsing history information.

**InPrivate Filtering** An Internet Explorer mode that blocks third-party sites from tracking a browsing session across multiple Web locations.

## K

**Kerberos** An authentication protocol that enables users to log on to an Active Directory Domain Services domain without transmitting passwords and other sensitive information over unsecured channels.

**KMS** Key Management Services.

## L

**language pack** A Microsoft operating system module that provides all of the localization code needed for an operating system to support a particular language.

**latency interval** The time it takes to transmit data between two computers.

**Lite-Touch Installation (LTI)** A deployment methodology supported by Microsoft Deployment Toolkit 2010 that enables administrators to install computers with a minimum of interaction.

## M

**MAK** Multiple Activation Key.

**mandatory profile** A read-only roaming user profile that provides workstations with a standardized desktop environment each time a user logs on.

**Microsoft Application Virtualization (App-V)** A technology that enables Windows servers to virtualize applications, much in the way that Hyper-V virtualizes operating systems. With App-V, servers supply applications to a client running on the workstation, and the client executes them locally in a sandboxed environment.

**Microsoft Assessment And Planning (MAP) Toolkit**

**4.0** A free software product that can perform agentless hardware and software inventories of networked computers and compile reports and proposals that assess the readiness of the computers for upgrades to the latest Windows operating systems.

**Microsoft Deployment Toolkit (MDT) 2010** A free collection of tools and documentation designed to help system administrators deploy large numbers of Windows computers on an enterprise network.

**Microsoft Operations Framework (MOF) 4.0** A collection of white papers and other documents that define a complete organizational and management life cycle for an IT service.

**Microsoft Solutions Framework (MSF)** A collection of white papers and other documents that define the planning, development, and delivery processes for an application development or other IT process.

**Microsoft System Center Configuration Manager (SCCM) 2007** A software product that provides a comprehensive set of system and network management functions for Windows computers, including operating system deployment, software distribution, update management, remote administration, and hardware and software inventory.

**Microsoft Visual Basic Scripting Edition (VBScript)** A variant of the Visual Basic programming language that Windows administrators use to create scripts, particularly startup, shutdown, logon, and logoff scripts.

**monolithic GPO** A type of Group Policy object (GPO) that contains all of the settings needed for a complete workstation configuration.

**multicast** A type of IP communication that transmits data to multiple destinations simultaneously, conserving network bandwidth in the process.

## N

**Network Monitor** A graphical diagnostic application that captures samples of the data packets transmitted over a network and examines their contents.

## O

**offline image** A file-based image file that is not currently loaded into a computer's memory.

**online image** A file-based image that is currently loaded into a computer's memory.

## P

**package (System Center Configuration Manager)**

A software element, typically containing source files and programs, that SCCM distributes to clients on a network. Unlike Windows Installer packages, SCCM packages do not use a single file database format.

**package (Windows Installer)** A database file with an .msi extension that contains everything a computer needs to install and run a particular application. Not to be confused with *package (System Center Configuration Manager)*.

**Ping.exe** A command-line program that is the Windows version of a standard TCP/IP network testing tool that transmits a series of Echo Request messages by using a protocol called Internet Control Message Protocol. The computer receiving those messages then replies with a series of Echo Reply messages, which Ping.exe displays.

**Pre-Boot Execution Environment (PXE)** A hardcoded environment build into network interface adapters, which enables a computer to boot by downloading configuration data and startup files from servers on the network.

**program** In System Center Configuration Manager 2007, a package component that contains the command that the target computers execute to install the application in a package.

## Q

**quiet mode** A command-line parameter that causes a program to execute without displaying any indications of its progress.

## R

**reference computer** A computer that administrators use as a model from which to create customized Windows Imaging files.

**Remote Desktop Connection** The Remote Desktop Services client program running on a workstation.

**Remote Desktop Protocol (RDP)** The communications protocol that connects the Remote Desktop Connection client to the Remote Desktop Session Host service on the Remote Desktop Services server.

**Remote Desktop Services (RDS)** A client/server application, implemented as a Windows Server 2008 R2 role, which provides clients with access to applications and entire Windows desktops. Formerly known as Terminal Services.

**Remote Desktop Session Host** The core service running on a Remote Desktop Services server, hosting individual applications and full desktops.

**RemoteApp** A Remote Desktop Services feature that delivers individual applications to clients in separate windows.

**Replica mode** A Windows Server Update Services (WSUS) server deployment in which a WSUS server receives update approval data from another WSUS server in the organization.

**Resultant Set of Policy (RSoP)** A snap-in for Microsoft Management Console that displays information about the Group Policy settings that apply to a particular client workstation. This tool has been deprecated with the release of Windows Vista.

**roaming profile** A user profile that is stored on a shared server drive so that users can access it from any workstation on the network.

## S

**sandbox** An isolated environment in which software can run without affecting or being affected by other software running on the system.

**sector-based image** A type of archive file containing an exact replica of a disk and in which the smallest data storage unit is the sector.

**Service management functions (SMFs)** The designation assigned to the individual white papers that make up the Microsoft Operations Framework (MOF). Each SMF defines a stage, phase, or level of the MOF life cycle.

**shim** See *compatibility fix*.

**starter GPO** A specialized type of Group Policy object (GPO) that contains only administrative templates. Administrators use starter GPOs as templates with which they can create fully configured GPOs.

**super-mandatory profile** A type of mandatory profile that prevents workstations from starting if they are unable to access the profile on the network.

**synchronous processing** A type of Group Policy processing in which the Windows workstation waits to display the logged-on user's desktop until it has finished downloading and processing the Group Policy objects from the domain controller.

## T

**target computer** A production computer to which administrators deploy Windows Imaging files.

**thick image** A Windows Imaging file that contains a complete workstation configuration, including all applications, drivers, updates, and language packs.

**thin image** A Windows Imaging file that contains an operating system, but few applications or other software components, if any at all. Instead of deploying the applications, updates, device drivers, and language packs with the operating system, as in a thick image, administrators deploy them afterward, typically using a software distribution product.

**Tracert.exe** A command-line program that is the Windows version of a UNIX tool called traceroute, which can help administrators locate a malfunctioning router. Tracert.exe works by transmitting groups of ICMP Echo Request messages, with each group configured to go one hop beyond the previous one. The program then resolves the address of the router at each hop into a name and displays a trace that lists the routers between the source and the destination systems.

## U

**user profile** A collection of folders and registry settings in which a Windows computer stores its desktop environment and user configuration.

## V

**VBScript** See *Microsoft Visual Basic Scripting Edition (VBScript)*.

## W

**Wi-Fi Protected Access (WPA and WPA2)** A wireless security protocol that can use various encryption algorithms to provide a more secure environment than Wired Equivalent Privacy.

**Windows 7 Automated Installation Kit (Windows AIK)** A collection of tools and documentation that enables administrators to perform unattended operating system installations.

**Windows Deployment Services (WDS)** A service included in Windows Server 2008 R2 and Windows Server 2008 that can deploy boot images and install images to computers over the network.

**Windows Error Reporting** A Windows technology that automatically collects information about error conditions and forwards it to a server for administrative attention.

**Windows Imaging** A file-based image format, developed by Microsoft, which contains a complete image of one or more operating systems.

**Windows Installer** An installation engine included with Windows 7 and earlier Windows versions that reads the contents of package files and uses them to install an application or other software entity.

**Windows Preinstallation Environment (Windows PE)** A minimal version of the Windows operating system used to boot bare metal computers, in preparation for deployment of an image file.

**Windows System Image Manager (SIM)** A graphical tool, included in the Windows 7 Automated Installation Kit, which enables administrators to create properly formatted XML answer files for unattended operating system installations.

**Wired Equivalent Privacy (WEP)** A wireless security protocol that, because of some serious shortcomings, has been largely replaced with newer technologies.

## Z

**Zero-Touch Installation (ZTI)** A deployment methodology supported by Microsoft Deployment Toolkit 2010 that enables administrators to install computers with no interaction.

# Index

## A

accelerators, 208–209  
accelerators (*Internet Explorer*), 208  
account policies, 181–182  
activating branch office and head office  
    (case scenario), 72  
activating volume licenses, 45–49  
activating Windows 7, 44  
    multiple activations, 45–46  
    online process, 44  
    overview of, 44  
activation client (practice), 73  
activation servers, on local area networks, 48–49  
AD DS deployment strategy, 397–398  
AD DS domain logon failures, 488–496  
Add a Script dialog box, 144  
add-ons, 208–209  
add-ons (*Internet Explorer*)  
    policies for, 208  
    troubleshooting, 449  
Add/Remove Programs control panel, removing  
    applications from, 401  
advertisements  
    creating, 315–316, 414  
    scheduling, 316  
AIK. *See* Windows 7 AIK  
answer files  
    applying to images, 109  
    creating, 80–81  
    editing, 81  
application bundling, 357

Application Compatibility Manager, 378–380  
Application Compatibility Toolkit  
    analyzing data from, 380  
    components of, 378  
    configuring (practice), 384–385  
    installing (practice), 384  
    Setup Analysis Tool, 383  
application deployment  
    AD DS strategy, 397–398  
    Assign vs. Publish, 396–397  
    auditing clients for, 359–360  
    automatic application installation, 400  
    client-based, 362–363  
    compatibility, 357  
    with Group Policy, 365, 393–402  
    legacy considerations, 370  
    local method, choosing, 402  
    manual, 364  
    with Microsoft Application Virtualization, 366  
    mixed method, 363  
    package-based, 364  
    with Remote Desktop Services, 417  
    scaling, 3–5, 362  
    with SCCM 2007, 365  
    selecting method for, 360–362  
    server-based, 363, 365–366  
    software distribution points, 398  
    thin-client vs. fat-client models, 361–362  
application incompatibilities, 369–370  
    compatibility modes, 373–374  
    database for, 372  
    testing for, 372

## application inventory

application inventory, 370–372  
application testing, 358  
application virtualization, 366  
applications  
    compatibility, 357  
    deployment versatility, 357  
    hardware requirements, 358  
    requirement overview, 358  
    selecting, 356–360  
    software prerequisites, 359  
    supplemental, 89  
    uninstalling when out of scope of management, 401  
    user requirements for, identifying, 356–357  
AppLocker  
    category restrictions, 185–186  
    policies, configuring (practice), 192–193  
    settings, 185–186  
App-V. *See Microsoft Application Virtualization*  
Asset Inventory Service (AIS), 371  
Assign deployment, 396–397  
Audit Object Access Policy, 163  
auditing policies  
    configuring, 162–165  
    creating, 155–157  
authentication exemption rules, 180  
authorization failures, troubleshooting, 496–497  
auto-cast multicasting, 294  
Automated Installation Kit (AIK). *See Windows 7 AIK*

## B

bandwidth considerations, 270–271, 292–294  
baseline configurations  
    with GPO Accelerator, 151–153  
    overview of, 150  
batch files, 140  
binary property values, 287  
BitLocker  
    configuring, 173–176  
    enabling, 285  
    encryption and, 176  
    overview of, 173  
    startup options, 174

BitLocker To Go  
    configuring, 176–178  
    configuring to limit USB flash storage device usage (practice), 191–192  
    removable device policies, 187–188  
blocking GPO inheritance, 136  
blocking InPrivate Browsing, 205–206  
book errors, reporting, xxiii  
boot disks, creating, 274  
boot image packages, 84, 304  
boot images  
    creating, 274  
    deploying to reference computer, 85  
boot media, creating, 317–319  
booting from VHD, 55–57  
branch office activation (case scenario), 72  
BranchCache, 333, 478  
browsing history, 205  
BTO (build-to-order), 231  
BTP (build-to-plan), 231  
build computer, 267  
    connecting to production network, 270  
    creating, 83  
build server for image files, 87  
Build stage of Deliver phase, 16–17  
build-to-order (BTO), 231  
build-to-plan (BTP), 231

## C

cache settings, 202  
case scenarios  
    activating branch office and head office, 72  
    branch office activation, 72  
    capturing WDS image, 262  
    client security at Contoso, 217  
    Fabrikam policies, 353  
    GPO deployment, 167  
    head office activation, 72  
    Image.exe, 114  
    Internet Explorer configuration, 217  
    migrating users to virtual machines, 72–73

refreshing workstations, 224–263  
user interface language modification, 114–115  
Windows 7 deployment, 38  
certificates, troubleshooting, 443–444  
Certification Mode practice test, xxii  
client baseline configuration  
    creating, 150–165  
    deploying, 150–151  
client boot methods, 274–275  
client deployment  
    bandwidth needed, 257–258  
    creating task sequence to install Windows 7 and  
        restore user state data (practice), 259  
    creating task sequence to save user state data  
        (practice), 258  
    dedicated deployment network, 258  
    multicasting, 258  
    number of workstations required, 256–257  
    off-hours deployment, 257  
    scaling process, 256–258  
    stagger deployment, 257  
client hardware platform  
    designing, 52–60  
    Windows 7 editions, 53  
    Windows 7 hardware requirements, 52–53  
client life cycle, designing, 41–73  
client security at Contoso (case scenario), 217  
client security, configuring, 172–193  
client-based application deployment, 362–363  
clients  
    auditing for application deployment, 359–360  
    deploying updates to, 343–348  
    designing configuration strategies, 118–148  
collections, creating, 314–315, 405  
committing system images, 109  
companion media, xx  
Compatibility Administrator, 380, 381  
compatibility controls, limiting, 375–376  
compatibility evaluators, 379  
compatibility fixes, 376  
compatibility modes, 373–374  
Compatibility View in Internet Explorer, 444–446  
    configuring (practice), 449–450  
compressed migration stores, 68

configuration  
    creating client baseline, 150–165  
    designing client strategies, 118–148  
    evaluating business requirements, 119  
    Group Policy, 121–140  
    matching settings to requirements, 119–120  
    method selection, 120–121  
configuration management, 110  
Configure ConfigMgr Integration Wizard, 299–300  
Config.xml, 66  
connection security rules, 180  
Contoso WSUS upgrade (case scenario), 353  
Create And Attach Virtual Hard Disk dialog box, 56  
Custom Mode practice test, xxii  
Custom Mode dialog box, xxii  
Customer Service process, 20  
CustomSettings.ini file  
    binary property values, 287  
    configuring individual computers in, 291  
    customization cost/benefit, 266  
    defining groups in, 290–291  
    editing manually, 288  
    formatting of, 287  
    ignoring wizard pages with, 289–290  
    ignoring wizard pages with (practice), 295–296  
    reference for, 288  
    in Zero-Touch Installation, 309

## D

data collection packages (DCPs), 379  
data collector set for performance baseline, 32  
data execution prevention (DEP), 369  
data recovery agents, 175  
Dcdiag.exe, 493  
default commands, modifying (practice), 294–295  
default gateway, troubleshooting, 473  
Deliver phase, 14–18  
    building, 16–17  
    deploying, 18  
    envisioning, 15  
    project planning, 15–16  
    stabilizing, 17–18

## Deploy Software dialog box

Deploy Software dialog box, 400  
deploying. *See also* application deployment;  
Lite-Touch Installation (LTI); Zero-Touch  
Installation (ZTI)  
bandwidth considerations, 270–271, 292–294  
choosing method, 248–259  
life cycle, 3–23  
Lite-Touch Installation (LTI) vs. Zero-Touch  
Installation (ZTI), 254–255  
planning for, 267  
storage space for, 268  
using Microsoft deployment tools, 224  
deploying GPOs, 131–135  
deploying scripts, 141–145  
deployment, scaling, 3–5  
deployment and restart, scheduling, 347  
Deployment Image Servicing and Management  
(DISM.exe). *See* DISM.exe  
deployment options, 248–250  
    customized target computer installations, 249  
    local installations, 249  
    reference computers, 249–250  
deployment scenarios, 250–252  
    new computer, 251  
    refresh computer, 252  
    replace computer, 252  
    upgrade computer, 251–252  
deployment share  
    adding images to, 270  
    building, 221–222  
    configuring for multicasting, 293  
    creating, 83, 267  
    creating (practice), 95–97  
    credentials, entering automatically, 295  
    populating, 83, 268  
    properties, modifying (practice), 294–295  
    replicating, 270  
    storage space for, 268  
    updating, 273–274  
Deployment Workbench, 270  
    image of, 3  
DES encryption support for Kerberos, 189

desktop composition, disabling, 374  
device drivers  
    adding to image files, 105  
    in system images, 89  
Device Manager, 474  
DHCP, troubleshooting, 438  
digital certificates, 443–444  
digital content for digital book readers, xx  
disabling services, 185  
Diskpart.exe, 77  
DISM.exe, 110–111, 230  
    committing images (practice), 111  
    disabling Windows 7 features (practice), 111  
    dismounting images (practice), 111  
    enabling Windows 7 features (practice), 111  
    installing device drivers to offline images  
        (practice), 110–111  
    mounting (practice), 110  
    operating system updates, installing, 106–107  
    overview of, 103  
distribution points  
    adding packages to, 409–410  
    creating, 310, 403–404  
    updating, 311  
DNS, troubleshooting, 439–440  
DNSLint.exe, 494  
drives, configuring removable policies, 187–188

## E

Encrypting File System, 178  
    configuring, 178  
    overview of, 173  
encryption, 173–178  
    configuring BitLocker, 173–176  
    configuring BitLocker To Go, 176–178  
    configuring Encrypting File System, 178  
    overview of, 173  
    troubleshooting, 480–482  
enforcing GPOs, 137, 458  
Enterprise edition, 53  
envisioning goals, 15

## F

Fabrikam software update policies  
(case scenario), 353

firewalls  
creating rules, 179–181  
troubleshooting, 441–443, 477  
turning off, 442

folder names for legacy applications, 370  
Folder Redirection, 157–159  
functional GPOs, 128  
functional specifications, 16

## G

Get Programs control panel, 395

goal envisioning, 15

governance, risk, and compliance (GRC).

*See Plan phase, GRC*

governance-risk-compliance (GRC) policies, 12

GPMC

downloading and installing (practice), 145–146  
GPO creation/management with, 121–123

GPO Accelerator, 151–153

GPOs

assigning multiple GPOs to one container, 134–135  
asynchronous vs. synchronous processing, 130  
blocked inheritance, checking, 456  
blocking inheritance, 136  
change frequency, 129  
computer configuration vs. user configuration,  
125–126, 455  
creating, 121–130  
creating (practice), 147–148, 414  
creating using GPMC, 121–125  
creating using Group Policy cmdlets, 125  
creating using starter GPOs, 126–128  
deploying, 131–135  
deploying (case scenario), 167  
enforcement, checking, 458  
enforcing, 137  
foreground vs. background processing, 129

Group Policy inheritance, 132–133  
Group Policy precedence, 133–134  
link speed, 129  
link status, checking, 454  
linking, 131–132  
linking to AD DS containers, 131–132  
monolithic vs. functional, 128  
object location, checking, 454  
performance issues, 129–130  
permissions, checking, 461  
policies and preferences, 126  
policy inheritance, checking, 455  
precedence, 456  
redundant, avoiding, 453  
security filtering, 137–139, 458  
selecting functional design strategies, 128–129  
starter, 126–127  
troubleshooting, 454–461  
updating, 455  
Gpresult.exe, 459–460  
HTML report (practice), 462  
running from command prompt (practice), 462  
graphics requirements  
for applications, 358  
for Windows 7, 52  
Group Policy  
Assign vs. Publish deployments, 396–397  
auditing policies, 155–157  
BranchCache setting, 478  
Compatibility View policies, 446–447  
configuration, 121–140  
configuring update-related, 345–347  
deploying applications with, 365, 393–402  
Folder Redirection, 155–157  
inheritance, blocking, 136  
Internet Explorer and, 199  
loopback processing, 461  
package creation with, 393–395  
package policies, setting, 400  
performance issues, 129–130  
Policies nodes, 126  
precedence, 133–134  
Preferences nodes, 126

Group Policy (*continued*)  
results, viewing, 459–460  
security zone settings, 448  
Software Installation extension, 395–396  
software installation policies, 397  
troubleshooting, 452–453  
turning off firewalls, 442  
Windows Error Reporting settings, 154–155

Group Policy cmdlets. *See GPOs, creating using Group Policy cmdlets*

Group Policy inheritance, 136–140  
blocking, 136–137  
enforcing GPOs, 137  
security filtering, 137–139  
WMI filtering, 140

Group Policy Management Console (GPMC).  
*See GPMC; GPOs, creating using GPMC*

Group Policy objects. *See GPOs*

grouping target computers, 290–291

groups, WSUS, 334–335

## H

hard disk requirements  
for Windows 7, 52

hard-link migration stores, 68

hardware ID, 44

hardware requirements  
for applications, 358  
compiling inventory for, 24–25, 26  
for practice exercises, xix  
for Windows 7, 52

head office activation (case scenario), 72

help desk interface, defining, 20

help with book, xxiii

hosts, virtualization, 55

hotfixes, installing to images, 106–107

hybrid images, 93

Hyper-V, 55

I

IEAK. *See Internet Explorer Administration Kit (IEAK)*

IEAK Profile Manager, 197

image creation design strategies, 77–99

image creation laboratory  
build server for, 87  
building, 86–88  
hardware requirements, 87  
infrastructure, 88  
infrastructure prerequisites, 88  
network, 87  
software requirements, 88

image modification tools, 103–109

Image.exe, capturing images using  
(case scenario), 114

images, system. *See system images*

ImageX.exe, 82, 103

importing target computers to database, 313–314

infrastructure  
configuring update testing, 336  
evaluating, 253–256

Lite-Touch Installation (LTI) vs. Zero-Touch  
Installation (ZTI), 254–255

SCCM 2007 requirements, 256

WDS requirements, 253–254

InPrivate  
browsing, 205–206  
filtering, 206–207

InPrivate Browsing, 205–206

InPrivate filtering, 206–207

installation ID, 44

installing Application Compatibility Test  
(practice), 384

installing applications manually, 364

installing practice tests, xxi

Install.wim file, 100

Internet Explorer  
add-ons, troubleshooting, 449  
add-ons and accelerators, 208–209  
browsing history, controlling, 205

cache settings, 202  
 Compatibility View, 444–446  
 Compatibility View configuration (practice), 449–450  
 configuration (case scenario), 217  
 configuring, 196–214  
 configuring security zones, 199–201  
 Group Policy and, 199  
 InPrivate browsing, 205–206  
 InPrivate filtering, 205–206  
 Internet Explorer Administration Kit (practice), 210–214  
 managing browsing history, 205  
 managing cache settings, 202  
 managing Windows add-ons using Group Policy (practice), 209  
 privacy settings, 203–207  
 proxy server connections, 207  
 security levels, 201  
 security zone configuration (practice), 450  
 security zone troubleshooting, 447–449  
 security zones, 199  
 Internet Explorer Administration Kit (IEAK), 196–198  
 Internet Explorer Compatibility Test Tool, 381  
 Internet Group Management Protocol (IGMP), 294  
 Internet security zone, 200  
 inventorying applications, 370–372  
 inventorying hardware, 24–25  
     manually, 26  
     with Microsoft Assessment And Planning Toolkit 4.0, 29–31  
     with SCCM 2007, 28  
     with System Information, 26–28  
 Ipconfig.exe, 471–473  
 IPSec protocol, 180  
 isolation rules, 180  
 IT Pro Quick Start Kit (practice), 39

## K

Kerberos  
 DES encryption support, 189  
 troubleshooting, 492–496

Kerbtray.exe, 495  
 Key Management Service (KMS), 48–49  
     activation limits, 49  
     activation threshold, 49  
     configuring hosts as servers for, 49  
 KMS. *See* Key Management Service (KMS)

## L

lab creation, 269  
 language packs, 90  
     installing to images, 106–107, 108  
 language settings for offline images, 108  
 legacy application considerations, 370  
 lesson review options, xxii  
 licenses  
     OEM, 43  
     planning and managing, 43–50  
     planning and managing client (practice), 73  
     retail keys, 43  
     virtualization and, 54  
     Volume License keys, 43  
     Windows 7, 43  
 link pulse indicators, 474  
 linking GPOs to AD DS containers, 131–132  
 Lite-Touch Installation (LTI)  
     build computer, 267  
     flexibility of, 266  
     multicasting, 292–294  
     planning, 267  
     reference computer, 268, 269  
     vs. Zero-Touch Installation (ZTI), 254–255  
 loadstate.exe, 67  
 Local Intranet security zone, 200  
 Local Security Policy Editor, 184  
 local update policy, setting (practice), 348–349  
 local user profiles, 159  
 localizing system images, 90  
 locking down services, 185  
 logon failures, troubleshooting, 488–496  
 logon/logoff scripts, 120  
 loopback processing, 461

# M

MAC addresses, displaying, 291–292  
MAK Independent Activation, 45  
MAK keys, 45–46  
MAK Proxy Activation, 46  
mandatory integrity control (MIC), legacy applications and, 370  
manual application deployment, 364  
manual update, verifying (practice), 340  
manually inventorying hardware, 26  
MAP Toolkit 5.0, 371  
MBSA  
    installing and using (practice), 340–341  
    verifying update deployments, 338–339  
MDT 2010, 221  
    build computer, creating, 83  
    creating images with, 82–86  
    deploying with, 235–245  
    deploying with (practice video), 320–321  
    downloading and installing, 268  
    downloading and installing (practice), 95  
    SQL databases and, 292  
MDT deployment  
    compared with MOF 3.0 and 4.0, 5  
    compared with MSF, 5  
    placing in the MOF life cycle, 10–22  
    Plan phase, 11–14  
memory requirements, 52  
    for applications, 358  
    for Windows 7, 52  
Microsoft Application Compatibility Toolkit, 377  
Microsoft Application Virtualization  
    application deployment with, 366  
    compatibility issues and, 377  
Microsoft Assessment And Planning (MAP)  
    Toolkit 4.0  
    hardware inventory with, 29–31  
    for installing and running, 2  
Microsoft Baseline Security Analyzer (MBSA).  
    See MBSA  
Microsoft Certified Professional Program, xxiii

Microsoft Deployment Toolkit 2010. *See MDT 2010*  
Microsoft Deployment Toolkit Files package, 306  
Microsoft deployment tools, 224  
Microsoft Knowledge Base, xx  
Microsoft Operations Framework (MOF).  
    *See MOF life cycle*  
Microsoft Press contact information, xxiv  
Microsoft System Center Configuration Manager.  
    *See SCCM (System Center Configuration Manager)*  
MigApp.xml, 66  
MigDocs.xml, 66–65  
migrating user profiles, 61–70  
    choosing a type, 64  
    estimating storage requirements, 68  
    offline, 66  
    side-by-side, 64  
    understanding reasons for, 62–64  
    upgrading when, 64  
    with Windows Easy Transfer, 63  
    wipe-and-load, 64  
migration store  
    compressed, 68  
    estimating size of, 68–69  
    selecting, 67–68  
    types of, 67–68  
    uncompressed, 68  
migration types, choosing, 64  
MigUser.xml, 65  
MOF 4.0  
    downloading free from Microsoft, 5  
    and the Microsoft Solutions Framework (MSF), 7  
MOF life cycle, 4–22  
    periodic management reviews, 9  
    phases, 5–6  
    version comparison, 5  
monolithic GPOs, 128  
mounting images, 104  
MSI packages, 364  
MSP files, deploying, 395  
multicasting deployments, 228, 292–294

## N

network bandwidth considerations, 270–271, 292–294  
 network connections  
     hardware, troubleshooting, 474  
     remote, troubleshooting, 482–483  
     routers, troubleshooting, 475–476  
     wired, troubleshooting, 470–478  
     wireless, troubleshooting, 479–482  
     WPA security, 480  
 Network Monitor, 31–33, 477  
 network requirements for applications, 358  
 network security settings, 189–190  
 NItest.exe, 492, 498  
 non-PXE clients and WDS, 228  
 NTLM authentication, 189

## O

OEM licenses, 43  
 offline image file modification, 102–103  
 offline migration, 66  
 Operate phase, 19–21  
     customer service, 20  
     management review, 20  
     monitoring and control, 20  
     operational health, 21  
     operations, 19–21  
     problem management, 20–21  
 operational health management review, 9, 21  
 organizing system images, 89

## P

package-based deployment, 364, 393–395  
 packages  
     adding to distribution points, 409–410  
     creating with SCCM, 405–409  
 passwords  
     history, enforcing, 181  
     minimum/maximum age, 181  
     setting, 283–284, 294–295

patch files, deploying, 395  
 performance baseline (practice), 39  
 Performance Monitor, 31–33  
 permissions, GPO, troubleshooting, 461  
 physical hardware virtualization strategy (practice), 73  
 Ping.exe  
     running (practice), 485  
     testing success and failure, 473  
 Plan phase  
     business/IT alignment, 13  
     GRC, 12  
     policy, 13  
     reliability, 13  
 Planning Guide, deprecation of, 4  
 policies  
     auditing, 155–157  
     configuring auditing, 162–165  
     configuring file and folder auditing (practice), 163–165  
     configuring removable drive, 187–188  
     configuring standard audit (practice), 162–163  
     configuring update-related, 345–347  
     configuring user rights and security, 183–184  
     defining account, 181–182  
     defining user account control, 182–183  
     designing, 13  
     Fabrikam software update (case scenario), 353  
     folder redirection, 157–159  
     setting local update (practice), 348–349  
 policy and control management review, 9, 20  
 populating deployment share, 83  
 portfolio management review, 9, 14  
 PowerShell, 141  
 practice  
     ACT, installing and configuring, 383–385  
     asset intelligence, gathering with SCCM 2007, 366–367  
     audit, configuring, 162–165  
     boot from VHD, preparing, 57–60  
     client security standards, implementing, 190–193  
     CustomSettings.ini file, customizing, 294–296  
     deployment share, creating, 94–97  
     DISM.exe, using, 110–111

**practice (continued)**

- GPO in Windows 7, creating, 145–148
  - Gpresult.exe, using, 462
  - Internet Explorer, configuring, 209–214
  - Internet Explorer Compatibility View settings, configuring, 449–450
  - Kerberos troubleshooting tools, using, 498
  - MAP toolkit, installing, 34–35
  - network troubleshooting tools, using, 485
  - packages, deploying with GPO, 414–415
  - RemoteApp, deploying applications with, 423–425
  - SCCM deployment scenarios, comparing, 320
  - size of migration store, estimating, 69–70
  - task sequences, creating, 258–259
  - update deployment, verifying, 339–341
  - update-related policies, configuring, 348–350
  - Windows SIM, using, 240–246
  - workstation build team, leading, 21–22
- practice exercises**
- hardware requirements, xix
  - software requirements, xx
- practice tests**
- installing, xxi
  - modes, xxii
  - uninstalling, xxiii
- privacy settings in Internet Explorer, 203–204, 207
- Problem Management service, 20–21
- processor requirements
- for applications, 358
  - for Windows 7, 52
- product activation for Windows 7, 44
- multiple activations, 45–46
  - online process, 44
  - overview of, 44
- product ID, 44
- Professional edition, 53
- profiles
- creating roaming, 160–162
  - designing user, 159–162
- Program Compatibility Troubleshooter, 375
- programs (SCCM), 403, 410–413
- project plan approved management review, 9, 16
- project planning, 15
- proxy server connections in Internet Explorer, 207
- Publish deployment, 396–397

**R**

- recreating system images, 102
- reference computer
- building, 269
  - capturing image, 223
  - performing installation, 81, 222
  - selecting, 268
- reference installation, 222
- Refresh Computer scenario, 268
- release readiness management review, 9, 18
- Remote Desktop Gateway, 483
- Remote Desktop Protocol (RDP), 417, 420–421
- Remote Desktop Services (RDS)
- application deployment with, 363, 365–366, 417
  - compatibility issues and, 377
  - deployment options, 418
  - troubleshooting, 482–483
- Remote Desktop Web Access (RD Web Access)
- connecting to (practice), 424–425
  - defining, 422–423
  - and full RDS desktop, 423
- RemoteApp, 418
- adding programs to (practice), 423–424
  - application deployment with, 419–420
  - configuring applications, 419
  - packaging applications, 420–423
- removable drive policies, configuring, 187–188
- Replace Computer scenario, 268, 273
- Request For Change (RFC), 14
- restart, scheduling. *See deployment and restart, scheduling*
- Restricted Sites security zone, 201
- Resultant Set of Policy (RSOP), 460.
- See also Gpresult.exe*
- retail keys, 43
- roaming profiles
- creating, 159
  - overview of, 160
- rolling back updates, 348
- routers, troubleshooting, 475–476

# S

scaling application deployment, 3–5, 362  
 scaling client deployment, 256–258  
 scanstate.exe  
   offline mode, 66  
   overview of, 66–67  
 SCCM (System Center Configuration Manager)  
   adding computers to database, 313–314  
   advertisement creation, 315–316  
   application deployment with, 365, 402–414  
   application inventory with, 370  
   client package installation, 307  
   collection creation, 314–315, 405  
   distribution points, creating, 403–404  
   hardware inventory with, 28  
   infrastructure prerequisites, 256, 298–299  
   integrating with MDT 2010, 299–300  
   overview of, 28  
   package creation with, 405–409  
   programs in, 403, 410–413  
   task sequence creation, 300–310.  
     *See also* task sequence  
   updating with, 339–341  
 Windows 7 deployment (practice video), 320  
 SCCM Asset Intelligence (video practice), 366–367  
 scheduled-cast multicasting, 294  
 screen resolution, configuring, 374  
 scripting languages  
   choosing, 140–141  
   deploying, 141–145  
   supporting, 141  
 scripts, 140–148  
   choosing languages, 140–141  
   deploying, 141–145  
   deploying logon in user objects, 141–142  
   deploying using Group Policy, 142–145  
   supporting languages, 141  
 sector-based image files, 76  
 security  
   add-ons and accelerators in Internet Explorer,  
 208–209  
   client, at Contoso (case scenario), 217

configuring BitLocker, 173–176  
 configuring BitLocker To Go, 176–178  
 configuring client, 172–193  
 configuring Encrypting File System, 178  
 configuring Internet Explorer, 196–214  
 configuring security zones for Internet Explorer,  
   199–201  
 defining AppLocker settings, 185–186  
 InPrivate browsing, 205–206  
 InPrivate filtering, 206–207  
 locking down services, 185  
 managing browsing history in Internet Explorer, 205  
 managing cache settings in Internet Explorer, 202  
 modifying network settings, 189–190  
 privacy settings in Internet Explorer, 203–207  
 proxy server connections, 207  
 user account control policies, 182–183  
   user rights and, 183–184  
 security filtering, 137–139  
 security protocol settings, troubleshooting, 480–482  
 security zones  
   configuring, 199  
   configuring (practice), 450  
   Group Policy configuration, 448  
   troubleshooting, 447–449  
 server-based application deployment, 363, 365–366  
 server-to-server rules, 181  
 service alignment management review, 9, 11  
 service management functions (SMFs)  
   for the MOF Manage Layer, 8  
   for the MOF Operate Phase, 8  
   overview of, 6–7  
   understanding the sequence, 10  
 Service Monitoring and Control, 20  
 service packs, installing to images, 106–107  
 services, locking down, 185  
 session 0 isolation, 370  
 Setup Analysis Tool, 383  
 shims, 376  
 side-by-side migration, 64  
 signal acquisition failure in wireless networks,  
   479–480  
 slmgr.vbs command, 44, 50

- software. *See* applications
- software distribution points, 398
- Software Installation extension for Group Policy, 395–396
  - setting policies, 400
- Software Installation policies
  - creating (practice), 414–415
- software licenses, 400
- software licensing management tool, 50
- software requirements
  - for practice exercises, xx
- SQL databases, 292
- stabilization process
  - planning (practice), 22
- stabilization team
  - assembling (practice), 21–22
- Stabilize stage of Deliver phase, 17–18
- Standard Client Task Sequence template, 272
- Standard User Analyzer, 382
- starter GPOs, 126–127
- startup/shutdown scripts, 120
- storage requirements for applications, 358
  - estimating, 68
- Study Mode practice tests, xxii
- subnet masks, troubleshooting, 472
- super-mandatory profiles
  - creating, 162
  - overview of, 159
- supplemental applications, 89
- support for book, xx
- synchronous processing, 130
- Sysprep.exe (System Preparation), 82, 230
- System Center Configuration Manager (SCCM) 2007.
  - See* SCCM (System Center Configuration Manager)
- system images
  - adding device drivers, 105–106
  - answer files, applying, 109
  - applying answer file settings, 109
  - applying operating system updates, 106–107
  - changing interface languages, 108–109
  - committing and unmounting, 109
  - configuring operating system features, 108
  - core and supplemental applications needed, 89
  - creating and managing, 75–115
- creating manually, 80
- creating with MDT 2010, 82–86
- creating with Windows 7 AIK, 80–82
- customizing, 100
- deploying to target computers, 269
- determining quantity needed, 88–90
- device drivers in, 89, 105
- hotfixes, installing, 106–107
- hybrid images, 93
- image modification tools, 103–109
- language configuration, 108
- language packs, installing, 106–107
- localizing, 90
- modification tools, 103
- modifying existing image files, 102–103
- modifying image deployment, 102
- mounting, 104
- number needed, 88
- offline modification, 102–103
- organizing, 89
- reasons to modify, 101
- recreating, 102
- service packs, installing, 106–107
- supplemental applications, 89
- testing, 110–111
- thick images, 90–91, 364
- thin images, 91–92
- types, 90–93
- unmounting, 109
- updating, 101–103
- versioning, 103

## System Information

- accessing, 26
- hardware inventory with, 26–28

## System Preparation (Sysprep.exe)

- 82, 230

## system settings design standard (practice)

- 168

## T

### target computer

- accessing image, 224
- adding to database, 313–314
- boot media, creating, 317–319

- boot methods, 274–275
- booting using Windows PE, 223–224
- collections, adding to, 314–315
- grouping, 290–291
- installing Windows, 224
- joining to workgroup, 280
- MAC addresses, 291–292
- migration type, selecting, 278
- password, setting, 283–284
- starting, 276–286
- target deployment, 271–273
- task sequence
  - creating, 84
  - creating from scratch, 273
  - creating to install Windows 7 and save user state data (practice), 259
  - creating to save user state data (practice), 258
  - customizing, 311–312
  - modifying settings, 272
  - selecting, 277
  - for target deployment, 271–273, 310
  - template for, 272
  - for Zero-Touch Installation deployment, 300–301
- TCP/IP, troubleshooting, 471–473
- Temporary Internet Files folder
  - size configuration, 202
- test workstations, application testing, 358
- testing system images, 110
- thick images, 90–91, 364
- thin-client vs. fat-client deployment models, 361–362
- Tracert.exe
  - overview of, 476
  - running (practice), 485
- transmission issues, troubleshooting, 479–480
- troubleshooting
  - authorization failures, 496–497
  - certificates, 443–444
  - DHCP, 438
  - DNS, 439–440
  - encryption, 480–482
  - firewalls, 441–443, 477
  - GPOs, 454–461
  - Group Policy, 452–453
  - Internet Explorer add-ons, 449
  - Internet Explorer compatibility issues, 444–446
  - Kerberos, 492–496
  - logon failures, 488–496
  - network hardware, 474
  - network problems, 437
  - Remote Desktop Services (RDS), 482–483
  - remote network connections, 482–483
  - routers, 475–476
  - security zones, 447–449
  - TCP/IP connections, 471–473
  - virtual private network (VPN) connections, 484–485
- Web site access, 436–444
- wired network connections, 470–478
- wireless network connections, 479–482
- workstation authentication, 490–491
- troubleshooting hierarchy, 434–436
- troubleshooting procedures
  - applying solution, 434
  - determining scope, 433
  - gathering information, 436–437
  - identifying symptoms, 432
  - isolating location, 434
  - political concerns, 433
  - reproducing problem, 437
  - testing results, 434
- Trusted Sites security zone, 201
- tunnel rules, 181
- 256 colors, configuring program for, 374

## U

- UAC policies, 182–183
- Ultimate edition, 53
- uncompressed migration stores, 68
- update classifications
  - important, 327
  - optional, 328
  - overview of, 327–328
  - recommended, 328
- update deployment, verifying, 336–339
- update management strategy, designing, 326–341
- update testing infrastructure, configuring, 336

- updates
- configuring testing infrastructure, 336
  - configuring update-related group policy, 345–347
  - deploying, 328–330
  - deploying to clients, 343–348
  - Fabrikam software policies (case scenario), 353
  - installing manually, 329–330
  - managing. *See* update management strategy, designing
  - managing Windows Update clients, 344
  - rolling back, 348
  - setting local policy (practice), 348–349
  - System Center Configuration Manager, 339–341
  - verifying deployment, 336–339
  - verifying manual (practice), 340
- updating GPOs, 455
- updating system images, 101
- upgrade information, gathering, 23–33
- upgrading operating systems, 64
- user account control policies, 182–183
- User Account Control (UAC)
  - legacy applications and, 369
  - policies, 182–183
- user interface languages, modifying (case scenario), 114–115
- user profile strategy, designing, 159–162
- user profiles
  - local, 159
  - migrating, 61–70
  - roaming, 159
  - super-mandatory, 159
  - viewing data, 62
- user rights and security policies, 183–184
- user state data
  - creating task sequence to install Windows 7 and restore user state data (practice), 259
  - creating task sequence to save (practice), 258
- user state migration strategies (practice), 73
- User State Migration Tool (USMT)
  - configuring settings, 65–66
  - estimating size of migration store (practice), 69–70
- loadstate.exe, 67
- migration store selection, 67–68
- overview of, 65
- package creation, 308
- scanstate.exe, 66–67
- storage requirements, 68–69
- users, migrating to virtual machines (case scenario), 72–73
- USMT. *See* User State Migration Tool (USMT)

**V**

- VAMT. *See* Volume Activation Management Tool (VAMT)
- VBScript, 140
- version control, for system images, 103
- VHD
  - booting from, 55–57
  - converting to WIM, 56
  - creating files, 56
  - installing VHD boot, 57–60
  - native boot limitations, 57
  - preparing for VHD boot, 57–60
- virtual hard disk file. *See* VHD
- virtual machines
  - compatibility issues and, 377
  - migrating users to (case scenario), 72–73
- Virtual PC 2007, 55
- virtual private network (VPN) connections, troubleshooting, 484–485
- Virtual Server 2005, 55
- virtualization
  - compatibility issues and, 377
  - hosts, 55
  - planning and managing physical hardware strategy (practice), 73
- Windows 7, 54
- Windows 7 editions, 54
- virtualization hosts, 55
- visual themes, configuring, 374
- Volume Activation Management Tool (VAMT), 46–48

Volume License keys, 43  
 volume licensing  
   activation methods, 45–49  
   Key Management Service (KMS), 48–49  
   MAK keys, 45–46  
   multiple activation keys, 45–46  
   Volume Activation Management Tool (VAMT),  
     46–48

## W

WAIK (Windows Automated Installation Kit)  
   downloading, 42  
 Watson Feedback Platform (WFP).  
   *See* Windows Error Reporting (WER)  
 WDS  
   capturing image (case scenario), 262  
   capturing images with, 228  
   communications, 225  
   configuring server, 226–227  
   deploying images using multicasts, 228  
   for image creation laboratory, 88  
   infrastructure requirements, 253–254  
   and non-PXE clients, 228  
   providing complete deployment solution, 227–228  
 Web browsers, compatibility troubleshooting,  
   444–446  
 Web site compatibility, 381  
 WER. *See* Windows Error Reporting (WER)  
 WER (Windows Error Reporting), 153–155  
 WIM. *See* Windows Imaging Files (WIM)  
 .wim files. *See* Windows Imaging Files (WIM)  
 WIM to VHD conversion, 56  
 Windows 7  
   Automated Installation Kit (AIK). *See* Windows 7 AIK  
   deployment basics, 221–224  
   deployment life cycle, 3–23  
   editions and licenses, 43  
   editions of, 53  
   hardware requirements, 52  
   preparing to deploy, 1–40  
   product activation, 44

virtualization, 54  
 volume licensing activation, 45–49  
 x86 version vs. x64 version, 53  
 Windows 7 AIK  
   creating images with, 80–82  
   deploying with, 230–235  
   downloading and installing (practice), 94  
 Windows 7 deployment  
   making decisions (case scenario), 38  
   overview of, 221  
   preparing for (case scenario), 38  
 Windows 7 Enterprise, overview of, 53  
 Windows 7 Professional, overview of, 53  
 Windows 7 Ultimate, overview of, 53  
 Windows 7 virtualization, 54  
 Windows Automated Installation Kit, 69–70  
   downloading, 42  
 Windows CE, booting target computer, 223–224  
 Windows Deployment Services (WDS). *See* WDS  
 Windows Deployment Wizard  
   suppressing pages, 289–290  
   suppressing pages (practice), 295–296  
 Windows Easy Transfer, 63  
 Windows Error Reporting (WER), 153–155  
 Windows Firewall with Advanced Security,  
   configuring, 179–180  
 Windows Imaging Files (WIM), 77–79.  
   *See also* system images  
   advantages of, 77–79  
   Automated Installation Kit (AIK), 80–82  
   creating, 79–86  
   creating manually, 80  
   creating with MDT 2010, 82–86  
   creating with Windows 7 AIK, 80–82  
   manual creation, 80  
   MDT 2010, 82–86  
   workstation considerations, 79–80  
 Windows Installer, 395  
 Windows Installer package files, 394.  
   *See also* package-based deployment  
   packaging RemoteApp applications with, 422  
 Windows Internet Explorer. *See* Internet Explorer

## **Windows Management Instrumentation (WMI)**

Windows Management Instrumentation (WMI).

*See also* Group Policy inheritance, WMI filtering  
filtering with, 140

Windows PE

boot disk, creating, 82  
booting a target computer with, 223–224  
defined, 221  
in Windows 7 AIK, 230

Windows Preinstallation Environment (Windows PE).

*See* Windows PE

Windows Product Activation

multiple activations, 45–46  
online process, 44  
overview of, 44

Windows Server Update Services (WSUS). *See* WSUS

Windows SIM

creating a distribution share (practice), 240–241  
partitioning a disk with an answer file (practice),  
242–246  
practice, 240–246

in Windows 7 AIK, 230

Windows System Image Manager (Windows SIM).

*See* Windows SIM

Windows Time service, 491

Windows Update clients, 344

Windows Update Stand-alone installer, 330

Windows Virtual PC, 55

Windows XP Mode, 377

wipe-and-load migration, 64

WMI filtering, 140

workgroup, joining computer to, 280

workstation hardware inventory

compiling, 24–30

manual method of compiling, 26

Microsoft Assessment And Planning Toolkit 4.0

method of compiling, 29–30

Microsoft System Center Configuration Manager

(SCCM) method of compiling, 28, 359

system information method of compiling, 26–28

workstation performance benchmarks, 31–33, 35

workstations

configuration management, 357

number required for client deployment, 256–257

refreshing (case scenario), 224–263

requirements for, 119–120

synchronous processing, 130

troubleshooting authentication, 490–491

WPA security, 480

WSUS, 325, 330–335

and BranchCache, 333

Contoso upgrade (case scenario), 353

deployment types, 332

groups, 334–335

overview of, 325

servers used as update locations, 331–332

topologies, 332

WSUS reports, 337

## **Z**

Zero-Touch Installation (ZTI). *See also* SCCM (System

Center Configuration Manager)

distribution points, 310–311

infrastructure prerequisites, 298–299

vs. Lite-Touch Installation, 254–255

task sequence creation, 300–310

# About the Authors

**Craig Zacker** is a writer, editor, and educator whose computing experience began in the days of teletypes and paper tape. After moving from minicomputers to PCs, he worked as a network administrator and desktop support technician while operating a freelance desktop publishing business. After earning a Masters Degree in English and American Literature from New York University, Craig supported fleets of Windows workstations and was employed as a technical writer, content provider, and Webmaster for the online services group of a large software company. Craig is the author of *Windows Small Business Server 2008 Administrator's Pocket Consultant* (Microsoft Press, 2009) and the Microsoft Official Academic Curriculum textbook and lab manual for 70-680: *Windows 7 Configuring*. He has also authored and contributed to dozens of other books on operating systems, networking topics, and PC hardware. He has developed educational texts for college courses, written online training courses for the Web, and published articles in top industry publications.

**Orin Thomas**, MCSE, MCTS, MCITP, MCT, MVP is an author, trainer, and regular public speaker who has authored more than a dozen books for Microsoft Press. He has professionally supported, configured, and deployed Windows Client operating systems since Windows for Workgroups 3.11. He holds several MCITP-level credentials, including the MCITP: Enterprise Desktop Administrator 7 certification.





# Practice. Practice. Practice. Pass.

## Get more practice with MeasureUp® & ace the exam!

You've practiced — but have you practiced enough? The disk included with this book has dozens of quality questions from the publisher to get you started. MeasureUp offers additional practice tests with more than **100 new and different questions** at [MeasureUp.com](http://MeasureUp.com). And when you use our practice test you'll pass — **guaranteed**.

- **Performance-based simulation questions** — similar to the ones found on Microsoft exams, and are available online, via download, or on CD
- **Study Mode** helps you review the material and identify areas where you need more study
- **Certification Mode** simulates the timed test environment

**Get certified today! Purchase your complete practice test at [www.measureup.com](http://www.measureup.com).**

For tips on installing the CD software located in this Training Kit, visit the FAQ section at [MeasureUp.com](http://MeasureUp.com). For questions about the content, or the physical condition of the CD, visit [microsoft.com/learning/en/us/training/format-books-support.aspx](http://microsoft.com/learning/en/us/training/format-books-support.aspx).

### Microsoft Press Users Save 20% on MeasureUp Practice Tests!

Prepare for your MCSE, MCSA, MCITP and many more exams with MeasureUp Practice Tests and you'll be ready to pass. **We guarantee it.**

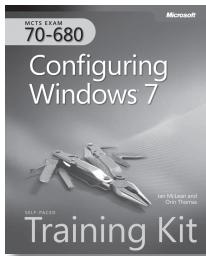
Save 20% on MeasureUp Practice Tests when you use this coupon code at checkout on [www.measureup.com](http://www.measureup.com).

Coupon Code: MSP020113



# Get Certified—Windows® 7

Desktop support technicians and administrators—demonstrate your expertise with Windows 7 by earning a Microsoft® Certification focusing on core technical (MCTS) or professional (MCITP) skills. With our 2-in-1 *Self-Paced Training Kits*, you get a comprehensive, cost-effective way to prepare for the certification exams. Combining official exam-prep guides + practice tests, these kits are designed to maximize the impact of your study time.



## EXAM 70-680

### MCTS Self-Paced Training Kit: Configuring Windows 7

Ian McLean and Orin Thomas  
ISBN 9780735627086



## EXAM 70-685

### MCITP Self-Paced Training Kit: Windows 7 Enterprise Desktop Support Technician

Tony Northrup and J.C. Mackin  
ISBN 9780735627093



## EXAM 70-686

### MCITP Self-Paced Training Kit: Windows 7 Desktop Administrator

Craig Zacker and Orin Thomas  
ISBN 9780735627178

## GREAT FOR ON THE JOB



**Windows 7  
Resource Kit**  
Mitch Tulloch,  
Tony Northrup,  
Jerry Honeycutt,  
Ed Wilson, and the  
Windows 7 Team  
at Microsoft  
ISBN 9780735627000



**Windows 7  
Inside Out**  
Ed Bott, Carl Siechert,  
Craig Stinson  
ISBN 9780735626652



**Windows 7  
Administrator's  
Pocket Consultant**  
William R. Stanek  
ISBN 9780735626997

# Windows Server 2008— Resources for Administrators



**Windows Server® 2008  
Administrator's Companion**  
Charlie Russel and Sharon  
Crawford  
ISBN 9780735625051

Your comprehensive, one-volume guide to deployment, administration, and support. Delve into core system capabilities and administration topics, including Active Directory®, security issues, disaster planning/recovery, interoperability, IIS 7.0, virtualization, clustering, and performance tuning.



**Windows Server 2008  
Resource Kit**  
Microsoft MVPs with Microsoft  
Windows Server Team  
ISBN 9780735623613

Six volumes! Your definitive resource for deployment and operations—from the experts who know the technology best. Get in-depth technical information on Active Directory, Windows PowerShell® scripting, advanced administration, networking and network access protection, security administration, IIS, and more—plus an essential toolkit of resources on CD.



**Windows PowerShell 2.0  
Administrator's  
Pocket Consultant**  
William R. Stanek  
ISBN 9780735625952

The practical, portable guide to using cmdlets and scripts to automate everyday system administration—including configuring server roles, services, features, and security settings; managing TCP/IP networking; monitoring and tuning performance; and other essential tasks.



**Windows Server 2008  
Administrator's  
Pocket Consultant,  
Second Edition**  
William R. Stanek  
ISBN 9780735627116

Portable and precise—with the focused information you need for administering server roles, Active Directory, user/group accounts, rights and permissions, file-system management, TCP/IP, DHCP, DNS, printers, network performance, backup, and restoration.



**Internet Information  
Services (IIS) 7.0  
Administrator's  
Pocket Consultant**  
William R. Stanek  
ISBN 9780735623644

This pocket-sized guide delivers immediate answers for administering IIS 7.0. Topics include customizing installation; configuration and XML schema; application management; user access and security; Web sites, directories, and content; and performance, backup, and recovery.

## ALSO SEE

**Windows  
PowerShell 2.0  
Best Practices**  
ISBN 9780735626461

**Windows Server 2008  
Hyper-V™  
Resource Kit**  
ISBN 9780735625174

**Windows® Administration  
Resource Kit:  
Productivity Solutions  
for IT Professionals**  
ISBN 9780735624313

**Windows Server 2008  
Security Resource Kit**  
ISBN 9780735625044

# System Requirements

We recommend that you use a test workstation, test server, or staging server to complete the practice exercises in each lesson. However, it would be beneficial for you to have access to production-ready data in your organization. If you need to set up a workstation to complete the practices, the minimum system requirements follow:

- Personal computer with at least a 1-GHz 32-bit (x86) or 64-bit (x64) processor
- At least 1 GB of RAM (x86 systems) or 2 GB of RAM (x64 systems)
- At least a 40-GB hard disk
- DVD-ROM drive
- Super VGA (800 × 600) or higher resolution video adapter and monitor
- Keyboard and Microsoft mouse or compatible pointing device

For some chapters, your workstation must have access to an Active Directory Domain Services network. Chapter 10, "Using Application Deployment Tools," requires access to a computer running Windows Server 2008 R2.

To use the companion CD, you need a computer running Windows 7, Windows Vista, or Windows XP. The computer must meet the following minimum requirements:

- 1 GHz 32-bit (x86) or 64-bit (x64) processor (depending on the minimum requirements of the operating system)
- 1 GB of system memory (depending on the minimum requirements of the operating system)
- A hard-disk partition with at least 700 MB of available space
- A monitor capable of at least 800 × 600 display resolution
- A keyboard
- A mouse or other pointing device
- An optical drive capable of reading CDs

The computer must also have the following software:

- A Web browser, such as Windows Internet Explorer
- An application that can display PDF files, such as Adobe Reader, which can be downloaded at <http://www.adobe.com/reader>

These requirements support your use of the companion CD. To perform the practice exercises in this training kit, you might require additional hardware or software. See the Introduction to the book for detailed hardware requirements.

# What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

[microsoft.com/learning/booksurvey](http://microsoft.com/learning/booksurvey)

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

**Microsoft®**  
Press

## Stay in touch!

To subscribe to the *Microsoft Press® Book Connection Newsletter*—for news on upcoming books, events, and special offers—please visit:

[microsoft.com/learning/books/newsletter](http://microsoft.com/learning/books/newsletter)