

Microsoft®

MCTS EXAM

70-680

# Configuring Windows® 7



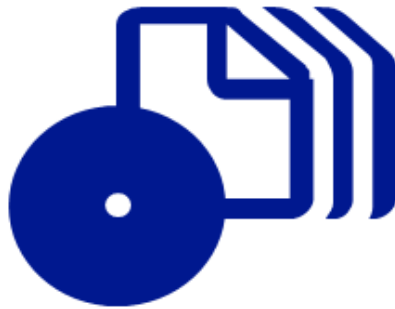
Ian McLean and  
Orin Thomas

SELF-PACED

# Training Kit



# How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to <http://aka.ms/627086/files>, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: [mspinput@microsoft.com](mailto:mspinput@microsoft.com)

Microsoft Press





# MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows® 7

Ian McLean  
Orin Thomas



**PUBLISHED BY**

Microsoft Press

A Division of Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052-6399

Copyright © 2010 by Ian McLean 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: 2009932326

ISBN: 978-0-7356-2708-6

Printed and bound in the United States of America.

13 14 15 16 17 18 19 20 21 QG 8 7 6 5 4 3

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

Microsoft, Microsoft Press, Access, Active Directory, ActiveX, Aero, BitLocker, DirectX, Excel, Hyper-V, Internet Explorer, MS, MS-DOS, Natural, Outlook, PowerPoint, ReadyBoost, SQL Server, Visual Basic, Win32, Windows, Windows Live, Windows Media, Windows Mobile, Windows NT, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

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:** Ken Jones

**Developmental Editor:** Laura Sackerman

**Project Editor:** Rosemary Caperton

**Editorial Production:** Ashley Schneider, S4Carlisle Publishing Services

**Technical Reviewer:** Rozanne Whalen; Technical Review services provided by Content Master, a member of CM Group, Ltd.

**Cover:** Tom Draper Design

Body Part No. X16-10711

*It's unusual to dedicate a book to one of its authors, but when Orin Thomas agreed to be my writing partner it was my lucky day. Orin is the most competent and capable professional I have ever come across. Not only can he do things, he can write about them too. He's my peer reviewer as well as my co-author and his reviews are both informative and ruthless, for which I'm eternally grateful. He is always ready and willing to step in with assistance if I am having any sort of problem. Orin, please keep tearing my text to shreds. By the way I'll do the same for you given the opportunity. I appreciate working with a true professional.*

—IAN McLEAN

*To all of you who are beginning your certification journey, I hope that you find your journey as rewarding, as useful, and as fulfilling as I have found my own. Good luck on your Windows 7 exam!*

—ORIN THOMAS





# Contents at a Glance

	<i>Introduction</i>	<i>xxiii</i>
<b>CHAPTER 1</b>	<b>Install, Migrate, or Upgrade to Windows 7</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Configuring System Images</b>	<b>53</b>
<b>CHAPTER 3</b>	<b>Deploying System Images</b>	<b>113</b>
<b>CHAPTER 4</b>	<b>Managing Devices and Disks</b>	<b>195</b>
<b>CHAPTER 5</b>	<b>Managing Applications</b>	<b>255</b>
<b>CHAPTER 6</b>	<b>Network Settings</b>	<b>297</b>
<b>CHAPTER 7</b>	<b>Windows Firewall and Remote Management</b>	<b>381</b>
<b>CHAPTER 8</b>	<b>BranchCache and Resource Sharing</b>	<b>421</b>
<b>CHAPTER 9</b>	<b>Authentication and Account Control</b>	<b>477</b>
<b>CHAPTER 10</b>	<b>DirectAccess and VPN Connections</b>	<b>513</b>
<b>CHAPTER 11</b>	<b>BitLocker and Mobility Options</b>	<b>553</b>
<b>CHAPTER 12</b>	<b>Windows Update and Windows Internet Explorer</b>	<b>599</b>
<b>CHAPTER 13</b>	<b>Monitoring and Performance</b>	<b>647</b>
<b>CHAPTER 14</b>	<b>Recovery and Backup</b>	<b>729</b>
	<i>Answers</i>	<i>783</i>
	<i>Glossary</i>	<i>843</i>
	<i>Index</i>	<i>847</i>





# Contents

<b>Introduction</b>	<b>xxiii</b>
Lab Setup Instructions . . . . .	xxiv
Hardware Requirements	xxiv
Using the DVD . . . . .	xxv
How to Install the Practice Tests	xxv
How to Use the Practice Tests	xxvi
How to Uninstall the Practice Tests	xxvii
Microsoft Certified Professional Program . . . . .	xxvii
Technical Support . . . . .	xxvii

<b>Chapter 1 Install, Migrate, or Upgrade to Windows 7</b>	<b>1</b>
Before You Begin . . . . .	2
Lesson 1: Installing Windows 7 . . . . .	3
Windows 7 Editions	3
Windows 7 Hardware Requirements	5
Preparing the Windows 7 Installation Source	6
Installing Windows 7	9
Lesson Summary	22
Lesson Review	23
Lesson 2: Upgrading to Windows 7 . . . . .	25
Upgrading from Windows 7 Editions	25
Upgrading from Windows Vista	26
Migrating from Windows XP	29
Lesson Summary	32
Lesson Review	32

**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/)



Lesson 3: Managing User Profiles . . . . .	34
Migrating User Profile Data . . . . .	34
Windows Easy Transfer . . . . .	35
User State Migration Tool . . . . .	39
Lesson Summary . . . . .	46
Lesson Review . . . . .	46
Chapter Review . . . . .	48
Chapter Summary . . . . .	48
Key Terms . . . . .	48
Case Scenarios . . . . .	49
Case Scenario 1: Installing Windows 7 at Contoso . . . . .	49
Case Scenario 2: Migrating User Data at Fabrikam . . . . .	49
Suggested Practices . . . . .	50
Perform a Clean Installation . . . . .	50
Upgrade to Windows 7 from a Previous Version of Windows . . . . .	50
Migrate User Profiles . . . . .	50
Take a Practice Test . . . . .	51

## **Chapter 2 Configuring System Images 53**

Before You Begin . . . . .	54
Lesson 1: Capturing System Images . . . . .	56
Installing and Using the Windows Automated Installation Toolkit . . . . .	56
Using the Windows Preinstallation Environment . . . . .	58
Creating a Reference Image . . . . .	58
Distributing an Image to Many Computers . . . . .	72
Using the Deployment Image Servicing and Management Tool . . . . .	75
Using Sysprep to Prepare a Windows 7 Installation . . . . .	77
Lesson Summary . . . . .	86
Lesson Review . . . . .	87
Lesson 2: Managing Virtual Hard Disk Files . . . . .	89
Using Native VHDs in Windows 7 . . . . .	89
Using the Windows Image to Virtual Hard Disk Tool . . . . .	94

Using the Offline Virtual Machine Servicing Tool to Update a VHD	96
Deploying to an Online VHD Using Windows Deployment Services	98
Lesson Review	108
Chapter Review	110
Chapter Summary	110
Key Terms	110
Case Scenarios	111
Case Scenario 1: Generating a System Image	111
Case Scenario 2: Working with VHDs	111
Suggested Practices	111
Use Windows SIM and Sysprep	112
Work with VHDs	112
Take a Practice Test	112
<b>Chapter 3 Deploying System Images</b>	<b>113</b>
Before You Begin	114
Lesson 1: Managing a System Image Before Deployment	116
Using DISM WIM Commands and Mounting an Image	116
Servicing Drivers, Applications, Patches, Packages, and Features	123
Servicing Windows PE Images	135
Unattended Servicing Command-Line Options	137
Lesson Summary	143
Lesson Review	144
Lesson 2: Deploying Images	146
Using the Microsoft Deployment Toolkit	146
Managing and Distributing Images with MDT 2010	151
Deploying Images with WDS	169
Using SCCM 2007	175
Installing an Image Manually	180

Lesson Summary	187
Lesson Review	188
Chapter Review . . . . .	190
Chapter Summary . . . . .	190
Key Terms . . . . .	190
Case Scenarios . . . . .	191
Case Scenario 1: Deploying an Image with More Than One Language Pack	191
Case Scenario 2: Deploying an Image to 100 Client Computers	191
Suggested Practices . . . . .	192
Manage and Manipulate a System Image	192
Become Familiar with the Deployment Tools	192
Take a Practice Test . . . . .	193
<b>Chapter 4 Managing Devices and Disks</b>	<b>195</b>
Before You Begin . . . . .	196
Lesson 1: Managing Device Drivers and Devices . . . . .	197
Using Device Manager to View Device Information	197
Installing Devices and Managing Device Drivers	203
Lesson Summary	226
Lesson Review	226
Lesson 2: Managing Disks . . . . .	228
Disk Maintenance	228
Changing Disk Type and Partition Style	235
Managing Disk Volumes	240
Lesson Summary	248
Lesson Review	249
Chapter Review . . . . .	251
Chapter Summary . . . . .	251
Key Terms . . . . .	251
Case Scenarios . . . . .	252
Case Scenario 1: Enforcing a Driver Signing Policy	252
Case Scenario 2: Managing Disks	252

Suggested Practices . . . . .	253
Investigate the Group Policies Available for Managing Device Installation . . . . .	253
Use the Driver Verifier Monitor Tool . . . . .	253
Use Diskpart . . . . .	253
Take a Practice Test. . . . .	253

**Chapter 5 Managing Applications 255**

Before You Begin. . . . .	256
Lesson 1: Application Compatibility . . . . .	257
Configuring Compatibility Options . . . . .	257
The Application Compatibility Toolkit . . . . .	260
Application Compatibility Diagnostics Policies . . . . .	264
Windows XP Mode for Windows 7 . . . . .	265
Lesson Summary . . . . .	269
Lesson Review . . . . .	269
Lesson 2: Managing AppLocker and Software Restriction Policies. . . . .	271
Software Restriction Policies . . . . .	271
AppLocker Application Control Policies . . . . .	276
Lesson Summary . . . . .	290
Lesson Review . . . . .	290
Chapter Review . . . . .	293
Chapter Summary. . . . .	293
Key Terms . . . . .	293
Case Scenarios. . . . .	294
Case Scenario 1: Configuring Application Compatibility at Fabrikam . . . . .	294
Case Scenario 2: Restricting Applications at Contoso . . . . .	294
Suggested Practices . . . . .	295
Configure Application Compatibility . . . . .	295
Configure Application Restrictions . . . . .	295
Take a Practice Test. . . . .	296

<b>Chapter 6 Network Settings</b>	<b>297</b>
Before You Begin . . . . .	298
Lesson 1: Configuring IPv4 . . . . .	300
Introduction to IPv4 Addressing	301
Connecting to a Network	307
Troubleshooting Network Connectivity	311
Lesson Summary	325
Lesson Review	326
Lesson 2: Configuring IPv6 . . . . .	328
Analyzing the IPv6 Address Structure	328
The Advantages of IPv6	333
Implementing IPv4-to-IPv6 Compatibility	334
Configuring IPv6 Connectivity	338
Lesson Summary	345
Lesson Review	346
Lesson 3: Network Configuration . . . . .	348
Connecting to a Network	348
Managing Network Connections	362
Troubleshooting Wireless Networks	363
Configuring Wireless Network Security	367
Windows 7 Printing Enhancements	368
Lesson Summary	373
Lesson Review	373
Chapter Review . . . . .	376
Chapter Summary . . . . .	376
Key Terms . . . . .	376
Case Scenarios . . . . .	377
Case Scenario 1: Implementing IPv4 Connectivity	377
Case Scenario 2: Implementing IPv6 Connectivity	377
Case Scenario 3: Using Laptop Computers Running Windows 7 on Wireless Networks	377
Suggested Practices . . . . .	378
Configure IPv4	378

Configure IPv6	378
Configure Networks	379
Take a Practice Test. . . . .	379
<b>Chapter 7 Windows Firewall and Remote Management</b>	<b>381</b>
Before You Begin. . . . .	382
Lesson 1: Managing Windows Firewall . . . . .	383
Windows Firewall	383
Windows Firewall with Advanced Security	389
Lesson Summary	399
Lesson Review	400
Lesson 2: Windows 7 Remote Management . . . . .	402
Remote Desktop	402
Remote Assistance	405
Windows Remote Management Service	408
Lesson Summary	415
Lesson Review	415
Chapter Review . . . . .	418
Chapter Summary. . . . .	418
Key Terms. . . . .	418
Case Scenarios. . . . .	418
Case Scenario 1: University Client Firewalls	419
Case Scenario 2: Antarctic Desktop Support	419
Suggested Practices . . . . .	419
Configure Windows Firewall	420
Configure Remote Management	420
Take a Practice Test. . . . .	420
<b>Chapter 8 BranchCache and Resource Sharing</b>	<b>421</b>
Before You Begin. . . . .	422
Lesson 1: Sharing Resources . . . . .	423
Network And Sharing Center	423
HomeGroups	425

Shared Folders	428
Libraries	432
Sharing Printers	434
Lesson Summary	440
Lesson Review	440
Lesson 2: Folder and File Access . . . . .	442
File and Folder Permissions	442
Configuring Auditing	449
Encrypting File System	451
Lesson Summary	459
Lesson Review	459
Lesson 3: Managing BranchCache . . . . .	461
BranchCache Concepts	461
Hosted Cache Mode	462
Distributed Cache Mode	463
Configuring BranchCache Clients Running Windows 7	463
Configuring File and Web Servers Running Windows Server 2008 R2	468
Lesson Summary	471
Lesson Review	471
Chapter Review . . . . .	473
Chapter Summary . . . . .	473
Key Terms . . . . .	473
Case Scenarios . . . . .	473
Case Scenario 1: Permissions and Encryption	474
Case Scenario 2: Configuring Contoso Branch Offices	474
Suggested Practices . . . . .	474
Configure Shared Resources	474
Configure File and Folder Access	475
Configure BranchCache	475
Take a Practice Test . . . . .	475
<b>Chapter 9 Authentication and Account Control</b>	<b>477</b>
Before You Begin . . . . .	478



Lesson 1: Managing User Account Control . . . . .	479
User Account Control (UAC)	479
UAC Settings	480
User Account Control Policies	482
Secpol and Local Security Policy	487
Lesson Summary	490
Lesson Review	491
Lesson 2: Windows 7 Authentication and Authorization . . . . .	493
Credential Manager	493
Using Runas to Run Programs as Another User	495
Configuring User Rights	496
Smart Cards	497
Account Policies	499
Resolving Authentication Issues	500
Managing Certificates	502
Lesson Summary	507
Lesson Review	508
Chapter Review . . . . .	510
Chapter Summary . . . . .	510
Key Terms . . . . .	510
Case Scenarios . . . . .	511
Case Scenario 1: User Account Control at Coho Vineyard	511
Case Scenario 2: Resolving Password Problems at Wingtip Toys	511
Suggested Practices . . . . .	512
Configure User Account Control (UAC)	512
Configure Authentication and Authorization	512
Take a Practice Test . . . . .	512

**Chapter 10 DirectAccess and VPN Connections 513**

Before You Begin . . . . .	514
Lesson 1: Managing DirectAccess . . . . .	515
Understanding DirectAccess	515
The DirectAccess Process	516

DirectAccess Client Configuration	517
Configuring the DirectAccess server	521
Lesson Summary	527
Lesson Review	527
Lesson 2: Remote Connections . . . . .	530
Virtual Private Networks	530
VPN Authentication Protocols	533
VPN Reconnect	535
NAP Remediation	536
Remote Desktop and Application Publishing	537
Dialup Connections	540
Configuring Windows 7 to Accept Incoming Connections	541
Auditing Remote Connections	544
Lesson Summary	547
Lesson Review	548
Chapter Review . . . . .	550
Chapter Summary . . . . .	550
Key Terms . . . . .	550
Case Scenarios . . . . .	550
Case Scenario 1: Wingtip Toys DirectAccess	551
Case Scenario 2: Remote Access at Tailspin Toys	551
Suggested Practices . . . . .	551
Configure DirectAccess	552
Configure Remote Connections	552
Take a Practice Test . . . . .	552

## **Chapter 11 BitLocker and Mobility Options 553**

Before You Begin . . . . .	554
Lesson 1: Managing BitLocker . . . . .	555
BitLocker	555
BitLocker To Go	564
Lesson Summary	571
Lesson Review	572

Lesson 2: Windows 7 Mobility . . . . .	574
Offline Files . . . . .	574
Windows 7 Power Configuration . . . . .	582
Lesson Summary . . . . .	592
Lesson Review . . . . .	593
Chapter Review . . . . .	595
Chapter Summary . . . . .	595
Key Terms . . . . .	595
Case Scenarios . . . . .	596
Case Scenario 1: Accessing Offline Files at Contoso . . . . .	596
Case Scenario 2: Using BitLocker at Tailspin Toys . . . . .	596
Suggested Practices . . . . .	597
Configure BitLocker and BitLocker To Go . . . . .	597
Configure Mobility Options . . . . .	597
Take a Practice Test . . . . .	598

## **Chapter 12 Windows Update and Windows Internet Explorer 599**

Before You Begin . . . . .	600
Lesson 1: Updating Windows 7 . . . . .	601
Configuring Windows Update . . . . .	601
Action Center . . . . .	609
Understanding Windows Server Update Services . . . . .	610
Windows Update Policies . . . . .	612
Microsoft Baseline Security Analyzer . . . . .	616
Lesson Summary . . . . .	619
Lesson Review . . . . .	620
Lesson 2: Configuring Internet Explorer . . . . .	622
Internet Explorer Compatibility View . . . . .	622
Configuring Security Settings . . . . .	623
SmartScreen Filter . . . . .	626
Managing InPrivate Mode . . . . .	627
Add-Ons and Search Providers . . . . .	630
Pop-Up Blocker . . . . .	632
Configuring SSL Certificates . . . . .	633

Lesson Summary	640
Lesson Review	641
Chapter Review .....	643
Chapter Summary .....	643
Key Terms .....	643
Case Scenarios .....	643
Case Scenario 1: Windows Update at Contoso	644
Case Scenario 2: Internet Explorer at Wingtip Toys	644
Suggested Practices .....	645
Configure Updates to Windows 7	645
Configure Internet Explorer	645
Take a Practice Test .....	646
<b>Chapter 13 Monitoring and Performance</b>	<b>647</b>
Before You Begin .....	648
Lesson 1: Monitoring Systems .....	649
Performance Monitoring and Reporting	649
Tracking System Reliability, Stability, and Overall Performance	658
Using the Action Center	661
Using System Tools to Investigate Processes and Services	664
Logging and Forwarding Events and Event Subscriptions	673
Lesson Summary	686
Lesson Review	686
Lesson 2: Configuring Performance Settings .....	689
Obtaining System Information Using WMI	689
Using the System Configuration Tool	705
Using the Services Console	707
Configuring Performance Options	709
Configuring Hard Disk Write Caching	711
Troubleshooting Performance Problems with Event Viewer	712
Using Task Manager to Configure Processes	714
Configuring Networking Performance	715
Windows Performance Analysis Tools	717

Lesson Summary	721
Lesson Review	722
Chapter Review . . . . .	724
Chapter Summary . . . . .	724
Key Terms . . . . .	724
Case Scenarios . . . . .	725
Case Scenario 1: Using Data Collector Sets and Event Forwarding	725
Case Scenario 2: Troubleshooting Performance Issues on a Client Computer	725
Suggested Practices . . . . .	726
Use the Performance Monitoring Tools	726
Manage Event Logging	726
Write WMI Scripts	726
Take a Practice Test . . . . .	727

**Chapter 14 Recovery and Backup** **729**

Before You Begin . . . . .	730
Lesson 1: Backup . . . . .	731
Scheduling Backups with the Backup And Restore Console	731
Implementing System Image Backups	739
Lesson Summary	743
Lesson Review	743
Lesson 2: System Recovery . . . . .	746
Performing a System Restore	746
Advanced Boot Options and System Recovery Options	750
Windows 7 Boot Options	754
Rolling Back Drivers	755
Lesson Summary	760
Lesson Review	760
Lesson 3: Recovering Files and Folders . . . . .	762
Restoring Damaged or Deleted Files by Using Previous Versions	762
Configuring System Protection and Disk Usage	769

Lesson Summary	775
Lesson Review	775
Chapter Summary .....	778
Chapter Review .....	778
Key Terms .....	778
Case Scenarios .....	779
Case Scenario 1: Supporting Backup And Restore	779
Case Scenario 2: Addressing System and Configuration Issues	779
Suggested Practices .....	780
Perform Backups	780
Configure System Recovery	780
Recover Files and Folders	781
Take a Practice Test .....	781
<i>Answers</i>	783
<i>Glossary</i>	843
<i>Index</i>	847

# Acknowledgments

---

Writing a book is always a team effort, and we have the advantage of an excellent team working hard behind the scenes and, unlike the authors, never seeing their names on the front cover. We are grateful to Ken Jones, our acquisitions editor, for his continued faith in us whenever a new project comes along, to Laura Sackerman, our developmental editor, who guides us through the initial stages and helps us out with any problems regarding, for example, new templates, and to Heather Stafford, who performs a function close to our hearts—she draws up our contract.

Possibly the key person in the entire team is the project editor, who holds the whole team together. We had worked with the indefatigable and highly competent Rosemary Caperton before and were very pleased to work with her again. We were also pleased that Rozanne Whalen was available as our technical reviewer, and was there to point out any slips we made and to question our assumptions. Rozanne is unfailingly polite, which doesn't stop her being very sharp indeed.

Adherence to standards of layout and literacy is vital to the quality of a book and to the reader experience. We are grateful for the considerable contribution made by our copyeditor, Susan McClung; our editorial proofreader, Nicole Schlutt; our indexer, Maureen Johnson; and last but definitely not least, Ashley Schneider, the S4Carlisle project editor, who pulls it all together.

Few creatures are as antisocial as an author in mid-book, and we are both lucky to have understanding and supportive wives. So, many thanks, Oksana and Anne. You are an essential and much-valued part of the team.

—Orin and Ian





# Introduction

---

This training kit is designed for IT professionals who operate in enterprise environments that use Windows 7 as a desktop operating system. You should have at least one year of experience in the IT field, as well as experience implementing and administering any Windows client operating system in a networked environment.

You should be able to install, deploy, and upgrade to Windows 7, including ensuring hardware and software compatibility. Additionally, you should be able to configure preinstallation and postinstallation system settings, Windows security features, network connectivity applications included with Windows 7, and mobile computing. You should also be able to maintain systems, including monitoring for and resolving performance and reliability issues and have a basic understanding of Windows PowerShell syntax.

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

- Install, upgrade, and migrate to Windows 7.
- Deploy Windows 7.
- Configure hardware and applications.
- Configure network connectivity.
- Configure access to resources.
- Configure mobile computing.
- Monitor and maintain systems that run Windows 7.
- Configure backup and recovery options.

## Lab Setup Instructions

The exercises in this training kit require a minimum of two client computers or virtual machines running Windows 7 Enterprise or Ultimate editions. Instructions for configuring the first of these computers are given in Chapter 1, “Install, Migrate, or Upgrade to Windows 7.” Instructions for configuring the second of these computers are given in Chapter 6, “Network Settings.” You need an additional hard disk (internal or external), formatted using the NTFS file system, installed on the first of these computers.

All computers must be physically connected to the same network. We recommend that you use an isolated network that is not part of your production network to do the practices in this book. To minimize the time and expense of configuring physical computers, we recommend you use virtual machines. To run computers as virtual machines within Windows, you can use Hyper-V, or third-party virtual machine software.

## Hardware Requirements

You can complete almost all the practice exercises in this book using virtual machines rather than real hardware. The minimum and recommended hardware requirements for Windows 7 are listed in Table 1.

**TABLE 1** Windows 7 Hardware Requirements

HARDWARE COMPONENT	MINIMUM REQUIREMENTS	RECOMMENDED
Processor	1 GHz 32-bit (x86) or 64-bit (x64) processor	2 GHz or faster
RAM	1 GB	2 GB
Disk space	40 GB	60 GB
Graphics adapter	Supports DirectX 9 graphics Has a Windows Display Driver Model (WDDM) driver Pixel Shader 2.0 hardware 32 bits per pixel 128 MB graphics memory	As minimum requirement, but with 256 MB of graphics memory

If you intend to implement two virtual machines on the same computer (which is recommended), a higher specification will enhance your user experience. In particular, a computer with 4 GB RAM and 60 GB available disk space can host all the virtual machines specified for all the practice exercises in this book.

## Using the DVD

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

- **Practice tests** You can reinforce your understanding of how to configure Windows 7 by using electronic practice tests you customize to meet your needs from the pool of Lesson Review questions in this book. Or you can practice for the 70-680 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. The eBook is in Portable Document Format (PDF), and you can view it by using Adobe Acrobat or Adobe Reader.
- **Sample chapters** Sample chapters from other Microsoft Press titles on Windows Server 2008. These chapters are in PDF format.

**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 DVD. Visit <http://www.microsoftpressstore.com/title/9780735627086> to get your downloadable content.

## How to Install the Practice Tests

To install the practice test software from the companion DVD to your hard disk, do the following:

1. Insert the companion DVD into your DVD drive and accept the license agreement. A DVD menu appears.

### **NOTE IF THE DVD MENU DOES NOT APPEAR**

If the DVD menu or the license agreement does not appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the DVD-ROM for alternate installation instructions.

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

## How to Use the Practice Tests

To start the practice test software, follow these steps:

1. Click Start, 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 VERSUS PRACTICE TESTS

Select the (70-680) Windows 7, Configuring *lesson review* to use the questions from the “Lesson Review” sections of this book. Select (70-680) Windows 7, Configuring *practice test* to use a pool of 200 questions similar to those that appear on the 70-680 certification exam.

## Lesson Review Options

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

After you click OK, your lesson review starts.

- **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 user interface when you are taking the test 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, a “References” section is provided that lists where in the training kit you can find the information that relates to that question and provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

## How to Uninstall the Practice Tests

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

## Microsoft Certified Professional Program

The Microsoft certifications provide the best method to prove 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 <http://www.microsoft.com/learning/mcp/default.asp>.

## Technical Support

Every effort has been made to ensure the accuracy of this book and the contents of the companion DVD. If you have comments, questions, or ideas regarding this book or the companion DVD, please send them to Microsoft Press:

### **E-mail**

- [mspinput@microsoft.com](mailto:mspinput@microsoft.com)

For additional support information regarding this book and the DVD-ROM (including answers to commonly asked questions about installation and use), visit the Microsoft Press Technical Support Web site at <http://www.microsoft.com/learning/support/books/>. To connect directly to the Microsoft Knowledge Base and enter a query, visit <http://support.microsoft.com/search/>. For support information regarding Microsoft software, connect to <http://support.microsoft.com>.



# BranchCache and Resource Sharing

People in the workplace rarely create documents that only they access. This is because organizational data is generally useful only when it is shared among people in the organization. People generally spend countless hours creating and formatting documents in Microsoft Office Word because they expect other people to read those documents. They write documents to explain ideas or to transmit data to other people because, generally, it is not necessary to write a document to explain something to *yourself*. The first part of this chapter looks at the methods you can use to share data stored on computers running Windows 7. This includes the simplified technique of sharing data through HomeGroups and the more complex technique of configuring shared folders. The second part of this chapter looks at how you can restrict the sharing of data, ensuring that only the people who should be able to view that data are actually able to view it. You can do this by applying file and folder permissions restricting who can access the data and by using encryption to ensure that data is encoded so that only specific people can decode it. The final part of this chapter looks at how you can speed up data access for people that are located in small branch offices in larger organizations through a new Windows 7 feature named BranchCache.

## Exam objectives in this chapter:

- Configure shared resources.
- Configure file and folder access.
- Configure BranchCache.

## Lessons in this chapter:

- Lesson 1: Sharing Resources **423**
- Lesson 2: Folder and File Access **442**
- Lesson 3: Managing BranchCache **461**



## Before You Begin

---

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

- Installed Windows 7 on a stand-alone client PC named Canberra, as described in Chapter 1, “Install, Migrate, or Upgrade to Windows 7.”



### **REAL WORLD**

Orin Thomas

**A**lthough file and folder sharing at the client rather than the server level can be quite useful for small businesses that do not have the resources to deploy a dedicated file server, I’ve found that if people are not paying attention, shared folders on client computers can cause a lot of problems. Perhaps this is because people think about shared folders on a server and shared folders on a client computer quite differently. When you have a file server, people are very aware that files saved in that location will be visible to other people in the organization. When you deploy file servers, it is relatively simple to set up file shares on the basis of group membership, and people remember that a file that should be visible only to managers gets put in the Managers shared folder. Sure, you can do this with client computers, but it generally takes more effort to configure different shares with specific permissions on each client computer. It takes even more effort to get the people that actually use these computers to remember how permissions actually work.

A colleague of mine had to deal with a meltdown that occurred at one client he worked for because a manager had saved performance reviews to a local folder that was visible to everyone on the network. Although there had been a specific shared folder set up that did limit document access to the administrative assistant and the company director, the manager hadn’t paid attention when this was explained to him. He worked off the assumption that no one else would see the reviews because he told only his administrative assistant and the company’s director that the documents were present in the shared folder.

Shared printers can cause similar problems. In many small businesses, the people who run the company get the best hardware. The person that ends up with the most fully featured printer gets it because she is the person who owns the company and signs the purchase orders. The printer ends up shared so that the people who might use features such as automatic double-sided printing and collation can actually do so. The downside to this is that these people have to keep going across to the senior staff member’s work space to retrieve their printing. At one organization I know, several people had to be given keys to the boss’s office so they could access their printing when he was away on business. Rather than move the printer to a more public location, the boss ended up authorizing the purchase of another printer.

# Lesson 1: Sharing Resources

---

Most home networks and very small businesses do not need a dedicated file and print server. There are usually only a few computers, and the number of files that people need to share is minimal. When you do not have access to a dedicated file and print server, you can use the resource sharing options included in Windows 7 to share files, folders, and printers. Windows 7 includes a new feature named HomeGroups, which simplifies the process of sharing files and printers on small networks where Active Directory Domain Services (AD DS) is not present.

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

- Configure HomeGroup settings.
- Configure sharing settings using Network And Sharing Center.
- Share folders.
- Manage printer permissions.

**Estimated lesson time: 40 minutes**

## Network And Sharing Center

You can use the Network And Sharing Center, displayed in Figure 8-1, to configure HomeGroup and advanced sharing options. You can use Network And Sharing Center to determine which networks the computer is currently joined to and the network designation assigned to those networks. You can use this tool to reset the designation assigned to an existing network. For example, you can change a Work network to a Home network by clicking the Work Network item under the network name and then clicking the Home Network option in the Set Network Location dialog box. You will learn more about the HomeGroup sharing options later in this lesson.

You can access the Advanced Sharing Settings dialog box by clicking the Change Advanced Sharing Settings item in Network And Sharing Center. You can use this dialog box, shown in Figure 8-2, to configure the sharing options for each different network profile. Because network profiles apply on a per-network interface basis, this means that different sharing options apply on a per-interface basis when a client running Windows 7 connects to multiple networks; for example, when you connect to a home network using a wireless network adapter and to an organizational network using DirectAccess.

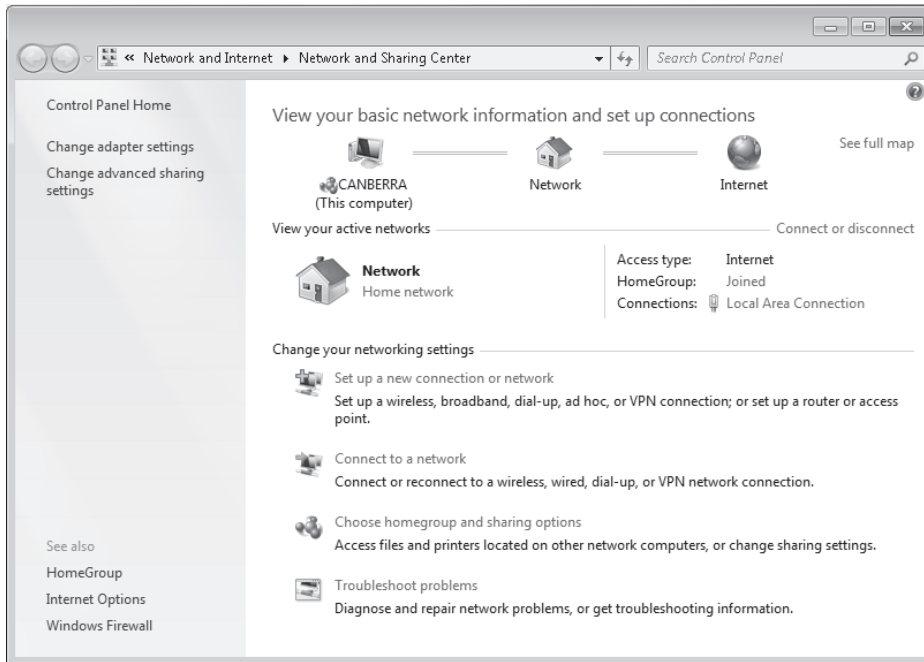


FIGURE 8-1 Network And Sharing Center

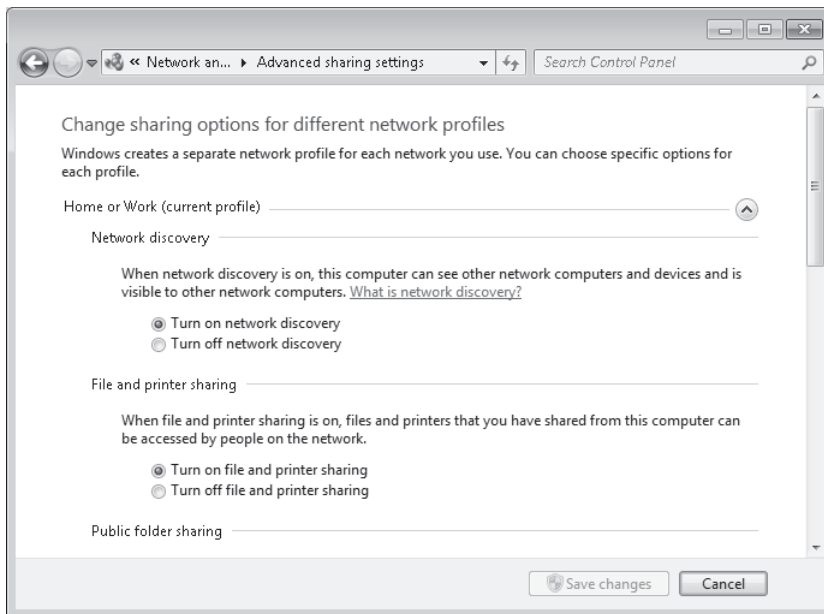


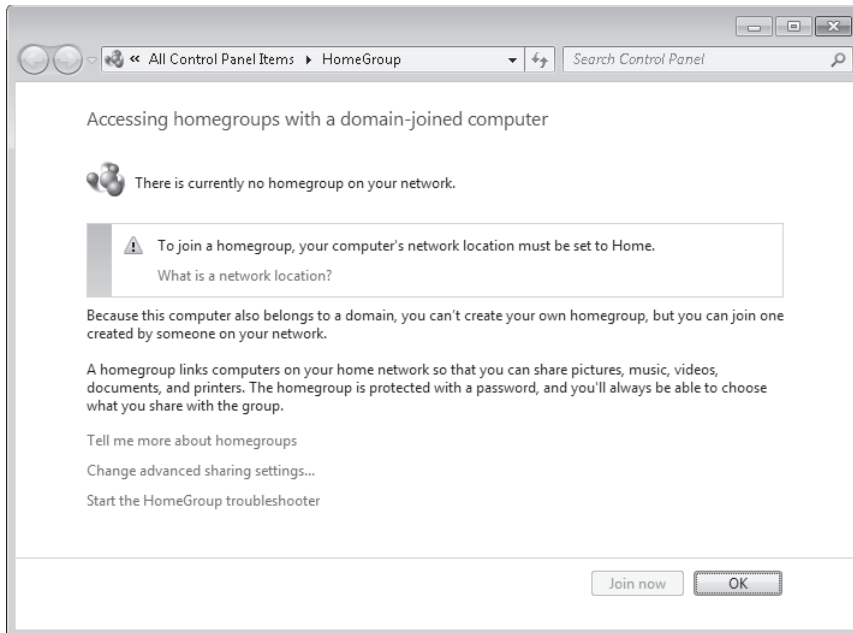
FIGURE 8-2 Advanced Sharing Settings

The sharing options that you can enable, disable, or configure using Advanced Sharing Settings are as follows:

- **Network Discovery** Network Discovery allows the client running Windows 7 to locate other computers and devices on the network. It also makes the client visible to other computers on the network. Disabling Network Discovery does not turn off other forms of sharing.
- **File And Printer Sharing** This setting enables files and printers to be shared with other clients on the network.
- **Public Folder Sharing** Enabling this setting allows network users read and write access to a public folder location. If you disable this folder, users can read and write data only to shared folders to which they have appropriate permissions.
- **Media Streaming** When you enable this setting, users on the network are able to access pictures, music, and videos hosted on the client running Windows 7. The client is also able to locate pictures, music, and videos hosted on other clients running Windows 7 on the network.
- **File Sharing Connections** This option allows you to choose between protecting file-sharing connections using 128-bit encryption or 40- or 56-bit encryption. You would choose the 40- or 56-bit encryption option for devices that do not support 128-bit encryption.
- **Password Protected Sharing** Enabling this option means that only users who have accounts configured locally on the client running Windows 7 are able to access shared resources. To allow users that do not have local accounts access to shared resources, you must disable this option.
- **HomeGroup Connections** This option decides how authentication works for connections to HomeGroup resources. If all computers in the HomeGroup have the same user name and passwords configured, you can set this option to allow Windows to manage HomeGroup connections. If different user accounts and passwords are present, you should configure the option to use user accounts and passwords to connect to other computers. This option is available only in the Home/Work network profile.

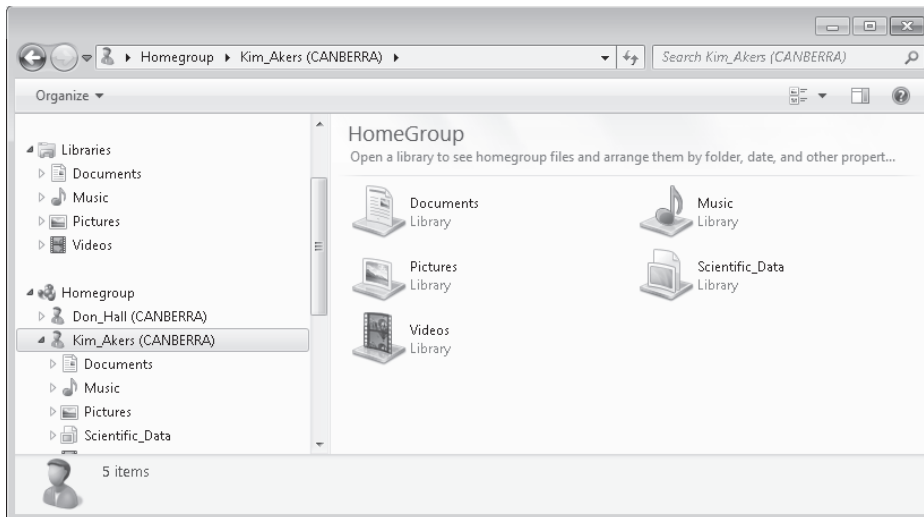
## HomeGroups

*HomeGroups* are a simple method through which you can share resources on a home network. You can use HomeGroups only on networks that you have designated as Home networks. You cannot create a HomeGroup on a domain network, but you can join an existing HomeGroup, as shown in Figure 8-3, if one is detected. For example, you could join an existing HomeGroup when you are using your client running Windows 7 on your home network, but where you also have a connection to your organization's domain network through DirectAccess.



**FIGURE 8-3** No HomeGroup on domain network

HomeGroups are visible as a separate node in Windows Explorer. Windows 7 displays HomeGroups by user name and computer name. This is because each user on a client running Windows 7 will share different resources with the network depending on their individual sharing settings. Figure 8-4 shows the Don\_Hall (CANBERRA) and Kim\_Akers (CANBERRA) HomeGroups. The Kim\_Akers (CANBERRA) HomeGroup includes a custom library named Scientific Data. You will create and share this custom library in the practice at the end of this lesson.



**FIGURE 8-4** Viewing HomeGroups

Although only users with Administrative privileges are able to enable the HomeGroup, each standard user can choose which of their libraries to share with the HomeGroup. For example, Kim\_Akers can choose to share her Documents, Music, Pictures, and Videos libraries, whereas Don\_Hall may choose to share only his Documents library. Users do not need to be logged on for their HomeGroups to be available to other users on the network. Each user's HomeGroup share is available so long as the computer that hosts it is turned on and connected to the home network.

If a HomeGroup is present on the network, the details are displayed when you open the HomeGroup item in the Network And Sharing Center.

To join a HomeGroup if one already exists on your network, perform the following steps:

1. Open the HomeGroup item from the Network And Sharing Center.
2. If a HomeGroup is detected on another computer, the details of this HomeGroup are displayed. Contact the person who configured the HomeGroup and then click Join Now.
3. On the Join A HomeGroup page, shown in Figure 8-5, select which items you want to share with the other computers that are members of the HomeGroup, and click Next.



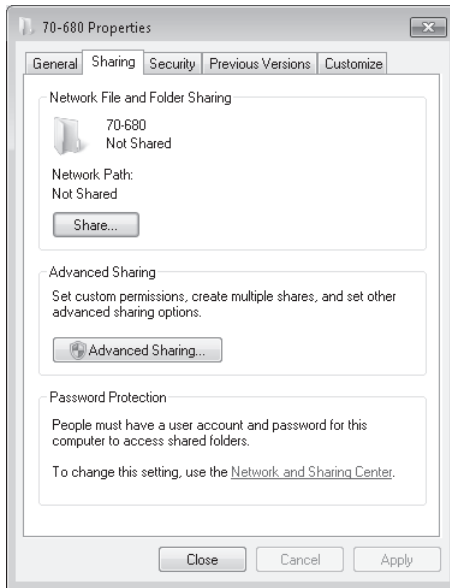
**FIGURE 8-5** Share items with HomeGroup

4. Enter the HomeGroup password that you have acquired from the person who created the HomeGroup. Once the password has been accepted, you have joined the HomeGroup.

To leave the HomeGroup, open the HomeGroup item in the Network And Sharing Center and then click Leave.

## Shared Folders

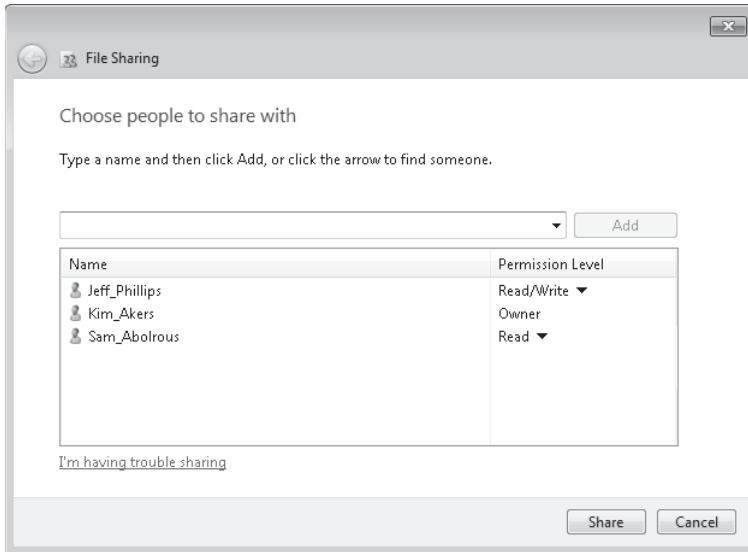
Shared folders allow you to share data stored on your computer with other users on your network. You can share individual folders by right-clicking the folder you wish to share, choosing Properties, and then clicking the Sharing tab of the folder's properties, as shown in Figure 8-6. This page provides two different sharing options: Share and Advanced Sharing. You can use shared folders when you cannot use HomeGroups, such as when you want to share resources on a Work network.



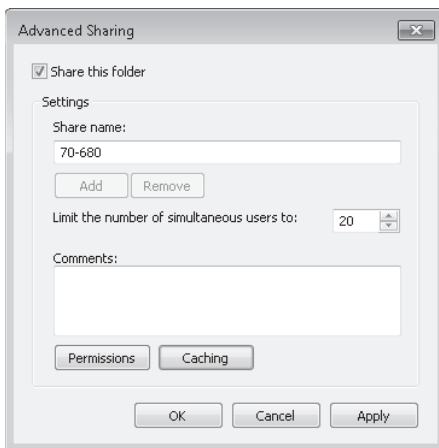
**FIGURE 8-6** Sharing tab of folder properties

Clicking Share brings up the File Sharing dialog box, shown in Figure 8-7. You can use this dialog box to set share permissions for local user accounts, the Everyone group, or the HomeGroup. When you connect a client running Windows 7 to a domain, you can also specify domain user accounts and groups. You cannot use this dialog box to specify local groups. The user account that you use to share the folder with is assigned the Owner permission automatically. It is also possible to assign the Read/Write permissions, which allows users to add files, delete files, and modify files in the shared folder, and the Read permission, which allows users to access files in the shared folder but not modify or delete them.

Clicking Advanced Sharing brings up the Advanced Sharing dialog box, shown in Figure 8-8. This dialog box allows you to limit the number of users who are able to access the share. Use this when you need to restrict the number of people that are connected to a share for performance reasons. Clicking Permissions allows you to configure permissions for local groups, local users, domain groups, or domain users.



**FIGURE 8-7** Basic file sharing

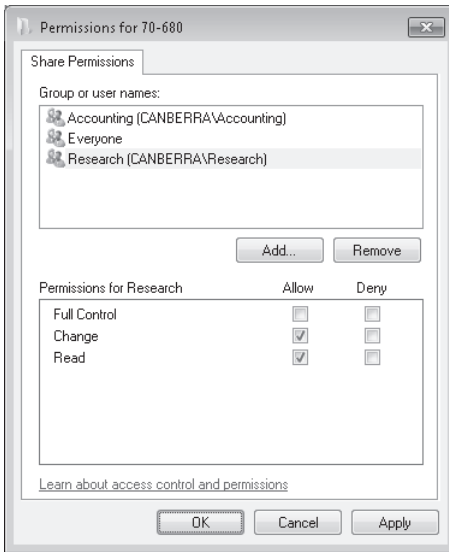


**FIGURE 8-8** Advanced Sharing

As you can see in Figure 8-9, these permissions have different names from those that are available from the basic File Sharing dialog box but allow you to do the same things. The Read permission allows a user or group to access a file or folder but does not allow modification or deletion. The Change permission includes the read permission but also allows you to add files, delete files, and modify files in the shared folder. This permission is equivalent to the Read/Write permission in the basic File Sharing dialog box. The Full Control permission includes all the rights conferred by the Change and Read permissions. It also

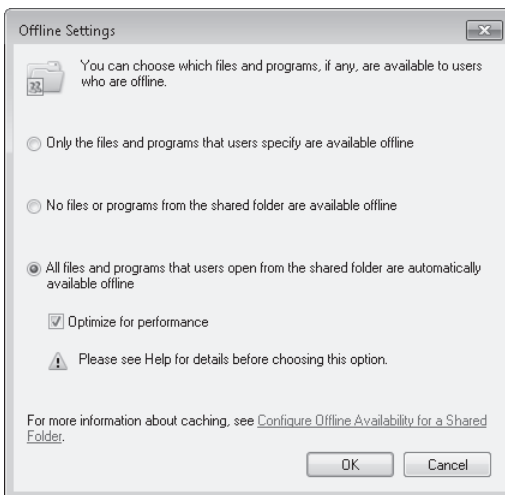


allows the user assigned that permission to modify the permissions of other users. Full Control is equivalent to the basic sharing Owner permission, though unlike basic sharing, where there can only be one user assigned the Owner permission, you can assign the Full Control permission to users and groups.



**FIGURE 8-9** Advanced permissions

Clicking Caching on the Advanced Sharing dialog box allows you to access the Offline Settings dialog box, as shown in Figure 8-10. Offline settings determine whether programs and files hosted on the shared folder are available when the user, or the computer hosting them, is not available to the network. You will learn more about offline settings in Chapter 11, “BitLocker and Mobility Options.”



**FIGURE 8-10** Shared folder offline settings

You can manage all shared folders on a client running Windows 7 centrally using the Shared Folders node of the Computer Management console. The Shares node, shown in Figure 8-11, displays all shared folders on the computer. The Sessions node provides details on which remote users currently are connected to shared folders, where they are connecting from and how long they have been connected. The Open Files node displays the folders and files that remote users are accessing. You can edit the properties of an existing share by right-clicking it within this console and selecting properties. You can create a shared folder by right-clicking the Shares node and then clicking New Share. This starts the Create A Shared Folder Wizard. You use this wizard to create a shared folder in a practice exercise at the end of this lesson.

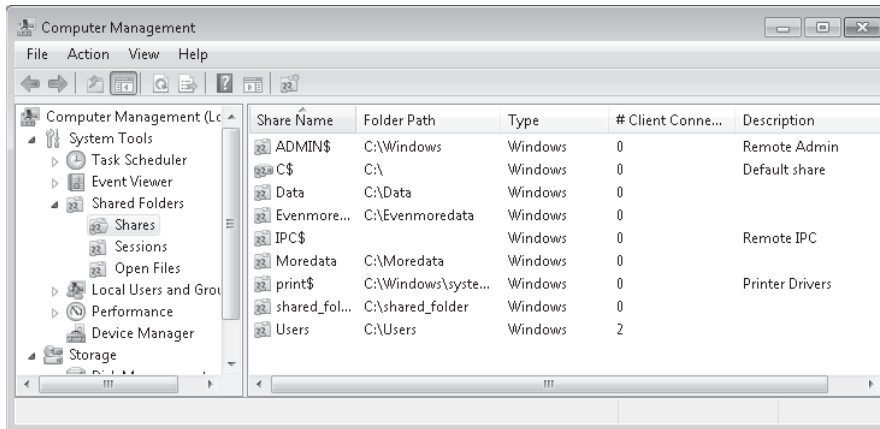


FIGURE 8-11 Viewing shares

The *Net Share* command allows for management of shared folders from the command line. You can script this command to automate the creation of shared folders on clients running Windows 7. To create a shared folder, use the command:

```
net share sharename=drive:path
```

To assign permissions when creating the shared folder, use the command:

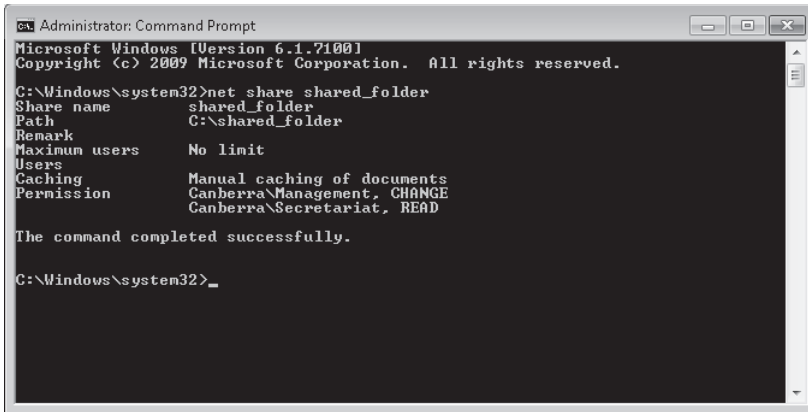
```
net share sharename=[path] /grant:user,[Read/Change/Fu11]
```

(for example `net share tempus=c:\temp /grant:Bob,Change` )

You can also use the *Net Share* command to configure caching options as well as limit the number of users that can connect to the shared folder. You can view the properties of a shared folder by running the command

```
net share sharename
```

as shown in Figure 8-12. You can view the properties of all shared folders, including which directories are associated with particular folders, by using the *Net Share* command without any options.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net share shared_folder
Share name      shared_folder
Path            C:\shared_folder
Remark
Maximum users   No limit
Users
Caching         Manual caching of documents
Permission      Canberra\Management, CHANGE
                Canberra\Secretariat, READ

The command completed successfully.

C:\Windows\system32>_
```

FIGURE 8-12 Shared folder properties

#### **MORE INFO** SHARE PERMISSIONS AND NTFS PERMISSIONS

Share permissions and NTFS permissions are combined when determining what access a remote user has to files. You will learn about NTFS permissions and combined permissions in Lesson 2, “Folder and File Access.”

#### **Quick Check**

- Which tool can you use to determine which files and folders that users are accessing remotely on a client running Windows 7 configured with shared folders?

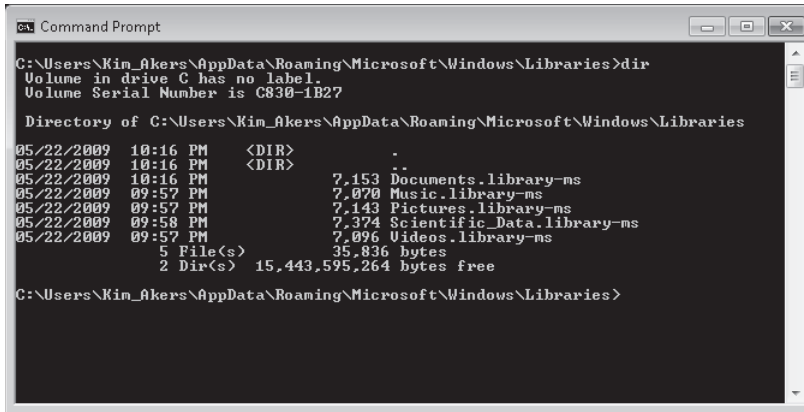
#### **Quick Check Answer**

- You can use the Shared Folders\Open Files node to determine which files and folders are being accessed remotely on a client running Windows 7.

## Libraries

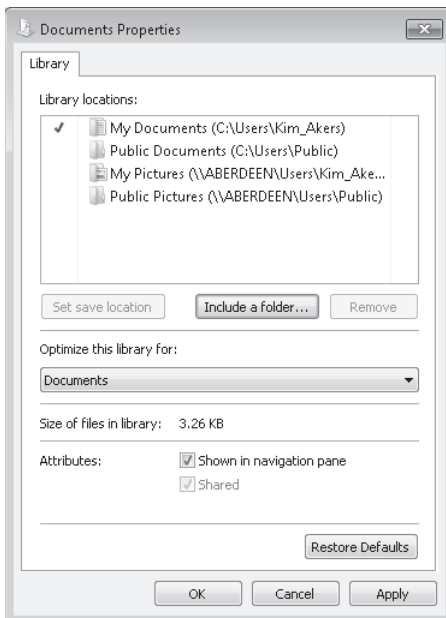
A *library* is a virtualized collection of folders. This means that a library is not a folder that you can locate on the hard disk that contain subfolders but is a collection of links to existing folders. If you navigate to the Libraries folder from the command prompt, you will see that it contains files with the extension *library-ms*, as shown in Figure 8-13. These files are the collection of folder links and each one of them is a separate library.

Libraries allow you to collect folders that exist in many different locations locally and on the network into a single location when viewed from within Windows Explorer. For example, you can configure the Documents library so that it includes document folders located on other computers in the HomeGroup as well as folders located on the computer’s hard disk drive. Libraries do not have to be limited to a certain type of file, though it is usually better to restrict them to a specific type of content as a means of simplifying navigation.



**FIGURE 8-13** Libraries from the command line

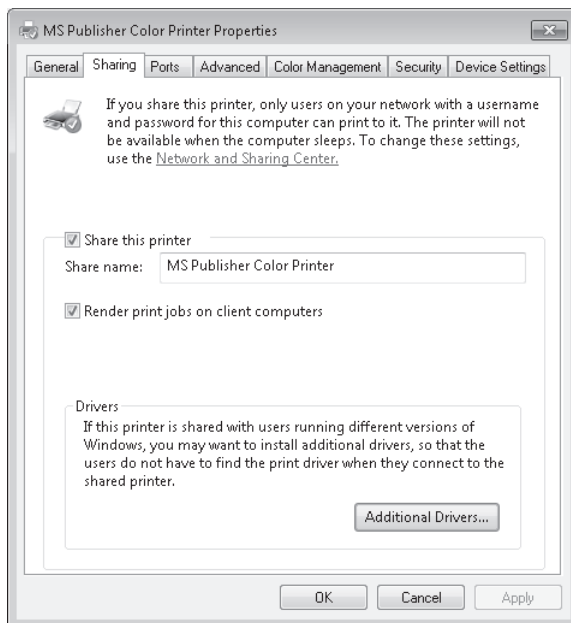
You can add folders to an existing library by editing that library's properties and clicking Include A Folder, as shown in Figure 8-14. You can use the same Properties page to remove existing folders from a library. You can create a new library by navigating to the Libraries folder and clicking New Library. You will create a new library in the practice exercise at the end of this lesson.



**FIGURE 8-14** Library locations

## Sharing Printers

Shared printers allow users on the network to send documents to a printer that is connected to a computer running Windows 7. To share a printer, enable printer sharing in HomeGroup or in Advanced Sharing Settings and then locate the printer within Devices And Printers. Right-click the printer that you wish to share, click Printer Properties, click the Sharing tab, and then enable Share This Printer, as shown in Figure 8-15. If you are going to be sharing a printer with computers running previous versions of Microsoft Windows, you can add the drivers for the printer using Additional Drivers. When you add additional drivers, other computers on the network that do not have the printer drivers installed are able to download them from the computer that is sharing the printer.

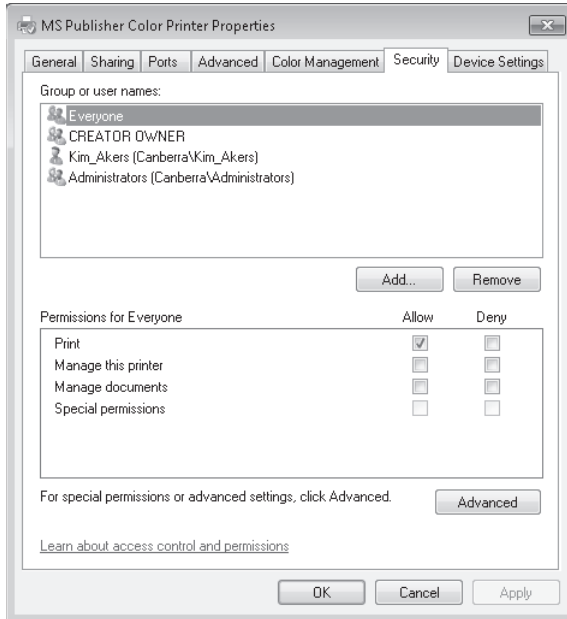


**FIGURE 8-15** Printer sharing options

When you share a printer, the Everyone group is assigned the Print permission by default, as shown in Figure 8-16. This means that all members of the HomeGroup or any user that is a member of the domain in a domain environment can send print jobs to the printer. If several people use the printer, you may wish to assign one of the other available permissions to allow better printer management. The available permissions are:

- **Print** This permission allows a user to print to the printer and rearrange the documents that they have submitted to the printer.
- **Manage This Printer** Users assigned the Manage This Printer permission can pause and restart the printer, change spooler settings, adjust printer permissions, change printer properties, and share a printer.

- **Manage Documents** This permission allows users or groups to pause, resume, restart, cancel, or reorder the documents submitted by users that are in the current print queue.



**FIGURE 8-16** Printer sharing properties

#### **MORE INFO** MANAGE PRINTER PERMISSIONS

To learn more about managing printer permissions, consult the following page on TechNet: [http://technet.microsoft.com/en-us/library/cc773372\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc773372(WS.10).aspx).



#### **EXAM TIP**

Remember what permissions to assign a group to allow them to manage their own documents, but not to manage other documents submitted to a shared printer.

### **PRACTICE** Sharing Resources

Rather than deploying a dedicated file server, many small businesses use shared folders hosted off workstations as a method of sharing documents. In this practice, you configure Windows 7 to share data using the built-in HomeGroup functionality as well as sharing through the creation of dedicated shared folders.

## EXERCISE 1 Configuring Libraries and HomeGroup Settings

In this exercise, you create a new library and then share it. You also modify the HomeGroup password from the one created during setup to one that is easier for other users of the HomeGroup to remember.

1. Log on to computer Canberra using the Kim\_Akers user account.
2. Using Windows Explorer, create the C:\Data, C:\Moredata, and the C:\Evenmoredata folders.
3. Click Start. In the Search Programs And Files text box, type **Libraries**. On the Start menu, click Libraries. This opens the Libraries virtual folder, as shown in Figure 8-17.

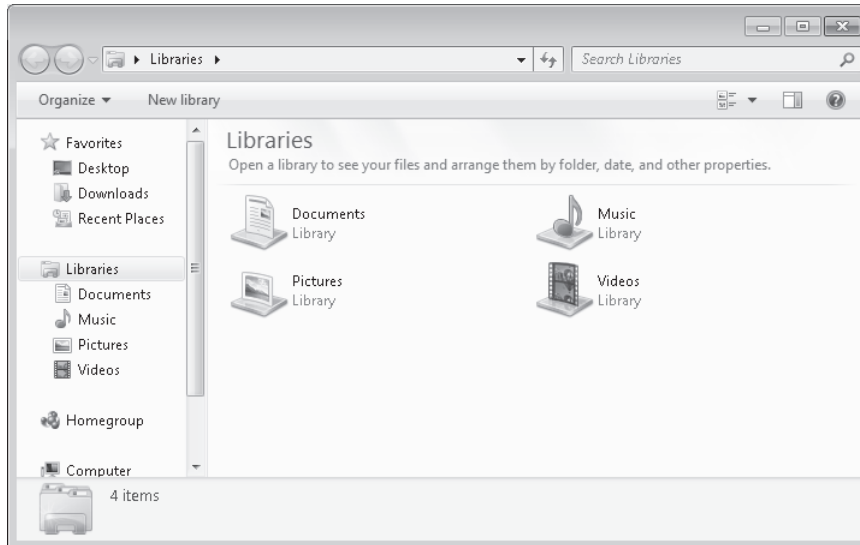
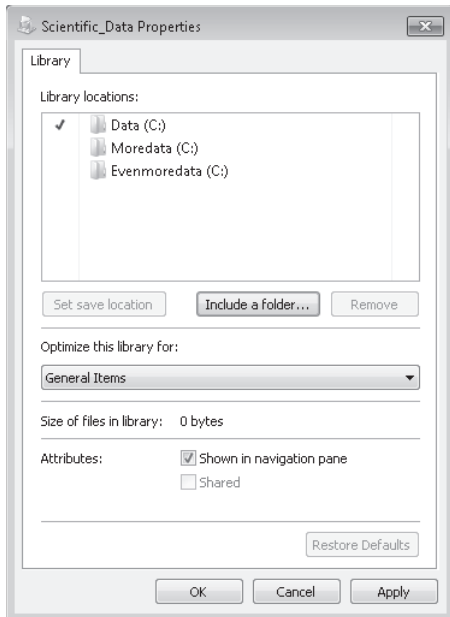
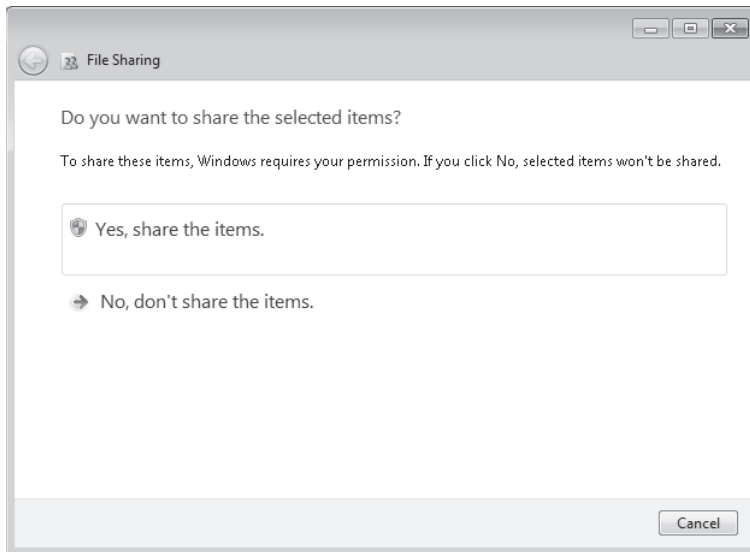


FIGURE 8-17 The Libraries virtual folder

4. Click the New Library item. This creates a new library. Name the library **Scientific\_Data**.
5. Right-click the Scientific\_Data folder and then choose Properties. This opens the Scientific\_Data Properties dialog box. Click Include A Folder, navigate to and select the C:\Data folder, and click Include Folder. Repeat this step for the C:\Moredata and C:\Evenmoredata folders.
6. Verify that the Scientific\_Data Properties dialog box matches Figure 8-18, and then click OK.
7. Right-click the Scientific\_Data library, choose Share With, and then click HomeGroup (Read).
8. If you are presented with the File Sharing dialog box, shown in Figure 8-19, click Yes, Share The Items.



**FIGURE 8-18** Library properties

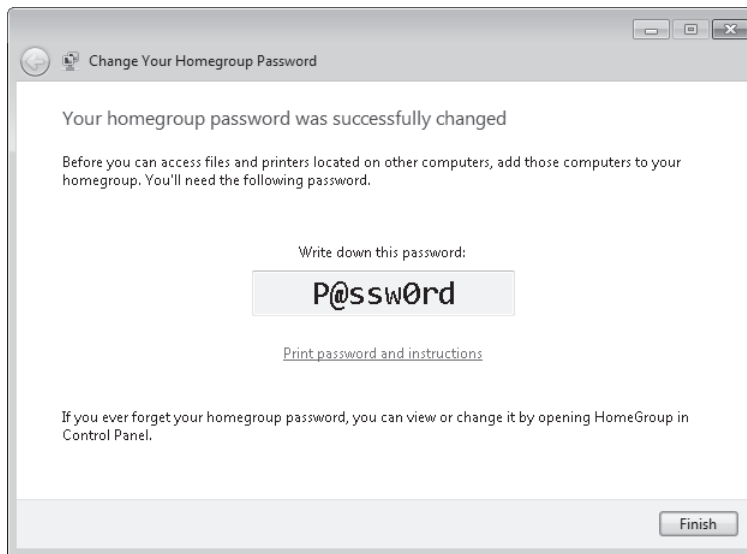


**FIGURE 8-19** Share items

9. Click Start. In the Search Programs And Files text box, type **HomeGroup**. In the Start menu, click the HomeGroup item. This opens the HomeGroup control panel.
10. Click the Change The Password item. On the Change Your HomeGroup Password dialog box, click Change The Password.



11. On the Type A New Password For Your HomeGroup page, enter the password **P@ssw0rd** and then click Next.
12. Verify that your HomeGroup password settings match those shown in Figure 8-20, and then click Finish.



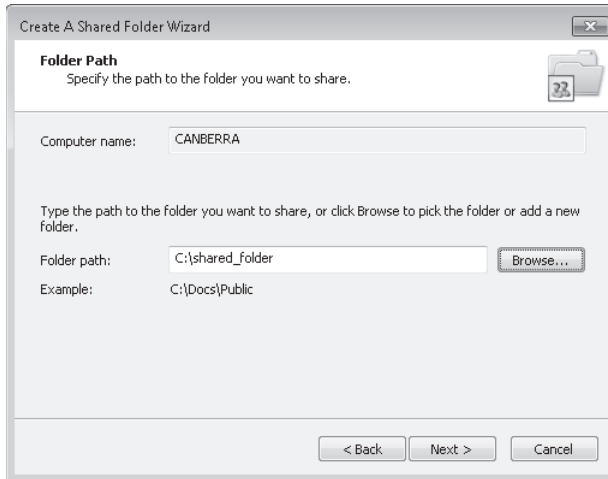
**FIGURE 8-20** HomeGroup password changed

## **EXERCISE 2** Advanced Folder Sharing

In this exercise, you share a folder using the Create A Shared Folder Wizard. You would use this method to share a folder when you connect your computer to a Domain network. When you connect your computer to a domain network, you cannot use the HomeGroup functionality of Windows 7, though it is possible to share libraries directly.

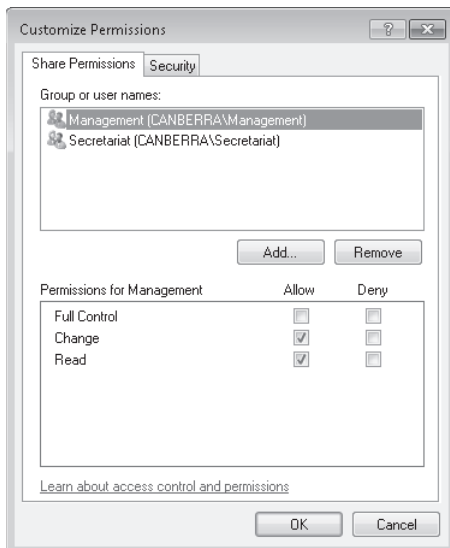
1. If necessary, log on to the Canberra computer using the Kim\_Akers user account.
2. Open an elevated command prompt and issue the following commands:

```
Net localgroup Management /add
Net localgroup Secretariat /add
Mkdir c:\shared_folder
```
3. Type **exit** to close the elevated command prompt.
4. Click Start. In the Search Programs And Files text box, type **Computer Management**. In the Start menu, click Computer Management. This opens the Computer Management console.
5. Expand the System Tools\Shared Folders node. Right-click the Shares node and then choose New Share. This starts the Create A Shared Folder Wizard. Click Next.
6. In the Folder Path: text box, type **c:\shared\_folder**, as shown in Figure 8-21, and then click Next.



**FIGURE 8-21** Specifying a shared folder path

7. In the Name, Description, And Settings page, accept the default settings, and then click Next.
8. On the Shared Folder Permissions page, select Customize Permissions and then click Custom.
9. On the Share Permissions tab, select the Everyone group and then click Remove. Click Add. In the Select Users Or Groups dialog box, type **Management; Secretariat** and then click OK.
10. Configure the Secretariat group with the Read (Allow) permission. Configure the Management group with the Change (Allow) permission, as shown in Figure 8-22. Click OK.



**FIGURE 8-22** Custom share permissions

11. Click Finish twice to close the Create A Shared Folder Wizard.
12. From an elevated command prompt, issue the command **net share shared\_folder** to verify that the Management group is assigned the Change permission and the Secretariat group has been assigned the Read permission.

## Lesson Summary

- HomeGroups can be used on networks that have the Home network location designation. They make it easier to share resources in environments without AD DS.
- Libraries are collections of folders. You can share libraries with the HomeGroup.
- Shared folders allow individual folders to be shared. Sharing options for folders are more detailed than for Libraries.
- You can manage shared folders through the Computer Management console, Windows Explorer, and the *Net Share* command. The Computer Management console allows for the centralized administration of shared folders.
- The Read printer permission allows users to control their own documents. The Manage Documents permission allows users to manage all documents submitted to the printer. The Manage Printers printer permission allows users to control printer settings and configure printer permissions.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Sharing Resources." The questions are also available on the companion DVD 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 responsible for maintaining a computer running Windows 7 Enterprise that is used in a university laboratory and is hooked up to four different scientific instruments. Each of these instruments outputs its data to a directory named Data. Each instrument's data directory is located on a different volume on the computer's hard disk drive. You want to share this data with other computers in the laboratory through the common HomeGroup. Which of the following should you do? (Choose all that apply; each answer forms part of a complete solution.)
  - A. Share each Data folder.
  - B. Create a library named Sci\_Data.
  - C. Add each instrument's separate Data folder to the Sci\_Data library.
  - D. Share the Sci\_Data library.

2. You do consulting work for a small business. This small business has a single color laser printer. This printer is shared off the administrative assistant's client running Windows 7. The administrative assistant is not a member of the local Administrators group. You want to allow the administrative assistant to reorder jobs in the print queue and delete them if necessary. The administrative assistant should be able to do this to any documents in the queue. The administrative assistant should not be able to reconfigure printer permissions. Which of the following should you do to accomplish this goal?
  - A. Assign the administrative assistant the Print permission.
  - B. Assign the administrative assistant the Manage This Printer permission.
  - C. Assign the administrative assistant the Manage Documents permission.
  - D. Add the administrative assistant's account to the Power Users group.
3. Which of the following tools can you use to determine which shared folders a client running Windows 7 hosts and the local folders that are associated with those shares? (Choose all that apply.)
  - A. The *Net Share* command
  - B. The Computer Management console
  - C. Libraries
  - D. Network And Sharing Center
4. You have created a local group on a client running Windows 7 named Accounting. Which of the following share permissions should you assign to the accounting group to ensure that users are able to add, modify, and delete files located in the Accounting shared folder without giving members of the group the ability to modify shared folder permissions?
  - A. Read
  - B. Change
  - C. Full Control
  - D. Owner
5. Which of the following Advanced Sharing Settings options should you configure to ensure that shared resources on a client running Windows 7 are visible to all other computers in the HomeGroup?
  - A. Public Folder Sharing
  - B. File Sharing Connections
  - C. Password Protected Sharing
  - D. Network Discovery

## Lesson 2: Folder and File Access

---

In many Windows 7 deployments, multiple people have to use the same computer. When multiple people use the same computer and store their files locally, it becomes necessary to ensure that some form of security exists so that one user is able to look at another user's files only if he has the appropriate permissions. Windows 7 allows you to do this through file and folder permissions, as well as encryption through Encrypting File System (EFS).

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

- Configure file and folder permissions.
- Resolve effective permissions issues.
- Encrypt files and folders.

**Estimated lesson time: 40 minutes**

### File and Folder Permissions

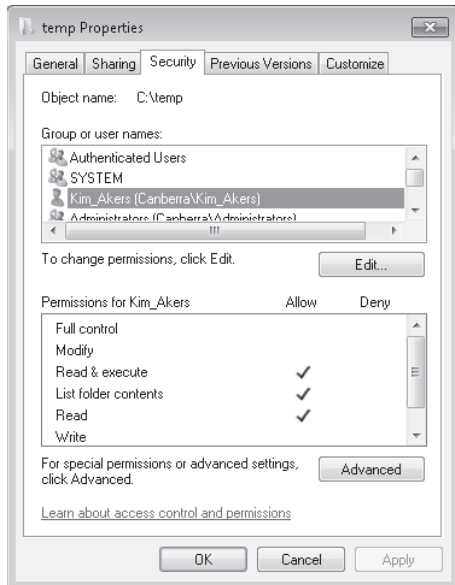
You can apply NTFS file and folder permissions to individual user accounts or groups. NTFS file and folder permissions determine access rights to files and folders. These access rights apply whether the user logs on directly to the client running Windows 7 or is accessing the client running Windows 7 over the network. You can set file and folder permissions only to files and folders hosted on NTFS volumes. It is not possible to set file and folder permissions to files and folders hosted on FAT or FAT32 volumes.

There are six standard permissions that can be assigned to a file or a folder. These permissions include the following:

- **Full Control** When applied to folders, allows the reading, writing, changing, and deletion of files and subfolders. When applied to a file, permits reading, writing, changing, and deletion of the file. Allows modification of permissions on files and folders.
- **Modify** When applied to folders, allows the reading, writing, changing, and deletion of files and subfolders. When applied to a file, permits reading, writing, changing, and deletion of the file. Does not allow the modification of permissions on files and folders.
- **Read & Execute** When applied to folders, allows the content of the folder to be accessed and executed. When applied to a file, allows the file to be accessed and executed.
- **List Folder Contents** Can be applied only to folders, allows the contents of the folder to be viewed.
- **Read** When applied to folders, allows content to be accessed. When applied to a file, allows the contents to be accessed. Differs from Read & Execute in that it does not allow files to be executed.
- **Write** When applied to folders, allows adding of files and subfolders. When applied to a file, allows a user to modify, but not delete, a file.

You can assign these permissions to a user or group by viewing a folder's properties and clicking the Security tab. You can configure permissions with the Allow or Deny setting, or provide no setting. Deny permissions always override Allow permissions. If a user is not explicitly assigned an Allow permission, she cannot perform that function.

Figure 8-23 shows that the user Kim Akers has the Read & Execute (Allow), List Folder Contents (Allow), and Read (Allow) permissions for the Temp folder. Other permissions, such as Modify, have been assigned no setting. Unless the Modify (Allow) permission is assigned through membership in another group, Kim Akers is unable to modify files in the Temp folder.



**FIGURE 8-23** Standard permissions

When you set the Allow permissions for some permission types, other Allow permissions are included automatically. For example, if you set the Read & Execute (Allow) permission, Windows automatically sets the List Folder Contents (Allow) and Read (Allow) permissions. Similarly, a Deny permission for one permission type can also apply to other permission types. The permissions that also apply when you assign a particular type of permission are included in Table 8-1.

**TABLE 8-1** Included Permissions

PERMISSION	INCLUDED
Full Control	Full Control, Modify, Read & Execute, List Folder Contents, Read, Write
Modify	Modify, Read & Execute, List Folder Contents, Read, Write
Read & Execute	Read & Execute, List Folder Contents, Read
List Folder Contents	List Folder Contents
Read	Read
Write	Write

## ✓ Quick Check

1. Which additional permissions are assigned when you assign the Modify (Allow) permission?
2. Which permission should you assign when you want to allow a user to modify the contents of a file, but not delete that file?

### Quick Check Answers

1. When you assign the Modify (Allow) permission, Windows also assigns the Read & Execute (Allow), List Folder Contents (Allow), Read (Allow), and Write (Allow) permissions automatically.
2. The Write permission allows a user to modify the contents of a file, but not delete it.

## Special Permissions

The six NTFS permissions are actually collections of special permissions. This is why other permissions are included automatically when you assign permissions such as Modify and Read & Execute. The collection of special permissions that are assigned when you assign the Read & Execute permission include all the special permissions that make up the List Folder Contents and Read permissions. The six NTFS permissions are adequate for the majority of situations. If you encounter an unusual situation where you want more granular permissions, you can modify the special permissions. This is done by clicking the Advanced button on the Security tab of a file or folder's properties, clicking Change Permissions, and then clicking Edit. The Permissions Entry dialog box is shown in Figure 8-24.

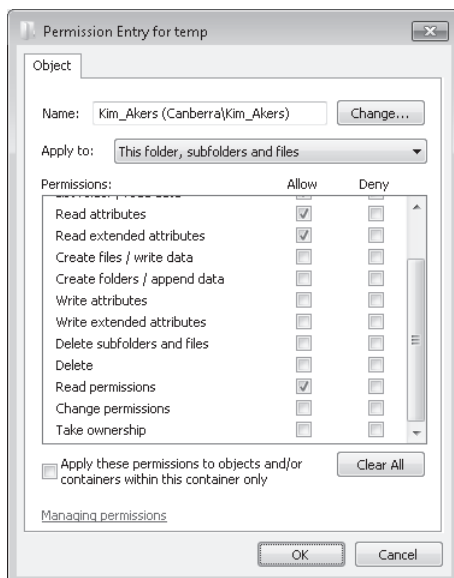


FIGURE 8-24 Special permissions

The special permissions that make up each of the six NTFS permissions is shown in Table 8-2. The List Folder Contents special permission applies only to folders and does not apply to individual files. Special permissions are included here for the sake of completeness and are unlikely to be addressed directly by the 70-680 exam.

**TABLE 8-2** Special Permissions and NTFS Permissions

<b>SPECIAL PERMISSION</b>	<b>FULL CONTROL</b>	<b>MODIFY</b>	<b>READ &amp; EXECUTE</b>	<b>LIST FOLDER CONTENTS</b>	<b>READ</b>	<b>WRITE</b>
Traverse Folder/Execute File	X	X	X	X		
List Folder/Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create Files/Write Data	X	X				X
Create Folders/Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					

## Inheriting Permissions

Newly created files and folders inherit the permissions that are assigned to the folder in which they are created. For example, if you have a folder named Alpha that has the Modify (Allow) permission assigned to the Development group, any files or folders that you create in folder Alpha also have the Modify (Allow) permission assigned to the Development group by default.



It is possible to override a file or folder's inherited permissions by editing the permissions, clicking Advanced, clicking Change Permissions, and then clearing the Include Inheritable Permissions From This Object's Parent option, as shown in Figure 8-25. When you clear the Include Inheritable Permissions From This Object's Parent option, you have the option of copying the existing permissions so that they apply to the object or removing all inherited permissions. When you edit the Advanced Security settings for a folder, you have the option of replacing the permissions of all existing child objects.

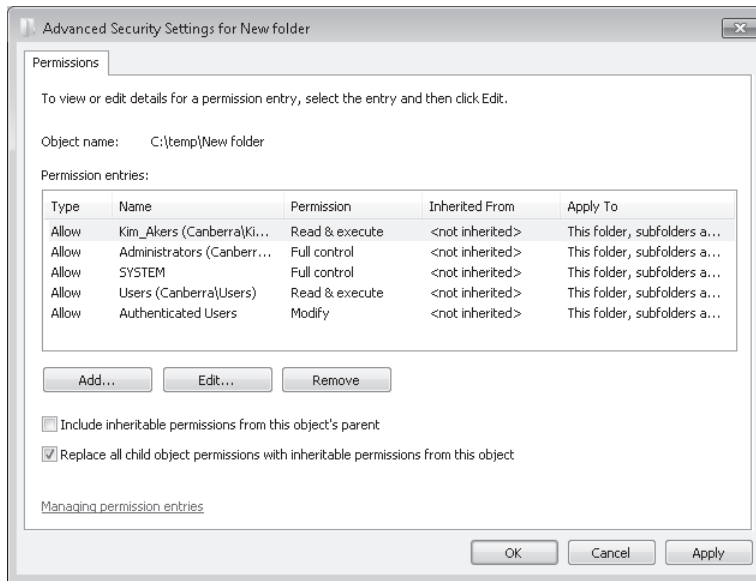


FIGURE 8-25 Permissions inheritance settings

## Configuring Permissions with Icacls

Icacls is a command-line utility that you can use to configure and view the NTFS permissions of files and folders on a computer running Windows 7. To use Icacls to view the permissions assigned to a specific file or folder, use the command *Icacls File\_or\_Folder*. You can use the syntax *Icacls file\_or\_folder /grant user\_or\_group:permission*. You can use the */deny* option to set Deny rather than Allow. The NTFS permissions you can assign are:

- F (Full Control)
- M (Modify)
- RX (Read and Execute)
- R (Read)
- W (Write)

For example, to assign the Kim\_Akers user account the Modify NTFS permission on the C:\Accounting folder, issue the command

```
Icacls.exe c:\accounting /grant Kim_Akers:(OI)M
```

To assign the Kim\_Akers user account the Read & Execute (Deny) permission to the C:\Research folder, issue the command

```
Icacls.exe c:\research /deny Kim_Akers:(OI)RX
```

Icacls can be used to save permissions assigned to files and folders and to restore them. To save all NTFS permissions C:\Test directory and all its subdirectories to a file named Permissions, issue the command

```
Icacls c:\test\* /save permissions /t
```

You can restore permissions using the */restore* option. You can use the ability to save and restore permissions when copying files and folders to different volumes. You will use Icacls to assign permissions in the practice at the end of this lesson.

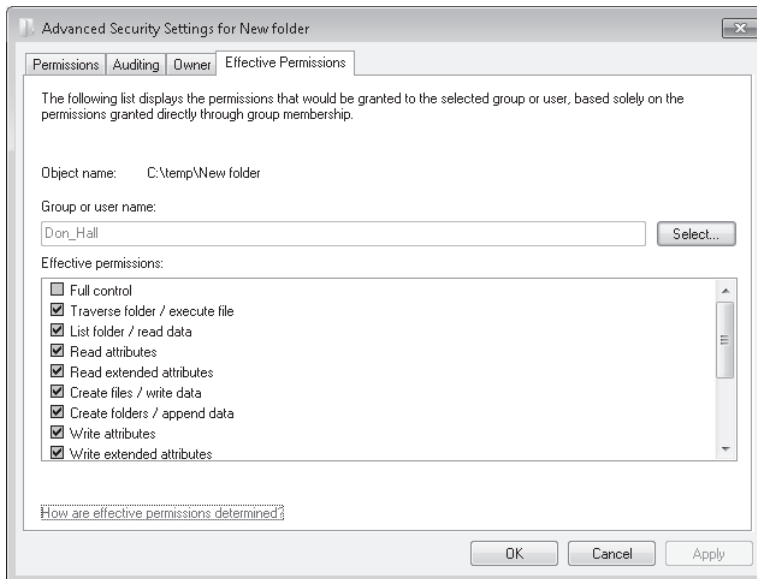
#### **MORE INFO** Icacls

To learn more about Icacls syntax and options, including how to assign special permissions, consult the following TechNet document: [http://technet.microsoft.com/en-us/library/cc753525\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc753525(ws.10).aspx).

## Determining Effective Permissions

When a user is a member of multiple groups and those groups are all assigned different permissions to the same folder, it can be difficult to determine the user's effective permission. Permissions are cumulative, and Deny permissions override Allow permissions. This can become very complicated when different groups have multiple Allow permissions. If you do not take a user's group memberships into account, you may miss something important when attempting to figure out the actual permissions that apply to them.

You can use the Effective Permissions tool to calculate a user or group's effective permissions on a file or folder. The Effective Permissions tool analyzes a user's permissions as well as the permissions of all the groups to which the user's account belongs to determine what special permissions the user has to the object in question. To access the Effective Permissions tool, click the Advanced button located on the Security tab of the target file or folder's properties and select the Effective Permissions tab. Click Select, as shown in Figure 8-26, to choose the group or user for which you wish to determine effective permissions. You will determine the effective permissions of a user in the practice exercise at the end of this lesson.



**FIGURE 8-26** Effective permissions tool

## Copying and Moving Files

Permissions work differently depending on whether you copy a file, move it to a different location on the same volume, or move the file to a different volume. The same inheritance rules that apply to copying or moving files also apply to copying or moving folders.

When you copy a file from one folder to another, the file inherits the permissions of the destination folder. This rule applies whether you are copying between folders on the same volume or folders on different volumes. For example, if you have assigned members of the Research group the Write (Deny) permission on folder Alpha and have assigned the same group the Modify (Allow) permission on folder Beta, members of the Research group have the Modify (Allow) permission on any file copied from folder Alpha to folder Beta. The rules that apply to copying files apply to copying folders. When you copy a folder from one parent folder to another, the folder and all that folder's contents inherit the permissions assigned to the destination folder.

Moving files from one folder to another works differently, depending on whether you are moving from one folder to another on the same volume, or from a folder on one volume to a folder on another. When you move a file between folders on the same volume, the file retains its original permissions. For example, if you have assigned members of the Research group the Write (Deny) permission on folder Alpha and have assigned the same group the Modify (Allow) permission on folder Beta and you move a file from folder Alpha to folder Beta, the file retains its original Write (Deny) permission for the Research group. The same applies if you move a folder. The folder and its contents retain their original permissions when moved to a new location on the same volume.

When you move a file from a folder on one volume to a folder on another volume, the file behaves the same way that it does when you copy it and inherits the permissions of the destination folder. The same applies to a folder. If you move a folder from one volume to another, that folder and all its contents inherit the permissions assigned to the destination folder.

Robocopy.exe is a command-line utility that is included with Windows 7 that allows you to copy files while retaining their existing NTFS permissions. You can also use Robocopy.exe to move files from one volume to another while allowing them to retain their permissions. You should consider Robocopy.exe to be an exception to the normal rules of copying and moving files. In an exam situation, you should assume that the normal rules apply unless the question mentions Robocopy.exe. To use Robocopy.exe to copy all files and folders from the folder name C:\Example\ to the folder D:\Destination, use the command

```
Robocopy.exe c:\example d:\destination /copyall /e
```

#### **NOTE MOVING TO FAT VOLUMES**

If you move a file or folder to a volume formatted with the FAT or FAT32 file system, all NTFS permissions are lost.

## Combined Share and NTFS Permissions

When a user accesses a file hosted on a shared folder, both the share permissions, which you learned about in Lesson 1, and the NTFS permissions apply. The most restrictive permission of the share and the NTFS permissions apply. For example, if a group is assigned the Read permission at the Share level and the Modify permission through file and folder permissions, the user has only Read access to files and folders when connecting to the shared folder over the network. Similarly, if a user has Full Control access at the share level and Read access assigned to the folder through NTFS permissions, the user has only Read access and is unable to modify or delete files and folders hosted on the share.

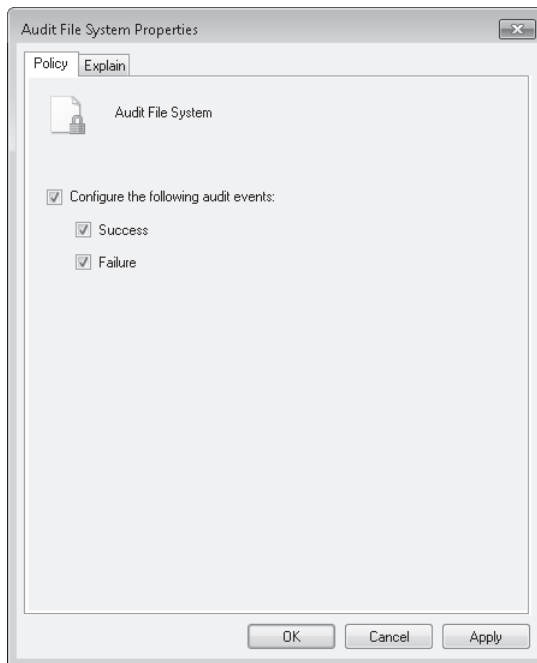
## Configuring Auditing

Auditing allows you to monitor which users and groups access specific files and folders. You most likely do not want to monitor who accesses every document in your organization; you are most likely to use auditing only on sensitive documents. For example, you would use auditing to track who accessed the spreadsheet containing employee salaries, but you would not use auditing to track who accessed the break room cleanup roster. Auditing can tell you who opened a document, who modified a document, and who tried to open a document and failed. You can audit the use of any of the special permissions listed in Table 8-2. You can perform auditing only on volumes that are formatted using the NTFS file system.

The audit policies in Windows 7 allow a greater degree of granularity in tracking audit events compared to the audit policies in previous versions of Windows. For example, in Windows XP, you could audit nine broad event categories: in Windows 7, there are 53 different event categories. This allows you to be more specific about the types of events you

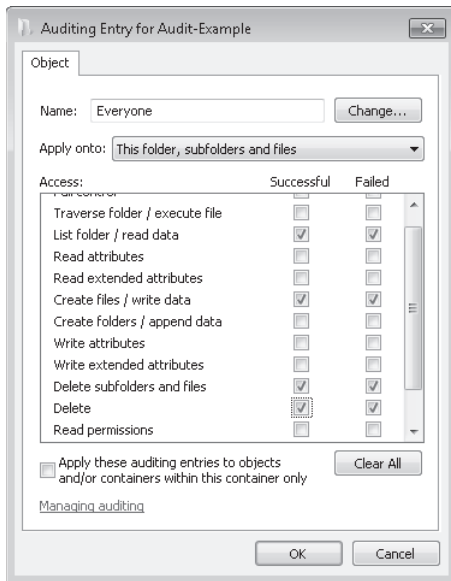
audit. To configure auditing to track which users access specific files and folders on clients running Windows 7, do the following:

1. Open the Local Group Policy Editor and navigate to the Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options node and set the Audit: Force Audit Policy Subcategory Settings (Windows Vista Or Later) To Override Audit Policy Category Settings policy to Enabled.
2. In the Local Group Policy Editor, navigate to the Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\Object Access Node and set the Audit File System policy, as shown in Figure 8-27.



**FIGURE 8-27** Configuring audit policies

3. Edit the properties of the file or folder that you wish to audit. On the Security tab, click Advanced, then click the Auditing tab, and then click Continue to elevate privileges.
4. Click Add and add the groups for which you want to audit access. If you want to audit the access of all users, select the Everyone group. Once you have selected the security group, you must select which of the special privileges you want to Audit. Figure 8-28 shows an auditing configuration to track successful file reads, writes, and deletes.
5. Auditing events will now be written to the Security log, which can be accessed using Event Viewer.



**FIGURE 8-28** Auditing entries

#### **MORE INFO** ADVANCED AUDIT POLICY

To learn more about the advanced auditing options that are available in Windows 7, consult the following TechNet Step-by-Step guide: [http://technet.microsoft.com/en-us/library/dd408940\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/dd408940(W.S.10).aspx).

#### **Quick Check**

- If you move a folder to a new location on the same volume, do the folder and its contents retain their original NTFS permissions?

#### **Quick Check Answer**

- Yes. When files or folders are moved to a new location on the same volume, they retain all their original NTFS permissions.

## Encrypting File System

*Encrypting File System (EFS)*, a technology available in the Professional, Enterprise, and Ultimate editions of Windows 7, allows for the encryption of individual files and folders. EFS differs from BitLocker To Go because BitLocker enables the encryption of full volumes and does not work directly at the file and folder level. For example, you can use BitLocker to encrypt a universal serial bus (USB) flash drive after you connect it to a client running

Windows 7, and all the files and folders hosted on that drive will be encrypted because the volume hosting them is encrypted. However, assuming that permissions are not configured restrictively, any files stored on that flash drive can be read by any user of that client running Windows 7 as the volume is encrypted to the client running Windows 7 and not any particular user of that client. EFS allows you to encrypt the files and folders stored on that USB flash drive to specific user accounts on the client running Windows 7. EFS encryption works so that even if a user has read access to a file, they cannot actually open the file unless they have the appropriate encryption certificate. You will learn more about BitLocker in Chapter 11.

EFS uses a process known as *public key encryption*. In public key encryption, a user has two keys: a public key, also known as a *certificate*, and a private key. The public key is kept in the computer's store and accessible to everyone. Users can use the public key to encrypt data. The private key is kept in the user's private certificate store and can only be used by the user. The private key decrypts data which has been encrypted using the public key. The first time a user encrypts a file on a computer running Windows 7, the computer creates an EFS certificate and private key.

#### **MORE INFO HOW EFS WORKS**

EFS certificates only indirectly encrypt files. During the file encryption process, the EFS certificate encrypts another key called the File Encryption Key (FEK). Each file has a unique FEK and the FEK is used to encrypt the target file or folder. Rather than encrypt the whole file multiple times when it needs to be encrypted to multiple keys, the file is encrypted once to the FEK and the FEK is encrypted multiple times, once to each EFS key. Any user that needs to access the encrypted file decrypts the FEK using their private key and then the FEK decrypts the file for access. To learn more about how EFS works, consult the following link on TechNet: <http://technet.microsoft.com/en-us/library/cc962103.aspx>.

You can use EFS only to encrypt files that are stored on volumes formatted with the NTFS file system. Because most USB flash drives come with volumes formatted using FAT32, this means that you need to format them with the NTFS file system prior to being able to use them to store EFS encrypted files and folders. When you encrypt a file or a folder, Windows Explorer displays it with green text rather than the standard black text.

When you encrypt a folder, Windows encrypts all files that you copy to that folder, and all new files that you create in that folder. EFS is not compatible with the file and folder compression feature of Windows 7. When you encrypt a file stored in a compressed folder, the file is decompressed prior to encryption and remains uncompressed while in its encrypted state. If you copy an encrypted file to a compressed folder, the file remains encrypted. If you move a compressed file to an encrypted folder, the file decompresses and encrypts. If you copy an EFS encrypted file or folder to a FAT32 volume, Windows 7 automatically decrypts the file when it is written to the destination volume.

You can use EFS to encrypt individual files to multiple users. When you do this, only users that the file is encrypted to are able to read the file contents. Even if other users have the appropriate NTFS permissions to open the file, they are unable to access the file's contents

because they are encrypted. You are able to encrypt a file to another user only if that user has an EFS certificate in the computer's store. If you want to encrypt a file to another user and are unable to locate their certificate, you need to get her to log on to the computer and encrypt a file. Once she does this, her EFS certificate is published to the computer store and you are able to use it to encrypt files to their account.

Although EFS allows you to encrypt individual files to multiple user accounts, it does not allow you to encrypt folders to multiple user accounts. It is also not possible to encrypt files to a group, only to multiple, but separate, individual users.

#### **NOTE EFS IN DOMAIN ENVIRONMENTS**

Active Directory Certificate Services allows the centralized management of EFS certificates in a domain environment. Because the 70-680 exam is primarily concerned with the client running Windows 7, so you will not need to be familiar with integrating EFS with AD DS.

## **EFS Recovery**

Recovery Agents are certificates that allow the restoration of EFS encrypted files. When a recovery agent has been specified using local policies, all EFS encrypted files can be recovered using the recovery agent private key. You should specify a recovery agent before you allow users to encrypt files on a client running Windows 7. You can recover all files that users encrypt after the creation of a recovery agent using the recovery agent's private key. You are not able to decrypt files that were encrypted before a recovery agent certificate was specified.

You create an EFS recovery agent by performing the following steps:

1. Log on to the client running Windows 7 using the first account created, which is the default administrator account.
2. Open a command prompt and issue the command  

```
Cipher.exe /r:recoveryagent
```
3. This creates two files: Recoveryagent.cer and Recoveryagent.pfx. Cipher.exe prompts you to specify a password when creating Recoveryagent.pfx.
4. Open the Local Group Policy Editor and navigate to the \Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System node. Right-click this node and then click Add Data Recovery Agent. Specify the location of Recoveryagent.cer to specify this certificate as the recovery agent.
5. To recover files, use the certificates console to import Recoveryagent.pfx. This is the recovery agent's private key. Keep it safe because it can be used to open any encrypted file on the client running Windows 7.

You can import the recovery agent to another computer running Windows 7 if you want to recover files encrypted on the first computer. You can also recover files on another computer running Windows 7 if you have exported the EFS keys from the original computer and imported them on the new computer. You can use the Certificates console to import and export EFS keys. You can also use Cipher.exe to back up EFS keys.



## EFS and HomeGroups

Sharing EFS-encrypted files in HomeGroup environments can be complicated because it requires that each computer in the HomeGroup has the same EFS certificates. In domain environments, it is possible to handle EFS certificates centrally through AD DS and Active Directory Certificate Services. No such central facility exists in HomeGroup environments. Even if users have the same local account names and passwords on each computer in the HomeGroup, each computer generates a unique EFS certificate pair.

If you want to share files encrypted using EFS amongst computers in a HomeGroup, get each user in the HomeGroup to encrypt a file on one computer and then get him to export their EFS keys to a removable USB flash drive using either the Certificates console or the Cipher.exe command. The keys should then be imported on the other computers running Windows 7 in the HomeGroup.

### **PRACTICE** Encryption and Permissions

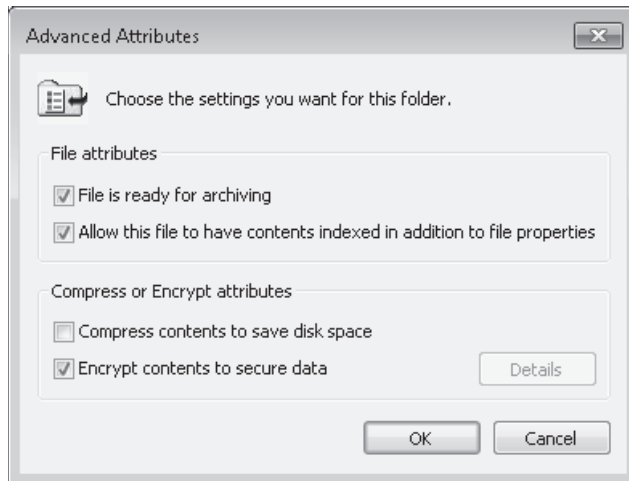
---

Although the EFS feature is included with several previous versions of Windows, not every user knows how to encrypt a file. Even experienced administrators have trouble remembering when NTFS permissions applied to files remain and when they are inherited in file move and copy scenarios. In this practice, you learn how to encrypt files and demonstrate to yourself how NTFS permissions are influenced during copy and move procedures.

#### **EXERCISE 1** Encrypting a Single File to Multiple Users

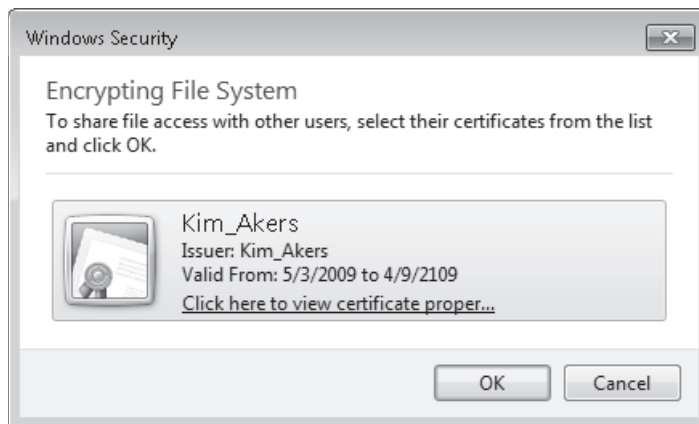
In this exercise, you create a text document and then encrypt it to two different user accounts. Because it is possible to encrypt a document to a user account only if that user account has an existing EFS certificate, the exercise requires you to encrypt a document using two different user accounts before you can encrypt a single document to both users.

1. Log on to computer Canberra with the Kim\_Akers user account.
2. Open the Control Panel and then click Add Or Remove User Accounts.
3. On the Manage Accounts page, click Create A New Account. Enter the account name Jeff\_Phillips, select Standard User, and then click Create Account.
4. On the Manage Accounts page, click the Jeff\_Phillips account and then click Create A Password. Enter the password **P@sswOrd** twice, and enter the page number of this page in the book as the password hint. Click Create Password. Close the Control Panel.
5. Right-click the Desktop, click New, and then click Folder. Name the folder **Encryption\_Test** and open it.
6. Right-click within the folder, click New, and then click Text Document. Name the document **Encrypt.txt**. Open the text document and enter the text **Configuring Windows 7**. Close the text document and save it.
7. Right-click Encrypt.txt and then choose Properties. On the General tab of the Encrypt.txt Properties dialog box, click Advanced. In the Advanced Attributes dialog box, select the Encrypt Contents To Secure Data check box, as shown in Figure 8-29. Click OK and then click Apply.



**FIGURE 8-29** Advanced Attributes

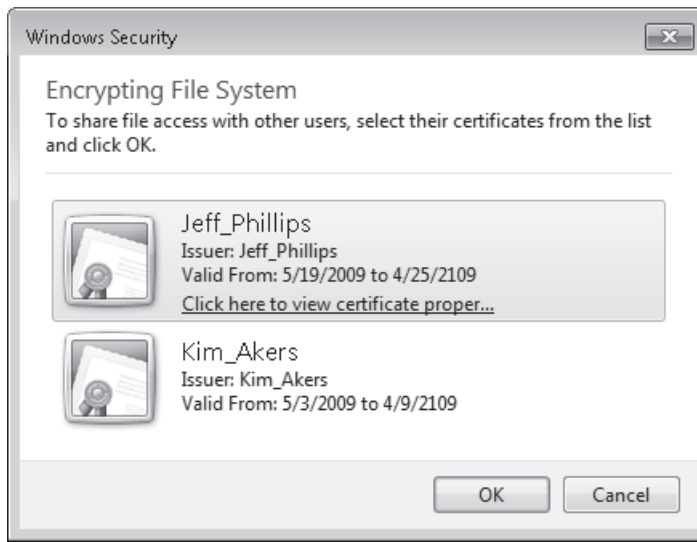
8. In the Encryption Warning dialog box, select the Encrypt The File Only check box and then click OK. The file is now encrypted.
9. On the General tab of the Encrypt.txt Properties dialog box, click Advanced. In the Advanced Attributes dialog box, click Details. In the User Access To Encrypt.txt dialog box, click Add.
10. In the Windows Security dialog box, shown in Figure 8-30, verify that the only certificate present is the one belonging to Kim\_Akers. Click OK.



**FIGURE 8-30** EFS certificate selection

11. On the Start menu, click the arrow next to Shut Down and then choose Switch User.
12. Log on using the Jeff\_Phillips user account.
13. Using the Jeff\_Phillips user account, perform steps 5 through 8 and then click OK to close the text file's Properties dialog box.

14. Log off as Jeff\_Phillips and resume the Kim\_Akers session. The User Access To Encrypt.txt dialog box should still be present on the screen because you switched to the other account and left the existing session active in memory.
15. In the User Access To Encrypt.txt dialog box, click Add. Verify that there are two encryption certificates present in the Windows Security dialog box. Click the Jeff\_Phillips certificate, as shown in Figure 8-31, and then click OK.



**FIGURE 8-31** Additional EFS certificate available

16. Click OK three times to close the Properties dialog box.

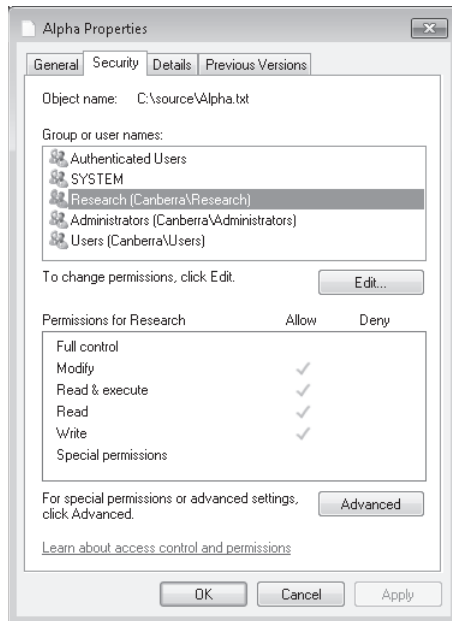
## **EXERCISE 2** Exploring File and Folder Permissions

In this exercise, you explore how file and folder permissions vary when you copy and move files between two folders. You use the Icacls and Effective Permissions tools during this exercise.

1. If you have not done so already, log on to Canberra using the Kim\_Akers user account.
2. Open an elevated command prompt and issue the following commands:

```
net localgroup Research /add
net localgroup Accounting /add
net localgroup Research Jeff_Phillips /Add
net localgroup Accounting Jeff_Phillips /Add
mkdir c:\source
mkdir c:\destination
icacls c:\source /grant Research:(OI)(CI)M
icacls c:\destination /grant Accounting:(OI)(CI)RX
icacls c:\destination /deny Jeff_Phillips:(OI)(CI)W
```

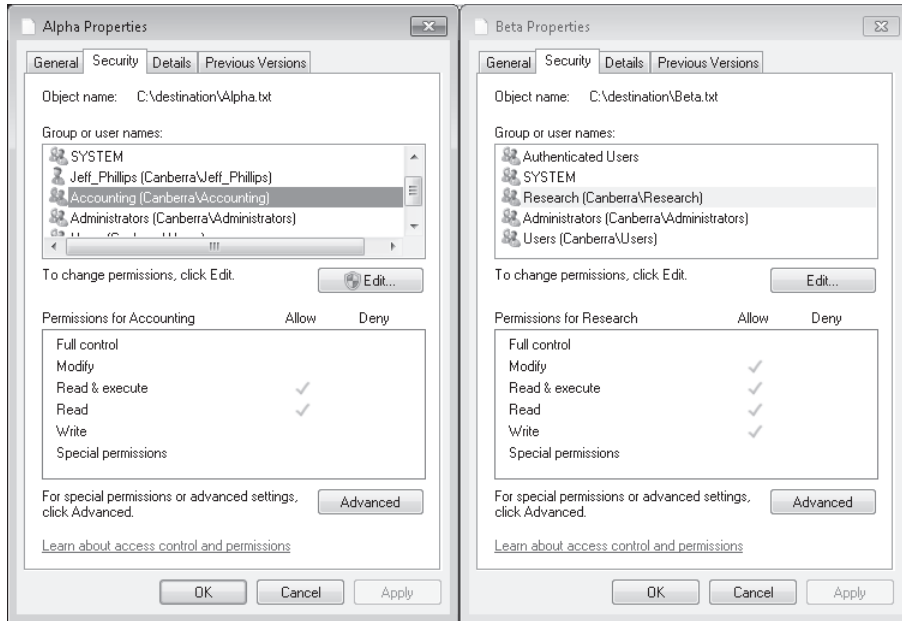
3. Open the C:\Source directory in Windows Explorer. Right-click within the folder and create two new text files named Alpha and Beta.
4. Right-click Alpha and then choose Properties. Click the Security tab and then click the Research group. Verify that the permissions are assigned as shown in Figure 8-32. Perform the same actions on Beta.txt to verify that permissions are set identically.



**FIGURE 8-32** Permissions for Research group on Alpha.txt

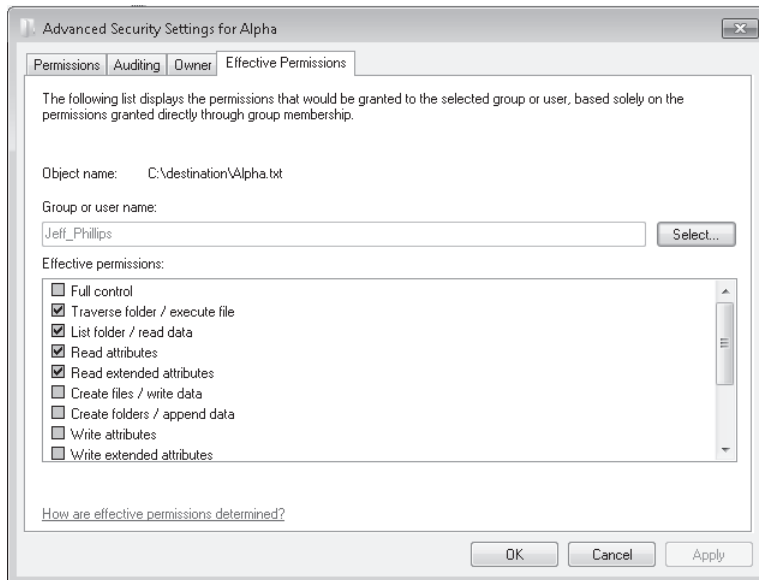
5. From the command prompt, issue the following commands:
 

```
copy c:\source\alpha.txt c:\destination
move c:\source\beta.txt c:\destination
```
6. View the properties of the file C:\Destination\Alpha.txt and compare it to the properties of C:\Destination\Beta.txt. Note that the permissions assigned to Beta.txt are the same as those prior to the move, but that the permissions of Alpha.txt have changed when the file is copied, specifically the Research and Accounting group permissions and the permissions for user Jeff\_Phillips, as shown in Figure 8-33.
7. Edit the properties of file Alpha, click the Security tab, and then click Jeff\_Phillips. Note that the Jeff\_Phillips account is assigned only the Write (Deny) permission.
8. Click Advanced. In the Advanced Security Settings dialog box, click the Effective Permissions tab.



**FIGURE 8-33** Permissions comparison

- Click Select. This opens the Select User Or Group dialog box. Enter the name Jeff\_Phillips and then click OK. Review the effective permissions of the Jeff\_Phillips user account, as shown in Figure 8-34. The permissions differ from those assigned to the user account because of permissions assigned through group membership.



**FIGURE 8-34** Determining effective permissions

## Lesson Summary

- The Icacls.exe utility can be used to manage NTFS permissions from the command line. You can use this utility to back up and restore current permissions settings.
- There are six basic NTFS permissions: Read, Write, List Folder Contents, Read & Execute, Modify, and Full Control. A Deny permission always overrides an Allow permission.
- You can use the Effective Permissions tool to calculate a user's effective permissions to a file or folder when she is a member of multiple groups that are assigned permission to the same resource.
- The most restrictive permission applies when attempting to determine the result of Share and NTFS permissions.
- Auditing allows you to record which files and folders have been accessed.
- When a file is copied, it inherits the permissions of the folder it is copied to. When a file is moved within the same volume, it retains the same permissions. When a file is moved to another volume, it inherits the permissions of the folder it is copied to.
- When you encrypt a file, it generates an EFS certificate and private key. You can encrypt a file to another user's account only if that user has an existing EFS certificate.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Folder and File Access." The questions are also available on the companion DVD 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 logged on to a computer running Windows 7 Enterprise that you share with Jeff Phillips. You want to store some files on an NTFS-formatted USB flash drive that both you and Jeff can access. You want to encrypt these files but do not want to use BitLocker To Go. You are able to encrypt the files, but when you try to add Jeff, you do not see his certificate listed. Which of the following should you do to allow you to use EFS to encrypt files to both your and Jeff's accounts?
  - A. Get Jeff to change his password.
  - B. Get Jeff to encrypt a file on the computer.
  - C. Give Jeff write permission to the files.
  - D. Let Jeff take ownership of the files.

2. Which of the following permissions are also set when you apply the Read & Execute (Deny) NTFS permission? (Choose all that apply.)
  - A. List Folder Contents (Deny)
  - B. Read (Deny)
  - C. Modify (Deny)
  - D. Write (Deny)
3. Jeff\_Phillips's user account is a member of four separate security groups that are each assigned different permissions to a folder on a client running Windows 7. Which of the following tools can you use to determine Jeff's permissions to a file hosted in that folder?
  - A. Robocopy
  - B. Icacls
  - C. Cipher
  - D. The Effective Permissions tool
4. The contents of the directory C:\Source are encrypted using EFS. The directory D:\Destination is compressed. Volumes C and D are both NTFS volumes. Which of the following happens when you use Windows Explorer to move a file named Example.txt from C:\Source to D:\Destination? (Choose all that apply; each answer forms part of a complete solution.)
  - A. Example.txt remains encrypted
  - B. Example.txt becomes compressed
  - C. Example.txt retains its original NTFS permissions
  - D. Example.txt inherits the NTFS permissions of the D:\destination folder
5. You want to have a record of which user accounts are used to access documents in a sensitive folder on a computer running Windows 7 Enterprise. Which of the following should you do to accomplish this goal?
  - A. Configure EFS
  - B. Configure auditing
  - C. Configure NTFS permissions
  - D. Configure BranchCache

## Lesson 3: Managing BranchCache

---

*BranchCache* is a technology that is new to Windows 7 and Windows Server 2008 R2 that speeds up branch office access to files and Web sites hosted on servers across WAN links. BranchCache works by caching content hosted on remote servers in a cache on the local area network (LAN). Rather than retrieving content across the slower WAN link, clients check the locally hosted cache to see if a copy of the data they are requesting is present. If it is present, and certain conditions are met, the client uses the cached copy. If the requested data is not present, the data is retrieved across the WAN link, stored in the local cache, and then accessed by the client. The advantage of BranchCache is that it stops the same file being transmitted multiple times across the WAN link and speeds up local access.

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

- Use Group Policy to configure BranchCache settings.
- Use *Netsh* to configure BranchCache settings.
- Understand the difference between BranchCache distributed cache mode and hosted mode.

**Estimated lesson time: 40 minutes**

## BranchCache Concepts

BranchCache is a feature that speeds up branch office access to files hosted on remote networks by using a local cache. Depending on which BranchCache mode is used, that cache is either hosted on a server running Windows Server 2008 R2 or in a distributed manner among clients running Windows 7 on the branch office network. The BranchCache feature is available only on computers running Windows 7 Enterprise and Ultimate editions. BranchCache can cache only data hosted on Windows Server 2008 R2 file and Web servers. You cannot use BranchCache to speed up access to data hosted on servers running Windows Server 2008, Windows Server 2003, or Windows Server 2003 R2.

BranchCache becomes active when the round-trip latency to a compatible server exceeds 80 milliseconds. Several checks occur when a client running Windows 7 uses BranchCache:

- The client checks if the server hosting the requested data supports BranchCache.
- The client checks if the round-trip latency exceeds the threshold value.
- The client checks the cache on the branch office LAN to determine whether the requested data is already cached.
  - If the data is cached already, a check is made to see if the data is up to date and whether the client has permission to access it.
  - If the data is not already cached, the data is retrieved from the server and placed in the cache on the branch office LAN.



Cache modes determine how the branch office cache functions. BranchCache can operate in one of two modes: Hosted Cache mode or Distributed Cache mode. You will learn about these modes during the rest of this lesson.

## Hosted Cache Mode

Hosted Cache mode uses a centralized local cache that is hosted on a branch office server running Windows Server 2008 R2. You can enable the hosted cache server functionality on a server running Windows Server 2008 R2 that you use for other functions without a significant impact on performance. This is because if you found that files hosted at another location across the WAN were being accessed so frequently that there was a performance impact, you would use a solution like Distributed File System (DFS) to replicate them to the branch office instead of using BranchCache. The advantage of Hosted Cache mode over Distributed Cache mode is that the cache is centralized and always available. Parts of the distributed cache become unavailable when the clients hosting them shut down. You will learn more about Distributed Cache mode later in this lesson.

Hosted Cache mode requires a computer running Windows Server 2008 R2 be present and configured properly in each branch office. You must configure each BranchCache client with the address of the BranchCache host server running Windows Server 2008 R2.

When setting up the Hosted Cache mode server, it is necessary to do the following:

- Install the BranchCache feature.
- Install an Secure Sockets Layer (SSL) certificate where the subject name is set to the fully qualified domain name (FQDN) of the hosted cache server. This involves importing the SSL certificate into the Local Computer's certificate store, making note of the certificate thumbprint, and then binding the certificate using the command 

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=<thumbprint> APPID={d673f5ee-a714-454d-8de2-492e4c1bd8f8}
```
- Ensure that all clients trust the certificate authority that issued the SSL certificate installed on the hosted cache server.

Hosted Cache mode is not appropriate for organizations that do not have their own Active Directory Certificate Services infrastructure or do not have the resources to deploy a dedicated server running Windows Server 2008 R2 to each branch office.

### **MORE INFO** CONFIGURING HOSTED CACHE SERVERS

To learn more about configuring a Windows Server 2008 R2 server as a hosted cache server, including how to change the default ports used, consult the following document on TechNet: [http://technet.microsoft.com/en-us/library/dd637793\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd637793(WS.10).aspx).

## Distributed Cache Mode

Distributed Cache mode uses peer caching to host the branch office cache among clients running Windows 7 on the branch office network. This means that each Distributed Cache mode client hosts part of the cache, but no single client hosts all the cache. When a client running Windows 7 retrieves content over the WAN, it places that content into its own cache. If another BranchCache client running Windows 7 attempts to access the same content, it is able to access that content directly from the first client rather than having to retrieve it over the WAN link. When it accesses the file from its peer, it also copies that file into its own cache.

The advantage of distributed cache mode is that you can deploy it without having to deploy a server running Windows Server 2008 R2 locally in each branch office. The drawback of Distributed Cache mode is that the contents of the cache available on the branch office LAN depend on which clients are currently online. If a client needs a file that is held in the cache of a computer that is shut down, the client needs to retrieve the file from the host server across the WAN.



### Quick Check

- Which BranchCache mode should you use if there are no servers running Windows Server 2008 R2 at your branch office?

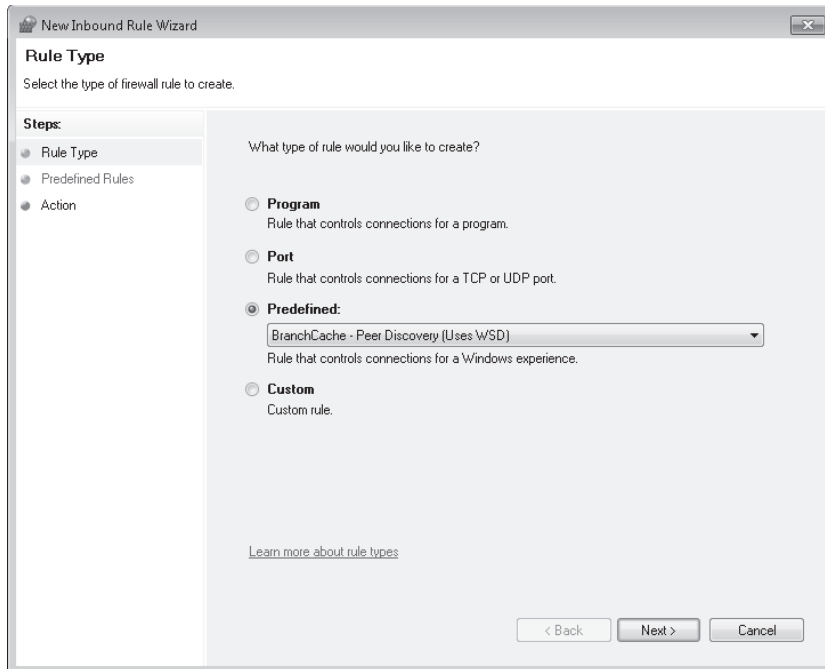
### Quick Check Answer

- You should use Distributed Cache mode. Hosted Cache mode requires a server running Windows Server 2008 R2 on the LAN.

## Configuring BranchCache Clients Running Windows 7

Configuring Windows 7 as a BranchCache client involves enabling BranchCache, selecting either Hosted Cache mode or Distributed Cache mode, and then configuring the client firewall to allow BranchCache traffic. You can configure BranchCache either using Group Policy or by using the *Netsh* command-line utility. The firewall rules that you configure depend on whether you are using Hosted Cache or Distributed Cache mode. You can use predefined firewall rules or manually create them based on protocol and port. The required firewall rules are as follows:

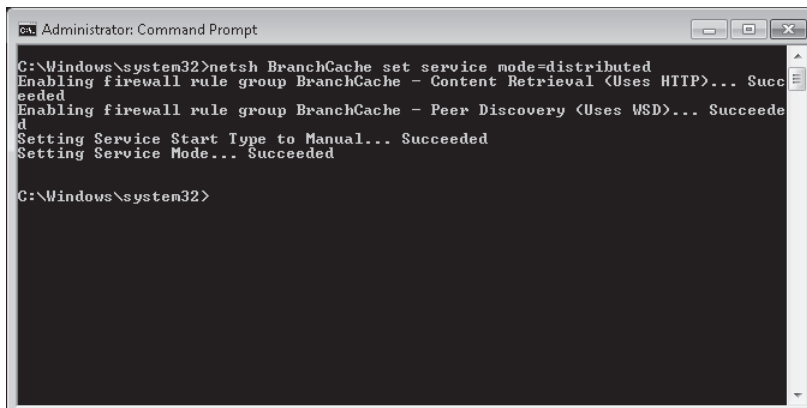
- The BranchCache – Content Retrieval (Uses HTTP) predefined rule. If this rule is not available, create rules that allow inbound and outbound traffic on TCP port 80. This rule is required for both Hosted Cache and Distributed Cache mode. You can create this rule using Windows Firewall With Advanced Security, as shown in Figure 8-35.



**FIGURE 8-35** Predefined BranchCache firewall rule

- The BranchCache – Peer-Discovery (Uses WSD) predefined rule. If this rule is not available, create rules that allow inbound and outbound traffic on UDP port 3702. This rule is only required when using Distributed Cache mode.
- The BranchCache – Hosted Cache Client (HTTPS-Out) predefined rule. If this rule is not available, configure a rule that allows outbound traffic on TCP port 443. This rule is required only when using Hosted Cache mode.

You need to configure the firewall rules only when you configure BranchCache using Group Policy. When you configure BranchCache using *Netsh*, the appropriate firewall rules are set up automatically, as shown in Figure 8-36.



**FIGURE 8-36** Firewall rules automatically configured

## Configuring BranchCache Using Group Policy

BranchCache can be configured using *Netsh* or through Group Policy. You are more likely to use Group Policy when you want to apply the same settings to a large number of computers. To configure BranchCache on clients running Windows 7 using Group Policy, open the Local Group Policy Editor and navigate to the Computer Configuration\Administrative Templates\Network\BranchCache node. As Figure 8-37 shows, there are five BranchCache-related policies.

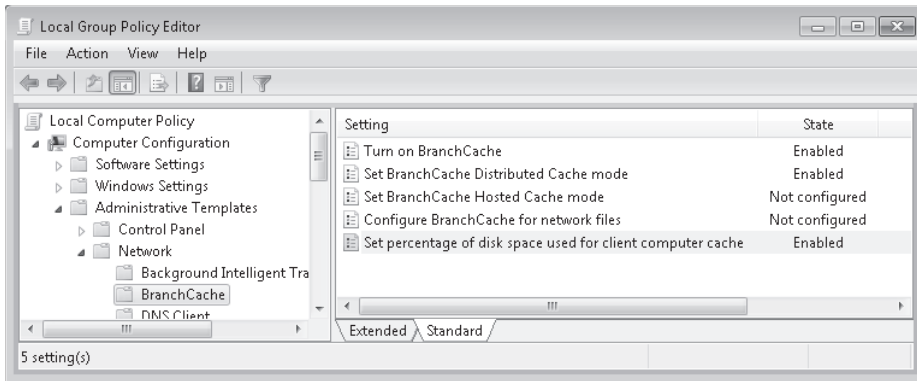
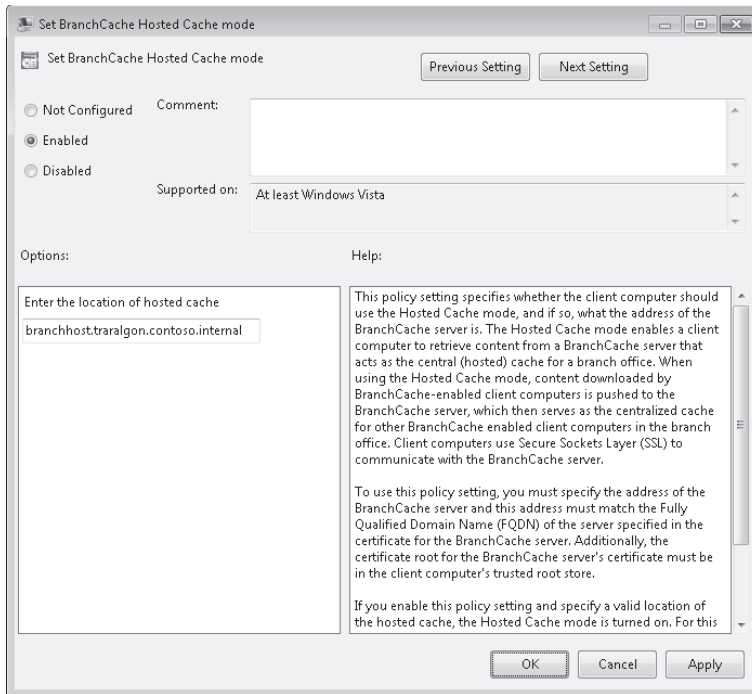


FIGURE 8-37 BranchCache policies

These policies have the following functions:

- **Turn On BranchCache** This policy enables BranchCache and configures the BranchCache service to start manually. Windows starts the service when you make an attempt to access data on a compatible remote server that exceeds the round-trip latency threshold.
- **Set BranchCache Distributed Cache Mode** This policy sets the client to use Distributed Cache mode. For this policy to work, you must also have enabled the Turn On BranchCache policy.
- **Set BranchCache Hosted Cache Mode** This policy sets the client to use Hosted Cache mode. When configuring this policy, as shown in Figure 8-38, it is necessary to specify the location of the host cache server by FQDN. The SSL certificate installed on the server must match the FQDN and the client must trust the issuing certificate authority. For this policy to work, you must also enable the Turn On BranchCache policy.
- **Configure BranchCache For Network Files** This policy allows you to specify the round-trip latency value that triggers the use of BranchCache. If you do not configure this policy, the default value is 80 milliseconds. You only need to configure this policy if the default value of 80 milliseconds is inappropriate for your organization's network environment.
- **Set Percentage Of Disk Space Used For Client Computer Cache** This policy allows you to set a custom amount of total disk space the computer uses to store BranchCache files. Other clients on the branch office network are able to access this content if the Distributed Cache mode is used. If you do not enable this policy, the cache size defaults to 5% of the total disk space of the client computer.



**FIGURE 8-38** BranchCache Hosted Cache Mode policy

## Configuring BranchCache Using *Netsh*

You can use *Netsh* in the BranchCache context to configure and diagnose problems with BranchCache. There are several options that you can configure using *Netsh*, such as the local caching option, that are not available when you configure BranchCache using Group Policy. Another advantage of using *Netsh* to configure BranchCache is that it automatically enables the relevant firewall rules for each caching mode. When you use Group Policy to enable BranchCache, you must also configure appropriate firewall rules. You learned about these firewall rules earlier in this lesson.

You must run all *Netsh* BranchCache configuration commands, except for the *show status* command, from an elevated command prompt. You can use the following commands to configure BranchCache:

- ***Netsh BranchCache reset*** This command resets the current BranchCache configuration, disabling and stopping the service, resetting the registry defaults, deleting any cache files, and setting the service start type to Manual. This command also disables any configured BranchCache firewall rules.
- ***Netsh BranchCache show status*** This command displays the current service mode, including whether that service mode is configured using Group Policy, and displays the current status of the BranchCache service.
- ***Netsh BranchCache set service mode=distributed*** This command sets the client to use the Distributed Cache mode, starts the BranchCache service, and changes the

startup type to Manual. It also enables the BranchCache - Content Retrieval (Uses HTTP) and BranchCache – Peer Discovery (Use WSD) firewall rules.

- **Netsh BranchCache set service mode=local** This command sets the client to use the local cache mode, starts the BranchCache service, and changes the startup type to Manual. It does not enable any firewall rules. When you set the local caching mode, the client stores files retrieved over the WAN in a local cache but does not share the contents of that cache with any other clients on the branch office network. It is only possible to set this mode using *Netsh*.
- **Netsh BranchCache set service mode=hostedclient location=hostedserver** This command sets the client to use the Hosted Cache mode, specifies the location of the hosted cache server, starts the BranchCache service, and changes its startup type to Manual. It also enables the BranchCache - Content Retrieval (Uses HTTP) and BranchCache – Hosted Cache Client (Uses HTTPS) firewall rules.
- **Netsh BranchCache set cachesize** This policy allows you to set the size of the local cache. You can do this as a percentage of hard disk space or by specifying a number of bytes.
- **Netsh BranchCache set localcache** This policy allows you to set the location of the local cache.

Configuration settings applied using Group Policy override settings applied using *Netsh*.

## Verifying the State of the BranchCache Service

You can verify the state of the BranchCache service, which must be operational for BranchCache to function, using the Services console. You can open this console by typing **services.msc** into the Search Programs And Files box on the Start menu. To view the properties of the service, double-click the BranchCache service. Verify that the service is started and the startup type is set to Manual, as shown in Figure 8-39.

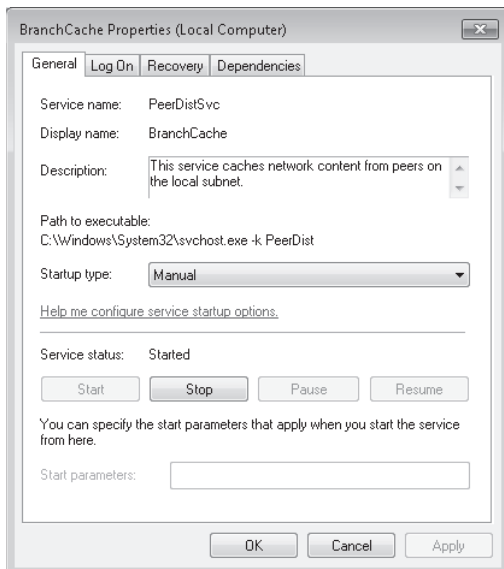
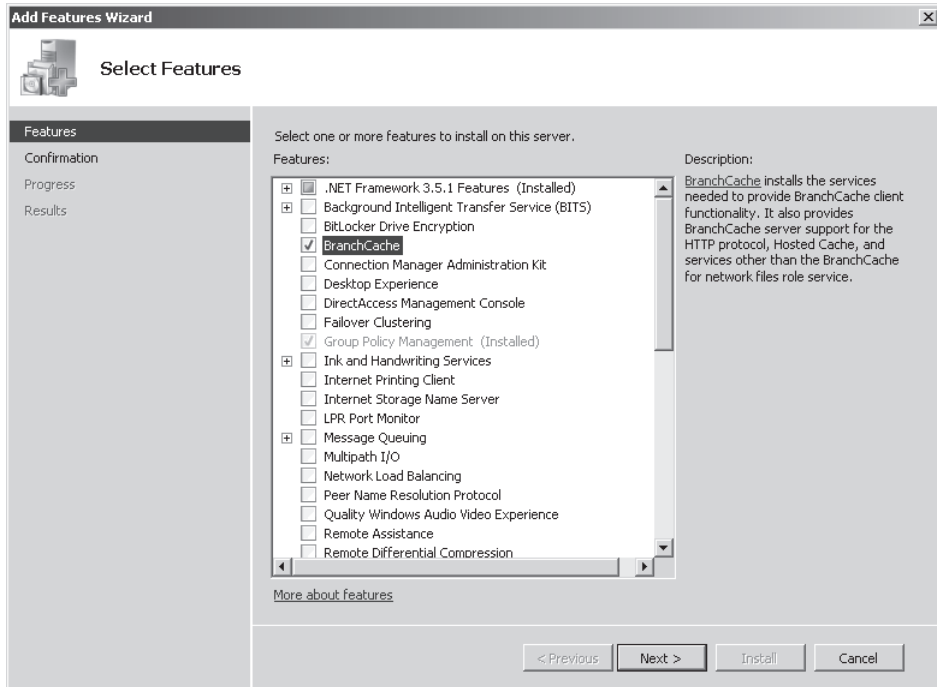


FIGURE 8-39 BranchCache service status

# Configuring File and Web Servers Running Windows Server 2008 R2

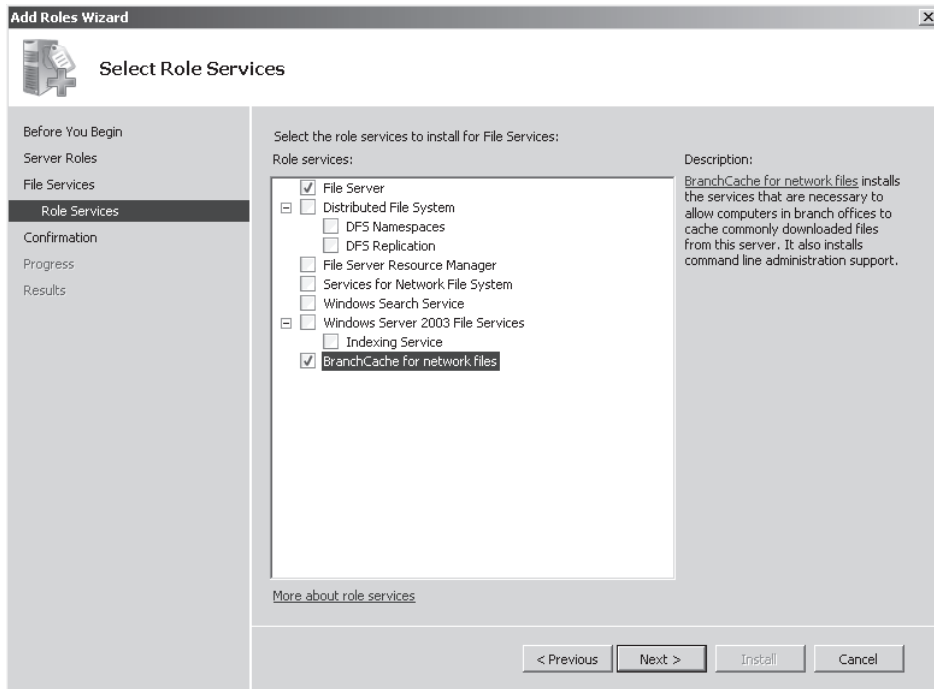
BranchCache works only when retrieving data hosted on Web and file servers running Windows Server 2008 R2. To configure a server to support BranchCache, perform the following steps:

1. Install the BranchCache feature on the server running Windows Server 2008 R2 using the Add Features Wizard, as shown in Figure 8-40. The Web server role of Windows Server 2008 R2 automatically uses BranchCache after you install the BranchCache feature.



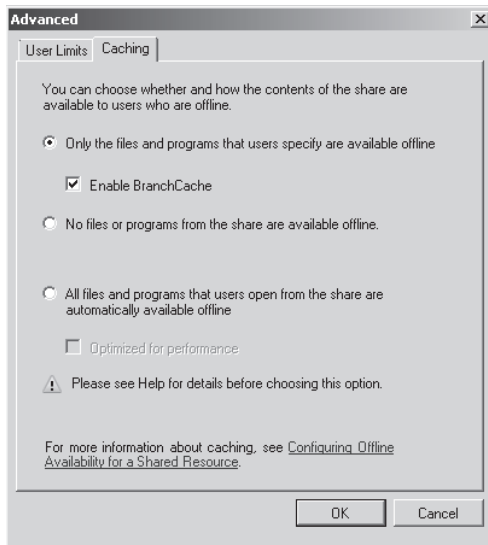
**FIGURE 8-40** Installing the BranchCache feature on Windows Server 2008 R2

2. When adding the File Server Role, ensure that you add the BranchCache For Network Files Role service, as shown in Figure 8-41.
3. Edit the Computer Configuration\Administrative Templates\Network\Lanman Server\Hash Publication for BranchCache policy. Enable the policy and select one of the following options:
  - Allow Hash Publication Only For Shared Folders On Which BranchCache Is Enabled
  - Allow Hash Publication For All Shared Folders



**FIGURE 8-41** Installing BranchCache for Network Files

4. If you choose to enable BranchCache only on selected shared folders, use the Share And Storage Management console on the file server running Windows Server 2008 R2 to edit the properties of the share that you want to use with BranchCache, and then click Advanced. In the Advanced dialog box, enable BranchCache, as shown in Figure 8-42.



**FIGURE 8-42** Enabling BranchCache on each share



### **MORE INFO** CONFIGURING SERVERS TO SUPPORT BRANCHCACHE

To learn more about configuring Windows Server 2008 R2 to support BranchCache, consult the following TechNet document: [http://technet.microsoft.com/en-us/library/dd637785\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/dd637785(W.S.10).aspx).



### **EXAM TIP**

Remember the syntax of the *netsh branchcache set service* command and that it configures the BranchCache service and firewall rules automatically.

## **PRACTICE** BranchCache Configuration

BranchCache can use the Distributed Cache mode to share a cache of remote files and Web server data among clients running Windows 7 on a branch office network. Distributed Cache mode can be configured using Group Policy or by using the *Netsh* command-line utility.

### **EXERCISE** Configuring BranchCache

In this exercise, you use the *Netsh* command-line utility to configure the BranchCache client settings of a computer running Windows 7. To complete this practice, perform the following steps:

1. Log on to computer Canberra using the Kim\_Akers user account.
2. Open an elevated command prompt.
3. Issue the following command:  

```
Netsh BranchCache show status
```
4. Verify that the service mode is set to disabled and the current status of the service is stopped.
5. Issue the following command:  

```
Netsh BranchCache set service mode=distributed
```
6. Verify that the status message indicates that two firewall rules have been enabled and the service startup type has been set to Manual.
7. Issue the following command:  

```
Netsh BranchCache show status
```
8. Verify that the service mode is set to Distributed Caching and the current status of the service is running.
9. Issue the following command:  

```
Netsh BranchCache set cachesize size=25 percent=True
```

10. Issue the following command:

```
Netsh BranchCache show localcache
```

11. Verify that the maximum cache size is set to 25% of hard disk.

12. Issue the following command:

```
Netsh BranchCache reset
```

## Lesson Summary

- BranchCache is a technology that allows files hosted on remote file servers running Windows Server 2008 R2 to be cached on a branch office network.
- Only Windows 7 Enterprise and Ultimate editions support BranchCache.
- Distributed Cache mode shares the cache among clients running Windows 7.
- Hosted Cache mode requires that a specially configured server running Windows Server 2008 R2 be present on the branch office network.
- When you enable Distributed Cache mode or Hosted Cache mode using *Netsh*, the BranchCache service and firewall rules are configured automatically.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 3, "Managing BranchCache." The questions are also available on the companion DVD 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 use BranchCache's hosted cache mode in your organization's branch offices. You have enabled BranchCache on your organization's head office servers. Which of the following steps must you take to accomplish this goal? (Choose all that apply; each answer forms part of a complete solution.)
  - A. Deploy at least one server running Windows Server 2008 R2 to each branch office.
  - B. Upgrade all branch office client computers to Windows 7 Enterprise.
  - C. Upgrade all branch office client computers to Windows 7 Professional.
  - D. Deploy at least one Windows Server 2008 Read-Only Domain Controller (RODC) to each branch office.

2. Which of the following tools can you use to configure a group of clients running Windows 7 to use BranchCache in peer caching mode? (Choose all that apply.)
- A. *Net share*
  - B. *Netsh*
  - C. *Ipconfig*
  - D. Local Group Policy Editor
3. You have two computers running Windows 7 Ultimate at one of your organization's branch office locations. All servers in this branch office use Windows Server 2008 R2. You want to configure one of these computers to cache content that it retrieves from a file server running Windows Server 2008 R2 located on the head office network. This file server has the name *fs-alpha.contoso.internal*. The data hosted on this file server is sensitive. The computer you are configuring should not provide cached content to the other computer running Windows 7 Ultimate on the network. Which of the following commands would you use to configure this computer?
- A. `netsh branchcache set service disabled`
  - B. `netsh branchcache set service mode=distributed`
  - C. `netsh branchcache set service mode=local`
  - D. `netsh branchcache set service mode=hostedclient location=fs-alpha.contoso.internal`
4. You want to configure clients running Windows 7 Enterprise in a branch office to use BranchCache in Hosted Cache mode. A server running Windows Server 2008 R2 named *branch-1.contoso.internal* functions as the host on the LAN. Which of the following commands, issued from an elevated command prompt, should you use to configure the clients running Windows 7?
- A. `netsh branchcache set service mode=distributed`
  - B. `netsh branchcache set service mode=local`
  - C. `netsh branchcache set service mode=hostedserver clientauthentication=domain`
  - D. `netsh branchcache set service mode=hostedclient location=branch-1.contoso.internal`
5. You want to configure clients running Windows 7 Enterprise in a branch office to use BranchCache only if the round-trip network latency when attempting to access files hosted over the WAN exceeds 120 ms. Which of the following policies should you configure to accomplish your goal?
- A. Configure BranchCache For Network Files
  - B. Set Percentage Of Disk Space Used For Client Computer Cache
  - C. Set BranchCache Distributed Cache Mode
  - D. Set BranchCache Hosted Cache Mode

## 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

---

- HomeGroups allow for the sharing of resources on home networks.
- You can manage shared folders centrally using the Computer Management console.
- Libraries are virtual collections of folders that host similar content.
- NTFS permissions determine which files a user or group can access on a computer.
- Print permissions determine what rights a user has to manage a printer or documents.
- BranchCache is a technology that speeds up branch office access to files in remote locations through the caching of previously accessed files on the branch office 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.

- **BranchCache**
- **Encrypting File System (EFS)**
- **HomeGroup**
- **library**

## Case Scenarios

---

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

## Case Scenario 1: Permissions and Encryption

A computer running Windows 7 Enterprise named Waverley has two NTFS-formatted volumes, volume C and volume D. The folder C:\Share is shared and has 15 subfolders and hundreds of files. Many of these folders have unique NTFS permissions. You want to move this folder so that it is hosted on volume D because volume C is running out of space. One of the users of computer Waverley will be changing to computer Warrandyte. This user has copied a large number of EFS-encrypted files onto a NTFS-formatted USB flash device.

With these facts in mind, answer the following questions:

1. What steps can you take so that the user is able to read the encrypted files on the USB flash device on computer Warrandyte?
2. What steps can you take to ensure that it is possible to recover all files that are encrypted in future?
3. What steps can you take to move the shared folder to volume D?

## Case Scenario 2: Configuring Contoso Branch Offices

You are trying to make the use of WAN bandwidth between Contoso's head office in Melbourne and branch offices in Wangaratta and Traralgon more efficient. All client computers at Contoso have Windows 7 Enterprise installed. Users turn their computers on and off during the day. If possible, you want to store any BranchCache data so that it is always available. There is a Windows Server 2008 R2 RODC at the Traralgon site named `rodc.traralgon.contoso.internal`, and there is a Windows Server 2008 RODC named `rodc.wangaratta.contoso.internal` at the Wangaratta site. You do not plan on upgrading any server operating systems in the near future.

With these facts in mind, answer the following questions:

1. Which BranchCache mode should you use at the Wangaratta branch office?
2. Which BranchCache mode should you use at the Traralgon branch office?
3. What steps do you need to take to prepare server `rodc.traralgon.contoso.internal` to support BranchCache?

## Suggested Practices

---

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

### Configure Shared Resources

Perform this practice when logged on to computer Canberra with the `Kim_Akers` user account.

- Configure a shared printer. Create a local group named PrinterManagers and assign the Manage Printers permission to this group.

## Configure File and Folder Access

Perform both of these practices when logged on to computer Canberra with the Kim\_Akers user account.

- **Practice 1** Use Gpedit.msc and Cipher.exe to configure and assign an EFS recovery agent certificate.
- **Practice 2** Create a file named Gamma.txt. Use Icacls.exe to assign the Modify (Deny) permission to the file. Use Robocopy.exe to copy Gamma.txt to a new folder while retaining its original permissions.

## Configure BranchCache

Perform this practice when logged on to computer Canberra with the Kim\_Akers user account.

- Configure computer Canberra using the *Netsh* command to use local caching only.

## Take a Practice Test

---

The practice tests on this book's companion DVD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-680 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 section entitled "How to Use the Practice Tests," in the Introduction to this book.

# Monitoring and Performance

This chapter looks at monitoring resources and performance on a computer running Windows 7. It considers the various tools that tell you what resources are available on a computer and report problems encountered in using a resource. The chapter discusses performance monitoring, establishing baselines and logs, and determining where bottlenecks might occur before they happen. It looks at checking the potential of the computer to perform resource-intensive tasks and how to capture both local events and events on other computers.

Sometimes services, processes, and applications encounter problems and the chapter considers how you can deal with them. Sometimes the tools provided by the operating system are not exactly what you require, and the chapter looks at how you can create standard scripts to address any problems you encounter without requiring a high level of programming expertise.

You need to manage and configure services, configure page files and memory cache, configure services, manage processes, configure your desktop, and, if necessary, change your boot environment. The chapter discusses all these requirements.

## Exam objectives in this chapter:

- Monitor systems.
- Configure performance settings.

## Lessons in this chapter:

- Lesson 1: Monitoring Systems **649**
- Lesson 2: Configuring Performance Settings **689**

## Before You Begin

---

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

- Installed the Windows 7 operating system on a stand-alone client PC, as described in Chapter 1, “Install, Migrate, or Upgrade to Windows 7.” You need Internet access to complete the exercises.
- Optionally installed Windows 7 on a second PC, as described in Chapter 6, “Network Settings.” A second computer is not required for the practice exercises but will enable you to complete the suggested practices at the end of this chapter.
- If you have two physical computers that are not otherwise on the same network, you need to connect their Ethernet ports with a crossover cable or by using an Ethernet switch.
- You need a universal serial bus (USB) flash memory device with at least 200 MB usable free space, or a second internal or external hard disk.
- The computer you use for the practice exercises (Canberra) needs to have an optical drive that can write to DVD-ROM.



### **REAL WORLD**

Ian McLean

**Y**ou can usually justify a server upgrade to management, even though many managers don't know what a server is.

There aren't many servers. With virtualization, they are fewer than ever before. They are mysterious black boxes that do incomprehensible things. If the network administrator says the servers need an upgrade, the expense probably isn't huge in the general scheme of things.

Senior managers may not typically be technically aware (when you find one that is, it can be scary) but they are emphatically not fools, especially where money is concerned. You can justify extra cash to upgrade half a dozen servers. When it comes to upgrading 500 workstations, it's a different ball game.

So gathering performance statistics about your workstations is just as important as gathering them about your servers. You can have the fastest servers on the market, but if your client computers aren't up to the job, you have a poorly performing network. Even the thinnest of thin clients have bottlenecks, especially when it comes to network resource.

You will need to upgrade your hardware, if not right now, then in a year or two. Start preparing your case. Ensure that you have defined sensible baselines. Keep track of the small but cumulative performance drops as your equipment ages and user expectations increase. Start preparing a good case right now for the upgrades you need in the future. Don't wait for tomorrow, or else tomorrow somebody else might be doing your job.



# Lesson 1: Monitoring Systems

---

As an IT professional with at least one year's experience, you will have come across some of, if not all, the tools and utilities described in this lesson. Windows 7 offers tools to measure performance, set baselines, identify bottlenecks, display resources, measure system stability and reliability, and so on.

It is sometimes not easy to select the right tool for the job. Often you can use several tools to obtain the same information or carry out the same configuration, but one of them does it more efficiently than the others. It is relatively straightforward to use one or more tools to gather information about a computer system. Interpreting that information may be more difficult. This lesson attempts to split the various tools into different functional groups and describe how the tools in each group complement each other.

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

- Use performance tools to view real-time performance data, collect data in Data Collector Sets (DCSs), and generate reports that identify actual or potential resource bottlenecks.
- Examine failures and potential problems related to software installations and other significant system changes.
- Gather event subscriptions from source computers and store them on a destination computer.
- Access the Windows Experience Index and choose computer software based on that index.

**Estimated lesson time: 50 minutes**

## Performance Monitoring and Reporting

Monitoring performance data and comparing it to established baselines is crucial to determining the health of your client computers, as is examining events in the event logs. Many events are informational, but you should not ignore them because of that. Your skill and experience as an administrator must determine what you should address and what you can safely ignore. You should never ignore warning and error events that indicate real and immediate problems.

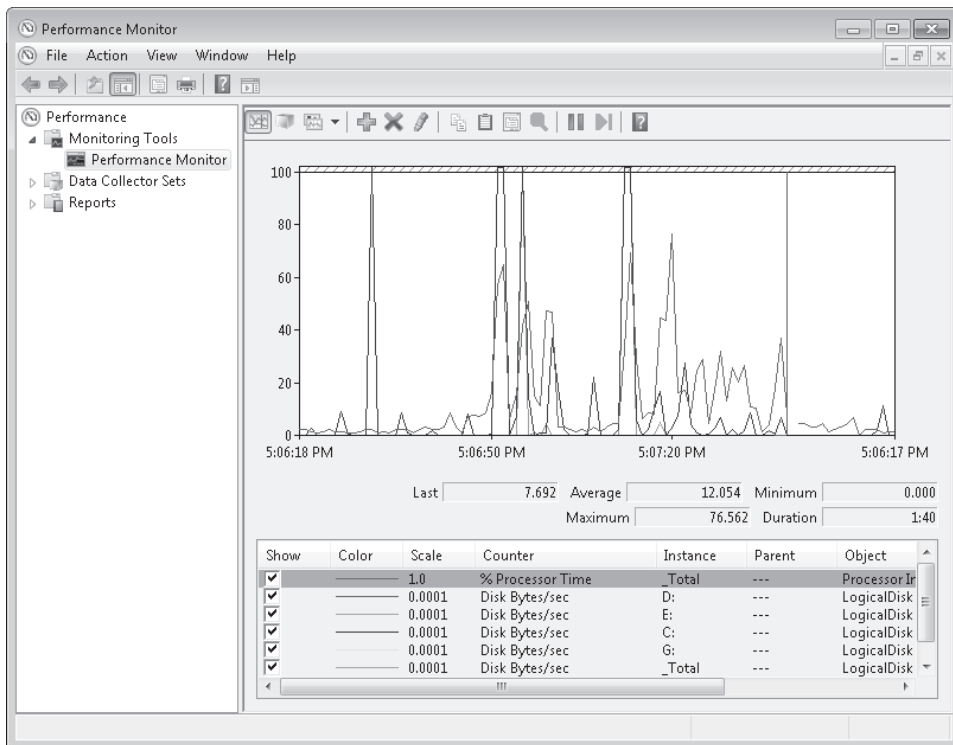
As an IT professional, you probably have experience with Windows performance tools such as Performance Monitor and the Reports tool. You might not be familiar with DCSs that use performance counters to generate performance logs and can, in turn, be read by Performance Monitor and the Reports tool. DCSs provide a replacement for Performance Logs and Alerts in earlier operating systems.

Your aim is to monitor and improve performance, identify potential bottlenecks, and upgrade the appropriate resources. You especially want to identify sources of critical performance problems that could make a computer unacceptably slow or completely unusable.

## Performance Monitor

In Windows 7, you can open Performance Monitor by accessing Control Panel, specifying All Control Panel Items, selecting Performance Information And Tools, clicking Advanced Tools in the Performance Information And Tools window, and clicking Open Performance Monitor. However it is easier to type **perfmon** in the Start menu search box (or at a command prompt). The Performance dialog box lets you access Performance Monitor, DCSs, and the Reports tool. Select Performance Monitor on the tree pane.

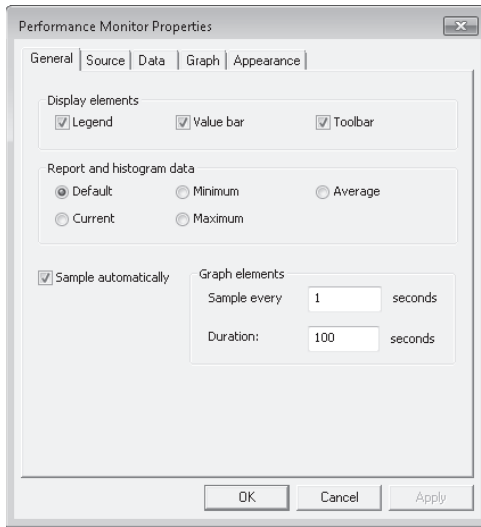
You can add counters by clicking the green + button on the Performance Monitor toolbar, expanding the object (such as Memory), selecting the counter, and clicking Add. You can specify whether you want to display a single instance of a counter or a total of all instances. For example, if a computer has more than one CPU, you could select a counter that monitors the usage of a single CPU or a counter that monitors total CPU usage. Figure 13-1 shows Performance Monitor displaying real-time data.



**FIGURE 13-1** Performance Monitor displaying real-time data

Each line on the graph appears in a different color. To make it easier to view a specific graph, select its counter and press Ctrl+H. The selected counter appears bold and in black on the graph. To change the appearance and refresh rate of the chart, right-click Performance Monitor and then select Properties. The five tabs of the Performance Monitor Properties dialog box provide access to different configuration options, as follows:

- **General** In the Graph Elements group, you can adjust the Sample Every box to change how frequently the graph updates. You can also specify whether the Legend, Value Bar, and Toolbar are displayed and whether the Report and Histogram views show Default, Maximum, Minimum, Average, or Current values. Figure 13-2 shows the General tab.



**FIGURE 13-2** The General tab of Performance Monitor Properties

- **Source** On this tab, you can choose whether to display current activity in real time or show log files that you have saved using a DCS
- **Data** On this tab, in the Counters list, select the counter that you want to configure and adjust Color, Width, and Style.
- **Graph** By default, Performance Monitor begins overwriting graphed counter values on the left portion of the chart after the specified duration is reached. If you want to record counter values over a long period of time, you likely want to see the chart scroll from right to left. To do this, select the Scroll style. You can also select one of the following chart types by clicking the Change Graph Type button on the toolbar or by pressing Ctrl+G:
  - **Line** This is the default setting and shows values as lines on the chart.
  - **Histogram** This shows a bar graph with the current, maximum, minimum, or average counter values displayed. If you have a large number of counters, a histogram is easier to read than a line chart.
  - **Report** This lists the current, maximum, minimum, or average counter values in a text report.
- **Appearance** If you keep multiple Performance Monitor windows open simultaneously, you can use this tab to change the color of the background or other elements.



### Quick Check

1. On which tab of the Performance Monitor Properties dialog box can you specify how often the graphs update?
2. Which rights does a user need to be able to monitor performance data remotely?

### Quick Check Answers

1. On the General tab, in the Graph Elements group, you can adjust the Sample Every box to change how frequently the graph updates.
2. At a minimum, the user's account must be a member of the Performance Log Users group and the Event Log Readers group on the remote computer.

## Data Collector Sets

*Data collector sets (DCSs)* gather system information, including configuration settings and performance data, and store it in a data file. You can use Performance Monitor to examine the data file and analyze detailed performance data, or you can generate a report that summarizes this information.

Windows 7 includes the following built-in DCSs:

- **System Performance** You can use this DCS when troubleshooting a slow computer or intermittent performance problems. It logs processor, disk, memory, and network performance (Internet Protocol versions 4 and 6) counters and kernel trace data.
- **System Diagnostics** You can use this DCS when troubleshooting reliability problems such as problematic hardware, driver failures, or STOP errors. It logs all the information included in the System Performance DCS, plus detailed system information. Figure 13-3 shows some of the counters included in the System Diagnostics data set.

To use a DCS, right-click it and then select Start. The System Performance DCS has a default overall duration of 1 minute. The System Diagnostics DCS collector set has a default overall duration of 10 minutes. To stop a DCS manually, right-click it and then click Stop.

After running a DCS, you can view a summary of the data that it has gathered in the *Performance Monitor\Reports* node. To view the most recent report for a DCS, right-click the DCS and then click *Latest Report*. You can then view the report by accessing it in the *Reports* node, as shown in Figure 13-4.

You can also add performance counter alerts to DCSs. This enables you to monitor and detect an alert, which you can then use to start a batch file, send you an e-mail, or call you on a pager. For example, if you configured an alert to trigger when free space on a logical volume falls below 30 percent, you could add this to a DCS and use it to trigger a batch file that archives the data on the volume.

The screenshot shows the Performance Monitor window with the 'System Diagnostics' data set selected in the left-hand tree. The main pane displays a list of system components and their associated data types and output paths.

Name	Type	Output
NT Kernel	Trace	C:\perflogs\System\Diagnosics\CANBERRA_
Operating System	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Processor	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
System Services	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Logical Disk Dirty Test	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
SMART Disk Check	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
AntiSpywareProduct	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
FirewallProduct	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
AntiVirusProduct	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
UAC Settings	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Windows Update Settings	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Performance Counter	Performance Counter	C:\perflogs\System\Diagnosics\CANBERRA_
BIOS	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Controller Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Cooling Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Input Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Memory Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Motherboard Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Network Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Port Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
PlugAndPlay Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Power Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_
Printing Classes	Configuration	C:\perflogs\System\Diagnosics\CANBERRA_

FIGURE 13-3 Counters included in the System Diagnostics data set

The screenshot shows the Performance Monitor window with a 'System Diagnostics Report' open. The report provides details about the system's health, including the computer name, collection time, duration, and diagnostic results.

**System Diagnostics Report**

**Computer:** CANBERRA  
**Collected:** Monday, June 22, 2009 8:39:13 PM  
**Duration:** 6 Seconds

**Diagnostic Results**

**Warnings**

**Error**

**Symptom:** Device drivers are not installed.

**Cause:** A driver has not been installed for this device preventing it from working properly.

**Details:** The device driver for AVerTV has not been installed. This device will not be available until the correct device driver is installed.

**Resolution:** 1. Try installing the drivers using Windows Update.  
 2. Install the drivers that are on the installation media that came with the device.  
 3. Check with the manufacturer for an updated driver.

**Related:** [Explanation of Error Codes Generated by Device Manager](#)

**Symptom:** Device cannot start.

**Cause:** A device has a configuration problem that prevents it from starting properly.

**Details:** The device, Belkin USB Easy Transfer Cable, cannot start properly. It may not have the correct driver installed or may be experiencing a hardware failure. The Plug and Play ID for this device is ROOT\UNKNOWN\0000.

**Resolution:** 1. Verify the correct driver is installed.  
 2. Try updating the drivers using Windows Update.  
 3. Check with the manufacturer for an updated driver.  
 4. Attempt to uninstall and then reinstall the device using Device Manager.

**Related:** [Explanation of Error Codes Generated by Device Manager](#)  
[Manage Devices in Windows](#)

FIGURE 13-4 Accessing a report for the System Diagnostics data set

Data logging uses a large amount of system resources, and performance log files can become very large. To minimize the performance impact of performance data logging, log the minimum amount of information you require. For example, use System Performance instead of System Diagnostics whenever possible because System Performance includes fewer counters.

## Creating a Data Collector Set

If you have a performance problem or want to analyze and possibly improve the performance of a client computer, you can use DCSs to gather performance data and compare it against your baselines. The following high-level procedure creates a custom DCS:

1. In the Performance Monitor console (not the Performance Monitor tool that you can access from the console), expand Data Collector Sets, right-click User Defined, select New, and then select Data Collector Set. This starts the Create New Data Collector Set Wizard.
2. On the Create New Data Collector Set page, specify a name for the set. Ensure that Create From A Template (Recommended) is selected. Click Next.
3. On the Which Template Would You Like To Use? page, choose from one of the standard templates (Basic, System Diagnostics, or System Performance). Click Next.
4. On the Where Would You Like The Data To Be Saved? page, click Next to accept the default location for the data.
5. On the Create The Data Collector Set page, leave Run As set to the default to create and run the DCS using the logged-on user's credentials. Alternatively, click Change and specify alternative administrative credentials.
6. Select one of the following three options, and then click Finish:
  - Open Properties For This Data Collector Set
  - Start This Data Collector Set Now
  - Save And Close

Custom DCSs are located under the User Defined node within Data Collector Sets. You can schedule when a DCS runs and configure its stop conditions. You can also start a DCS manually by right-clicking it and selecting Start.

### **MORE INFO** CREATING DCSS

For more information about the various methods of creating DCSs, see <http://technet.microsoft.com/en-us/library/cc749337.aspx>.

## Customizing Data Collector Sets

A custom DCS logs only the performance data defined in the template that you choose. To add your own data sources to a DCS, you must update it after you create it.

To add a performance data source (such as a performance counter) to a DCS, right-click the DCS, select **New**, and then select **Data Collector**. The **Create New Data Collector Wizard** opens. On the **What Type Of Data Collector Would You Like To Create?** page, specify the data collector name, select the type, and then click **Next**. You can choose from the following types of data collectors:

- **Performance Counter Data Collector** This type of data collector enables you to collect performance statistics over long periods of time for later analysis. You can use it to set baselines and analyze trends.
- **Event Trace Data Collector** This type of data collector enables you to collect information about system events and activities.
- **Configuration Data Collector** This type of data collector stores information about registry keys, Windows Management Instrumentation (WMI) management paths, and the system state.
- **Performance Counter Alert** This type of data collector (sometimes termed an *Alert data connector*) enables you to configure an alert that is generated when a particular performance counter exceeds or drops below a specific threshold value.

You can add as many data collectors to a DCS as you need. To edit a data collector, select it in the **Data Collector Sets\User Defined** node. In the **Details** pane, right-click the data collector and click **Properties**.

#### **MORE INFO** DCS PROPERTIES

For more information about configuring DCS properties, see <http://technet.microsoft.com/en-us/library/cc749267.aspx>.

If a DCS includes performance counters, you can view the counter values in **Performance Monitor** by right-clicking the report, clicking **View**, and then clicking **Performance Monitor**. **Performance Monitor** then displays the data logged by the DCS rather than real-time data.

## Creating Data Collectors from the Command Prompt

You can create data collectors from an elevated command prompt by using the *Logman* utility. For example, you can use the following commands to create the various types of data collector listed in the previous section:

- **Logman create counter** This command creates a **Performance Counter** data collector. For example, the `logman create counter my_perf_log -c "\Processor(_Total)\% Processor Time"` command creates a counter called `my_perf_log` that records values for the `% Processor Time` counter in the `Processor(_Total)` counter instance.
- **Logman create trace** This command creates an **Event Trace** data collector. For example, the `logman create trace my_trace_log -o c:\trace_log_file` command creates an event trace data collector called `my_trace_log` and outputs the results to the `C:\trace_log_file` location.

- **Logman create cfg** This command creates a Configuration data collector. For example, the `Logman create cfg my_cfg_log -reg HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\` command creates a configuration data collector called `my_cfg_log` using the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion` registry key.
- **Logman create alert** This command creates an Alert data collector. For example, the `logman create alert my_alert -th "\Processor(_Total)\% Processor Time>90"` command creates an alert called `my_alert` that fires when the `% Processor Time` performance counter in the `Processor(_Total)` counter instance exceeds a value of 90.

You can also use the *Logman* utility to query data collector output; for example, the `logman query "my_perf_log"` command lists the data collectors contained in the `my_perf_log` DCS. You can start and stop DCSs, for example, by using the commands `logman start my_perf_log` and `logman stop my_perf_log`. You can delete a DCS, for example, by using the command `logman delete my_perf_log`, and you can use `logman update` to update a performance counter, a trace counter, an alert, or a configuration. *Logman* enables you to export the information in DCSs to and import information from an XML file.

#### **MORE INFO LOGMAN**

For more information about the *Logman* utility, see <http://technet.microsoft.com/en-us/library/cc753820.aspx>.

## Generating a System Diagnostics Report

When you create and use a DCS, you generate a report that is placed in User Defined Reports in the Reports tool in the Performance Tools console. However, the Reports tool also contains a system diagnostic report, sometimes known as a *computer health check* (although the term *health check* is more commonly used on server rather than client computers).

A system diagnostics report gives you details about the status of hardware resources, system response times, and processes on the local computer, along with system information and configuration data. You would generate a system diagnostics report if you were looking for ways to maximize performance and streamline system operation. You need to be a member of the local Administrators group or equivalent to generate a system diagnostics report.

If you use the Performance Tools console to look at the system diagnostics report, you see a copy of that report the last time it was compiled. To generate and display a system diagnostic report that is completely up to date, enter the following into the Search box on the Start menu:

```
perfmon /report
```

If you prefer, you can instead enter `perfmon.exe /report` in an elevated command prompt. Whatever method you choose, the command generates a diagnostics report (this typically takes 60 seconds) and displays it in the Resource and Performance Monitor, as shown in Figure 13-5. You can scroll down the report and expand any of its sections.



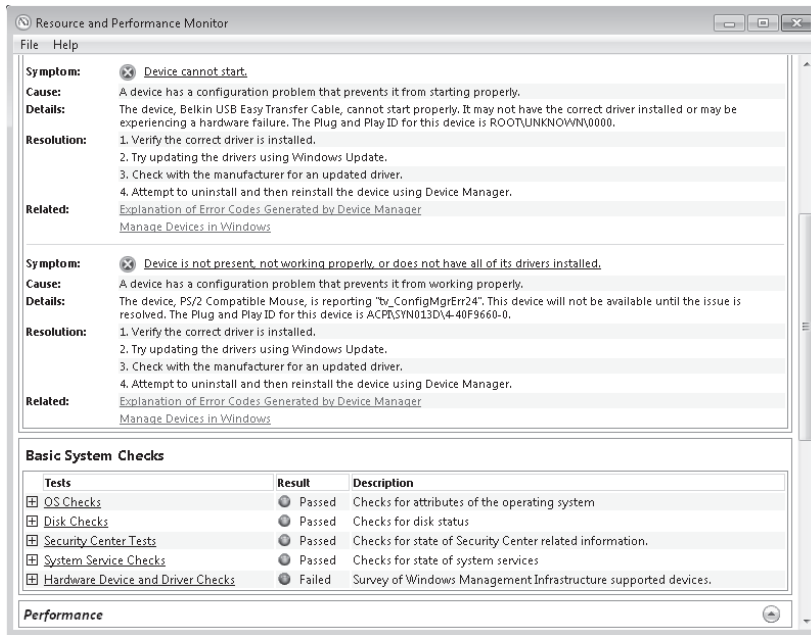


FIGURE 13-5 System diagnostics report in the Resource and Performance Monitor

For example, expanding the failed basic system check called Hardware Device And Driver Checks in the Resource and Performance Monitor results in the screen shown in Figure 13-6, which indicates there are problems with three of the Plug and Play (PnP) devices.

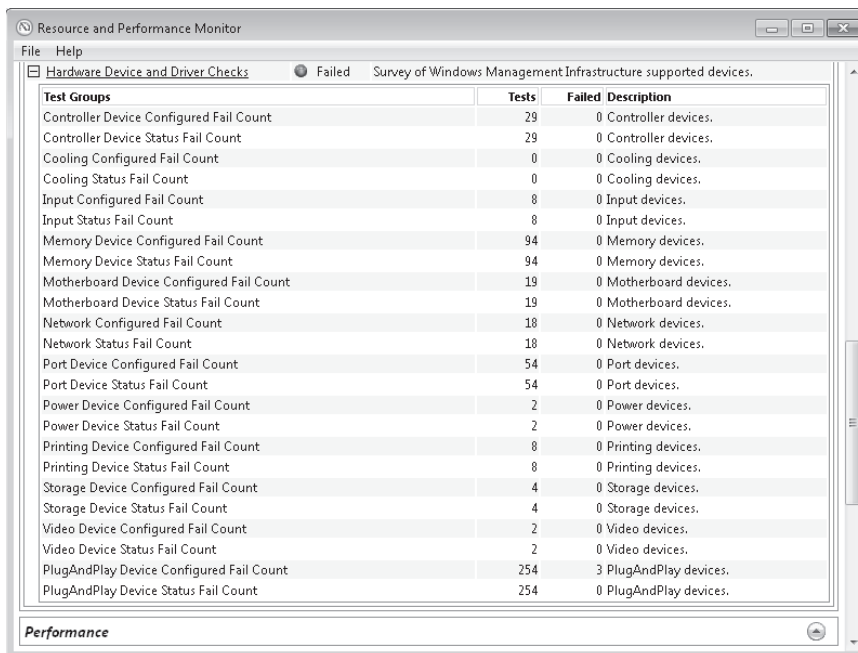


FIGURE 13-6 Displaying the basic system check for Hardware Device And Driver Checks

You can expand Performance, Software Configuration, Hardware Configuration, CPU, Network, Disk, Memory, and Report Statistics. For example, expanding Software Configuration lets you access more information, as shown in Figure 13-7, although no faults or warnings are displayed in this screen shot. If a fault was detected, you can explore further by expanding any of the nodes marked with a + symbol.

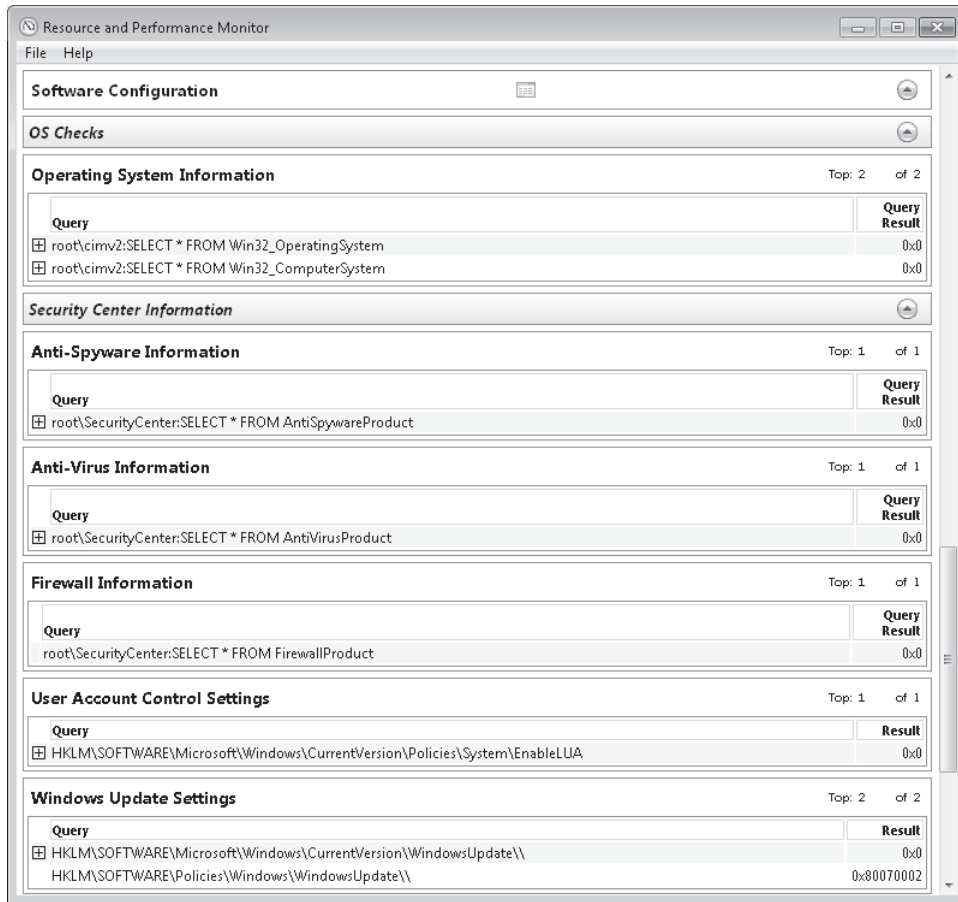
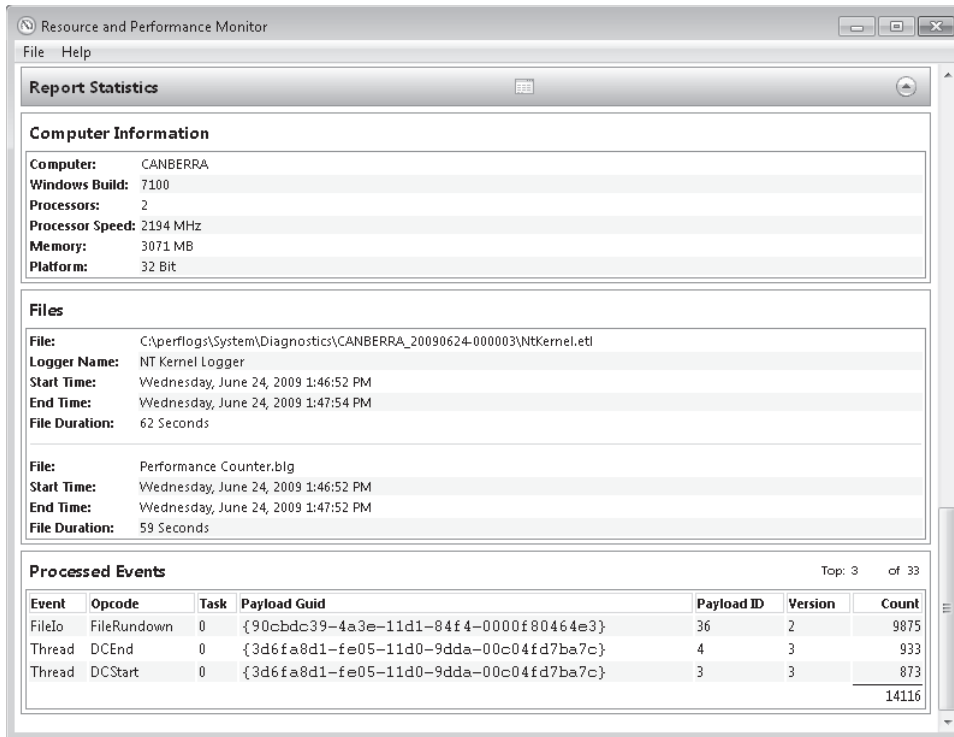


FIGURE 13-7 Expanding Software Configuration in Resource and Performance Monitor

Expanding Report Statistics lets you access computer information, files, and processed events and discover Payload GUIDs, as shown in Figure 13-8.

## Tracking System Reliability, Stability, and Overall Performance

Windows 7 offers several tools to assess system reliability and stability. Reliability Monitor keeps a record of software changes and updates and lets you correlate system changes with



**FIGURE 13-8** Expanding Report Statistics in Resource and Performance Monitor

crashes and reboots; the Action Center monitors your computer and reports problems with security, maintenance, and related services; and the Windows Experience Index measures the capability of your computer's hardware and software configuration and expresses this as a base score.

## Reliability Monitor

Reliability Monitor tracks a computer's stability. Computers that have no reboots or failures are considered stable and can (eventually) achieve the maximum system stability index of 10. The more reboots and failures that occur on a computer, the lower the system stability becomes. The minimum index value is zero. The system stability index is not an exact measure of reliability because, sometimes, installing a new service pack or update requires a reboot, which initially lowers the index value but ultimately makes a system more reliable than it was before. However, Reliability Monitor provides valuable information about what system changes were made before a problem occurred. The easiest way to open Reliability Monitor is to type **perfmon /rel** in the Start menu Search box and click View Reliability History

You can use Reliability Monitor to diagnose intermittent problems. For example, if you install an application that causes the operating system to fail intermittently, it is difficult to correlate the failures with the application installation. Figure 13-9 shows how Reliability

Monitor can be used to indicate that Windows and application failures and a video hardware error occurred on the Canberra computer on June 22 following an update of a video driver on June 21. If you obtained this result on a test network, you might consider obtaining more information before updating the driver on your production network.

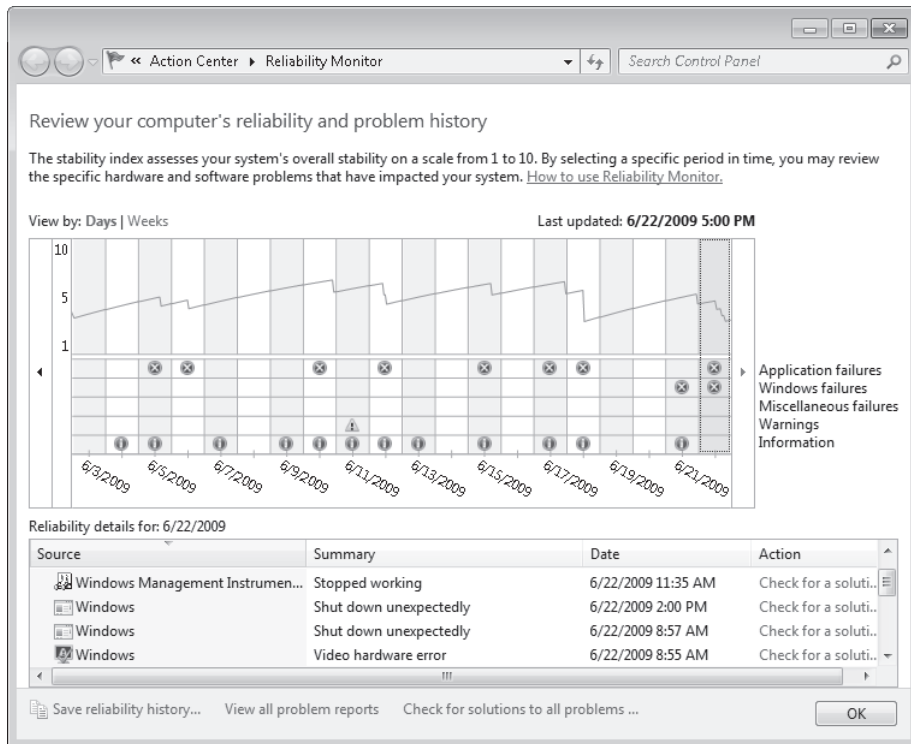


FIGURE 13-9 Reliability Monitor

## The Stability Index

The stability index is based on data collected over the lifetime of a system. Each day in the stability chart is associated with a graph point showing its stability index rating. The stability index is a weighted measurement calculated from the number of failures seen over a rolling historical period. The index value is calculated over the preceding 28 days, although the results for considerably more days can be displayed.

Recent failures are weighted more heavily than past failures so that improvement over time is reflected in an ascending stability index when a reliability issue has been resolved. Days when the computer is turned off or is in a sleep or hibernate state are not included when calculating the stability index.

If there is not enough data to calculate a steady stability index, the line on the graph is dotted. For example, until Reliability Monitor has 28 days of data, the stability index is

displayed as a dotted line, indicating that it has not yet established a valid baseline. When enough data has been recorded to generate a steady stability index, the line is solid. If there are any significant changes to the system time, an information icon appears on the graph for each day on which the system time was adjusted.

Reliability Monitor maintains up to a year of history for stability and reliability events. The Stability Chart displays a rolling graph organized by date.

### ✓ Quick Check

- What would a stability index of 10 indicate?

#### Quick Check Answer

- The maximum value of the stability index is 10. This value indicates that the computer has been stable over the previous 28 days with no failures or reboots. It also indicates that no software updates and service packs that require a reboot have been applied during that time.

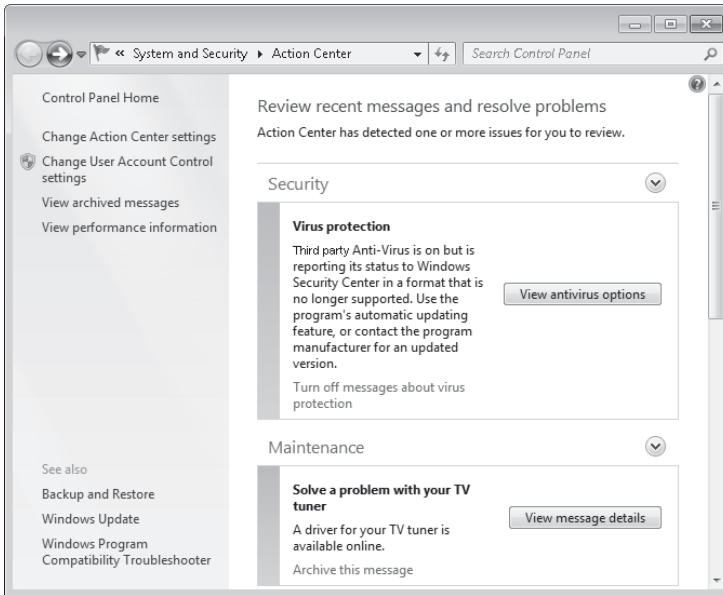
## The Stability Chart

The Stability Chart in Reliability Monitor displays a graph of the stability index on a day-to-day basis. Rows in the lower half of the chart track reliability events that either contribute to the stability measurement for the system or provide related information about software installation and removal. When one or more reliability events of each type are detected, an icon appears in the column for that date.

For software installs and uninstalls an information icon indicates a successful event and a warning icon indicates a failure. For all other reliability event types, an error icon indicates a failure. If more than 30 days of data are available, you can use the left and right arrow keys on the keyboard to find dates outside the visible range.

## Using the Action Center

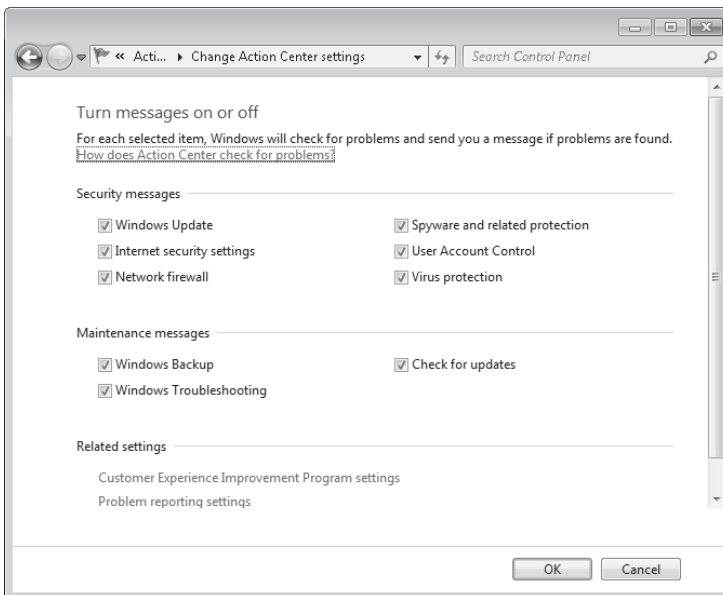
The Action Center, available under System And Security in Control Panel, monitors your computer and reports problems with security, maintenance, and related settings that help indicate your computer's overall performance. It notifies users if there is a problem with the network firewall, antivirus, anti-spyware, or Windows Update on their computers running Windows 7. When the status of a monitored item changes (for example, your antivirus software becomes out of date), Action Center notifies you with a message in the notification area on the taskbar. The status of the item in Action Center changes color to reflect the severity of the message, and Action Center recommends an action. The Action Center is shown in Figure 13-10.



**FIGURE 13-10** The Action Center

## Changing Action Center Settings

If you prefer to keep track of an item yourself and you do not want to see notifications about its status, you can turn off notifications for the item in the Change Action Center Settings dialog box, shown in Figure 13-11.

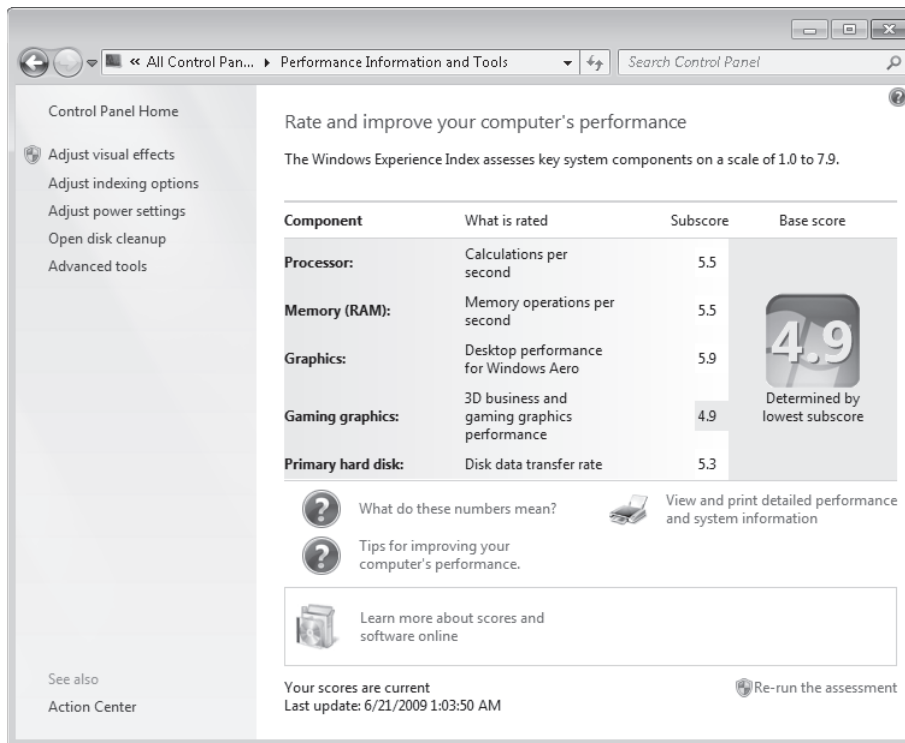


**FIGURE 13-11** The Change Action Center Settings dialog box

When you clear the check box for an item on the Change Action Center Settings dialog box, you no longer receive any messages and do not see the item's status in Action Center. Microsoft recommends checking the status of all items listed because that can help warn you about security issues.

## The Windows Experience Index

From Action Center, you can archive messages and view the messages you have archived. You can click a link to change User Account Control (UAC) settings, as described in Chapter 9, "Authentication and Account Control." However, the link in the Action Center that best measures the computer's current performance level is to the Windows Experience Index in the Performance Information And Tools dialog box, as shown in Figure 13-12.



**FIGURE 13-12** The Windows Experience Index

The Windows Experience Index measures the capability of your computer's hardware and software configuration and expresses this as a base score. A higher base score generally means that your computer will perform better and faster especially when performing resource-intensive tasks.

Each hardware feature receives an individual subscore and the base score is determined by the lowest subscore. The base score is not an average of the combined subscores. However, the subscores can give you a view of how the features that are most important to you will perform and can help you decide which features to upgrade. Remember that if you are not

interested in gaming and very high-quality three-dimensional graphics, you might purchase a computer that has very adequate processor, memory, and hard disk resources but has a lower-cost graphics hardware device. Such a computer is adequate for your purposes but does not have a high base score.

While bearing this in mind, you can use the base score as at least a rough guide when you are selecting software to run on your computer. For example, if your computer has a base score of 3.3, then you would be wise to purchase only software packages that require a base score of 3 or lower. Interactive games applications are a good example of the type of software package that require a high Windows Experience Index.

The scores range from 1.0 to 7.9. The Windows Experience Index is designed to accommodate advances in computer technology. As hardware speed and performance improve, higher score ranges will be enabled. The standards for each level of the index generally stay the same. However, in some cases, new tests might be developed that can result in lower scores. If you have replaced or upgraded hardware on your computer, you need to recalculate the Windows Experience Index.

## Using System Tools to Investigate Processes and Services

As an IT professional, you probably have used Task Manager and accessed Resource Manager from that tool, although you may not be aware of the Resource Manager enhancements that Windows 7 provides. Process Explorer is a downloadable advanced system tool that offers many of the features of Task Manager and Resource Manager and you can use this tool to investigate resource usage, handles, and dynamic-link library (DLL) files.

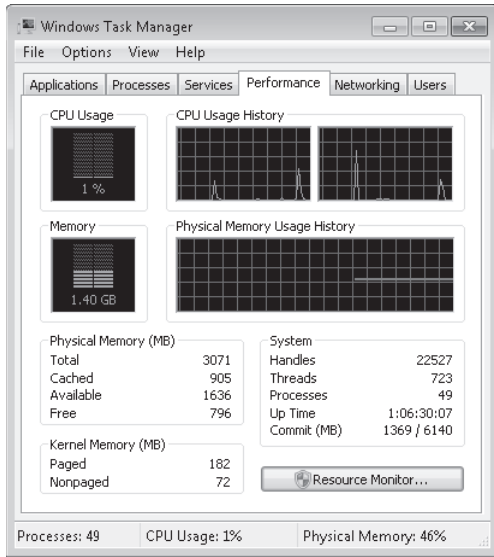
### Task Manager

If an application stops responding, Windows 7 tries to find the problem and fix it automatically. Alternatively, if the system seems to have crashed completely and Windows 7 has not resolved the problem, you can end the application by opening Task Manager and accessing the Applications tab.

The Performance tab in Task Manager provides details about how a computer is using system resources—for example, RAM and CPU. As shown in Figure 13-13, the Performance tab has four graphs. The first two show the percentage of CPU resource that the system is using, both at the moment and for the past few minutes. A high percentage usage over a significant period indicates that programs or processes require a lot of CPU resources. This can affect computer performance. If the percentage appears frozen at or near 100 percent, a program might not be responding. If the CPU Usage History graph is split, the computer either has multiple CPUs, a single dual-core CPU, or both.

If processor usage is consistently high—say 80 percent or higher for a significant period—you should consider installing a second processor or replacing the current processor even if the Windows Experience Index subscore does not identify the processor as a resource bottleneck. However, before you do so, it is worth capturing processor usage data by using Performance Monitor rather than relying on snapshots obtained by using Task Manager.





**FIGURE 13-13** The Performance tab in Task Manager

The next two graphs display how much RAM is being used, both at the moment and for the past few minutes. The percentage of memory being used is listed at the bottom of the Task Manager window. If memory use appears to be consistently high or slows your computer's performance noticeably, try reducing the number of programs that are open at one time (or encourage users you support to close any applications they are not currently using). If the problem persists, you might need to install more RAM or implement ReadyBoost.

Three tables below the graphs list various details about memory and resource usage. In the Physical Memory (MB) table, *Total* is the amount of RAM installed on your computer, *Cached* refers to the amount of physical memory used recently for system resources, and *Free* is the amount of memory that is currently unused and available.

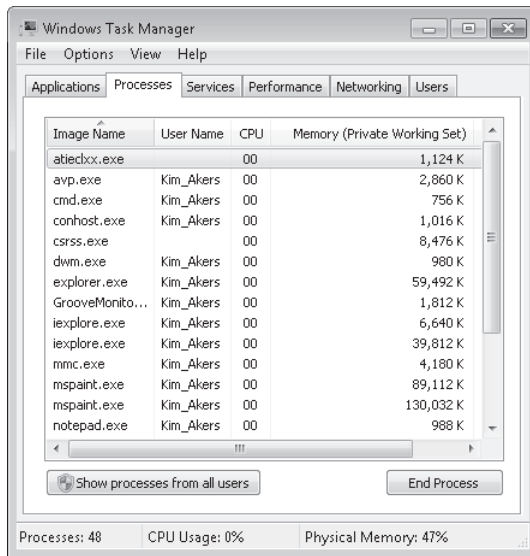
In the Kernel Memory (MB) table, *Paged* refers to the amount of virtual memory the kernel is using; *Nonpaged* is the amount of RAM memory used by the kernel.

The System table has five fields: Handles, Threads, Processes, Up Time, and Page File. Handles are pointers that refer to system elements. They include (but are not limited to) files, registry keys, events, or directories. Lesson 2, "Configuring Performance Settings," discusses page file configuration.

If you need more information about how memory and CPU resources are being used, click Resource Monitor. This displays the Resource Monitor, which is discussed later in this lesson. You require elevated privileges to access Resource Monitor.

You can determine how much memory an individual process uses by selecting the Task Manager Processes tab. As shown in Figure 13-14, the Memory (Private Working Set) column is selected by default. A private working set indicates the amount of memory a process is using that other processes cannot share. This information can be useful in identifying

a “leaky” application—an application which, if left open, uses more and more memory resource and does not release memory resource that it is no longer using.



**FIGURE 13-14** The Processes tab in Task Manager

You can click **View**, click **Select Columns**, and then select a memory value to view other memory usage details on the Processes tab. You can use the Task Manager Processes tab to end a process, to end a process tree (which stops the process and all processes on which it depends), and to set process priority. To change the priority of a process, right-click the process and click **Set Priority**. You can choose **Realtime**, **High**, **Above Normal**, **Normal**, **Below Normal**, or **Low**.

The Task Manager Services tab shows which services are running and which are stopped. You can stop or start a service or go to a process that depends on that service. If you want more details about or more control over the services available on a computer, you can click **Services** to access the Services administrative tool. You require elevated privileges to use the Services tool.

The Task Manager Networking tab lets you view network usage. The Users tab tells you what users are connected to the computer and lets you disconnect a user. The Applications tab shows you the running applications and (as previously stated) enables you to close a crashed application.

### ✓ Quick Check

- You want to change the priority of a process on a computer. How do you do this?

### Quick Check Answer

- Open Task Manager. In the Processes tab, right-click the process and click **Set Priority**. You can choose **Realtime**, **High**, **Above Normal**, **Normal**, **Below Normal**, or **Low**.



## EXAM TIP

In Windows 7, you right-click a process and click Set Priority to observe or configure its priority level. In Windows Vista, you click Select Priority. Examiners often test this sort of change to determine whether candidates have properly studied the new operating system or whether they are relying on their experience with the previous one.

## Resource Monitor

Windows 7 offers an enhanced version of the Resource Monitor tool. Windows 7 Resource Monitor allows you to view information about hardware and software resource use in real time. You can filter the results according to the processes or services that you want to monitor. You can also use Resource Monitor to start, stop, suspend, and resume processes and services, and to troubleshoot unresponsive applications. You can start Resource Monitor from the Performance tab of Task Manager or by entering **resmon** in the Search box on the Start menu.

Resource Monitor always starts in the same location and with the same display options as the previous session. You can save your display state at any time and then open the configuration file to use the saved settings. However, filtering selections are not saved as part of the configuration settings.

Resource Monitor includes five tabs: Overview, CPU, Memory, Disk, and Network. The Overview tab, shown in Figure 13-15, displays basic system resource usage information. The other tabs display information about each specific resource. If you have filtered results on one tab, only resources used by the selected processes or services are displayed on the other tabs. Filtered results are denoted by an orange bar below the title bar of each table.

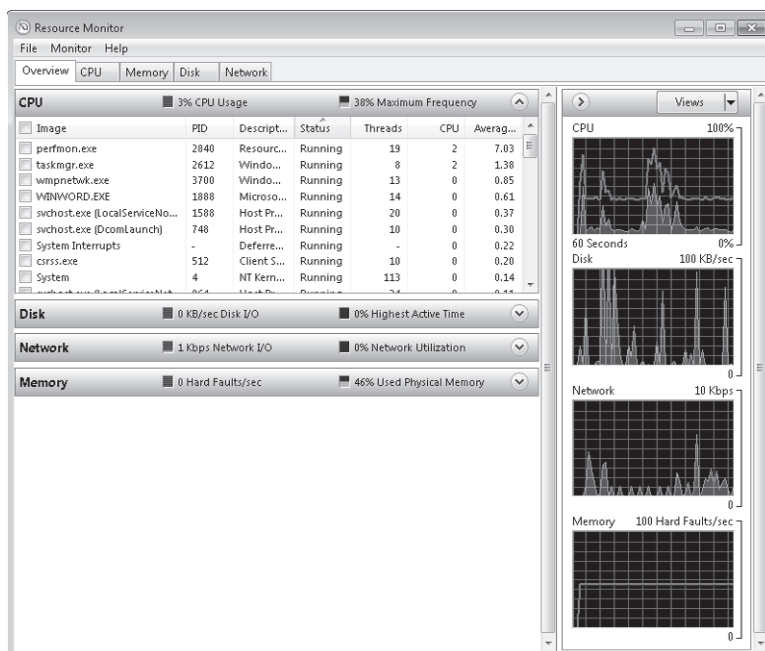


FIGURE 13-15 The Resource Monitor Overview tab

Each tab in Resource Monitor includes multiple tables that provide detailed information about the resource featured on that tab. The first table displayed is always the key table, and it contains a complete list of processes using the resource included on that tab. For example, the key table on the Overview tab contains a complete list of processes running on the system.

You can filter the detailed data in tables other than the key table by one or more processes or services. To filter, select the check box in the key table next to each process or service that you want to highlight. To stop filtering for a single process or service, clear its check box. To stop filtering altogether, clear the check box next to Image in the key table. If you have filtered results, the resources used by the selected processes or services are shown in the graphs as an orange line.

You can change the size of the graphs by clicking Views and selecting a different graph size. You can hide the chart pane by clicking the arrow at the top of the pane. To view definitions of data displayed in the tables, move the mouse pointer over the column title about which you want more information.

For example, to identify the network address that a process is connected to, click the Network tab and then click the title bar of TCP Connections to expand the table. Locate the process whose network connection you want to identify. You can then determine the Remote Address and Remote Port columns to see which network address and port the process is connected to. Figure 13-16 shows the System process is currently connected to IPv4 addresses 192.168.123.138 and 192.168.123.176, both on port 445.

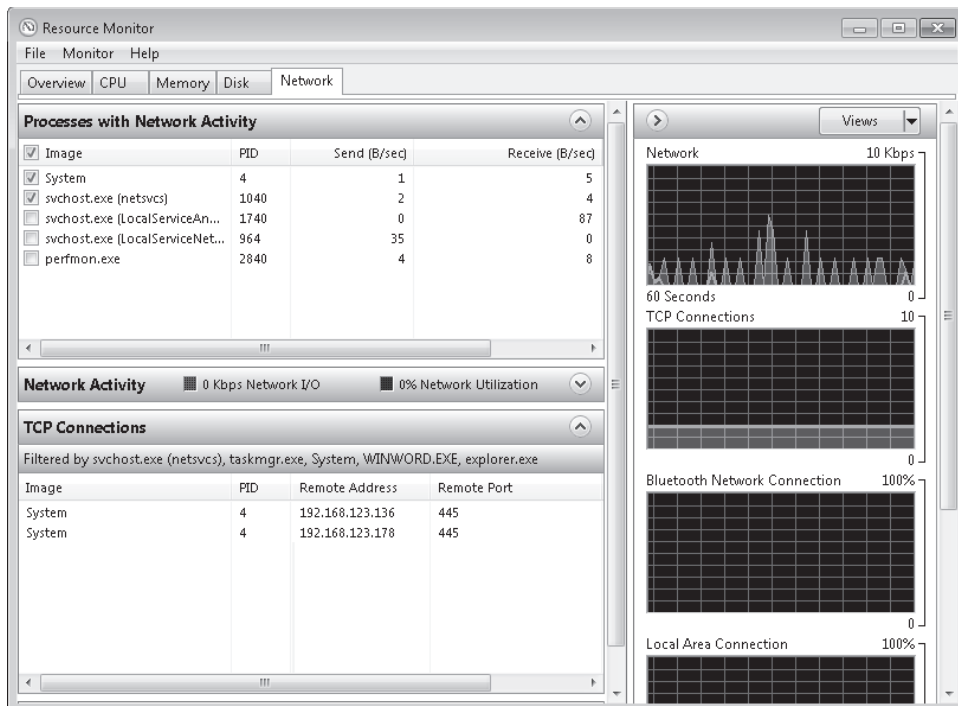


FIGURE 13-16 Identifying network addresses that a process is connected to

On the Memory tab, shown in Figure 13-17, you can review the memory available to programs. Available memory is the combined total of standby memory and free memory. Free memory includes zero page memory.

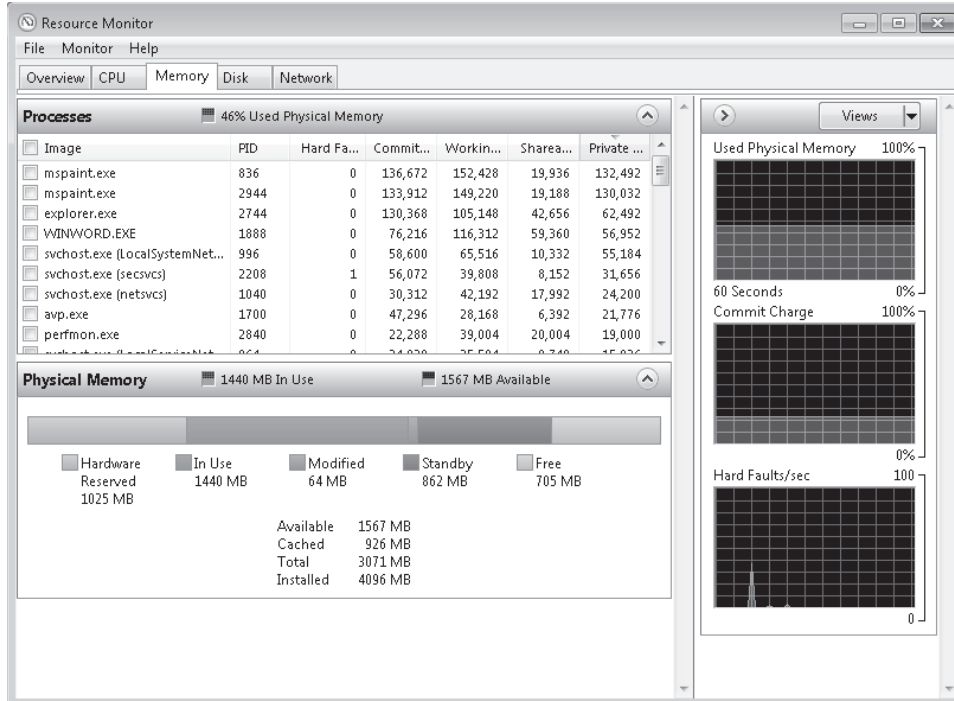


FIGURE 13-17 The Resource Monitor Memory tab

Resource Monitor displays real-time information about all the processes running on your system. If you want to view only the data related to selected processes, you can filter the detailed results by selecting the check boxes next to the names of the processes you want to monitor in any of the tabs. Selected processes are moved to the top of the Image column. After you have selected at least one process for filtering, the Associated Handles and Associated Modules tables on the CPU tab contain data related to your selection. Tables that contain only filtered results include an orange information bar below the title bar of the table.

Resource Monitor allows you to end or suspend processes and start, stop, or restart services. You should use Resource Monitor to end a process only if you are unable to close the program by normal means. If an open program is associated with the process, it closes immediately and you lose any unsaved data. If you end a system process, this might result in system instability and data loss.

To end a process, right-click the executable name of the process that you want to end in the Image column of the key table of any Resource Monitor tab and click End Process. To end all processes dependent on the selected process, click End Process Tree. To resume a process, right-click the executable name of the program that you want to resume, and then click Resume Process.

To stop, start, or restart a service using Resource Monitor access the CPU tab and click the title bar of Services to expand the table. In Name, right-click the service that you want to change, and then click Stop Service, Start Service, or Restart Service.

Applications that are not responding might be waiting for other processes to finish, or for system resources to become available. Resource Monitor allows you to view a process wait chain, and to end processes that are preventing a program from working properly.

A process that is not responding appears as a red entry in the CPU table of the Overview tab and in the Processes table of the CPU tab. To view the process wait chain, right-click the executable name of the process you want to analyze in the Image column on the key table of any Resource Monitor tab and click Analyze Wait Chain.

If the process is running normally and is not waiting for any other processes, no wait chain information is displayed. If, on the other hand, the process is waiting for another process, a tree organized by dependency on other processes is displayed. If a wait chain tree is displayed, you can end one or more of the processes in the tree by selecting the check boxes next to the process names and clicking End Process.

Handles (as stated previously in this section) are pointers that refer to system elements. They include (but are not limited to) files, registry keys, events, or directories. Modules are helper files or programs. They include (but are not limited to) DLL files.

To use Resource Monitor to view all handles and modules associated with a process, in the Image column of the CPU tab, select the check box next to the name of the process for which you want to see associated handles and modules. Selected processes move to the top of the column. Click the title bars of the Associated Handles and Associated Modules tables to expand them. An orange bar below the title bar of each table shows the processes you have selected. Review the results in the detail tables.

If you need to identify the processes that use a handle, click the Search Handles box in the title bar of the Associated Handles table. Type the name of the handle you want to search for, and then click Search. For example, searching for `c:\windows` returns all handles with `c:\windows` as part of the handle name. The search string is not case sensitive, and wildcards are not supported.

## Process Explorer

Process Explorer is not part of Windows 7, but you can download it at <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>, expand the archive into a folder (such as `C:\ProcessExplorer`), and start it by entering `c:\processexplorer\procexp.exe` in the Search box on the Start menu. Process Explorer tells you which program has a particular file or directory open and displays information about which handles and DLLs processes have opened or loaded. You can use either Process Explorer or Resource Monitor to determine which applications are responsible for activity on your hard disk, including which files and folders are being accessed.

When it opens, Process Explorer displays a list of the currently active processes, as shown in Figure 13-18. You can toggle the lower pane on and off and select to view handles or DLLs.

In Handle mode, you can see the handles that the process selected in the top window has opened. The Process Explorer search capability discovers which processes have particular handles opened or DLLs loaded.

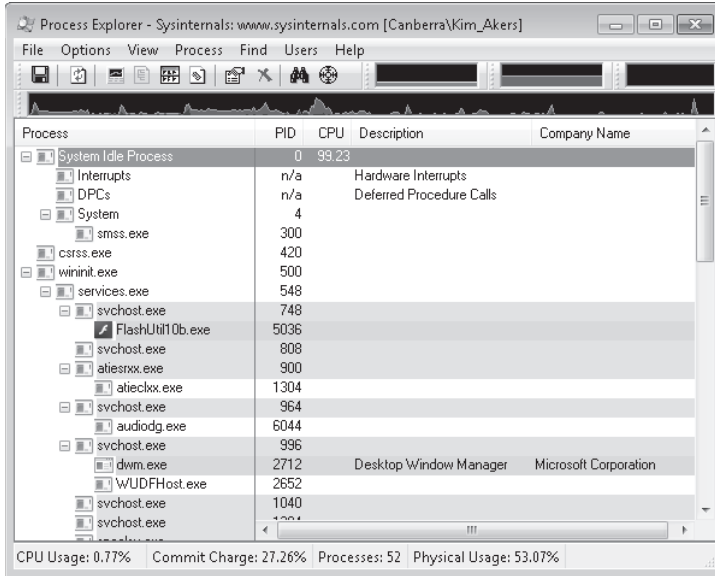


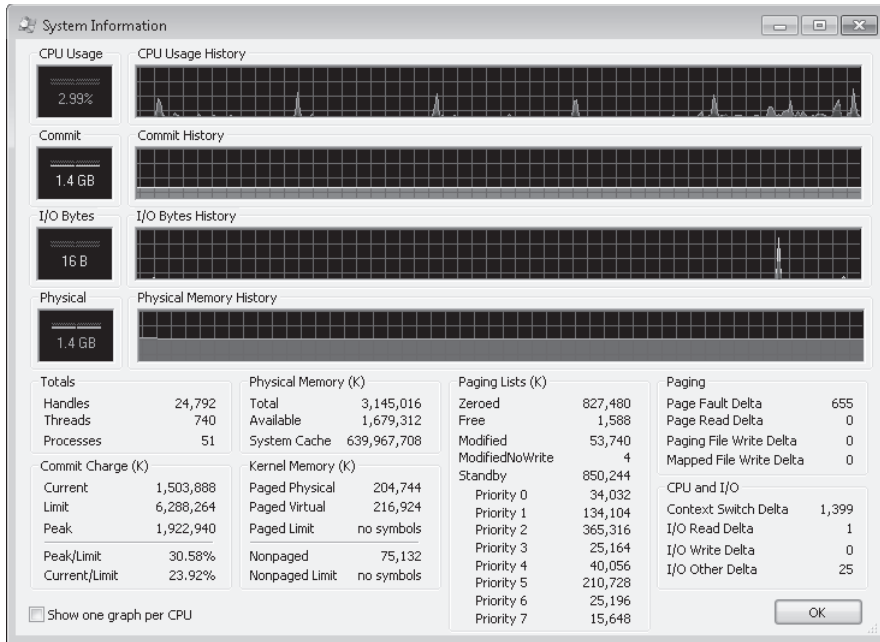
FIGURE 13-18 Process Explorer opening page

#### **MORE INFO ADVANCED SYSTEM TOOLS AND COMMAND-LINE UTILITIES**

For more information about advanced system tools for Windows, including their corresponding command-line utilities, see <http://technet.microsoft.com/en-us/sysinternals/default.aspx>.

Process Explorer includes a toolbar and mini-graphs for CPU, memory, and I/O history. The mini-graphs show history of system activity, and resting the mouse over a point on a graph displays the associated time and the process information. For example, the tooltip for the mini-CPU graph shows the process that was the largest consumer of CPU. Clicking on any of the mini-graphs opens the System Information screen, as shown in Figure 13-19. Difference highlighting helps you see what items change between refreshes. Items—including processes, DLLs, and handles—that exit or are closed show in red and new items show in green.

System Information graphs display the CPU usage history of the system, committed virtual memory usage, and I/O throughput history. Red in the CPU usage graph indicates CPU usage in kernel mode, whereas green is the sum of kernel-mode and user-mode execution. When Committed Virtual Memory reaches the system Commit Limit, applications and the system become unstable. The Commit Limit is the sum of most of the physical memory and the sizes of any paging files. In the I/O graph, the blue line indicates total I/O traffic, which is the sum of all process I/O reads and writes between refreshes, and the pink line shows write traffic.



**FIGURE 13-19** Process Explorer System Information screen

You can reorder columns in Process Explorer by dragging them to their new position. To select which columns of data you want visible in each of the views and the status bar, click **Select Columns** on the **View** menu or right-click a column header and click **Select Columns**. You can save a column configuration and its associated settings by clicking **Save Column Set** on the **View** menu.

On the **Options** menu, you can choose to have Process Explorer open instead of Task Manager whenever Task Manager is started, or you can ensure that the Processor Explorer window is always on top and always visible. You can specify that only one instance of Process Explorer is open at any one time.

**NOTE THE VIEWING ADVANCED DETAILS IN SYSTEM INFORMATION OPTION**

The **View Advanced Details In System Information** option, available when you click **Advanced Tools** in **The Performance Information And Tools** dialog box, provides detailed information about system configuration. It does not, however, directly address performance issues. The dialog box in which this information is presented is called **System Information**. Take care to distinguish between this dialog box, which is provided in Windows 7, and the **System Information** feature of Process Explorer, which is a downloadable tool.



# Logging and Forwarding Events and Event Subscriptions

As an experienced IT professional, you almost certainly have used Event Viewer and event logs, and this section discusses these tools only briefly before going on to event forwarding and event subscriptions, with which you might be less familiar.

Details about event subscriptions can be found in the Subscriptions tab of the event log Properties dialog box. The General tab of this dialog box gives details such as current log size, maximum log size, and the action to take when maximum log size is reached. The easiest way to start Event Viewer is to enter **eventvwr** in the Start menu Search box.

Event Viewer displays event logs, which are files that record significant events on a computer—for example, when a user logs on or when a program encounters an error. You will find the details in event logs helpful when troubleshooting problems. The events recorded fall into the following categories:

- Critical
- Error
- Warning
- Information

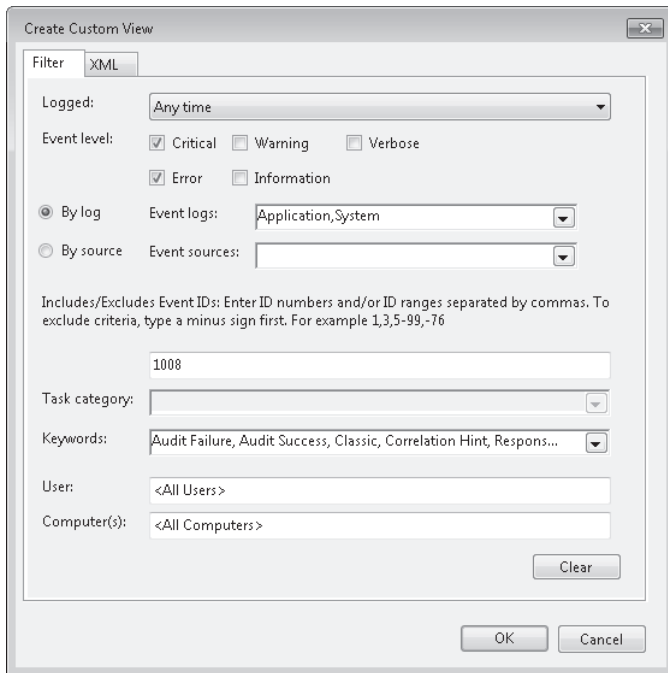
The security log contains two more event categories, Audit Success and Audit Failure, that are used for auditing purposes.

Event Viewer tracks information in several different logs. Windows logs include the following:

- **Application** Stores program events. Events are classified as error, warning, or information, depending on the severity of the event. The critical error classification is not used in the Application log.
- **Security** Stores security-related audit events that can be successful or failed. For example, the security log will record an audit success if a user trying to log on to the computer was successful.
- **System** Stores system events that are logged by Windows 7 and system services. System events are classified as critical, error, warning, or information.
- **Forwarded Events** Stores events that are forwarded by other computers.

## Custom Views

You can create custom views by clicking Create Custom View on the Event Viewer Action menu, specifying the source logs or events and filtering by level, time logged, event ID, task category, keywords, user, or computer. You are unlikely to specify all these criteria, but this facility enables you to refine your search to where you think a problem might be occurring rather than searching through a very large number of events. Figure 13-20 shows a custom view specification.



**FIGURE 13-20** Specifying a custom view

A filter is not persistent. If you set up a filter to view specific information in an event log, you need to configure the same filter again the next time you want to see the same information. Custom views are persistent, which means you can access them whenever you open Event Viewer. You can save a filter as a custom view so it becomes persistent and you do not need to configure it for each use. The Action menu also allows you to import custom views from another source and to connect to another computer. You need to have an administrator-level account on that computer.

## Applications and Services Logs

Event Viewer provides a number of Applications and Services logs. These include logs for programs that run on the computer and detailed logs that store information about specific Windows services. For example, these logs can include the following:

- Hardware Events
- Internet Explorer
- Key Management Service
- Media Center
- A large number of Microsoft Windows logs
- Microsoft Office Diagnosis
- Microsoft Office Sessions
- Windows PowerShell

## Attaching Tasks to Events

Sometimes you want to be notified by e-mail if a particular event occurs, or you might want a specified program to start, such as one that activates a pager. Typically, you might want an event in the Security log—such as a failed logon, or a successful logon by a user who should not be able to log on to a particular computer—to trigger this action. To implement this functionality, you attach a task to the event so that you receive a notification.

To do this, open Event Viewer and navigate to the log that contains the event about which you want to be notified. Typically, this would be the Security log in Windows logs, but you can implement this in other Windows logs or in Applications and Services logs if you want to. You click the event and click Action, click the event and go to the Actions pane, or right-click the event. You then select Attach Task To This Event.

This opens the Create A Basic Task Wizard. You name and describe the task and then click Next. The next screen summarizes the event, and you can check that you have chosen the correct event before clicking Next. The next screen gives you the option of starting a program, sending an e-mail, or specifying a message. When you make your choice and click Next, you configure the task. For example, if you want to send an e-mail, you would specify source address, destination address, subject, task, attachment (if required), and Simple Mail Transfer Protocol (SMTP) server. You click Next and then click Finish.

## Using Network Diagnostics with Event Viewer

When you run Windows Network Diagnostics, as described in Chapter 6, any problem found, along with solution or solutions, is displayed in the Network Diagnostics dialog box. If, however, more detailed information about the problem and potential solutions is available, Windows 7 saves this in one or more event logs. You can use the information in the event logs to analyze connectivity problems or help interpret the conclusions.

You can filter for network diagnostics and Transmission Control Protocol/Internet Protocol (TCP/IP) events by specifying (for example) Tcpip and Tcpiv6 event sources and capturing events from these sources in a custom view.

If Network Diagnostics identifies a problem with a wireless network, it saves information in the event logs as either helper class events or informational events. Helper class events provide a summary of the diagnostics results and repeat information displayed in the Network Diagnostics dialog box. They can also provide additional information for troubleshooting, such as details about the connection that was diagnosed, diagnostics results, and the capabilities of the wireless network and the adapter being diagnosed.

Informational events can include information about the connection that was diagnosed, the wireless network settings on the computer and the network, visible networks and routers or access points in range at the time of diagnosis, the computer's preferred wireless network list, connection history, and connection statistics—for example, packet statistics and roaming history. They also summarize connection attempts, list their status, and tell you what phases of the connection failed or did not start.

## Event Forwarding and Event Subscriptions

*Event forwarding* enables you to transfer events that match specific criteria to an administrative (or collector) computer. This enables you to manage events centrally. A single *event log* on the collector computer holds important events from computers anywhere in your organization. You do not need to connect to the local event logs on individual computers.

Event forwarding uses Hypertext Transfer Protocol (HTTP) or, if you need to provide an additional encryption and authentication layer for greater security, Hypertext Transfer Protocol Secure (HTTPS) to send events from a source computer to a collector computer. Because event forwarding uses the same protocols that you use to browse Web sites, it works through most firewalls and proxy servers. Event forwarding traffic is encrypted whether it uses HTTP or HTTPS.

To use event forwarding, you must configure both the source and collector computers. On both computers, start the Windows Remote Management (WinRM) and the Windows Event Collector services. On the source computer, configure a Windows Firewall exception for the HTTP protocol. You might also need to create a Windows Firewall exception on the collector computer, depending on the delivery optimization technique you choose.

You can configure collector-initiated or source-initiated subscriptions. In collector-initiated subscriptions, the collector computer retrieves events from the computer that generated the event. You would use a collector-initiated subscription when you have a limited number of source computers and these are already identified. In this type of subscription, you configure each computer manually.

### Subscriptions

In a source-initiated subscription (sometimes termed a *source computer–initiated subscription*), the computer on which an event is generated (the source computer) sends the event to the collector computer. You would use a source-initiated subscription when you have a large number of source computers and you configure these computers through Group Policy.

In a source-initiated subscription, you can add additional source computers after the subscription is established and you do not need to know immediately which computers in your network are to be source computers. In collector-initiated subscriptions, the collector computer retrieves events from one or more source computers. Collector-initiated subscriptions are typically used in small networks. In source-initiated subscriptions, the source computers forward events to the collector computer. Enterprise networks use source-initiated subscriptions.

A collector computer needs to run Windows Server 2008 R2, Windows Server 2008, Windows 7, Windows Vista, or Windows Server 2003 R2. A source computer needs to run Windows XP with SP2, Windows Server 2003 with SP1 or SP2, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2.

## NOTE FORWARDING COMPUTERS

Much of the literature on this subject uses the term *forwarding computer* rather than *source computer*, sometimes inaccurately. In collector-initiated subscriptions, the collector computer retrieves events from the source computer. The source computer does not forward events. Only in source-initiated subscriptions does the source computer forward events and can accurately be called a forwarding computer. To prevent confusion, the term *source computer*, rather than *forwarding computer*, is used throughout this chapter.

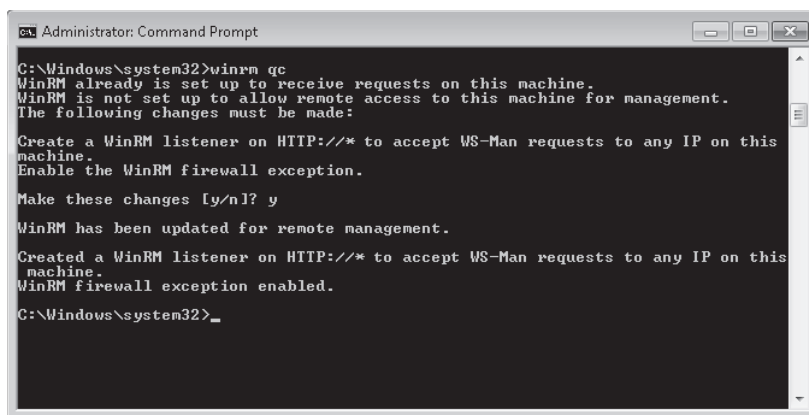
In a collector-initiated subscription, you first manually configure one or more source computers and the collector computer. When the source computers and the collector computer are configured, you can create an *event subscription* to determine what events should be transferred.

## Configuring a Collector-Initiated Subscription

To configure a computer running Windows 7 so that a collector computer can retrieve events from it, open an elevated command prompt and use the *Winrm* (Windows Remote Management) command-line tool to configure the WinRM service by entering the following command:

```
winrm quickconfig
```

You can abbreviate this to *winrm qc*. Windows displays a message similar to that shown in Figure 13-21. The changes that must be made depend on how the operating system is configured. You enter **Y** to make these changes. Note that if any of your network connection types is set to public, you must set it to private for this command to work.



```
Administrator: Command Prompt
C:\Windows\system32>winrm qc
WinRM already is set up to receive requests on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this
machine.
Enable the WinRM firewall exception.

Make these changes [y/n]? y
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this
machine.
WinRM firewall exception enabled.
C:\Windows\system32>_
```

FIGURE 13-21 Configuring the WinRM service

Next, add the computer account of the collector computer to the local Event Log Readers group or the local Administrators group on the source computer. You can do this by using the Local Users And Groups MMC snap-in or by entering a net command in an elevated command prompt.

You can add the collector computer account to the local Administrators group or the Event Log Readers group on the source computer. If you do not require the collector computer to retrieve events in Security Event logs, it is considered best practice to use the Event Log Readers group. However, if you do need to transfer Security Event log information, you must use the local Administrators group.

By default, the Local Users And Groups MMC snap-in does not permit you to add computer accounts. You must click the Object Types button in the Select Users, Computers, Or Groups dialog box and select the Computers check box. You can then add computer accounts.

To configure a computer running Windows 7 to collect events, open an elevated command prompt and enter the following command to configure the Windows Event Collector service:

```
wecutil qc
```

When you have configured the source and collector computers, you next configure the event subscription by specifying what events the collector computer needs to retrieve and the event sources (specifically the source computers) from which it must retrieve them.



---

**EXAM TIP**

Distinguish between *Winrm* and *Wecutil*. *Winrm* is used to configure WinRM and is typically used on the source computer. *Wecutil* is used to configure the Windows Event Collector service and is typically used on the collector computer.

---

## Configuring a Source-Initiated Subscription

Source-initiated subscriptions are typically used in enterprise networks in which you can use Group Policy to configure a number of source computers. To configure a source-initiated subscription, you configure the collector computer manually and then use Group Policy to configure the source computers. When the collector computer and source computers are configured, you can create an event subscription to determine which events are forwarded.

Source-initiated subscriptions (sometimes termed *source computer-initiated subscriptions*) enable you to configure a subscription on a collector computer without defining the event source computers. You can then set up multiple remote event source computers by using Group Policy to forward events to the event collector computer. By contrast, in the collector-initiated subscription model, you must define all the event sources in the event subscription.

To configure the collector computer in a source-initiated subscription, you need to use command-line commands entered in an elevated command prompt. If the collector and source computers are in the same domain, you must create an event subscription Extensible Markup Language (XML) file (called, for example, Subscription.xml) on the collector computer, open an elevated command prompt on that computer, and configure WinRM by entering the following command:

```
winrm qc -q
```

Configure the Event Collector service on the same computer by entering the following command:

```
wecutil qc -q
```

Create a source-initiated subscription on the collector computer by entering the following command:

```
wecutil cs configuration.xml
```

To configure a source computer to use a source-initiated subscription, you first configure WinRM on that computer by entering the following command:

```
winrm qc -q
```

You then use Group Policy to add the address of the event collector computer to the SubscriptionManager setting. From an elevated command prompt, start Group Policy by entering the following command:

```
%SYSTEMROOT%\System32\gpedit.msc
```

In Local Group Policy Editor, under Computer Configuration, expand Administrative Templates, expand Windows Components, and select Event Forwarding. Note that you do not have this option if you have already configured your computer as a collector computer.

Right-click the SubscriptionManager setting and select Properties. Enable the SubscriptionManager setting and then click Show. Add at least one setting that specifies the event collector computer. The SubscriptionManager Properties window contains an Explain tab that describes the syntax for the setting.

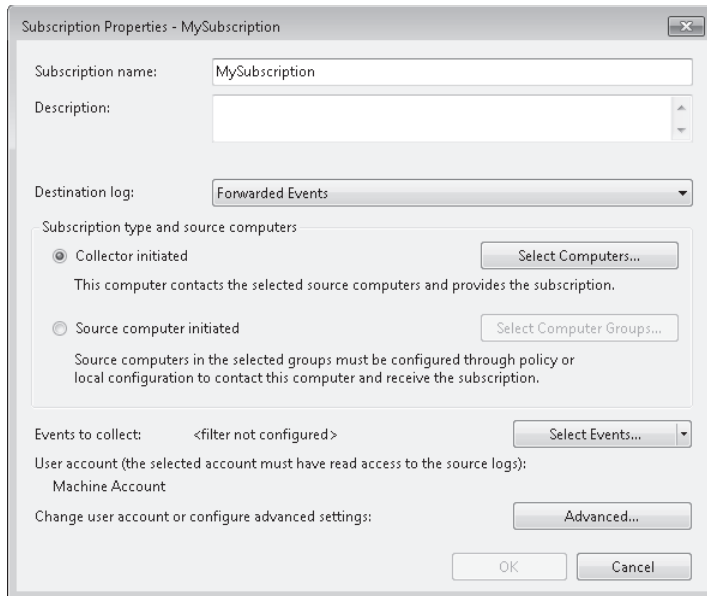
After the SubscriptionManager setting has been added, run the following command to ensure that the policy is applied:

```
gpupdate /force
```

## Creating an Event Subscription

To receive events transferred from a source computer to a collector computer, you must create one or more event subscriptions. Before setting up a subscription, configure both the collector and source computers as previously described. To create a subscription on a collector computer, perform the following procedure:

1. In Event Viewer, right-click Subscriptions and select Create Subscription.
2. If prompted, click Yes to configure the Windows Event Collector Service to start automatically.
3. In the Subscription Properties dialog box shown in Figure 13-22, type a name for the subscription. You can also type a description if you want.
4. Select and configure the type of subscription you want to create—Collector Initiated or Source Computer Initiated. Specify Computers or Computer Groups.



**FIGURE 13-22** The Subscription Properties dialog box

5. Click the Select Events button in the Subscription Properties dialog box to open the Query Filter dialog box. Use this dialog box to define the criteria that forwarded events must match. Then click OK.
6. If you want, you can click the Advanced button in the Subscription Properties dialog box to open the Advanced Subscription Settings dialog box. You can configure three types of subscriptions: Normal, Minimize Bandwidth, and Minimize Latency.

**NOTE SPECIFYING THE ACCOUNT THE SUBSCRIPTION USES**

Use the Advanced Subscription Settings dialog box to configure the account the subscription uses. Whether you use the default Machine Account setting or specify a user, you must ensure that the account is a member of the source computer's Event Log Readers group (or, if you are collecting Security Event log information, the local Administrators group).

7. Click OK in the Subscription Properties dialog box to create the subscription.

**PRACTICE Using Performance Monitor to Generate a Snapshot of Disk Performance Data**

In this practice, you take a snapshot of performance data on your Canberra computer. You then view this data in graph, histogram, and report format. You will probably obtain different results from the Canberra computer in your practice network. Before you carry out this practice, connect a second storage device, such as a second hard disk or USB flash memory, to your computer.



## EXERCISE 1 Add and Monitor Disk Counters

In this exercise, you add counters that enable you to monitor the performance of your system (C:) hard disk volume. If you have additional volumes on a single hard disk or additional hard disks on your system, you can extend the exercise to monitor them as well.

### NOTE DISKPERF

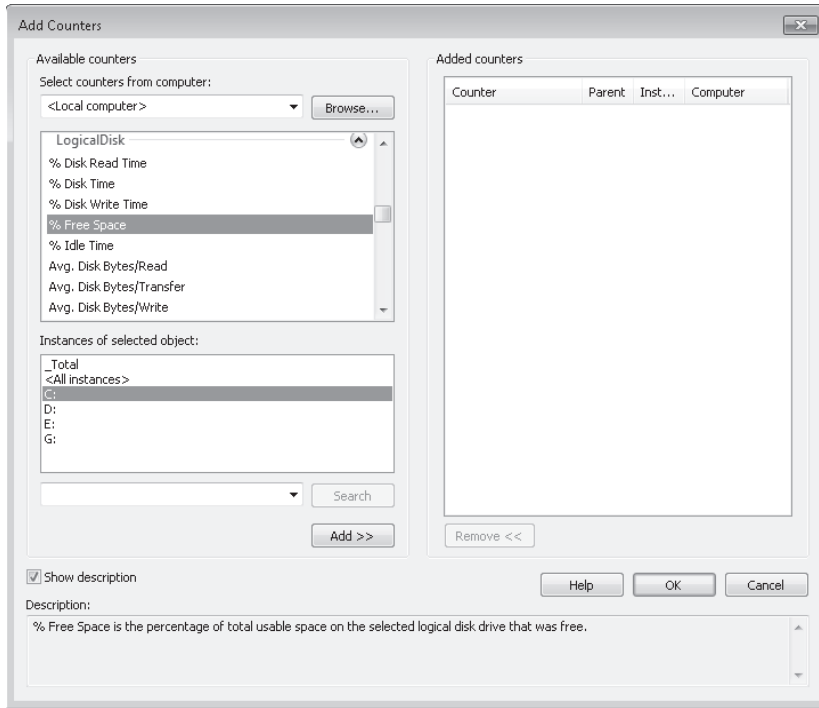
Both logical and physical disk performance counters are enabled on demand by default on Windows 7. The *Diskperf* command still exists, and you can use it to enable or disable disk counters forcibly for older applications that use *ioctl\_disk\_performance* to retrieve raw counters.

### MORE INFO THE IOCTL\_DISK\_PERFORMANCE FILE

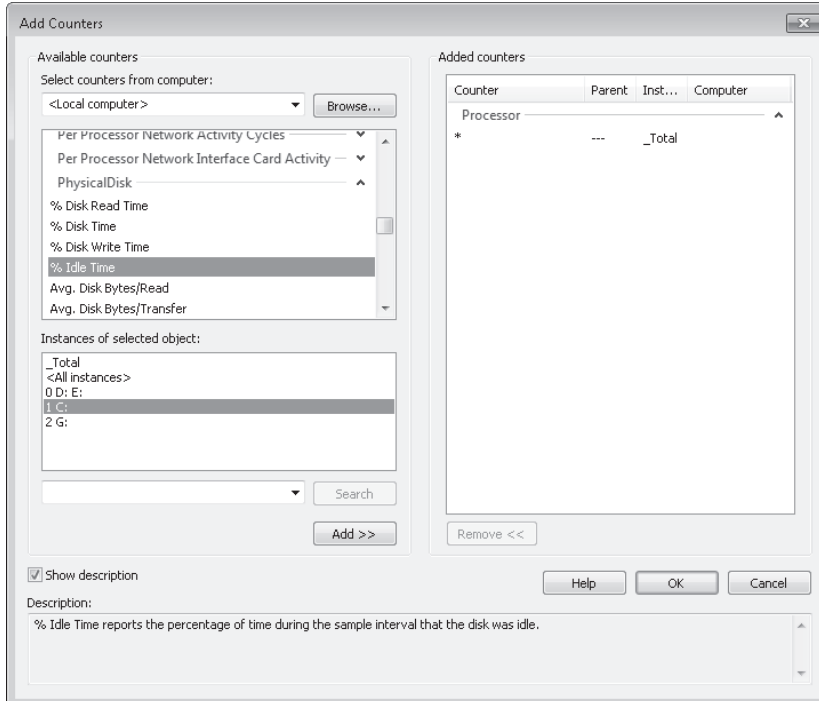
For more information about *ioctl\_disk\_performance*, see <http://msdn.microsoft.com/en-us/library/ms804569.aspx>. Note, however, that this is an older feature and is unlikely to be tested in the 70-680 examination.

A bottleneck affecting disk usage and speed has a significant impact on a computer's overall performance. To add counters that monitor disk performance, perform the following procedure:

1. Log on to the Canberra computer using the Kim\_Akers account.
2. Open Performance Monitor.
3. In Performance Monitor, click the Add button (the green + symbol).
4. In the Add Counters dialog box, ensure that Local Computer is selected in the Select Counters From Computer drop-down list.
5. Select the Show Description check box.
6. Select any counters currently listed in the Added Counters pane and click Remove.
7. In the Counter Selection pane, expand LogicalDisk and select % Free Space. In the Instances Of Dialog Box pane, select C:, as shown in Figure 13-23. The LogicalDisk\% Free Space counter measures the percentage of free space on the selected logical disk drive. If this falls below 15 percent, you risk running out of free space for the operating system to store critical files.
8. Click Add to add this counter.
9. In the Counter Selection pane, expand PhysicalDisk and select % Idle Time. In the Instances Of Dialog Box pane, select C:, as shown in Figure 13-24. This counter measures the percentage of time the disk was idle during the sample interval. If this value falls below 20 percent, the disk system is said to be saturated, and you should consider installing a faster disk system.
10. Click Add to add this counter.



**FIGURE 13-23** Selecting the Logical Disk\% Free Space Counter for the C: drive



**FIGURE 13-24** Selecting the Physical Disk\% Idle Time Counter for the C: drive

11. Use the same technique to add the C: instance of the PhysicalDisk\Avg. Disk Sec/Read counter. This counter measures the average time in seconds to read data from the disk. If the value is larger than 25 milliseconds (ms), the disk system is experiencing latency (delay) when reading from the disk. In this case, consider installing a faster disk system.
12. Use the same technique to add the C: instance of the PhysicalDisk\Avg. Disk Sec/Write counter. This counter measures the average time in seconds to write data to the disk. If the value is larger than 25 ms, the disk system is experiencing latency (delay) when writing to the disk. In this case, consider installing a faster disk system.

#### **MORE INFO** PHYSICALDISK\% DISK TIME COUNTER

Because the value in the PhysicalDisk\% Disk Time counter can exceed 100 percent, many administrators prefer to use PhysicalDisk\% Idle Time, PhysicalDisk\Avg. Disk Sec/Read, and PhysicalDisk\Avg. Disk Sec/Write counters to obtain a more accurate indication of hard disk usage. For more information about the PhysicalDisk\% Disk Time counter, see <http://support.microsoft.com/kb/310067>.

13. Use the same technique to add the C: instance of the PhysicalDisk\Avg. Disk Queue Length counter. This counter indicates how many I/O operations are waiting for the hard drive to become available. If the value of this counter is larger than twice the number of spindles in a disk array the physical disk itself might be the bottleneck.
14. Use the same technique to add the Memory\Cache Bytes counter. This counter indicates the amount of memory being used for the file system cache. There might be a disk bottleneck if this value is greater than 300 MB.
15. Check that the Add Counters dialog box shows the same counters and instances as Figure 13-25. Click OK.

#### **NOTE** COUNTER INCLUDED BY DEFAULT

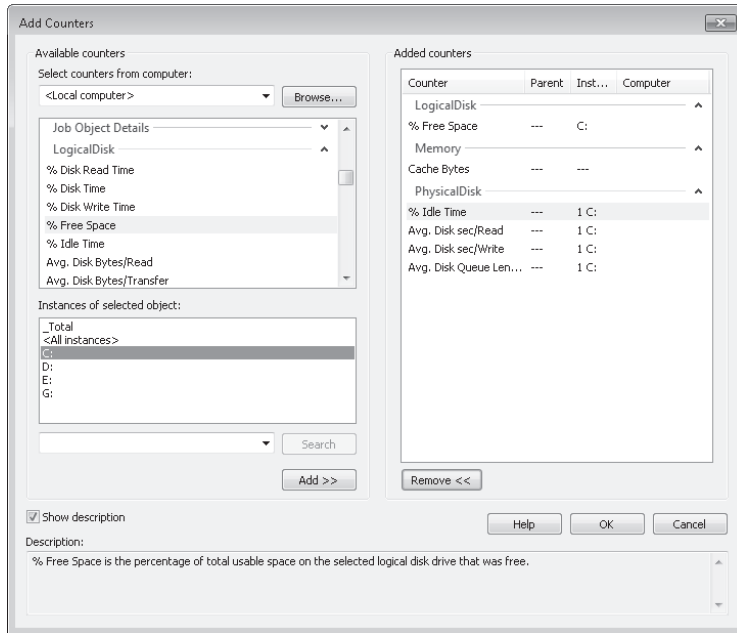
The Processor\%Processor Time counter is included by default and you do not need to add it. It does not appear in the list in Figure 13-25, but you can see it in the line graph, histogram, and report views shown in Exercise 2.

16. Do not close Performance Monitor. Go directly to Exercise 2.

### **EXERCISE 2** Set Performance Monitor Properties and Monitor Disk Performance

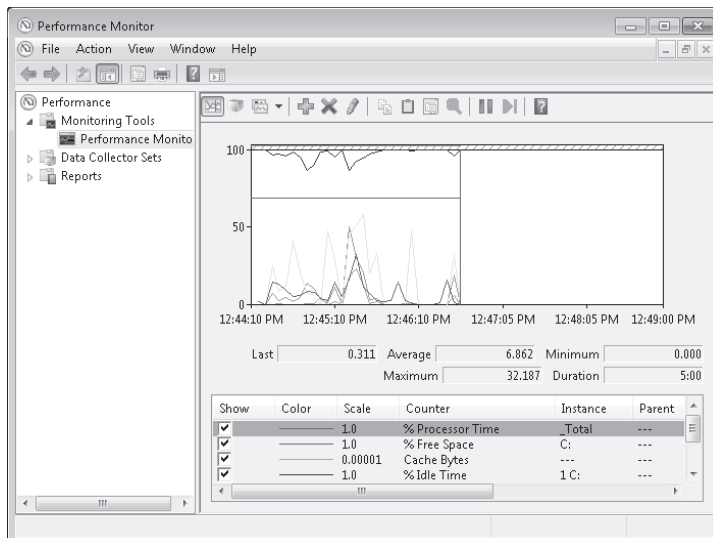
In this exercise, you set the sample interval and duration, read data from, and write data to the disk volume you are monitoring. You view the results in line, histogram, and report formats. Perform this exercise immediately after Exercise 1.

1. In the Performance Monitor Action pane, click More Actions and then click Properties.
2. On the General tab of the Performance Monitor Properties dialog box, in the Graph Elements section, change the Sample Every value to 5 and the Duration value to 300. Click OK.



**FIGURE 13-25** Counters and instances added

3. Copy a file or folder (about 100 MB in size) from your C: drive to your attached storage device.
4. Copy a file or folder (about 100 MB in size) from your attached storage device to your C: drive.
5. View the line graph in Performance Monitor, as shown in Figure 13-26. This might not easily provide the information you are looking for.



**FIGURE 13-26** Performance Monitor line graph view

- In the Change Graph drop-down list, select Histogram Bar. View the histogram in Performance Monitor, as shown in Figure 13-27.

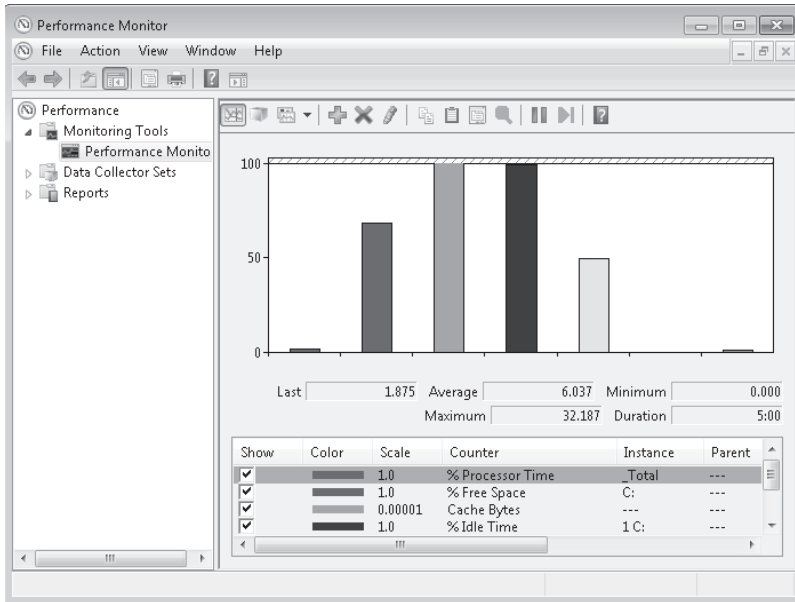


FIGURE 13-27 Performance Monitor histogram view

- In the Change Graph drop-down list, select Report. View the Report in Performance Monitor, as shown in Figure 13-28.

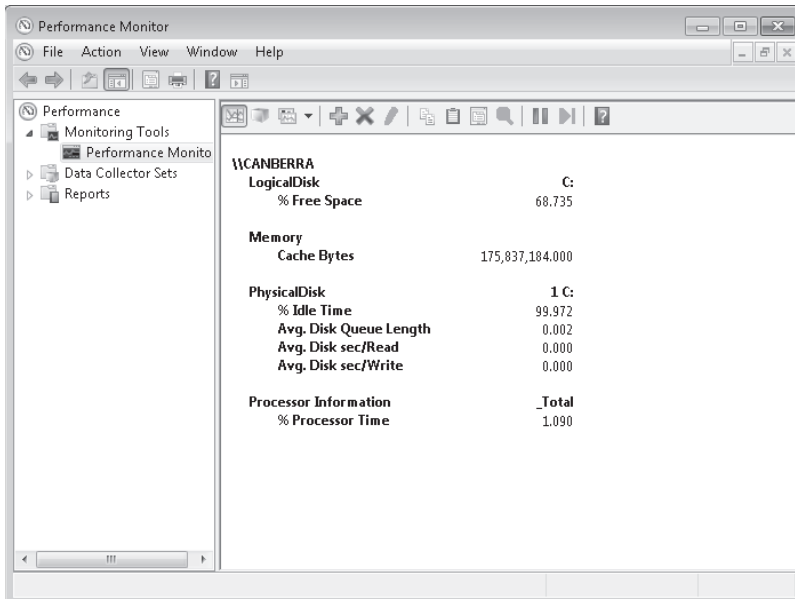


FIGURE 13-28 Performance Monitor report view

8. Analyze the counter values in light of the information given about each counter in Exercise 1. The results shown in the screen shots indicate that adequate free space remains on the C: volume and no problem occurred when copying a fairly large file or folder. Cache memory usage was significant, but this is normal and acceptable in this operation. The results you obtain are likely to be different.

#### **NOTE FILE CACHING**

To obtain meaningful results, Exercise 2 asked you to obtain line, histogram, and report views for the same copying operations. Had you been asked to repeat the copy operations to obtain the histogram and report views, the results would have been different. This is because Windows 7 would have cached the file or folder after the first copy and the subsequent results would have reflected only the impact of writing the file to disk and retrieving it from RAM. Using the tools is relatively straightforward; interpreting the results sometimes is not.

## Lesson Summary

- You can use Performance Monitor to view performance data in real time or performance counter values captured in DCSs. A system diagnostics report gives you details about the status of hardware resources, system response times, and processes on the local computer, along with system information and configuration data.
- Reliability Monitor tracks a computer's stability. It can also tell you when events that could affect stability (such as the installation of a software application) occurred and whether any restarts were required after these events. Action Center monitors your computer and reports problems with security, maintenance, and related settings. The Windows Experience Index indicates the suitability of your current computer hardware for running resource-intensive applications.
- Task Manager gives you a snapshot of resource usage and lets you manage applications, service, and protocols. Resource Monitor allows you to view information about hardware and software resource use in real time. Process Explorer performs the same functions as Task Manager but gives you additional controls and more detailed system information.
- Event Viewer lets you access and filter event logs and create custom views. You can attach tasks to events and configure event forwarding and event subscriptions so that a central computer can store events generated on one or more source computers.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Monitoring Systems." The questions are also available on the companion DVD 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 have upgraded the hardware on a computer so that it can run an application that requires a large amount of processor resource. You use the Windows Experience Index tool to generate a new base score. The subscores for each feature are as follows:

■ Processor	5.1
■ Physical Memory (RAM)	3.3
■ Graphics	3.6
■ Gaming Graphics	2.3
■ Primary Hard Disk	5.3

Based on these figures, what is the Windows Experience Index base score?

- A.** 2.3  
**B.** 3.9  
**C.** 5.1  
**D.** 4.4
2. A client running Windows 7 is experiencing intermittent performance problems. You suspect the problems might be caused by an application that you recently installed but you have forgotten exactly when you did this. Which tool or feature would you use to determine when the application was installed?
- A.** Reliability Monitor  
**B.** Action Center  
**C.** DCSs  
**D.** Performance Monitor
3. Which of the following types of information are stored in Reliability Monitor? (Choose all that apply; each correct answer presents part of a complete solution.)
- A.** An application failed and needs to be restarted.  
**B.** A Windows error occurred and the system was rebooted.  
**C.** An application was uninstalled.  
**D.** A service was stopped.  
**E.** A device driver failed.
4. You are configuring a client running Windows 7 named Canberra to retrieve events from a computer running Windows 7 named Aberdeen. Both computers are on the same workgroup. Which of the following commands would you run on the collector computer to configure the Event Collector service?
- A.** `wecutil qc`  
**B.** `winrm qc`

- C.** `winrm qc -q`
  - D.** `%SYSTEMROOT%\System32\gpedit.msc`
- 5.** You want to use Performance Monitor to display performance data captured in a DCS. You open the tool and access the Performance Monitor Properties dialog box. On which tab can you choose whether to display current activity in real time or log files that you have saved using a DCS?
- A.** General
  - B.** Source
  - C.** Data
  - D.** Graph
  - E.** Appearance



## Lesson 2: Configuring Performance Settings

---

This lesson looks at configurations that can affect the performance of your computer and the tools that Windows 7 provides to display and reconfigure performance settings and resolve performance issues. If you do not like the tools provided, you can use Windows Management Instrumentation (WMI) scripts to write your own.

Many factors affect performance, such as the appearance of your screen or your browser window, the services and processes that are running on your computer, and the priorities and processor affinity that you assign to various processes. Performance is affected by your cache and page file settings, by the services and applications that start automatically or run even when not required, and by what processes are running and the amount of resources each consumes.

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

- Use a variety of Windows tools to inspect and configure settings that affect Windows 7 performance.
- Write WMI scripts that return system information and use the WMI tools.
- Troubleshoot performance issues.

**Estimated lesson time: 45 minutes**

## Obtaining System Information Using WMI

WMI lets you access system management information and is designed to work across networks. It provides a consistent model of the managed environment and a WMI class for each manageable resource. A WMI class is a description of the properties of a managed resource and the actions that WMI can perform to manage that resource. A managed resource is any object (computer hardware, computer software, service, or user account) that can be managed by using WMI.

To use WMI, you write scripts that use the WMI scripting library. This library lets you work with WMI classes that correspond to managed resources. You can use this approach to manage resources such as disk drives, event logs, and installed software.

You can use Windows Script Host (WSH), Microsoft Visual Basic Scripting Edition (VBScript), Microsoft JScript, or scripting languages such as ActivePerl to write WMI scripts that automate the management of aspects of your network. Typically, Windows Management Instrumentation (WMI) files have `.vbs` extensions.

You can write scripts to manage event logs, file systems, printers, processes, registry settings, scheduled tasks, security, services, shared folders, and so on. You can create WMI-based scripts to manage network services, such as the Domain Name System (DNS), and to manage client-side network settings, such as whether a computer is configured with static

Internet Protocol version 4 (IPv4) address settings or whether it obtains these settings from a Dynamic Host Configuration Protocol (DHCP) server. WMI scripts can monitor and respond to entries in an event log, modifications to the file system or the registry, and other real-time operating system changes.

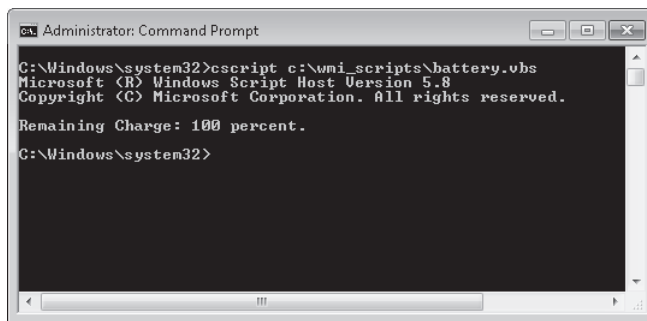
A WMI script works with WMI classes, which are representations of physical features or services on a computer. Each class can contain one or more objects or instances and the objects have attributes. You can display the value of each attribute or pass this on to another routine for analysis.

Typically, you type WMI scripts using a text editor such as Microsoft Notepad and save them as *.vbs* files in a directory (for example, *C:\WMI\_Scripts*) that you have created for this purpose. Be wary of using word processing software such as Microsoft Office Word for this process. Word processing software often uses different styles of quotation marks for different fonts (to cite one example), and this can cause syntax errors. You can run WMI scripts from an elevated command prompt by using the *Cscript* utility, and you can create batch files that run scripts at scheduled intervals or when triggered by an event.

For example, the following WMI script accesses instances of the *Win32\_Battery* class (there is only one) and prints out the value of the *EstimatedChargeRemaining* attribute. The code looks more complex than it actually is. You can substitute other WMI classes and find the values of their attributes by substituting the class and the attributes in this routine.

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\." & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf("Win32_Battery")
For Each objSWbemObject In colSWbemObjectSet
Wscript.Echo "Remaining Charge: " & objSWbemObject.EstimatedChargeRemaining & "
percent."
Next
```

Figure 13-29 shows the output from this script file, saved as *Battery.vbs* in the *C:\WMI\_Scripts* folder. Note that if you run this script on a desktop computer, it should complete without error, but it does not give an output.

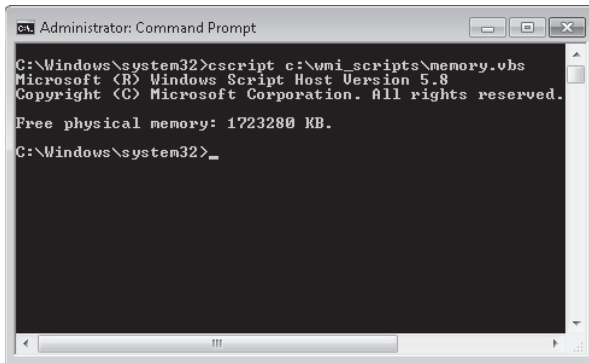


**FIGURE 13-29** Estimated battery charge remaining read by a WMI script

You can substitute other WMI classes and find the values of their attributes by substituting the class and the attributes in the previous script. For example, *FreePhysicalMemory* is an attribute of objects in the *Win32\_OperatingSystem* class (typically, there would be only one object in this class). The following WMI script outputs the free physical memory on a computer in kilobytes:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\." & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_OperatingSystem")
For Each objSWbemObject In colSWbemObjectSet
Wscript.Echo "Free physical memory: " & objSWbemObject.FreePhysicalMemory & " KB."
Next
```

Figure 13-30 shows the output from this script file, saved as *Memory.vbs* in the *C:\WMI\_Scripts* folder.



**FIGURE 13-30** Free physical memory read by a WMI script

#### **MORE INFO** LIST OF WMI CLASSES

You can obtain a list of WMI classes and their attributes at [http://msdn.microsoft.com/en-us/library/aa394554\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa394554(VS.85).aspx). For a complete WMI reference, see [http://msdn.microsoft.com/en-us/library/aa394572\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa394572(VS.85).aspx).

#### **WARNING** WMI CLASSES

If you use a WMI class, ensure that Windows 7 supports it. For example, the class *Win32\_LogicalMemoryConfiguration* is deprecated and not supported. If you specify this class and run your script on a computer running Windows 7, this generates a 0x80041010 error.

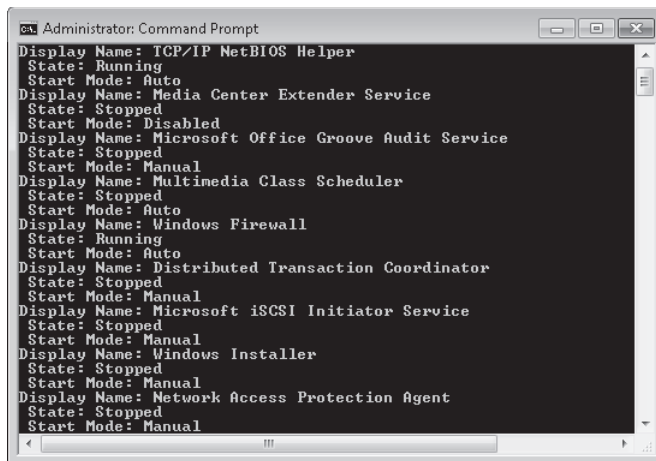
You can write scripts that manage WMI classes that contain a number of objects. For example, the *Win32\_Services* class contains all the services that run on a computer. The following script lists all these services:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\." & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_Service")
For Each objSWbemObject In colSWbemObjectSet
Wscript.Echo "Display Name: " & objSWbemObject.DisplayName & vbCrLf
Next
```

You can expand the previous script to determine the state (started or stopped) and the start mode for each service as follows:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\." & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_Service")
For Each objSWbemObject In colSWbemObjectSet
Wscript.Echo "Display Name: " & objSWbemObject.DisplayName & vbCrLf
& " State: " & objSWbemObject.State & vbCrLf
& " Start Mode: " & objSWbemObject.StartMode
Next
```

Figure 13-31 shows some of the output from the preceding script.



```
Administrator: Command Prompt
Display Name: TCP/IP NetBIOS Helper
State: Running
Start Mode: Auto
Display Name: Media Center Extender Service
State: Stopped
Start Mode: Disabled
Display Name: Microsoft Office Groove Audit Service
State: Stopped
Start Mode: Manual
Display Name: Multimedia Class Scheduler
State: Stopped
Start Mode: Auto
Display Name: Windows Firewall
State: Running
Start Mode: Auto
Display Name: Distributed Transaction Coordinator
State: Stopped
Start Mode: Manual
Display Name: Microsoft iSCSI Initiator Service
State: Stopped
Start Mode: Manual
Display Name: Windows Installer
State: Stopped
Start Mode: Manual
Display Name: Network Access Protection Agent
State: Stopped
Start Mode: Manual
```

**FIGURE 13-31** Determining the state and start mode of each service

You use WMI to administer managed resources. These include the computer system, Active Directory Domain Services (AD DS), disks, peripheral devices, event logs, files, folders, file systems, networking features, operating system subsystems, performance counters, printers, processes, registry settings, security, services, shared folders, users and groups, Windows Installer, device drivers, Simple Network Management Protocol (SNMP) management information base (MIB) data, and so on.

When you write scripts that interact with WMI-managed resources, the term *instance* is used to refer to the managed resource in the script. For example, the following script returns the drive letter for each logical disk drive on your computer:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\." & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_LogicalDisk")
For Each objSWbemObject In colSWbemObjectSet
Wscript.Echo objSWbemObject.DeviceID
Next
```

You can prompt for input in a WMI script and store this in a variable. For example, the following (partial) script prompts the user for a password and stores it in the string variable *strPassword*, which could, for example, be used with the *Connect.Server* function to connect to a server on the network:

```
strComputer = "."
Wscript.StdOut.Write "Please enter the administrator password: "
strPassword = Wscript.StdIn.ReadLine
```

The next script is a more complete routine that you can adapt for your own purposes. It uses the *inputbox* function to prompt for a computer name and then uses the *MsgBox* function to display information about that computer's printers, processes, and processor. The code is not significantly more complex than the previous examples—you are simply displaying the values of object attributes—but using the built-in functions gives the script a professional feel:

```
computer = inputbox ("What computer do you want to check? (Press Enter if this
computer)", "Computer")
set WMI = GetObject("WinMgmts://" & computer)
If computer="" then computer = "this computer"

List = ""
Set objs = WMI.InstancesOf("Win32_Printer")
For each obj in objs
    List = List & obj.Caption & ", "
Next
List=Left(List, Len(List)-2)
MsgBox List,64,"Printers on " & computer

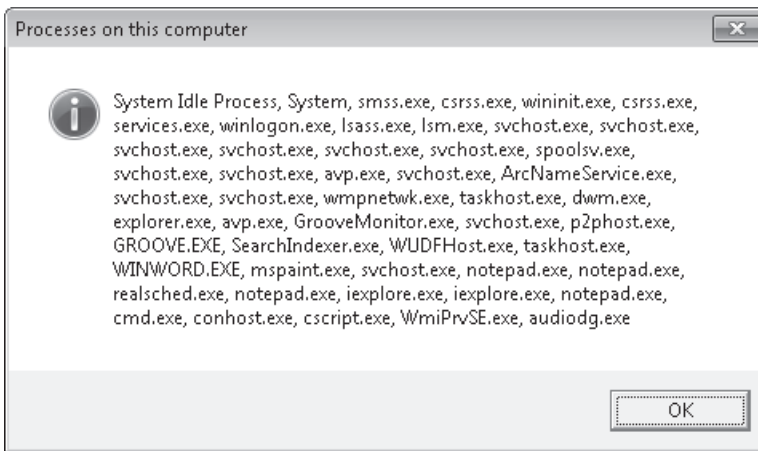
List = ""
Set objs = WMI.InstancesOf("Win32_Process")
For each obj in objs
List = List & obj.Description & ", "
Next
List=Left(List, Len(List)-2)
MsgBox List,64,"Processes on " & computer
```

```

List = ""
set objs = WMI.InstancesOf("Win32_Processor")
For each obj in objs
    List = List & obj.Description & ", "
Next
List=Left(List, Len(List)-2)
MsgBox List,64,"Processor on " & computer

```

Note that if you specify the Aberdeen computer when you run this script on Canberra, you need to ensure the \\Canberra\Kim\_Akers account has administrator rights on Aberdeen. Only a local administrator can run a WMI script on a computer, although if you have the appropriate rights, running WMI scripts on remote computers is straightforward. The script is possibly more relevant to an enterprise environment where Domain and Enterprise Admins have rights on every machine. Also, ensure that the firewalls are not blocking the information. Figure 13-32 shows the list of processes on Canberra displayed in a message box.



**FIGURE 13-32** Processes on this computer (Canberra)

WMI consists of three primary features: the Common Information Model Object Manager (CIMOM), also known as the WMI service; the Common Information Model (CIM) repository, also known as the WMI repository; and WMI providers. Together, these features provide an infrastructure through which configuration and management data is defined, exposed, accessed, and retrieved.

## WMI Providers

WMI providers, such as Win32 and the built-in Event Log provider, act as intermediaries between the CIMOM and a managed resource. Providers request information from and send instructions to WMI-managed resources on behalf of applications and scripts. Providers expose the managed resource to the WMI infrastructure using a standards-based access model, communicate with their respective managed resources by using the native application programming interfaces (APIs) of the managed resource, and communicate with the CIMOM

by using WMI programming interfaces. Windows 7 introduces additional providers for Windows PowerShell and virtualization.

To create an application that manages Windows subsystems, you typically use the Win32 APIs. Without WMI, you would need to call these APIs yourself. Unfortunately, Win32 APIs cannot be called from a script, and you would need to use a programming language such as C++ or Microsoft Visual Basic. Writing C++ or Virtual Basic code is typically much more difficult than writing a script.

When you use WMI providers, you do not have to worry about calling the Win32 APIs because WMI does that for you. Also, you do not have to worry about differences between various APIs because you use a standard set of WMI commands and WMI translates those commands into commands that the APIs understand.

WMI providers are generally implemented as DLLs in the `SystemRoot\System32\Wbem` directory. The built-in providers, also known as *standard providers*, supply data and management functions from well-known operating system sources, such as the Win32 subsystem, event logs, performance counters, and the registry.

## The CIMOM

The CIMOM handles the interaction between consumers and providers. It acts as the WMI information broker and all WMI requests and data flow through the CIMOM. When you write a WMI script, the script is directed to the CIMOM. However, the CIMOM does not directly handle your request. For example, suppose that you request a list of all the services installed on a computer. The CIMOM does not actually retrieve the list of services for you. Instead, it locates the appropriate WMI provider and asks the provider to retrieve the list. When the list has been retrieved, the CIMOM returns the information to you.

## The WMI Service

The WMI service (`Winmgmt.exe`) implements the CIMOM on Windows 7. You can start and stop it from an elevated command prompt like any other service (for example, `net stop winmgmt`). Be aware, however, that if you stop the WMI service, this also stops the Security Center and IP Helper services. If the WMI service is stopped and you run a script or an application that requires WMI, the service automatically restarts.

## The CIM Repository

Management applications, administrative tools, and scripts make requests to the CIMOM to retrieve data, subscribe to events, or to perform some other management-related task. The CIMOM retrieves the provider and class information necessary to service consumer requests from the CIM repository. The CIMOM uses the information obtained from the CIM repository to hand off consumer requests to the appropriate WMI provider.

The CIM repository holds the schema, also called the *object repository* or *class store*, which defines all data exposed by WMI. The schema is similar to the AD DS schema and is built on the concept of classes. A class is a blueprint of a WMI-manageable resource. However, unlike

AD DS classes, CIM classes typically represent dynamic resources. Instances of resources are not stored in the CIM repository but are dynamically retrieved by a provider based on a consumer request. This means that the term *repository* is somewhat misleading. Although the CIM is a repository and is capable of storing static data, its primary role is storing the blueprints for managed resources.

The operational state for most WMI-managed resources changes frequently (for example, all the events in all event logs on a computer) and is read on demand to ensure that the most up-to-date information is retrieved. This can sometimes cause queries to run slowly if a lot of information needs to be retrieved, but this is preferable to using the computer resource that would be required to maintain an up-to-date repository of frequently changing data.

## CIM Classes

CIM classes are organized hierarchically and child classes inherit from parent classes. The Distributed Management Task Force (DMTF) maintains the set of core and common base classes from which system and application software developers derive and create system-specific or application-specific extension classes. Classes are grouped into namespaces, logical groups representing a specific area of management. CIM classes include both properties and methods. Properties describe the configuration and state of a WMI-managed resource; methods are executable functions that perform actions on the WMI-managed resource associated with the corresponding class.

### **MORE INFO** DMTF

For more information about the Distributed Management Task Force, visit the DMTF home page at <http://www.dmtf.org/home/>.

## WMI Consumers

A WMI consumer can be a script, an enterprise management application, a Web-based application, or some other administrative tool that accesses and controls management information available through the WMI infrastructure. For example, the script listed earlier that discovered and listed the logical disk drives on your computer is a WMI consumer. An application can be both a WMI provider and a WMI consumer (for example, Microsoft Application Center and Microsoft Operations Manager).

## WMI Scripting Library

The WMI scripting library provides the set of automation objects through which scripting languages such as VBScript access the WMI infrastructure. The WMI scripting library is implemented in a single automation feature named `Wbemdisp.dll` that is stored in the `SystemRoot\System32\Wbem` directory. The Automation objects in the WMI scripting library provide a consistent and uniform scripting model for WMI-managed resources.





### EXAM TIP

It is important to distinguish between managed resource class definitions and automation objects. Managed resource class definitions reside in the CIM repository (Cim.rep) and provide the blueprints for the computer resources exposed through WMI. A general-purpose set of automation objects reside in the WMI scripting library and scripts can use these objects to authenticate and connect to WMI. After you obtain an instance of a WMI-managed resource using the WMI scripting library, you can access the methods and properties defined by the class definition of the managed resource.

## Variable Naming Convention

WMI scripts typically follow a consistent convention when naming variables. Each variable is named according to the automation object name in the WMI scripting library and is prefaced with *obj* (to indicate an object reference) or *col* (to indicate a collection object reference). For example, a variable that references an object called *SWbemServices* is named *objSWbemServices*; a variable that references an object called *SWbemObject* is named *objSWbemObject*; and a variable that references an object called *SWbemObjectSet* is named *colSWbemObjectSet*.

This convention is not mandatory, but it helps you understand the type of WMI object that you are working with in a WMI script. Following a consistent naming convention makes your code easier to read and to maintain, especially if you are not the person doing the maintenance.

## The WMI Administrative Tools

You can download the WMI Administrative Tools at <http://www.microsoft.com/downloads/details.aspx?FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314&DisplayLang=en>, although it is probably easier to go to <http://www.microsoft.com/downloads> and search for “WMI Administrative Tools.”

The WMI Administrative Tools include the following:

- **WMI Common Information Model (CIM) Studio** Enables you to view and edit classes, properties, qualifiers, and instances in a CIM repository; run selected methods; and generate and compile Managed Object Format (MOF) files.
- **WMI Object Browser** Enables you to view objects, edit property values and qualifiers, and run methods.
- **WMI Event Registration Tool** Enables you to configure permanent event consumers, and to create or view instances of event consumers, filters, bindings, and timer system classes.
- **WMI Event Viewer** Displays events for all instances of registered consumers.

## WMI CIM Studio

WMI CIM Studio is designed primarily for use by developers, particularly those who are writing providers. It assists developers to create WMI classes in the CIM repository. WMI CIM Studio uses a Web interface to display information and relies on a collection of ActiveX features installed on the system when it runs for the first time. The tool enables developers to:

- Connect to a chosen system and browse the CIM repository in any namespace available
- Search for classes by their name, by their descriptions, or by property names
- Review the properties, methods, and associations related to a given class
- See the instances available for a given class of the examined system
- Perform queries in the WMI Query Language (WQL)
- Generate an MOF file based on selected classes
- Compile an MOF file to load it in the CIM repository

WMI CIM Studio also provides wizards for generating and compiling MOF files and for generating framework provider code. When you start WMI CIM Studio from the WMI Tools menu, you first need to click the Information bar and permit ActiveX tools to run. You then select a namespace in the Connect To Namespace dialog box or use the default namespace *Root\CIMV2*. Figure 13-33 shows the WMI CIM Studio tool.

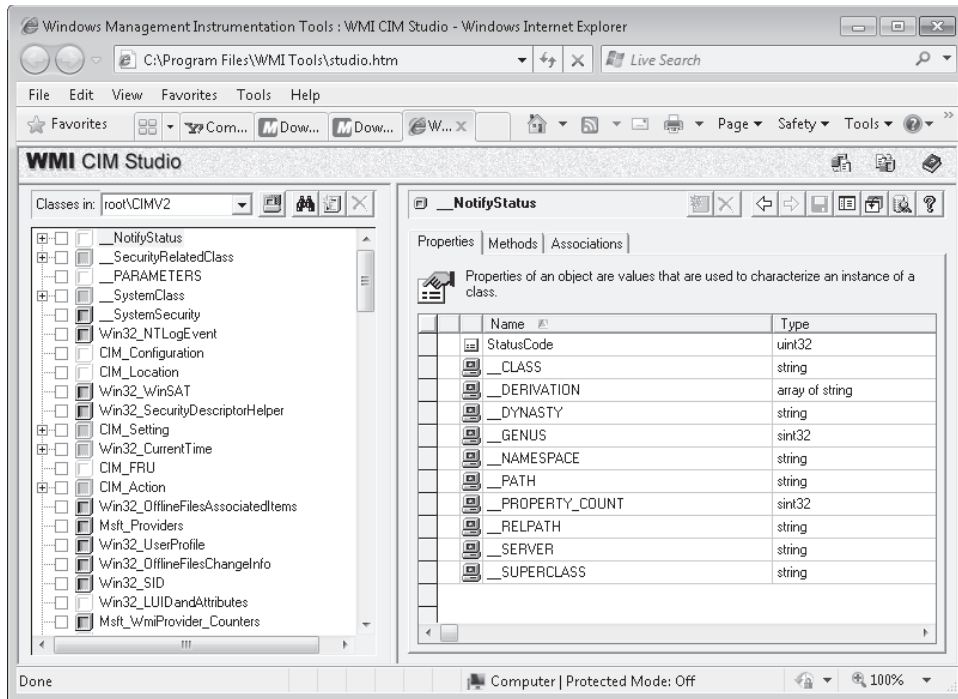


FIGURE 13-33 WMI CIM Studio

WMI CIM Studio contains a Class Explorer and a Class Viewer. When you select classes in the Class Explorer, their details appear in the Class Viewer. WMI CIM Studio wizards generate and compile MOF files.

You can use WMI CIM Studio to view the class inheritance tree for any namespace in your system or on a network by specifying the namespace path in the Classes In box, by clicking the Classes In arrow and selecting the namespace in the history list, or by browsing to a namespace.

You can search for a specific class in the namespace by clicking Search For Class in Class Explorer. In the Search For Class dialog box, select one or more check boxes under Search Options to select the type of search to perform: by class name, class description, or property name. Enter the full or partial text value to use for this search, and click Go. The results of the search appear in the Search Results pane. Click the class to view and then click OK. This displays the chosen class in Class Explorer.

You can display the properties of a class by selecting the class in Class Explorer and then clicking the Properties tab in Class Viewer. Symbols (for example, a key represents a key property) let you identify the following information about a class:

- Key properties
- System properties
- Inherited properties
- Writable properties
- The values contained in property arrays

WMI CIM Studio lets you display instances of an existing class by accessing a table of all instances of the class and viewing the associations of an instance. You can also define and display custom views of instances. You can add and delete class definitions in Class Explorer, and you can modify class definitions by adding, editing, or deleting properties, qualifiers, and methods. You can add and delete instances of a class.

You can execute regular methods on instances in WMI CIM Studio if the instances are implemented and not disabled. Click the class in Class Viewer and click Instances. Right-click the instance you want to work with and select Go To Object. Click the Methods tab in Class Viewer, right-click the method, and select Execute Method. The Parameters column shows the parameters defined for the method and their default values. Before executing the method, you can configure the parameters by editing their values.

The WQL Query Builder lets you write, save, and execute WQL queries. To use this feature, click the WQL Query symbol in Class Viewer. The MOF Generator Wizard in Class Explorer enables you to generate an MOF file for class definitions and instances from an existing repository. Typically, you run this wizard when you have created a new class or when you want to export existing repository information to another computer. You can compile the MOF file into a repository—importing any class definitions or instances from the MOF file into the current repository—by using the MOF Compiler Wizard. This wizard checks the syntax of an MOF file and creates binary MOF files.

## WMI Object Browser

Unlike WMI CIM Studio, the WMI Object Browser is designed for use by system managers. This tool enables you to display the object tree for a CIM repository, view object details, edit object information, and run selected methods. You start WMI Object Browser from the WMI Tools menu and you need to click the Information bar and enable ActiveX controls. You can select a namespace or accept the default.

WMI Object Browser contains an Object Explorer and an Object Viewer. When you select objects in the Object Explorer, their details appear in the Object Viewer. Figure 13-34 shows the WMI Object Browser.

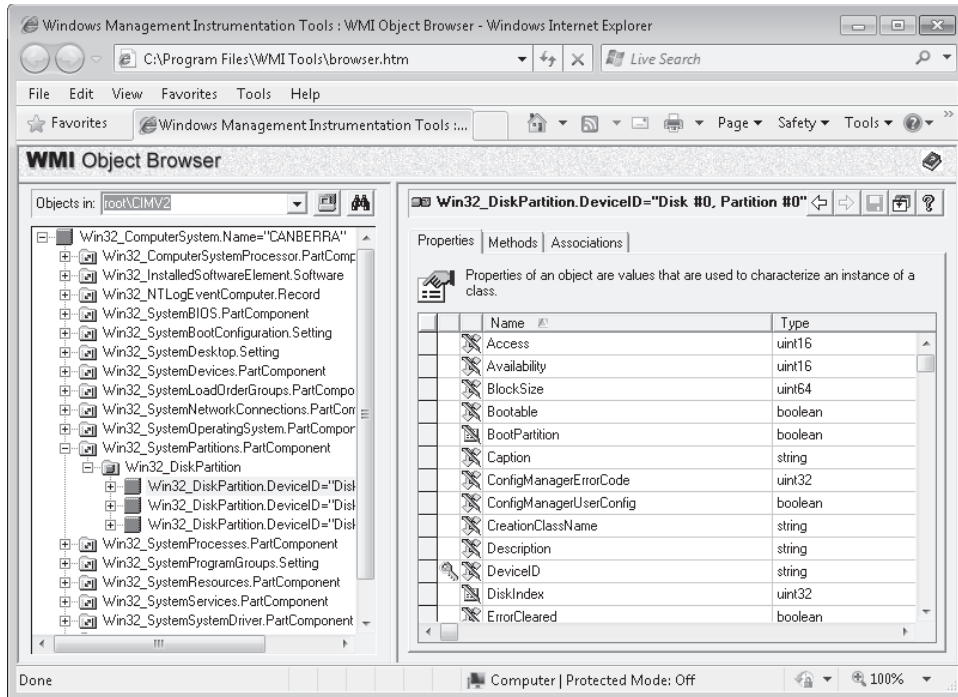
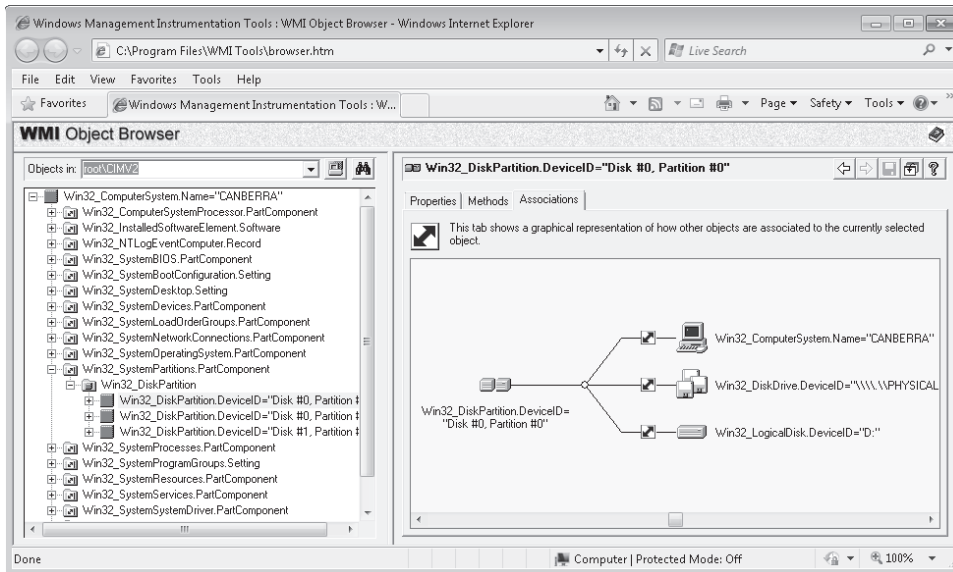


FIGURE 13-34 The WMI Object Browser

The left pane of the WMI Object Browser contains the Object Explorer, which shows the object tree for the current namespace (by default, the *Root\CIMV2* namespace on the local computer). You can select a different local namespace or a namespace on a remote computer. The Object Explorer shows a hierarchy of the instances that are found in the selected namespace and any instance in the namespace can be selected as the root of the tree.

The tree shows regular objects and grouping nodes. Grouping nodes are not objects themselves but instead are used to organize objects. The symbols next to the names indicate the type of object or node. Resting the mouse over an object in the tree displays the object's path, which identifies the object in the namespace.

The right pane of WMI Object Browser shows the Object Viewer. You can select the Properties, Methods, or Associations tab for an object. Figure 13-35 displays the Associations tab. The Object Viewer displays the title of the current view above the tabs. For a single object, the title is the object path of the instance currently displayed. For a multiple-object table, the title describes the group of objects currently displayed.



**FIGURE 13-35** WMI Object Browser Associations tab

WMI Object Browser enables you to do the following:

- Display the object tree contained in a specified CIM repository.
- Reroot the object tree.
- Display properties, methods, and associations for a selected object.
- Display instances of grouped objects.
- Display property and object qualifiers.
- Execute methods on a selected object.
- Edit property values and object and property qualifiers.

You can view the object tree for any namespace in your system or on a network by entering the namespace path in the Objects In box or selecting it in the history list. You can also browse for a namespace or right-click the object whose namespace you want to display and click Go To Namespace. The root of the namespace can be changed temporarily in a session or permanently through the schema.

When you select a grouping node in the Object Explorer, the Object Viewer displays an instance table showing all objects in the namespace that belong to the selected group and

the common properties of those objects. You can also display the details for any individual instance from the instance table by right-clicking the instance and clicking Go To Object. This displays the object's Properties tab. From the Properties tab, you can double-click a property to display property qualifiers. When the Properties tab is selected, you can right-click anywhere in the Object Viewer grid and select Object Qualifiers. Selecting the Properties tab also enables you to edit the Value field of properties that are not read-only. To return to the instance table, reselect the grouping node.

From the Methods tab in the Object Viewer, you can right-click a method and select Execute Method. The Method Parameters window displays the parameters used when executing the selected method. The Parameters column shows the parameters defined for this method and their default values. You can configure parameters by editing the values in this table before you execute the method.

## WMI Event Registration

The WMI Event Registration tool is designed primarily for developers. It provides a graphical interface for what you can also accomplish programmatically. You need to install Windows Management and create a repository of classes on the target computer before you can use the WMI Event Registration Tool. You can do this by compiling an MOF file in the system directory where the WMI Core is installed. To compile the MOF file, type the following at the command-line prompt:

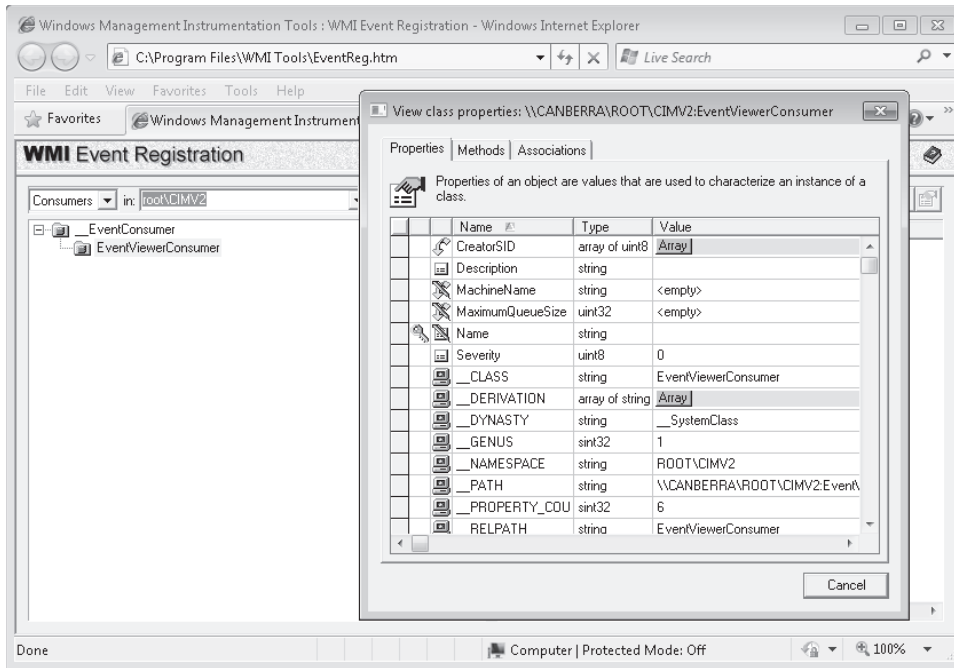
```
mofcomp <filename>.mof
```

However, by default, the WMI Event Registration tool uses the Eviewer.mof file found in the WMI Tools directory. This file is compiled automatically when Windows Management first starts, so the WMI Event Viewer consumer is registered as a permanent event consumer by default and you can open the WMI Event Registration tool and investigate its features.

### **MORE INFO** COMPILING MOF FILES

You can find out more about compiling MOF files by downloading the Windows 7 Platform software development kit (SDK) and accessing the "Mofcomp" topic in the Windows Management Instrumentation (WMI) section. However, this topic is beyond the scope of this book and the 70-680 examination.

You start the WMI Event Registration Tool from the WMI Tools menu and need to allow blocked ActiveX content on the Information bar and specify a root, as with the other tools. From the drop-down menu near the top-left of the WMI Event Registration Tool, you can select Filters, Consumers, or Timers. Double-clicking an item in the left pane opens the View Class Properties dialog box, as shown in Figure 13-36. This lets you access the Properties, Methods, and Associations tabs.



**FIGURE 13-36** The WMI Event Registration tool

The WMI Event Registration Tool enables you to create, display, and modify the event consumers, filters, and timers for a given namespace and any bindings between filters and consumers. You can use the tool to do the following:

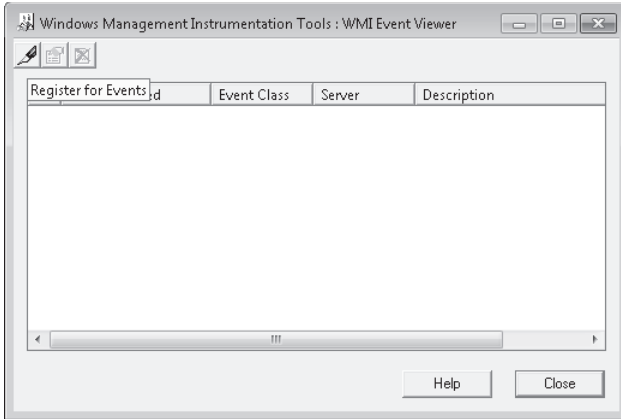
- View properties of the defined consumer, filter, and timer system classes and instances
- Add or delete event consumer instances
- Add or delete event filter instances
- Add or delete event timer instances
- Edit instance properties
- Register consumers for events by binding consumer and filters

## WMI Event Viewer

WMI Event Viewer is a permanent event consumer that lets you sort and view the details of events generated in WMI by Windows Management or by event providers. Event objects are forwarded to any consumers registered for these types of events. You can register WMI Event Viewer for any event filters and view incoming events that match the filters.

You can open WMI Event Viewer from the WMI Tools menu. However, as a permanent event consumer, it is started automatically by WMI whenever an event occurs that needs to be forwarded to it. To register WMI Event Viewer for different types of events, you use the

WMI Event Registration Tool. This tool can be started either independently from the WMI Tools menu or from WMI Event Viewer tool by clicking the Register For Events control, as shown in Figure 13-37.



**FIGURE 13-37** The Register For Events control in WMI Event Viewer

WMI Event Viewer enables you to carry out the following tasks:

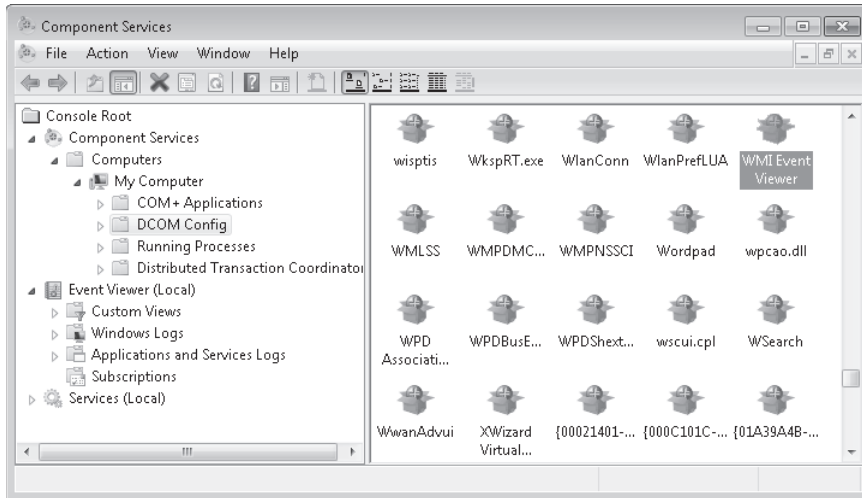
- View Windows Management–generated events and event information, such as the event’s date and time, class, point of origin, and description
- View event instance properties
- Start the WMI Event Registration Tool
- Clear the display

The `Eviewer.mof` file, installed in the WMI Tools directory along with WMI Event Viewer, contains the classes and instances required to declare and register the WMI Event Viewer Consumer Provider with the WMI event subsystem. This MOF file is compiled automatically when the Windows Management Service is first started, so that the WMI Event Viewer consumer is registered as a permanent event consumer by default.

All permanent event consumers, including WMI Event Viewer, require specific distributed component object model (DCOM) permissions to start automatically on a remote computer for a registered event. To set the DCOM launch permissions for WMI Event Viewer so you can monitor events on a remote computer, carry out the following procedure:

1. Run the `Dcomcnfg.exe` program from an elevated command prompt on the remote computer.
2. On the Applications tab of the Distributed COM Configuration Properties dialog box, select WMI Event Viewer, as shown in Figure 13-38, and click Properties.
3. On the Security tab of the WMI Event Viewer Properties dialog box, select Customize and click Edit.
4. Click Add.





**FIGURE 13-38** Selecting WMI Event Viewer in Component Services

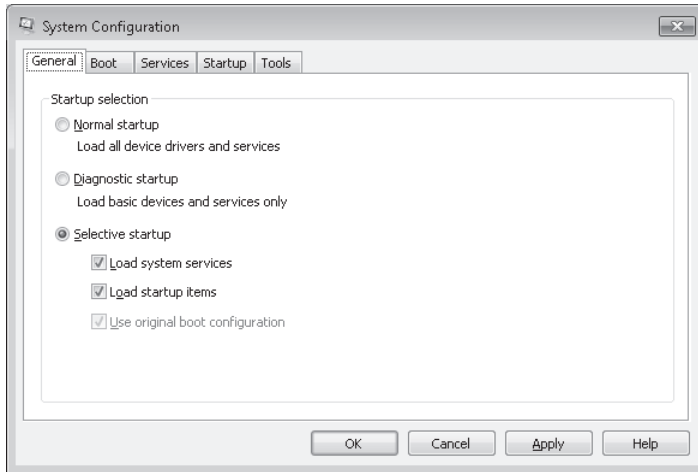
5. In the Add Users And Groups dialog box, type **Everyone**.
6. Click Add. Ensure that all permissions check boxes are selected and then click OK. Note that WMI Event Viewer enables users and event consumers to access event information. It is not a configuration tool. Therefore, there are no security implications to setting these permissions.

## Using the System Configuration Tool

You open System Configuration (MSConfig) by entering **msconfig** in the Start menu Search box, the Run box, or the command prompt. The principal purpose of this tool is to troubleshoot the Windows startup process. MSConfig modifies which programs run at startup, edits configuration files, and enables you to control Windows services and access Windows Performance and Troubleshooting tools.

You can use the System Configuration tool to configure Windows 7 to perform a diagnostic startup that loads a minimum set of drivers, programs, and services. Figure 13-39 shows the General tab of the System Configuration tool, on which you can specify Normal Setup or Diagnostic Setup. You can also customize a Selective Setup and control whether to load System Services and Startup Items. You can select the System Services and Startup Items to load and start on the Services and Startup tabs, respectively, in the System Configuration tool.

It is a good idea to look carefully at the list of programs on the Startup tab. Some software packages—for example, software that detects viruses and other malware—should run at startup and continue to run unless you have a reason to disable them. Other software packages, particularly third-party software, install themselves so that they run at startup whether they need to or not. The more unnecessary programs you have running, the slower your computer goes.



**FIGURE 13-39** The General tab of System Configuration

Services are more difficult to manage than packages because of service dependencies. You might see that a service you have never heard of before runs at startup and decide to change its startup type, only to find that half a dozen essential services all depend on the one that is no longer running. The System Configuration tool lets you experiment with a computer on your test network before making changes to production computers.

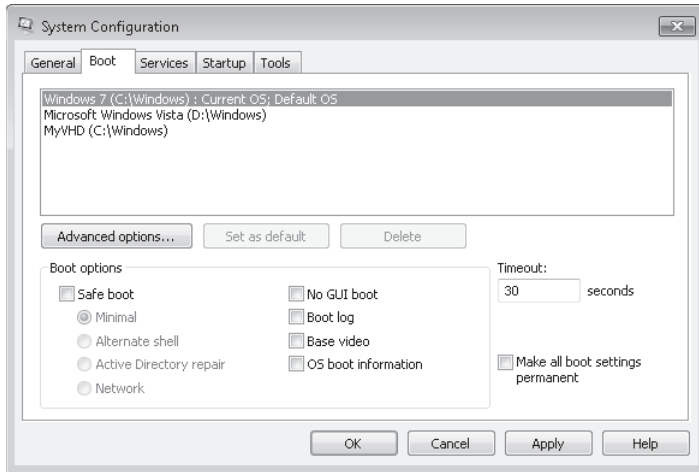
**NOTE** **DISABLING SERVICES WITH MSCONFIG**

Although you can use MSConfig to disable services, this does not change the current state of the service. For example, you can use MSConfig to disable the running Diagnostic Policy service, but the service remains running until you reboot the computer.

The Boot tab of the System Configuration tool lets you specify the source of your boot files and, if desired, make that source the default. For example, in the Boot tab shown in Figure 13-40, the computer is dual-boot, with operating systems on both the C: and D: volumes. It can also boot into Windows 7 Ultimate from a virtual hard drive (VHD). On the Boot tab, you can specify the timeout, which is how long the boot system waits for instructions before booting from its default source.

You can specify Safe Boot and the type of Safe Boot to use (Minimal, Alternate Shell, Active Directory Repair, or Network). You can specify a No-Graphical User Interface (GUI) boot, or, if you are having problems with a video driver, specify a boot that uses the Base Video (lowest-resolution and color-depth) driver. You can require a Boot Log and Operating System (OS) Information. You can use reconfigured boot settings only once or make them permanent.

Clicking Advanced on the Boot tab lets you specify a Debug Port and Baud Rate for remote debugging and the Number Of Processors and Maximum Memory available to the boot process.



**FIGURE 13-40** The Boot tab of System Configuration

On the Startup tab, you can disable automatic startup for an application by clearing the check box beside the item. You can disable automatic startup for all items by clicking Disable All. This does not prevent the software from running—it merely stops it from starting automatically when the computer boots. The Services tab works in much the same way, in that you can disable or enable automatic startup of a single service or of all services. You can also determine what third-party services are running by selecting the Hide All Microsoft Services check box.

The Tools tab performs a very useful function. Not only are all the available tools listed, but you can enable any tool from this tab. This is often easier than trying to remember or deduce the tool's place in the Control Panel hierarchy, whether the tool is a Microsoft Management Console (MMC) snap-in, or what file you need to access from the command prompt to start the tool. The tab also lists the file and file path for the application that runs each tool.



---

**EXAM TIP**

You can use either Task Manager or the Services Console to start and stop services on a computer running Windows 7 without rebooting the computer.

---

## Using the Services Console

The Services console, an MMC snap-in, lists the same services as does the Services tab of the System Configuration tool, but it provides more information about each service and more service management options. For example, the Services console tells you the service startup type (not just whether or not it is running) and the logon details.

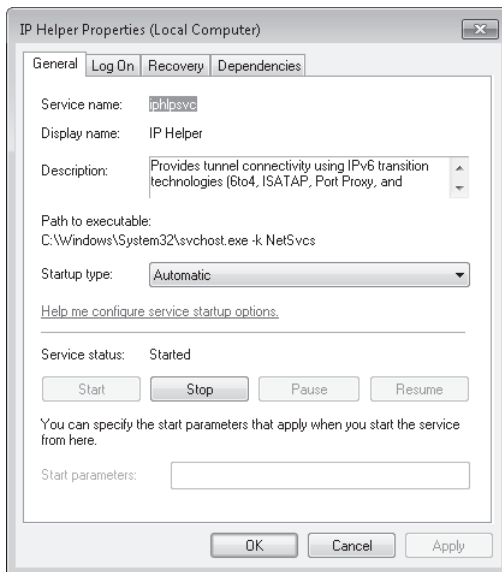
You can access the Services console by entering **services.msc** in the Search box on the Start menu, in the Run box, or in a command-prompt window.

When you right-click a service in the Services console, you can start it, stop it, restart it, pause it, and resume it. You can access the Properties dialog box for the service and select the General, Log On, Recovery, and Dependencies tabs.

The General tab lets you specify the startup type. This can be Automatic, Automatic (Delayed Start) Manual, or Disabled. You should consider the following when specifying the startup type:

- If a service is configured as Automatic, it starts at boot time. Some services also automatically stop when no longer required. However, if you find that you do not need a service, configure its start type as Manual or Disabled.
- If a service is configured as Automatic (Delayed Start), it starts just after boot time. Configuring this setting can result in a faster boot, but if you need the service to be up and running when you boot, configure it as Automatic. If, on the other hand, you do not need a service, configure its start type as Manual or Disabled.
- Manual mode allows Windows 7 to start a service when needed. In practice, some services do not start up when required in Manual mode. If you find that you need a service, configure it as Automatic.
- If you configure a service as Disabled, it does not start even if needed. Unless you have a very good reason for disabling a service, configure its startup type as Manual instead.

The General tab, shown in Figure 13-41, also tells you whether a service is currently started, lets you start or stop it (as appropriate), and specifies the start parameters.



**FIGURE 13-41** The General tab of the Service Properties dialog box

The Logon tab typically specifies that the service logs on with a Local System account. You can specify another account if you need to do so, typically a local Administrator account on the computer on which the service is running.

The Recovery tab specifies the actions that you take if a service fails. You can specify actions for the first failure, the second failure, and subsequent failures.

If you click Run A Program, you need to type the full path for the program that you want to run. Programs or scripts that you specify should not require user input. If you click Restart The Computer, you need to specify how long the computer waits before restarting. You can also create a message to send automatically to remote users before the computer restarts.

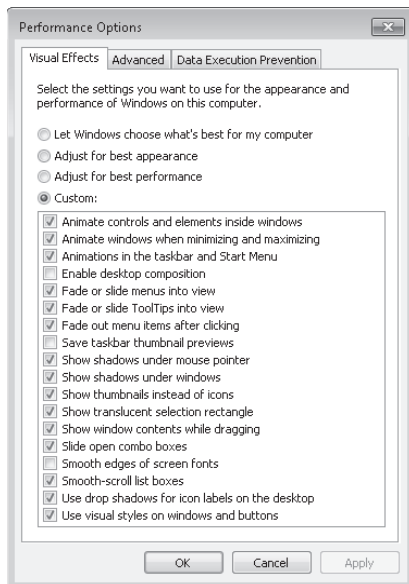
If you select Enable Actions For Stops With Errors, you can trigger the recovery actions when service stops with an error.

The Dependencies tab lists the services, system drivers, and load order groups that a service depends on. If a service is not running when you expect it to be, you might have disabled another service that it depends on.

## Configuring Performance Options

The Performance Options tool is a Windows 7 Performance And Analysis tool that you can access by clicking Advanced Tools on the Performance Information And Tools dialog box and then clicking Adjust The Appearance And Performance Of Windows.

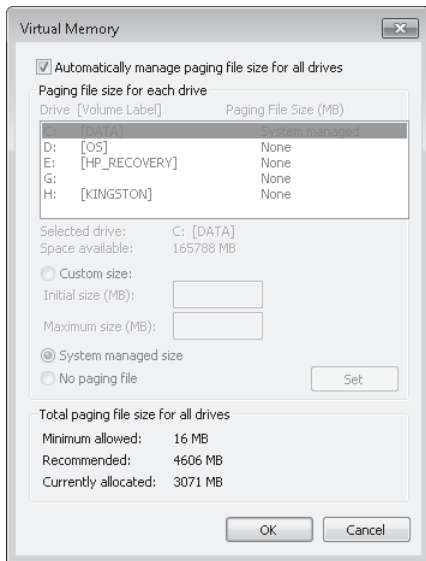
The Visual Effects tab of this tool is shown in Figure 13-42. You can let Windows decide what is best for your computer, adjust for best appearance, adjust for best performance, or select Custom and specify the appearance settings for your computer manually. If you select Custom, you can choose which visual effects to turn off, one by one. There are 18 visual effects that you can control, such as whether shadows are displayed under screen icons or under the mouse pointer.



**FIGURE 13-42** The Visual Effects tab of the Performance Options tool

On the Advanced tab, you can adjust for the best performance of programs or background services. If your computer is running applications (as a typical workstation does), you would specify Adjust For Best Performance Of Programs. On a server that is functioning as a Web server (for example), you would specify Adjust For Best Performance Of Background Services.

On the same tab, you can adjust page file settings. A page file is an area of disk space that can be used as paged virtual memory when running memory-intensive operations (such as print spooling) or if the system RAM is not adequate to cope with the demands of applications that are running. You can allow Windows 7 to manage memory paging (the default), as shown in Figure 13-43, or you can manually specify virtual memory allocation. If RAM is a serious bottleneck on your computer or you are running some extremely memory-intensive applications, you might want to specify memory-paging settings manually. Otherwise, you should accept the defaults.



**FIGURE 13-43** Virtual memory default settings

Data Execution Prevention (DEP) helps prevent damage to your computer from viruses and other security threats. Malware attacks your operating system by attempting to execute code from the sections of a computer's memory reserved for Windows 7 and other authorized programs. DEP helps to protect your computer by monitoring programs and ensuring that they use computer memory safely. If DEP detects a program on your computer that attempts to use memory incorrectly, it closes the program and notifies you.

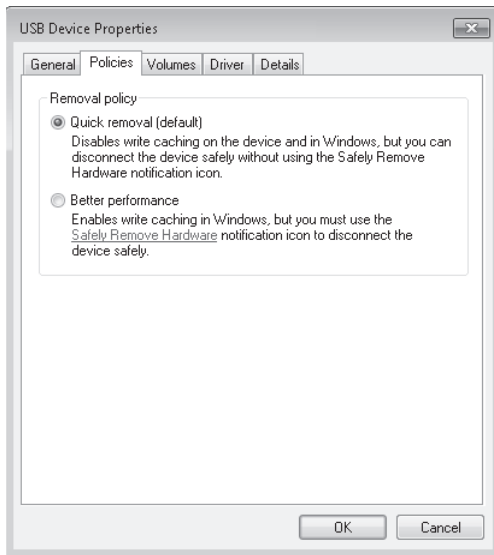
The Data Execution Prevention tab on the Performance Options tool lets you choose whether to turn on DEP for essential Windows programs and services only (the default) or to turn on DEP for all programs and services except those that you specify. For example, in a test environment where application developers are testing applications that could inadvertently

cause security problems on the computer, you would choose to enforce DEP for all programs and services and possibly specify only those in which you have complete confidence as exceptions.

## Configuring Hard Disk Write Caching

Write caching uses high-speed volatile RAM to collect write commands sent to data storage devices and cache them until the slower storage media (either physical disks or flash memory) can deal with them. You can manage write caching on the Policies tab of the device's Properties dialog box that you access from Device Manager.

For USB flash memory devices (for example), you can specify the Quick Removal option, as shown in Figure 13-44. This option is typically the best choice for devices that you are likely to remove from the system frequently, such as USB flash drives, memory cards, or other externally attached storage devices.



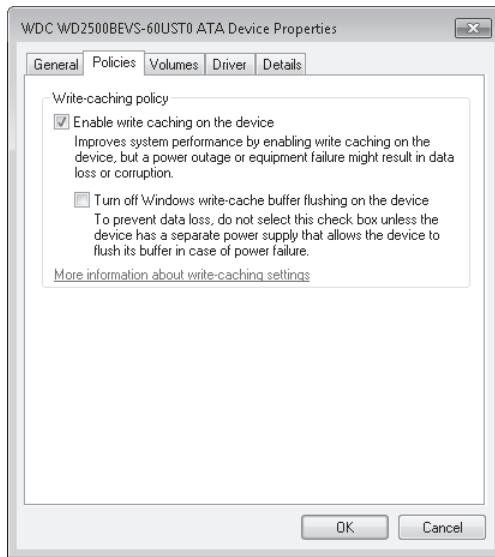
**FIGURE 13-44** The Quick Removal option for removable storage

When you select the Quick Removal option, Windows 7 manages commands sent to the device using write-through caching. In write-through caching, the device operates on write commands as if there were no cache. The cache may still provide a small performance benefit, but the emphasis is on treating the data as safely as possible. The main benefit is that you can remove the storage device from the system quickly without risking data loss. For example, if a flash drive were to be accidentally pulled out of its port, the data being written to it is much less likely to be lost if the Quick Removal option is specified.

You should select the Better Performance option for devices that you intend to remove from the system infrequently. If you choose this option and the device is disconnected from

the system before all the data is written to it (for example, if you remove a USB flash drive), you could lose data.

If you select Enable Write Caching On This Device (the default) on a hard disk, this improves system performance but a power outage or system failure might result in data loss. By default, Windows 7 employs cache flushing and periodically instructs the storage device to transfer all data waiting in the cache to the storage media. If you select Turn Off Windows Write Cache Flushing On The Device, these periodic data transfer commands are inhibited. Not all hard disk devices support this feature. Figure 13-45 shows the Policies tab for a hard disk.



**FIGURE 13-45** The Policies tab for a hard disk

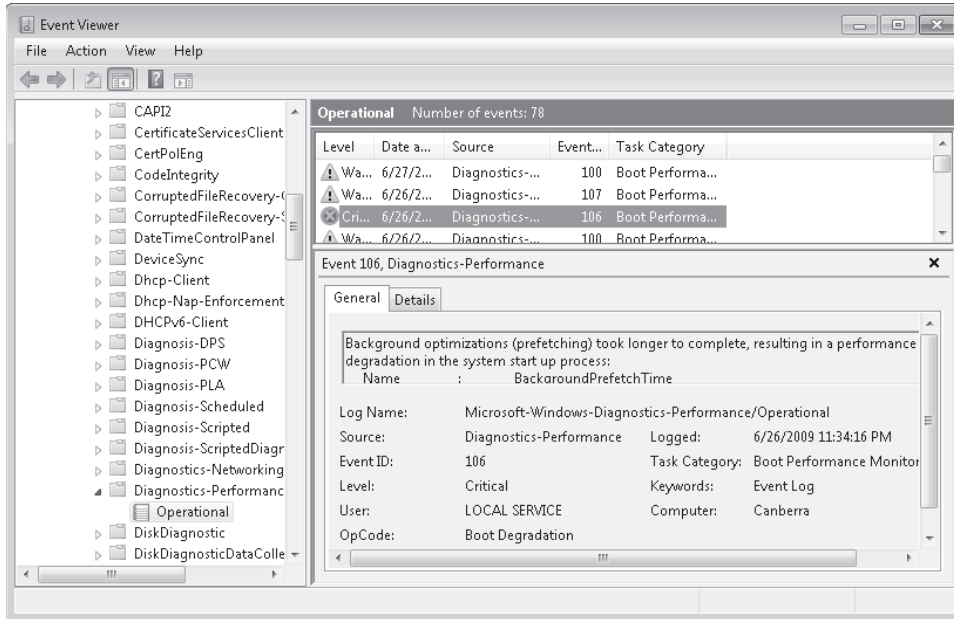
If high data transfer performance is your main objective, you should select the Better Performance option for removable storage and select Enable Write Caching On The Device for hard disks. These are the defaults if the system hardware and storage device support these features. However, if your system or power source has known issues with sustaining power, you should not use these settings. In general, it is best to use the Safe Removal applet before you remove any external storage device from your system.

## Troubleshooting Performance Problems with Event Viewer

As an IT professional, you sometimes are required to view details of software and hardware problems affecting Windows performance to troubleshoot these problems. You can view event logs in Event Viewer, as described in Lesson 1 of this chapter, and filter by event type. The events you are looking for are mostly found in the Operational container under Diagnostic-Performance, which you access by expanding Microsoft and then Windows in the Event Viewer tree pane.



However, there is a more straightforward method of accessing this information. Click the Performance Information And Tools item of Control Panel. Click Advanced Tools in this dialog box, and then click View Performance Details In Event Log. This opens Event Viewer and displays the events in the Operational container, as shown in Figure 13-46. Examining a critical error shows that, for example, the Canberra computer had a problem during the boot process.



**FIGURE 13-46** Viewing performance diagnostic events in the Operational container

#### **NOTE** DEVICE DRIVERS

If a device is not working properly, then this has an effect on performance that is often catastrophic. You need to ensure that (in general) the latest device drivers are installed for all your devices. The exception is when a new device driver does not work as well as its predecessor, in which case you need to roll back to the old device driver. Chapter 4, “Managing Devices and Disks,” discusses this topic in detail.

#### **NOTE** POWER PLANS

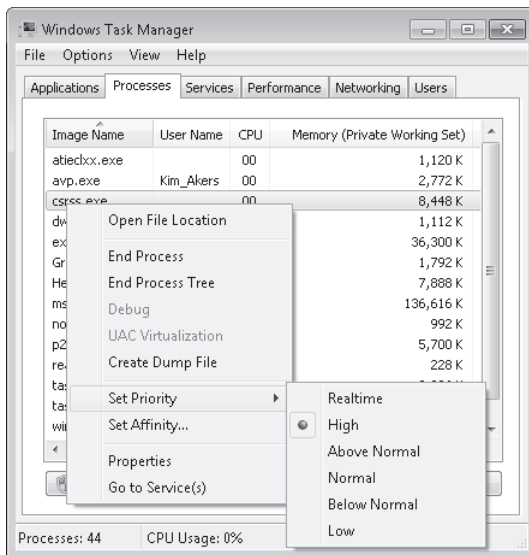
Power plans and configuring power settings are mentioned in the examination objectives covered in this chapter. However, Chapter 11, “BitLocker and Mobility Options,” discusses these topics in depth, and there is no point duplicating that material here.

# Using Task Manager to Configure Processes

Lesson 1 described how you use Task Manager to close failed applications and manage services. You can also use the tool to configure the processes that implement services. If a process is particularly significant and should be allocated more resources, you can set a higher priority for that process. If a process is using too many resources, or if the speed at which a process works is unimportant, you can assign it a lower priority and hence free resources for other processes.

If your computer has more than one processor, you can configure the affinity of your processes to use a particular processor. By default, processes that install on a multiprocessor computer are set to use whatever processor is available. If an additional processor is added retrospectively to a computer, however, processes might require configuration so they can use that processor. For example, if Task Manager or Performance Monitor counters show that one processor on a dual-processor computer is heavily used and the other is not, you should change the affinity so resource-intensive processes use both processors. You also have the option of changing the affinity of some processes so that they use only the second processor.

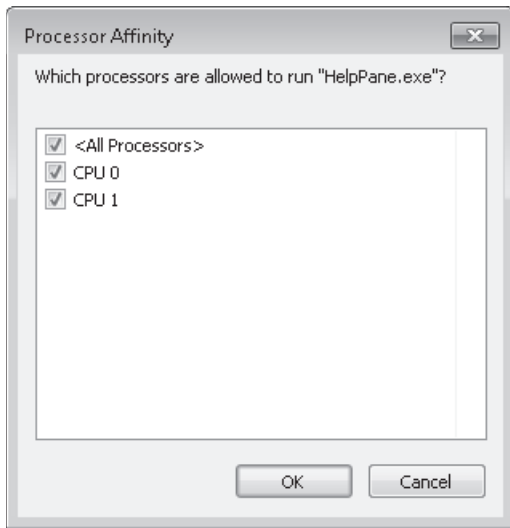
To determine what process or processes are used by a service, right-click the service in the Services tab of Task Manager and click Go To Process. This selects the Processes tab and highlights the relevant process. To change the priority of a process, right-click the process and click Priority. As shown in Figure 13-47, you can choose one of six priority levels. Do not select Realtime, though—this could seriously affect the operation of other processes on your computer.



**FIGURE 13-47** Setting process priority in Task Manager

To determine the affinity of a process and change it if necessary, right-click the process and click Set Affinity. You cannot change the affinity of certain system processes, and you

cannot change affinity if the computer has only one processor. Otherwise, the Processor Affinity dialog box appears, as shown in Figure 13-48, and you can configure process affinity.



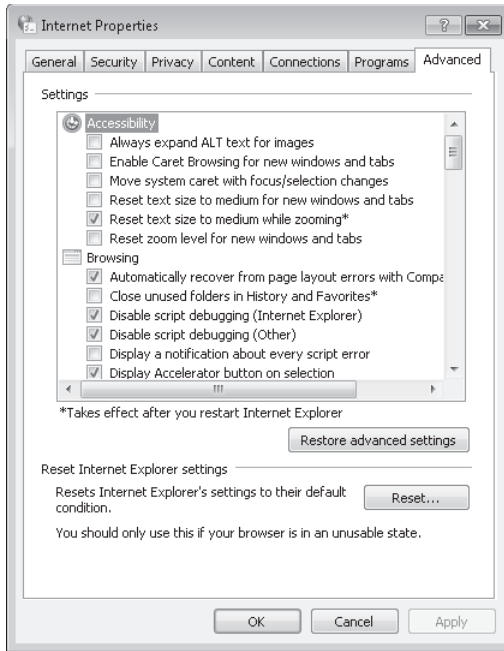
**FIGURE 13-48** The Processor Affinity dialog box

## Configuring Networking Performance

Networking performance on an enterprise network depends upon a large number of factors, such as the type of Ethernet or wireless connections used, the speed of switches and routers, the number of devices on a network, and so on. However, in a small network, users tend to define networking performance by the speed of connection to other computers on the network (if they are transferring files) and the performance of their Internet connections.

Configuring Internet Options can have a significant effect on networking performance and on computer performance in general. As an IT professional, you are aware that temporary Internet files can take up a considerable amount of disk space and should be deleted on a regular basis. You know that users with excessively large mailboxes can experience lengthy logon times, especially when they are downloading their profiles from a central server in the enterprise environment. These however, are matters that involve user training rather than configuration.

The Internet Options dialog box offers configuration options that can affect networking performance. You can access this dialog box from Network And Internet on Control Panel or from your browser. On the General tab, you can delete temporary Internet files and other downloaded information such as Web form information. However, in the context of networking performance settings, the most significant tab in the dialog box is the Advanced tab, shown in Figure 13-49.



**FIGURE 13-49** The Internet Options Advanced tab

The Advanced tab enables you to configure Accessibility, Browsing, International, Multimedia, Printing, and Security settings. Some of these have little or no impact on performance, whereas others can affect performance considerably. Typically, for example, Accessibility features would not be considered a performance issue, but if large font or caret browsing is set for a user that does not need them, then the perceived performance for that user is reduced.

The Browsing settings can impinge on performance. For example, if you do not disable script debugging and display notifications about script errors, the user's browsing experience slows down. These settings are useful if you are debugging a new Web site that runs scripts but are inappropriate for the standard user. Even the simplest setting, such as choosing to always underline links, can slow browsing on a slow or heavily used site.

If you are accessing sites that provide multimedia files for either streaming or downloading you can choose (for example) whether to play sounds and animations, automatically resize images, or use smart image dithering. In general effects that enhance the user's multimedia experience often also slow down site access and browsing.

The more secure a site is, the slower it tends to be because of additional security checks. Typically, this is something you and your users need to accept. You should not reduce security merely to shorten access times. Nevertheless, it is probably not necessary to warn users whenever they browse from an HTTPS secure site to an insecure HTTP site.

# Windows Performance Analysis Tools

The Windows Performance Toolkit (WPT) contains performance analysis tools that are new to the Windows SDK for Windows 7, Windows Server 2008, and Microsoft .NET Framework 3.5. WPT can be used by a range of IT Professionals including system administrators, network administrators, and application developers. The tools are designed for measuring and analyzing system and application performance on Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7.

Windows performance analysis tools analyze a wide range of performance problems including application start times, boot issues, deferred procedure calls (DPCs), interrupt service requests (ISRs), system responsiveness issues, application resource usage, and interrupt storms.

These tools ship with the Microsoft Windows SDK for Windows Server 2008 and .NET Framework 3.5, which you can download at <http://www.microsoft.com/downloads/details.aspx?FamilyId=F26B1AA4-741A-433A-9BE5-FA919850BDBF&displaylang=en> (although it is probably easier to go to the Microsoft Download Center at <http://www.microsoft.com/downloads> and search for it). This SDK provides documentation, samples, header files, libraries, and tools to develop applications for Windows XP; Windows Server 2003; Windows Vista; Windows Server 2008; Windows Server 2008 R2; Windows 7; and .NET Framework versions 2.0, 3.0, and 3.5. You download and install the SDK in the practice later in this lesson.

The WPT is released as an MSI installer (one per architecture) and contains the Performance Analyzer tool suite, consisting of the following tools:

- **The Trace Capture, Processing, and Command-Line Analysis tool (Xperf.exe)** This tool captures traces, processes them for use on a computer, and supports command-line (action-based) trace analysis.
- **The Visual Trace Analysis tool (Xperfview.exe)** This tool presents trace content in the form of interactive graphs and summary tables.
- **The On/Off Transition Trace Capture tool (Xbootmgr.exe)** This tool automates on/off state transitions and captures traces during these transitions.

## The Trace Capture, Processing, and Command-Line Analysis Tool

Xperf.exe is a command-line tool that provides the following features:

- Event Tracing for Windows (ETW) trace control
- ETW trace merging and enhancements by including other events
- Executable image and symbol identification
- Trace dump capabilities
- Support for post-processing

This tool manages the end-to-end operations that are needed to generate a trace file for analysis. You use Xperf.exe in the practice later in this lesson.

Xperf.exe enables events in the operating system by using groups and flags. These flags enable and disable events from providers in various parts of the operating system. For example, flags can direct the kernel, services, and applications to one or more trace files by using log sessions with custom configurations. You can then merge all traces into a single aggregate trace file that is referred to as a merged trace file.

When Xperf generates this file, it collects additional information from the operating system and adds it to the aggregate trace. You can process the merged trace file on any supported operating system without reference to the system that generated the trace. You can then use Performance Analyzer (Xperfview.exe) to analyze the merged file, you can post-process the merged file into a text file, or you can use actions to do other types of processing. Actions produce summarized outputs that are specific to an area of interest, such as boot, shutdown, suspend, and resume operations, or to a type of system event, such as sampled profile, context switches, DPCs and ISRs, disk I/O, registry accesses, file accesses, or system configuration.

## The Visual Trace Analysis Tool

The Visual Trace Analysis tool, or Performance Analyzer, is used to view the information from a single trace file generated by Xperf.exe. You can use the following command to start Performance Analyzer:

```
xperf file.etl
```

Xperf.exe forwards the file name to Performance Analyzer, which then opens and displays the data in the file. You can also run Performance Analyzer directly by entering **xperfview** in the Search box on the Start menu, the Run command box, or the command prompt. A Performance Analyzer trace is displayed in the practice later in this lesson.

## The On/Off Transition Trace Capture Tool

Xbootmgr.exe collects information during the on/off transition phases of Windows 7. You can capture data during any of the following phases:

- Boot
- Shutdown
- Sleep and resume
- Hibernate and resume

After issuing a trace command, the test computer resets within 5 seconds.

The On/Off Transition Trace Capture tool can automate a reboot cycle during which the computer running Windows 7 is shut down and rebooted multiple times. You can analyze the captured data by using the Xperf.exe and Xperfview.exe tools.

In this practice, you download and install the Microsoft Windows SDK for Windows Server 2008 and .NET Framework 3.5, then install the WPT and use the Xperf.exe tool to generate a trace.

**EXERCISE 1 Downloading and Installing the SDK**

In this exercise, you download and install the SDK. The exercise gives a direct link to the SDK download file, but you might find it easier to browse to this link. Perform the following steps:

1. Log on to the Canberra computer with the Kim\_Akers account.
2. Insert a blank recordable DVD-ROM into your optical drive. Close the Autoplay box.
3. Open your browser and access <http://www.microsoft.com/downloads/details.aspx?FamilyId=F26B1AA4-741A-433A-9BE5-FA919850BDBF&displaylang=en>.
4. Click Download.
5. In the File Download box, click Open. The download takes some time.
6. If prompted, click Allow to close the Internet Explorer Security dialog box.
7. In the Windows Disc Image Burner, select Verify The Disc After Burning, and then click Burn.
8. When you have burned and verified the DVD-ROM, it ejects automatically. Close the Windows Disc Image Burner. Insert the DVD-ROM into the optical drive.
9. In the Autoplay box, click Run Setup.exe.
10. If prompted, click Yes to clear the User Account Control (UAC) dialog box.
11. The Windows SDK Setup Wizard opens. Click Next.
12. Read the License terms, select I Agree, and then click Next.
13. Click Next to accept the Folder defaults.
14. Click Next to accept the Installation Options defaults.
15. Click Next to start the Installation.
16. Click Finish when installation completes. Read the SDK release notes.

**EXERCISE 2 Installing the Windows Performance Toolkit**

In this exercise, you install the 32-bit version of the Windows Performance Toolkit. If your computer is running a 64-bit operating system, choose Xperf\_64.msi instead of Xperf\_86.msi. You need to have installed the SDK in Exercise 1 before you attempt this exercise.

1. If necessary, log on to the Canberra computer with the Kim\_Akers account.
2. Open My Computer and navigate to C:\Program Files\Microsoft SDKs\Windows\v6.1\Bin.

3. Double-click the Xperf\_86.msi file. The Microsoft Windows Performance Toolkit Setup Wizard starts. Click Next.
4. Accept the License Agreement. Click Next.
5. Click Typical and then click Install.
6. If prompted, click Yes to clear the UAC dialog box.
7. Click Finish when setup completes.

### EXERCISE 3 Using Xperf.exe to Generate Traces

In this exercise, you use the Trace Capture, Processing, and Command-Line Analysis Tool (Xperf.exe) to generate a kernel trace and a user trace. You combine the traces and process the results into a text file. You need to have completed Exercises 1 and 2 before you attempt this exercise.

1. If necessary, log on to the Canberra computer with the Kim\_Akers account.
2. Open an elevated command prompt.
3. Start the kernel trace. The kernel session does not need a specified name because its name is unique. The groups Base and Network are enabled on the kernel provider. The trace is collected in a file called *Kernel.etl*. To accomplish this, enter the following command:

```
xperf -on Base+Network -f kernel.etl
```

4. Start a user trace named UserTrace and enable the provider's Microsoft-Windows-Firewall to it. This trace is collected in a file called *User.etl*. To accomplish this task, enter the following command:

```
xperf -start UserTrace -on Microsoft-Windows-Firewall -f user.etl
```

5. Stop the UserTrace session so the user-mode provider no longer produces events to this session. To accomplish this, enter the following command:

```
xperf -stop UserTrace
```

6. Stop the kernel session. To accomplish this, enter the following command:

```
xperf -stop
```

7. Merge the user and kernel traces into a single trace called *Single.etl*. To accomplish this, enter the following command:

```
xperf -merge user.etl kernel.etl single.etl
```

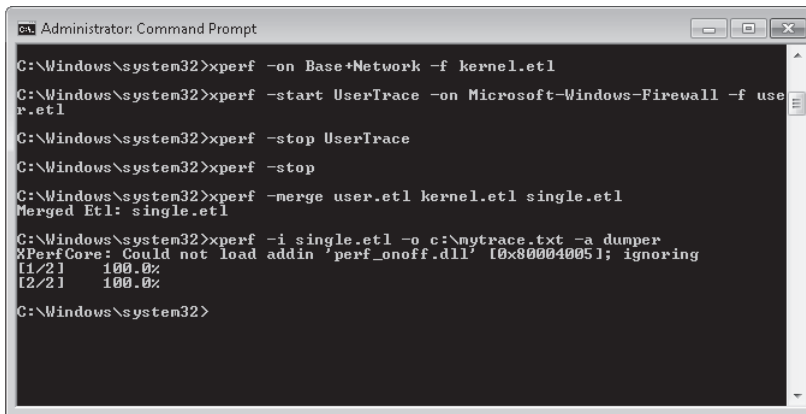
8. Process the binary trace file *Single.etl* into a text file called *C:\Mytrace.txt*. To accomplish this, enter the following command:

```
xperf -i single.etl -o c:\mytrace.txt -a dumper
```

Figure 13-50 shows the Xperf commands used in this procedure. Note that there was a problem loading a DLL associated with the On/Off Transition Trace Capture Tool, but this tool was not used so the procedure completed satisfactorily. Figure 13-51 shows a portion of

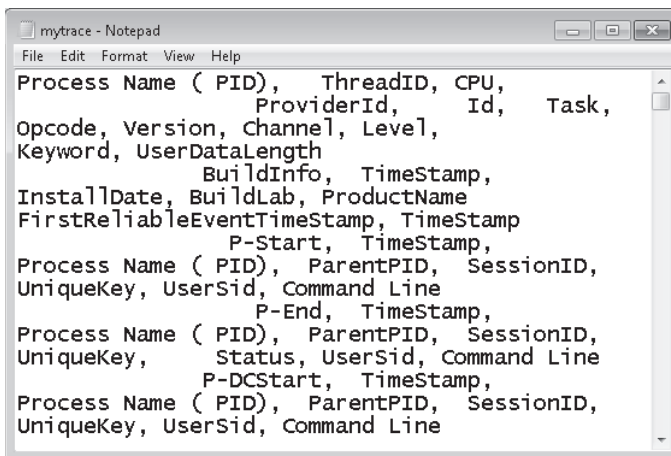


the text file that was created. Figure 13-52 shows the combined trace (Single.etl) displayed in the Performance Analyzer.



```
Administrator: Command Prompt
C:\Windows\system32>xperf -on Base+Network -f kernel.etl
C:\Windows\system32>xperf -start UserTrace -on Microsoft-Windows-Firewall -f user.etl
C:\Windows\system32>xperf -stop UserTrace
C:\Windows\system32>xperf -stop
C:\Windows\system32>xperf -merge user.etl kernel.etl single.etl
Merged Etl: single.etl
C:\Windows\system32>xperf -i single.etl -o c:\mytrace.txt -a dumper
XPrefCore: Could not load addin 'perf_onoff.dll' [0x80004005]; ignoring
[1/21] 100.0%
[2/21] 100.0%
C:\Windows\system32>
```

FIGURE 13-50 Xperf commands used to capture and merge traces

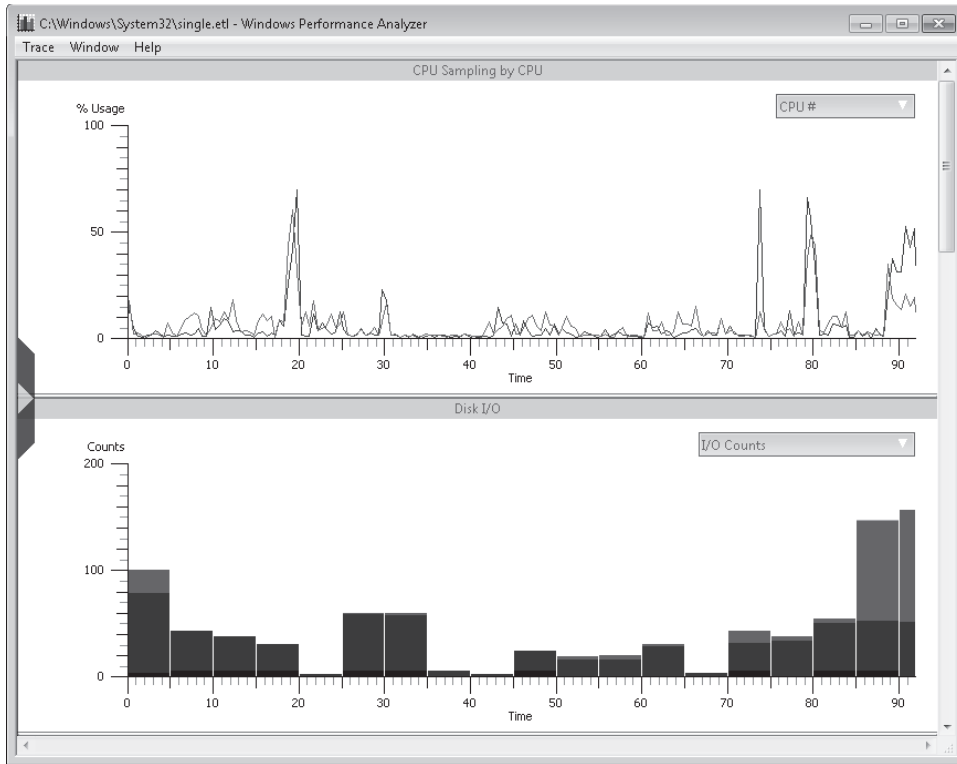


```
mytrace - Notepad
File Edit Format View Help
Process Name ( PID), ThreadID, CPU,
ProviderId, Id, Task,
Opcode, Version, Channel, Level,
Keyword, UserDataLength
BuildInfo, TimeStamp,
InstallDate, BuildLab, ProductName
FirstReliableEventTimeStamp, TimeStamp
P-Start, TimeStamp,
Process Name ( PID), ParentPID, SessionID,
UniqueKey, UserSid, Command Line
P-End, TimeStamp,
Process Name ( PID), ParentPID, SessionID,
UniqueKey, Status, UserSid, Command Line
P-DCStart, TimeStamp,
Process Name ( PID), ParentPID, SessionID,
UniqueKey, UserSid, Command Line
```

FIGURE 13-51 Trace information captured in a text file

## Lesson Summary

- You can write WMI scripts to customize the system information you retrieve from a computer and generate your own performance-measuring tools.
- The System Configuration Tool modifies which programs run at startup, edits configuration files, and enables you to control Windows services and access Windows Performance and Troubleshooting tools. The Services console lets you manage and configure services and gives you more options than either the Services tab of Task Manager or the Services tab of the System Configuration tool.



**FIGURE 13-52** Captured trace displayed in Performance Analyzer

- The Performance Options tool lets you configure visual effects and specify whether the system is adjusted for best performance of applications or background services. It lets you configure page file (virtual memory) settings and DEP.
- The Windows Performance Analysis tools, downloaded as part of the Windows Server 2008 SDK, analyze a wide range of performance problems including application start times, boot issues, DPCs, ISRs, system responsiveness issues, application resource usage, and interrupt storms.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, “Configuring Performance Settings.” The questions are also available on the companion DVD 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 WMI tool do you use to view Windows Management–generated events and event information, such as the event’s date and time, class, point of origin, and description?
  - A. WMI CIM Studio
  - B. WMI Object Browser
  - C. WMI Event Registration Tool
  - D. WMI Event Viewer
2. Which Windows Performance Analysis tool captures user and kernel traces and can merge them to form a combined trace?
  - A. Performance Analyzer
  - B. On/Off Transition Trace Capture
  - C. Trace Capture, Processing, and Command-Line Analysis
  - D. Visual Trace Analysis
3. Which tool provided by Windows 7 helps you determine which applications are responsible for activity on your hard disk, including which files and folders are being accessed?
  - A. Process Explorer
  - B. Resource Monitor
  - C. Task Manager
  - D. Windows Experience Index
4. A number of processor-intensive applications have been performing slowly on your computer. As a result, you add a second processor. This does not solve your problem, however, and you examine processor usage with Task Manager and Performance Monitor. You deduce that several key processes are using only the original processor. How do you ensure that these processes use whatever processor is available?
  - A. Configure Process Affinity on the Processes tab of Task Manager.
  - B. Configure Process Priority on the Processes tab of Task Manager.
  - C. Select Adjust For Best Performance Of Programs on the Advanced tab of the Performance Options tool.
  - D. Reconfigure Virtual Memory settings on the Advanced tab of the Performance Options tool.
5. Your computer is configured to dual-boot between Windows Vista Professional and Windows 7 Enterprise. Currently, it boots into Windows Vista by default. You want to specify Windows 7 as the startup default operating system and configure how Windows 7 reacts in the event of a system failure. You boot the computer into Windows 7. What tool do you use to accomplish your goal?
  - A. The Services console
  - B. Performance Options
  - C. Task Manager
  - D. System Configuration

## 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 7 tools such as Performance Monitor, Reliability Monitor, the Action Center, and the Windows Reliability Index let you gauge whether your computer is performing as it should, whether it needs more resources to do what you want it to do, and where performance bottlenecks are occurring.
- Tools such as Task Manager give you a snapshot of how your computer is currently performing, whereas event logs can store historical events in addition to warning you when problems occur, and DCSs can hold both current and historical counter values so you can compare a computer's performance with how it was performing at a specified past time.
- Tools specific to measuring and troubleshooting computer performance include WMI scripts, the System Configuration tool, the Services console, the Performance Options tool, and the Windows Performance Analysis tools.

## 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.

- **Data Collector Set (DCS)**
- **event forwarding**
- **event log**
- **event subscription**
- **performance counter**

## Case Scenarios

---

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

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

James Seymour is an IT professional administering the production network at Tailspin Toys. Recently, users have been experiencing intermittent performance problems when accessing a file server running Windows Server 2008 R2 from their computers running Windows 7. James checks resource usage on the file server by using Task Manager but sees no indication of excessive processor, memory, disk, or network resource usage. He needs to monitor these resources over a period of time rather than look at a real-time snapshot, and to monitor resources both when the performance problems are occurring and when they are not. From his computer running Windows 7, James opens Performance Monitor and connects to the file server.

With these facts in mind, answer the following questions:

1. How does James generate performance logs that help him analyze disk, network, processor, and memory resource usage on the server, both when problems are occurring and when performance is normal?
2. James knows roughly when problems started to occur. How can he check what applications were installed or upgraded at that time?
3. Recently, a number of your users have had problems downloading files and e-mail because the space on their local disks had reached a critical limit. James needs to create a proactive method of identifying low disk space problems on computers running Windows 7 on the Tailspin Toys network so he can ask his desktop support technicians to free disk space on client computers before critical limits are reached. How does he monitor client computers for low disk space events?

### Case Scenario 2: Troubleshooting Performance Issues on a Client Computer

James is troubleshooting performance issues on a client running Windows 7 at Wingtip Toys. This is normally a desktop support job, but the computer belongs to the CEO, so James needs to do the job himself and come up with some quick solutions.

With these facts in mind, answer the following questions:

1. James runs Task Manager and finds that one of the two processors on the computer is heavily used whereas the second is hardly used at all. He checks the records and finds that one of his team had installed the second processor retrospectively because the

CEO had heard that another processor would improve performance on her computer. How does James ensure the processor resource is properly used?

2. James needs to quickly scan events in the event logs that are specifically related to performance. He knows he can create filters and custom views, but this would take time, and he needs answers now. How does James quickly access the appropriate events?
3. The CEO has a habit of pulling her USB flash memory device out of her computer without using the Safe Removal applet, especially when she is in a hurry. She has previously lost data on the USB device, but when a CEO loses data, it is (of course) the fault of technical support, not the CEO. How should James minimize the risk of data loss on the USB device?

## Suggested Practices

---

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

### Use the Performance Monitoring Tools

- **Practice 1** Look at the standard DCSs available and experiment with creating your own. DCSs provide a powerful method of managing current and historical performance on your computer, and the only way to become comfortable with them is to use them.
- **Practice 2** It is part of any IT professional's job not only to carry out the tasks required to keep computer and network equipment performing efficiently, but also to report on these tasks to colleagues and to management. You will be judged on the clarity and relevance of your reports, and they will be a factor in your budget allocation. Learn to generate good reports.

### Manage Event Logging

- This topic often seems complex at first, but it becomes clearer when you have practiced configuring subscriptions and forwarding events. You can do this initially with only two computers on your test network. Become proficient before you need to do it on a production network.

### Write WMI Scripts

- Sample WMI scripts can be found on the Internet and in textbooks in your organization's library. The easiest way to learn scripting (or any other type of programming) is to understand and adapt other people's scripts before you try to write your own from scratch.

## Take a Practice Test

---

The practice tests on this book's companion DVD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-680 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 section entitled "How to Use the Practice Tests," in the Introduction to this book.

# Index

## Symbols and Numbers

- .bat files, 279
- .cmd files, 279
- .com files, 274, 278
- .js files, 279
- .ocx files, 279–80
- .ps1 files, 279
- .swm files, 95
- .vbs files, 274, 279
- .xml migration files, 40
- .zip files, 735, 738–39
- 16-bit components, installation, 263
- 32-bit platforms
  - images, cross-architecture tools, 71
  - servicing images, 75
- 64-bit platforms
  - images, cross-architecture tools, 71
  - servicing images, 75
- 6to4, 335, 337, 516, 519
- 6to4 Relay Name, 518

## A

- Accelerators, 631
- access control lists (ACL), 39
- Account Is Locked Out, 501
- Account Lockout Duration, 499
- account lockout policies, 499–501
- Account Lockout Threshold, 500
- ACL (access control lists), 39
- ACT (Application Compatibility Toolkit), 260–64
- Action Center, 609–10, 661–64
- Action package, 139
- activation, resetting, 82
- Active Directory Certificate Services, 454, 520, 533.
  - See also* certificates
- Active Directory Domain Services (AD DS), 385, 454, 559
- Active Directory Security Group Discovery, 176
- Active Directory System Discovery, 176
- Active Directory System Group Discovery, 176
- Active Directory User Discovery, 176
- Active Directory Users and Computers, 103–04
- ActiveX, 625
- AD DS (Active Directory Domain Services), 385, 454, 559
- AD DS servers, 103
- ad hoc networks, 350, 360, 371–73
- Add Application Wizard, 127
- Add Features Wizard, DirectAccess, 522
- Add Features Wizard, Windows Server 2008, 468
- Add Hardware Wizard, 206
- Add Printer Wizard, 369
- Add-Drivers, 124
- Additional Data, 734
- addresses
  - IPv4, configuring
    - addressing, 301–07
    - connecting to network, 307–11
    - overview, 300–01
    - practice, configuring, 321–24
    - troubleshooting, 311–21
  - IPv6, configuring
    - address structure, 328–32
    - advantages of IPv6, 333–34
    - connectivity, 338–43
    - IPv4 compatibility, 334–37
    - practice, configuring IPv6 connectivity, 343–45
- network connections, Windows Firewall, 385
- Admin Approval mode, 480, 482–83
- Admin Approval Mode for Built-In Administrator Account, 482–83
- administrative rights and privileges
  - backup, 737
  - case scenario, UAC and passwords, 511
  - compatibility modes, 260, 265
  - User Account Control (UAC) overview, 479–80
  - policies, 482–87
  - practice, configuring, 488–90
  - Secpol and Local Security Policy, 487–88
  - settings, 480–82
  - verification of, 205
  - Windows Installer rules, 278
- administrator passwords, wireless networks, 367
- Administrators group, 496
- Advanced Boot Options, 750–53
- Advanced Encryption Standard (AES), 358–60
- Advanced Recovery Methods, 748–49
- Advanced Sharing dialog box, 428
- Advanced Sharing Settings, 312, 350, 423, 434
- AES (Advanced Encryption Standard), 358–60
- aggregation, route, 333
- alerts, performance counters, 652
- Allow Access To BitLocker-Protected Removable Data Drives, 565
- Allow Log On Through Remote Desktop Services, 496
- Allow UIAccess Applications To Prompt For Elevation Without Using Secure Desktop, 486–87
- Analyze Disk, 230



answer file

- booting to audit file, 83
- building, 59–64
- creating, 139–40
- package installation, 131
- reference installation, building, 65–66
- settings, saving, 64–65
- Sysprep, 80–81
- Unattended.xml, 127, 137–40

anti-spyware, 661–64

antivirus, 661–64

anycast, 329, 332

API (application programming interface), compatibility, 262

APIPA (Automatic Private Internet Protocol), 300, 305, 307

AppData, 734

Application Compatibility

- Diagnostics policies, 264–65

Application Compatibility Toolkit (ACT), 260–64

application control policies.

- See* AppLocker

Application Identity Service, 277

application programming interface (API), compatibility, 262

application settings, 40

applications

- event logs, 674
- performance, 717
- RemoteApp, 539–40
- system restore, 747

applications, managing.

- See also* AppLocker

adding, MDT, 164–66

Application Compatibility

- Diagnostics policies, 264–65

Application Compatibility Toolkit (ACT), 260–64

case scenarios, 294–95

compatibility, configuring options, 257–60

inventories, 175–76

overview, 255

practice, compatibility, 267–69

practice, restricting applications, 286–89

servicing, 125–27

Software Restriction Policies, 271–76

WIM images, 120

Windows XP Mode, 265–66

AppLocker

- application control policies, overview, 276–77

auditing, 285–86

- configuring exceptions, 283
- practice, restricting applications, 286–89
- rules, 277–83
- Software Restriction Policies, 271–76

architecture, cross-architecture

- tools, 71

auditing

- AppLocker, 285–86
- audit mode, booting to, 83
- auditSystem, configuration pass, 80
- auditUser, configuration pass, 80–81
- remote connections, 544
- Security event log, 673–80
- shared resources, 449–51

authentication

- account policies, 499–500
- BitLocker requirements, 561
- case scenario, UAC and passwords, 511
- certificates, managing, 502–04
- Credential Manager, 493–95
- DirectAccess, 516, 520–21
- event forwarding, 676
- HomeGroup Connections, 425
- internal wireless adapters, 357–60
- Network Security Key, 355
- port-based, 358–60
- practice, managing credentials, 504–07
- Remote Desktop, 539
- remote management, 409–10
- removable data drives, 564
- resolving issues, 500–01
- Runas, 495–96
- smart cards, 497–99
- User Account Control (UAC)
  - overview, 479–80
  - policies, 482–87
  - practice, configuring, 488–90
  - Secpol and Local Security Policy, 487–88
  - settings, 480–82
  - user rights, 496–97
- virtual private networks (VPNs), 531–33
- Windows Firewall with Advanced Security (WFAS), 393–94
- wireless networks, 367

Authentication exemption

- rules, 393

authorization

- account policies, 499–500
- case scenario, UAC and passwords, 511
- certificates, managing, 502–04
- Credential Manager, 493–95
- practice, managing credentials, 504–07
- resolving authentication issues, 500–01
- Runas, 495–96
- smart cards, 497–99
- user rights, 496–97

Auto-Add policy, 99, 103–04

auto-connect, wireless

- networks, 368

Automated.xml, 138

automatic backups, 736–39

Automatic Private Internet Protocol (APIPA), 300, 305, 307

Automatic Updates, 613

Automatically Fix File System Errors, 233

Automatically Generate Rules wizard, 283

Autounattend.xml, 71

availability, 243–45

## B

Background Intelligent Transfer Service (BITS), 150

background services, 710

backup. *See also* Backup and Restore console; recovery, data case scenarios, 779–80

- Credential Manager, 493–95
- practice, configuring file and folder backup, 741–43
- scheduling, 731–39
- System Image backups, 739–41
- thick images, 150

Backup and Restore console

- Restore My files, 763
- scheduling backups, 731–39
- System Image backups, 739–41
- Volume Shadow Copy Service (VSS), 766

Backup Operators group, 497

Backup Set folder, 738

BackupGlobalCatalog, 740

backward compatibility, 117, 497

bandwidth, USB host controller, 203

- basic disks, 241–42, 248
- basic partitions, 235
- battery power, 582–89
- BCD (Boot Configuration Data), 754–55
- BCDBoot, 71, 173
- BCDEdit, 93–94, 148, 173, 754–55
- Behavior of the Elevation Prompt
  - for Administrators in Admin Approval Mode, 483
- Behavior of the Elevation Prompt for Standard Users, 485
- binary notation, 302
- Biometric authentication, 498
- BIOS, Windows XP Mode, 265–66
- BitLocker
  - BitLocker To Go, 564–67
    - data recovery agents (DRA), 559–61
    - enabling, 561–63
    - Encrypting File System (EFS) and, 451–52
    - modes, 556–57
    - offline migrations, 42–43
    - overview, 555–56
    - practice, BitLocker To Go, 568–71
    - TPM chip, 557
- BITS (Background Intelligent Transfer Service), 150
- Block rules, 277–78
- Blog accelerator, 631
- Bluetooth, 356
- Boot Configuration Data (BCD), 148, 754–55
- boot images
  - WDS, 74, 100–01, 170
  - Windows PE, 116
- bootable media. *See also* booting
  - discover images, 171–72
  - dual-boot installations, 14–19
  - LTI bootable media, configuring, 168–69
  - operating system packages, servicing, 127–30
  - practice, creating Windows PE boot DVD, 84–86
  - task sequence, deploy to VHD, 159–61
  - VHD, 90, 93
  - WIM2VHD, 94–96
  - Windows boot options, 754–55
  - Windows PE, 66–68
- booting. *See also* bootable media
  - audit mode or Windows Welcome, 83
  - boot environment, 556, 566–67

- boot options, 754–55
- boot time filtering, 384
- Bootmgr.exe, 754–55
- performance, 717
- System Configuration (MSConfig), 705–07
- target computers, manually, 173–74
- Xbootmgr.exe, 718
- BranchCache
  - configuring clients, 463–67
  - Distributed Cache Mode, 463
  - Hosted Cache mode, 462
  - overview, 461–62
  - practice, BranchCache configuration, 470–71
  - vs transparent caching, 577
  - Windows Server 2008, 468–70
- broadcast address, 303
- broadcast traffic, 333
- Browsing settings, 716
- bus-powered hubs, 202

## C

- cabinet (.cab) files, 127–28
- caching
  - BranchCache
    - configuring clients, 463–67
    - Distributed Cache mode, 463
    - Hosted Cache mode, 462
    - overview, 461–62
    - practice, BranchCache configuration, 470–71
    - Windows Server 2008, 468–70
  - negative, 314–15
  - neighbor cache, 341
  - offline files, 574–82
  - Offline Settings, 430
  - shared folder options, 431
  - transparent caching, 577
  - write caching, configuring, 711–12
- capture images, WDS, 74, 100, 172
- case scenarios
  - application compatibility, 294
  - applications, restricting, 294–95
  - backup and restore, 779
  - deploying an image, 191–92
  - driver signing policy, 252
  - installing Windows 7, 49
  - Internet Explorer, 644–45
  - IPv4 connectivity, 377
  - IPv6 connectivity, 377
  - managing disk volumes, 252
- offline files, 596–97
- passwords, problem
  - resolution, 511
- performance monitoring, 725–26
- remote access, 550–51
- remote management, 419
- shared resources, 474
- system and configuration issues, 779–80
- system image, generating, 111
- User Account Control (UAC), 511
- VHDs, working with, 111
- Windows Firewall, 419
- wireless networks, 377–78
- Catalogs folder, 739–40
- CD-ROM
  - backups, 736
  - bootable Windows PE, 66–68
  - Removable Disk policies, 234–35
- cell phones, 233–35, 540
- cellular modems, 360
- certificate authority (CA)
  - device drivers, 215–19
  - DirectAccess, 520
  - SSL certificates, configuring, 633
  - User Account Control (UAC), 485–87
  - Windows Firewall with Advanced Security (WFAS), 393
  - wireless adapter security, 359–60
- certificates
  - certificate of authenticity (COA), 82
  - certificate rules, 272, 276
  - certificate store, device drivers, 215–19
  - Credential Manager, 493
  - data recovery agents (DRAs), 559
  - DirectAccess, 520–21
  - EFS and HomeGroups, 454
  - Encrypting File System (EFS), 452
  - errors, 635
  - Group Policy, 521
  - Internet Explorer, revocation checks, 626
  - managing, 502–04
  - Recovery Agents, 453
  - smart cards, 497–99
  - SSL certificates, configuring, 633–36
    - VPN authentication protocols, 533
- Certificates Console (Certmgr.msc), 502–04
- Challenge Authentication Protocol (CHAP), 533
- Change Adapter Settings, 316

## Change Advanced Sharing Settings

- Change Advanced Sharing Settings, 350
- CHAP (Challenge Authentication Protocol), 533
- Check For Updates, 601–02
- Choose How BitLocker-Protected Removable Drives Can Be Recovered, 566
- CIDR notation, 303
- CIM (Common Information Model) classes, 696
- CIM (Common Information Model) repository, 694–96
- CIMOM (Common Information Model Object Manager), 694–95
- Cipher.exe, 453, 502–04
- Class Explorer, 699
- class store, 695–96
- Class Viewer, 699
- client computers. *See also* system images, configuring
  - backups, VHDs, 89
  - discovery, 176
  - images, distributing, 72–75
  - installing, small numbers, 66
  - IP configurations, 308
  - IP settings, 314
  - network share, deploying, 69–71
  - operating system packages, servicing, 127–30
  - pre-staging, 103–04
  - remote management
    - case scenarios, 419
    - practice, remote management options, 411–15
  - Remote Assistance, 405–08
  - Remote Desktop, 402–04
  - Windows Remote Management, 408–10
- Client for Microsoft Networks, 362
- client-side rendering (CSR), 369
- COA (certificate of authenticity), 82
- colors, 259, 369
- COM objects, policies, 265
- Command Prompt, 752
- command-line tools
  - BCDEdit, 93–94, 148, 173, 754–55
  - BitLocker, Manage-bde.exe, 567
  - Cipher.exe, 453, 502–04
  - Defrag, 231–32
  - Deployment Image Servicing and Management Tool (DISM), 56–58, 75–77, 116–23, 125, 128, 137–40
  - Diskpart, VHDs, create and attach, 91
  - Driver Verifier Monitor, 214–15
  - Icacls, 446–47
  - Ipconfig, 301
  - IPv6 connectivity, 338–43
  - More Info, 671
  - Net Share, 431
  - Netsh, 310–11, 352–56, 463–67, 608
  - Netstat, 319–21
  - PEimg.exe (Windows PE), 116
  - Ping, 312–15
  - power configuration, 587–89
  - Robocopy.exe, 449
  - Runas, 495–96
  - Secedit.exe, 487–88
  - Sysprep, 77–84
  - Unattend.xml answer files, 137–40
  - USMT (User State Migration Tool), 39–42
  - Wbadmin, 739
  - WDSUTIL, 99
  - WIM2VHD, 94–96
  - WinRS (Windows Remote Shell), 409–10
- common criteria mode, 497
- Common Information Model (CIM) repository, 694–96
- Common Information Model Object Manager (CIMOM), 694–95
- Compatibility Administrator, 261–62
- compatibility fix, defined, 262
- compatibility modes, defined, 262
- compatibility, applications
  - Application Compatibility Diagnostics policies, 264–65
  - Application Compatibility Toolkit (ACT), 260–64
    - backwards compatibility, 117, 497
    - case scenarios, 294–95
    - configuring, 257–60
    - practice, Windows 7 compatibility, 267–69
    - Windows XP modes, 265–66
- complete PC backup, 740
- complete recovery, 749–50
- compressed (.zip) files, 735, 738–39
- compressed folders, 452
- compressed migration stores, 42
- compression, backup, 730
- computer health check, 656–58
- Cone NATs, 337. *See also* NAT (Network Address Translation)
- Config.xml, 40
- Configuration Manager 2007, 163, 176–77, 179
- configuration passes, Windows Setup, 79–80
- Configure Schedule, 230
- Configure Use of Passwords For Removable Data Drives, 565
- Configure Use Of Smart Cards On Removable Data Drives, 564
- configuring. *See also* configuring, system images
  - application compatibility, 257–60
  - BranchCache, configuring clients, 463–67
  - default operating systems, dual-boot, 17–19
  - deployment points, 166–68
  - device installation policies, 207–08
  - DirectAccess, client configuration, 517–21
  - event subscriptions, 677–79
  - firewall exceptions, 387–88
  - HomeGroup settings, 435–38
  - Hosted Cache servers, 462
  - international settings, 131–33
  - Internet Explorer
    - add-ons and search providers, 630–32
    - case scenario, 644–45
    - Compatibility View, 622–23
    - InPrivate Mode, 627–30
    - pop-up blocker, 632–33
    - practice, InPrivate Mode and add-ons, 636–40
    - security settings, 623–26
    - SmartScreen filter, 626–27
    - SSL certificates, configuring, 633–36
- IPv4
  - addressing, 301–07
  - connecting to network, 307–11
  - overview, 300–01
  - practice, configuring network connectivity, 321–24
  - troubleshooting connectivity, 311–21
- IPv6
  - address structure, 328–32
  - advantages of IPv6, 333–34
  - connectivity, 338–43
  - IPv4 compatibility, 334–37
  - practice, configuring IPv6 connectivity, 343–45
  - LTI bootable media, 168–69
  - networking performance, 715–16
  - performance settings

- CIM Classes, 696
- CIM Repository, 695–96
- Performance Options, 709–11
- WMI Administrative Tools, 697–705
- WMI consumers, 696
- WMI providers, 694–95
- WMI scripting library, 696–97
- WMI Service, 695
- WMI, CIMOM, 695
- WMI, overview, 689–94
- permissions, lcacls, 446–47
- practice
  - BitLocker To Go, 568–71
  - BranchCache, 470–71
  - downloading, installing and configuring MDT 2010, 181–87
  - remote connections, 545–47
  - User Account Control (UAC), 488–90
  - Windows Firewall, 395–98
  - Windows Update, 617–19
- processing, Task Manager, 714–15
- Remote Desktop, 403–04
- shared folders, 580–81
- SSL certificates, 633–36
- system protection, 756–60
- system protection and disk usage, configuring, 769–71
- WDS, 169
- Windows PE options, 168
- Windows Update, 601–08
- write caching, 711–12
- configuring, system images
  - case scenario, generating system images, 111
- Deployment Image Servicing and Management Tool (DISM), 75–77
- distributing, 72–75
- Offline Virtual Machine Servicing Tool, 96–98
- overview, 53
- practice, creating bootable VHD, 105–08
- practice, creating WIM image, 84–86
- pre-staging client computers, 103–04
- reference image, creating, 58–72
- Sysprep, 77–84
- VHDs, native, 89–94
- WDS images, 74–75
- WDS, online VHD deployment, 98–104
- Windows Automated Installation Kit (Windows AIK), 56–58
- Windows Image to Virtual Hard Disk Tool (WIM2VHD), 94–96
- Windows Preinstallation Environment (WinPE), 58
- conflicts
  - device drivers, 209–14
  - offline files, 575, 578–80
- Connect To A More Preferred Network, 364
- Connect to Network Folder, task sequence, 178
- connections. *See also* remote management; Windows Firewall
  - DirectAccess
    - client configuration, 517–21
    - overview, 515–17
    - practice, configuring with Netsh, 526–27
    - server, configuring, 521–26
    - troubleshooting, 519–21
  - remote
    - auditing, 544
    - case scenarios, 550–51
    - dialup connections, 540
    - incoming connections, accepting, 541–43
    - NAP remediation, 536–37
    - practice, configuring remote connections, 545–47
    - Remote Desktop, 537–40
    - virtual private networks (VPNs), 530–32
    - VPN Reconnect, 535–36
  - statistics about, 319–21
- Windows Firewall with Advanced Security (WFAS), 393–94
- connectivity
  - ad hoc networks, 360
  - case scenario
    - IPv4 connectivity, 377
    - IPv6 connectivity, 377
    - wireless networks, 377–78
  - computer to computer, 312
  - internal wireless adapter security, 357–60
  - IPv6, configuring, 338–43
  - networks
    - managing connections, 362–63
    - overview, 348–50
    - setting up connections, 350–52
    - wireless computers, adding, 352–56
  - practice
    - configuring IPv6 connectivity, 343–45
    - creating ad hoc network, 371–73
    - wireless networks
      - managing, 356–57
      - security, 367–68
      - technologies, 361
      - troubleshooting, 363–67
  - consent, UAC, 484
  - Contacts, 734
  - Content Retrieval rule, 463
  - Control Use of BitLocker On Removable Drives, 564
  - Convert To Dynamic Disk, 237
  - copying files, 448–49
  - Cotype.cmd, 66–68
  - Core Networking Inbound Rules, 317–18
  - Core Networking Outbound Rules, 317–18
  - Create A Basic Task Wizard, 675
  - Create A Password Reset Disk, 500
  - Create A Shared Folder Wizard, 431
  - Create New Data Collector Wizard, 655
  - creating
    - answer files, Windows SIM, 81, 139–40
    - bootable DVD-ROM, 58
    - bootable Windows PE medium, 66–68
    - capture image, 100, 172
    - Data Collector Sets, 654
    - data collectors from command prompt, 655–56
    - discover images, WDS, 171–72
    - disk volumes, 241
    - distribution share, 139, 152–53
    - event subscriptions, 679–80
    - images, 75
    - mirrored volume (RAID-1), 243
    - power plan, custom, 586
    - practice
      - bootable VHD, 105–08
      - creating ad hoc network, 371–73
      - power plan, custom, 589–92
      - WIM image, 84–86
    - reference image, 58–72
    - scripts, network share
      - deployment, 70
    - simple volumes, 241
    - striped volume with parity (RAID-5), 243–45
    - striped volumes (RAID-0), 242–43
    - VHD, native, 90–91

- WDS, discover image, 101
- Windows Firewall with Advanced Security (WFAS) rules, 389–91
- Credential Manager, 493–95
- credentials, 484, 495–96, 504–07, 737
- cross-architecture tools, 71
- Cryptographic Operators group, 497
- Cscript, 94
- CSR (client-side rendering), 369

## D

- Data Collector Sets (DCS), 649, 652–58, 725
- data confidentiality protocol, 531
- Data Execution Prevention (DEP), 710–11
- data integrity protocol, 531
- data origin authentication protocol, 531
- data recovery agents (DRA), 559–61
- data-collection packages, 261
- DCOM (distributed component object model), 704
- DCS (Data Collector Sets), 649, 652–58, 725
- DDNS (Dynamic Domain Name Service), 305
- debugging. *See also* troubleshooting
  - boot configuration data, 754–55
  - network statistics, 319–21
  - operating system on VHD, 95
- Debugging Mode, 751–52
- default gateway, 304–05, 392
- Default Local Users Group, 497
- default rules, 272, 277
- deferred procedure calls (DPC), 717
- defragmenting disks, 230–32
- deleting volumes, 246
- deletion, files and folders, 442–43
- Deny Write Access To Removable Drives Not Protected By BitLocker, 565
- DEP (Date Execution Prevention), 710–11
- deploying. *See also* deploying, system images; Deployment Image Servicing and Management Tool (DISM)
  - network share, 69–71
  - updates, 161–63, 611
- WDS, online VHD deployment, 98–104
- Windows 7, More Info, 71
- deploying, system images
  - applications, servicing, 125–27
  - case scenarios, 191–92
  - DISM WIM commands, 116–23
  - drivers, servicing, 123–25
  - images, distributing, 72–75
  - international settings, 131–33
  - manual installations, 180–81
  - Microsoft Deployment Toolkit overview, 146–51
  - Microsoft Deployment Toolkit (MDT)
    - applications, adding, 164–66
    - deployment points, 166–68
    - device drivers, adding, 154–55
    - distribution shares, creating, 152–53
    - language packs, 164
    - LTI bootable media, 168–69
    - managing and distributing images, overview, 151–52
    - offline files, updating, 163–64
    - operating system image, adding, 153–54
    - program folders, 148
    - task sequences, 155–61
    - updates, adding, 161–63
    - Windows PE options, configuring, 168
  - operating system packages, servicing, 127–30
  - package installation, 131
  - practice
    - downloading, installing and configuring MDT 2010, 181–87
    - mounting offline image and installing language packs, 140–43
- SCCM 2007, 175–80
- unattended servicing, command-line, 137–40
- WDS, 169–75
- Windows editions, managing, 133–35
- Windows PE images, servicing, 135–36
- Deployment Image Servicing and Management Tool (DISM)
  - applications, servicing, 125
  - description, 57
  - operating system packages, servicing, 128
  - overview, 75–77
  - system images, configuring and modifying, 56–58
  - unattended servicing, command-line, 137–40
  - WIM commands, mounting an image, 116–23
- Deployment Workbench, 73, 148–51, 164–66
- Designated Files Types, 274
- desktop, 259
  - backup, 734
  - migrating user profile data, 34
  - Remote Desktop, 402–04, 411–13, 496–98, 537–40
  - Secure Desktop, 480, 483–84, 486–87
- Desktop Background Settings, 585
- Detect Application Failures, 265
- Detect Application Install Failures, 265
- Detect Application Installations and Prompt for Elevation, 485
- Detect Applications Unable to Launch Installers Under UAC, 265
- Device Installation Settings, 204
- Device Manager, 197–203, 209
- devices and drivers
  - Application Compatibility Manager, 261
  - case scenario, signing policy, 252
  - configuring installation policies, 207–08
  - conflict resolution, 210–14
  - driver signing and digital signatures, 215–19
  - Driver Verifier Monitor, 214–15
  - File Signature Verification, 218–19
  - installation, overview, 203–04
  - installing non-PnP devices, 206
  - installing, Windows Update, 204–06
  - Link-layer Topology Discovery Mapper I/O driver, 362
  - out-of-box, 66
  - plug and play, persisting, 81
  - practice, configuring policy and driver search, 220–25
  - printers, sharing, 434
  - staging, 205
  - System Diagnostics, 652
  - updates, 209
  - wireless, connections to WAP, 349
  - working with device drivers, 208–10

- DHCP (Dynamic Host Configuration Protocol), 169, 300, 304–07
- dialup connections, 540–43
- digital certificates. *See* certificates
- digital fingerprint, 275, 281–82
- digital signatures, 485–86
- device drivers, 215–19
  - User Account Control (UAC), 487
  - validation of, 205
- Direct Access
  - case scenarios, 550–51
  - client configuration, 517–21
  - HomeGroups, 425
  - overview, 513, 515–17
  - practice, configuring with Netsh, 526–27
  - server, configuring, 521–26
  - troubleshooting, 519–21
- DirectAccess Management Console, 522
- Directory Services Restore Mode, 751
- DirectX Diagnostic (DXdiag), 217–18
- Disable Automatic Restart On System Failure, 751
- Disable Driver Signal Enforcement, 751
- Disable Driver Signature Enforcement, 216–17
- Disconnect If A Remote Desktop Services Session, 498
- discover image, WDS, 74, 101, 171–72
- Discovery methods, 176
- Disk Cleanup, 228–29
- Disk Management tool
  - basic disk and dynamic disks, conversion, 237–38
  - creating disk volumes, 241–42
  - deleting volumes, 246
  - partitions, working with, 235–36
  - reactivating dynamic disks, 240
  - resizing volumes, 245–46
  - spanned volumes, creating, 241
  - striped volumes, creating, 242
  - VHD, attaching and detaching, 91
  - VHDs, native, 89
- disk steps, 178
- Diskpart
  - basic disk and dynamic disks, conversion, 237–38
  - creating volumes, 241–43, 245
  - deleting volumes, 246
  - format volumes, creating, 71
  - network share, deploying, 69–71
  - partitioning disks, 236
  - reactivating dynamic disks, 240
  - resizing volumes, 245–46
  - spanned volumes, creating, 242
  - striped volumes, creating, 243
  - VHD, create and attach, 91
  - VHDs, native, 89
- disks. *See also* Disk Management tool; Diskpart
  - backup storage, 733, 736
  - basic and dynamic disks, 236–38
  - case scenario, managing, 252
  - dynamic disks, 95, 240–42, 248
  - external hard disks, 36, 230–32, 711–12, 733
  - fixed disks, 95
  - floppy disks, 234–35
  - maintenance, 228–35
  - managing disk volumes, 240–46
  - MBR disks, 235, 241
  - moving, 239
  - partitions, working with, 235–36
  - performance monitoring, 652
  - policies, 233–35
  - practice, configuring policy and disk conversion, 247–48
  - reactivating dynamic disks, 240
  - system restore, 748
  - usage, 769–71
- DISM (Deployment Image Servicing and Management Tool)
  - applications, servicing, 125
  - description, 57
  - operating system packages, servicing, 128
  - overview, 75–77
  - system images, configuring and modifying, 56–58
  - unattended servicing, command-line, 137–40
  - WIM commands, mounting an image, 116–23
  - display, 259–60, 583, 586, 709
- Distributed Cache mode, 462
- Distributed COM Users group, 497
- distributed component object model (DCOM), 704
- Distributed Management Task Force (DMTF), 696
- distribution share, 139, 146, 149, 152–53, 184–87
- DLLs (dynamic link libraries), 263, 273–74, 279–80, 670
- DMTF (Distributed Management Task Force), 696
- Do Not Allow Write Access To Drives Configured in Another Organization, 565
- Domain Name System (DNS)
  - IPv4, configuring, 300
  - managing, 689–90
  - network services, 304–06
  - servers, adding IPv6 addresses, 340
  - servers, ping test, 314
  - WDS, 169
  - Windows Firewall with Advanced Security (WFAS), 392
- Domain Networks, 385
- dotted decimal notation, 302
- Downloads folder, 734
- Downloads, multimedia, 716
- downloads, updates, 613
- DRA (data recovery agents), 559–61
- drive letters, 239
- Driver Details, 210
- driver steps, 179
- Driver Verifier Monitor, 214–15
- drivers, device
  - adding, Microsoft Deployment Toolkit (MDT), 154–55
  - case scenario, enforcing signing policy, 252
  - information about, 122
  - keyboard drivers, 133
  - managing, 75
  - Microsoft Deployment Toolkit, 146
  - out-of-box, 66, 121–23
  - plug and play, persisting, 81
  - printers, sharing, 434
  - rolling back drivers, 755–56
  - servicing, 123–25
  - smart cards, 498
  - System Diagnostics, 652
  - updates, 209
  - WIM images, 120
  - Windows PE images, 135
- dual-boot installations, 14–19
- dummy restore, 762
- DVD-ROM
  - backup, 733, 736
  - bootable, 58, 66–68, 168–69
  - deployment points, 166
  - discover images, 171–72
  - Install.wim file mounting, 119
  - installation source, preparation, 6–7
  - practice, creating Windows PE boot DVD, 84–86
  - Removable Disk policies, 234–35



## DXdiag (DirectX Diagnostic)

DXdiag (DirectX Diagnostic), 217–18  
Dynamic Configuration Protocol (DHCP), 169  
dynamic disks, 95, 240–42, 248  
Dynamic Domain Name Service (DDNS), 305  
Dynamic Host Configuration Protocol (DHCP), 300, 304–07, 392  
dynamic link libraries (DLLs), 263, 273–74, 279–80, 670  
dynamic partitions, 235

## E

EAP (Extensible Authentication Protocol), 359, 532  
Easy Connect, 406–07  
Easy Transfer Cable, 36  
edge devices, 393  
edition-family images, 133  
Effective Permissions, 447  
EFS (Encrypting File System), 451–54, 501–04, 556, 735  
Eftsboot.com, 68  
El Torito boot sector file, 68  
e-mail accelerator, 631  
e-mail data, 34–39  
Enable Boot Logging, 750  
Enable Client Side Targeting, 611  
Enable Low Resolution Video, 751  
Encrypting File System (EFS), 451–54, 493, 501–04, 556, 735.  
*See also* encryption  
encryption. *See also* Encrypting File System (EFS)  
  backup and, 730  
  BitLocker  
    BitLocker To Go, 564–67  
    data recovery agents (DRA), 559–61  
    enabling, 561–63  
    modes, 556–57  
    overview, 555–56  
    practice, BitLocker To Go, 568–71  
    TPM chip, 557  
  event forwarding, 676  
  File Sharing Connections, 425  
  internal wireless adapters, 357–60  
  Network Security Key, 355  
  offline files, 577  
  payload encryption, 333  
  Recovery Agents, 453  
  shared resources  
    case scenarios, 474  
    practice, encryption and permissions, 454–58  
  SSL certificates, configuring, 633–36  
  virtual private networks (VPNs), 531–32  
  Windows Firewall with Advanced Security (WFAS), 393–94  
  wireless networks, 367  
energy use, 199, 202, 582–89  
Enforce Password History, 499  
Enforcement Properties, 273–74  
errors, hard disk, 232–33  
errors, STOP, 652  
Ethernet, 319–21, 349–52  
ETW (Event Tracing for Windows), 717  
Event Log Readers group, 497, 677  
event subscriptions, 676–77  
Event Tracing for Windows (ETW), 717  
Event Viewer, 712–13  
events  
  AppLocker audit event log, 285  
  auditing, 449–51  
  logging and forwarding, 673–80, 689–90, 725  
  performance monitoring and reporting, 649–58  
  troubleshooting performance, 712–13  
  WMI Event Registration, 702–03  
  WMI Event Viewer, 703–05  
Everyone group, 428–32  
exceptions, 383, 387–88, 409  
Exclude Files From Being Cached Policy, 578  
exclusive ORing (XORing), 335  
executable files  
  AppLocker rules, 278  
  Program Compatibility troubleshooter, 258  
  Removable Disk policies, 234–35  
  Software Restriction Policies, 274  
Experience Index, 663–64  
exporting  
  boot image, WDS, 102  
  firewall configuration, 394–95  
  security files, 487–88  
Extensible Authentication Protocol (EAP), 359, 532  
Extensible Firmware Interface (EFI), 104

Extensible Markup Language (XML) files, 740  
extension headers, 333  
external hard disks, 36, 230–32, 711–12, 733

## F

failover protection, 127–30, 243–45  
failures, monitoring, 658–60  
FAT file system, 7, 442, 449, 452, 565, 733–34, 771  
fault tolerance, 242  
Favorites folder, 734  
Feature IDs, 138  
feature properties, 138  
File and Printer Sharing, 362, 425  
file extensions, Software Restriction Policies, 274  
file hash, defined, 281–82  
file logging (profiling), 136  
File Sharing Connections, 425  
File Sharing dialog box, 428  
File Signature Verification (Sigverif), 218–19  
file-based storage, 71  
files  
  backup, 735–39  
  case scenario, migrating user data, 49–50  
  corrupted, 121  
  device drivers, 210  
  Disk Cleanup, 228–29  
  managing, 689–90  
  migrating user profile data, 34  
  offline files, 574–82  
  path rules, 274, 282  
  practice  
    configuring file and folder backup, 741–43  
    migrating user data, 43–46  
    recovering renamed files, 771–75  
  recovery of previous versions, 766  
  restoring damaged or deleted files, 762–69  
  restoring user profiles, 767–69  
  sharing. *See also* virtual private networks (VPN)  
    auditing, configuring, 449–51  
    BranchCache, configuring clients, 463–67  
    BranchCache, Distributed Cache mode, 463

BranchCache, Hosted Cache mode, 462

BranchCache, overview, 461–62

BranchCache, Windows Server 2008, 468–70

case scenarios, 474

DirectAccess, 526

Encrypting File System (EFS), 451–54

file and folder permissions, 442–49

libraries, 432–33

Network And Sharing Center, 423–25

practice, BranchCache configuration, 470–71

practice, encryption and permissions, 454–58

practice, sharing resources, 435–40

printers, 434–35

shared folders, 428–32

User State Migration Tool (USMT), 39–42

Volume Shadow Copy Service (VSS), 766

Windows Easy Transfer, 35–39

fingerprints, Operating System (OS), 384

firewalls

- Action Center, 609, 661–64
- BranchCache, configuring clients, 463–64, 466–67
- DirectAccess, 516, 526
- event forwarding, 676
- network settings, configuring, 317–19
- Ping tool and, 312–15
- virtual private networks (VPNs), 531
- Windows Firewall, 383–88
- Windows Firewall with Advanced Security (WFAS), 389–95
- Windows Update clients, 607–08
- wireless networks, 368

fixed disks, 95

floppy disks, 234–35

folders

- backups, 736–39
- case scenario, migrating user data, 49–50
- default Windows folders, 734
- managing, 689–90
- migrating user profile data, 34

offline files, 574–82

path rules, 274, 282

practice

- configuring file and folder backup, 741–43
- migrating user data, 43–46
- recovering renamed files, 771–75

recovery of previous file versions, 766

restoring damaged or deleted files, 762–69

restoring user profiles, 767–69

sharing. *See also* virtual private networks (VPN)

- auditing, configuring, 449–51
- BranchCache, 461–62
- BranchCache, configuring clients, 463–67
- BranchCache, Distributed Cache mode, 463
- BranchCache, Hosted Cache mode, 462
- BranchCache, Windows Server 2008, 468–70
- case scenarios, 474
- DirectAccess, 526
- Encrypting File System (EFS), 451–54
- file and folder permissions, 442–49
- libraries, 432–33
- Network And Sharing Center, 423–25
- offline files, 580–81
- practice, BranchCache configuration, 470–71
- practice, encryption and permissions, 454–58
- practice, sharing resources, 435–40
- printers, 434–35
- shared folders, 428–32
- User State Migration Tool (USMT), 39–42
- Volume Shadow Copy Service (VSS), 766
- Windows Easy Transfer, 35–39

font settings, 132–33

Force Logoff, 498

Forgotten Password Wizard, 500

Format Prefix (FP), 330

FP (Format Prefix), 330

Full Control permission, 429–30

fully qualified domain names (FQDNs), 305, 409

## G

generalize, configuration pass, 80

global unicast addresses, 330

GlobalCatalog.wbcats, 739–40

globally unique identifier (GUID), 125

GPT disk partitions, 235, 241

Graphical Identification and Authentication DLLs, 263

Group Policy. *See also* policies

- account policies, 499–500
- administrator account, 496
- BitLocker requirements, 561
- BranchCache, 463–67
- device drivers, 205, 216
- DirectAccess, 517–26
- event subscriptions, 678–79
- Internet Explorer Compatibility View, 623
- location-aware printing, 370
- power settings, 587
- Remote Desktop Gateway, 538–39
- remote management, 409–10
- User Account Control (UAC), 482–87
- user rights, 496–97
- Windows Update, 612–16

Group Policy Objects, 521–26

GUID (globally unique identifier), 125

## H

HAL (Hardware Abstraction Layer), 93

handles, 670

hard disks, 736, 748. *See also* disks

hard-link migration store, 42

hardware. *See also* devices and drivers; disks

- Application Compatibility Manager, 261
- BitLocker requirements, 561
- Hardware Abstraction Layer (HAL), 93
- inventories, 175–76
- performance monitoring and reporting
  - Action Center, 661–64
  - case scenarios, 725–26
  - CIM Classes, 696
  - CIM Repository, 695–96
  - events, logging and forwarding, 673–80



- networking, configuring, 715–16
  - overview, 649–58
  - Performance Options, 709–11
  - practice, Performance Monitor, 680–86
  - practice, Windows performance analysis tools, 719–21
  - Process Explorer, 670–72
  - reliability, stability and performance, 658–61
  - Resource Monitor, 667–70
  - Task Manager, 664–67, 714–15
  - troubleshooting, 712–13
  - Windows Performance Analysis Toolkit (WPT), 717–18
  - WMI Administrative Tools, 697–705
  - WMI consumers, 696
  - WMI providers, 694–95
  - WMI scripting library, 696–97
  - WMI Service, 695
  - WMI, CIMOM, 695
  - WMI, overview, 689–94
  - write caching, configuring, 711–12
  - power configurations, 582–89
  - practice, configuring access policy and disk conversion, 247–48
  - RAM requirements, Windows XP Mode, 265–66
  - System Configuration (MSConfig), 705–07
  - Windows 7 requirements, 5–6
  - Windows 7 Upgrade Advisor, 27
  - Windows Memory Diagnostic, 752
  - Hardware Abstraction Layer (HAL), 93
  - Hardware Resource, Msinfo32, 212
  - hash rules, 256, 272, 275, 279, 281–82
  - header size, 333
  - Heartbeat Discovery, 176
  - help-desk, remote access, 405–08
  - hexadecimal notation, 302
  - hibernate mode, 402–03, 613, 718
  - hibernation files, 228–29
  - hibernation mode, 583, 586
  - hidden devices, 198
  - High Performance power plan, 582–89
  - Home or Work (Private) Networks, 385, 423–25
  - HomeGroup, 434–38, 454
  - HomeGroup Connections, 425–27
  - Hosted Cache Client, 464
  - hotfix patches, 95
  - HTTP (Hypertext Transfer Protocol), 177, 676
  - HTTPS (Hypertext Transfer Protocol Secure), 177, 676
  - hybrid images, 151
  - hybrid network, 349
  - hybrid sleep mode, 584, 586
  - Hypertext Transfer Protocol (HTTP), 177, 676
  - Hypertext Transfer Protocol Secure (HTTPS), 177, 676
  - Hyper-V, 89–90
- I**
- IANA (Internet Assigned Numbers Authority), 306–07
  - Icacls, 446–47
  - ICMP (Internet Control Message Protocol), 312–15
  - ICMPv4 Echo Requests, 317
  - ICMPv4 protocols, 320
  - ICMPv6 Echo Requests, 317, 341
  - ICMPv6 protocols, 320
  - ICMPv6 traffic, 526
  - ICS, 304–07, 323–24
  - ID Attribute, 138
  - IEEE 802.11i standard, 358–60
  - IKEv2 protocol, 530, 532, 535
  - image steps, 178
  - images, system
    - case scenario, generating system images, 111
    - configuring
      - Deployment Image Servicing and Management Tool (DISM), 75–77
      - distributing, 72–75
      - Offline Virtual Machine Servicing Tool, 96–98
      - overview, 53
      - practice, creating bootable VHD, 105–08
      - practice, creating WIM image, 84–86
      - pre-staging client computers, 103–04
      - reference image, creating, 58–72
      - Sysprep, 77–84
      - VHDs, native, 89–94
      - WDS images, 74–75
      - WDS, online VHD deployment, 98–104
    - Windows Automated Installation Kit (Windows AIK), 56–58
    - Windows Image to Virtual Hard Disk Tool (WIM2VHD), 94–96
    - Windows Imaging (WIM), 71–72
    - Windows Preinstallation Environment (WinPE), 58
    - information about, 117–18
  - ImageX
    - booting from VHD, 93
    - description, 57
    - images, information about, 118
    - images, mounting, 117, 119
    - network share, image storage, 68–69
    - system images, capturing, 56–58
    - Wimscript.ini, 68
    - Windows PE images, 135
  - Important Updates, 602
  - importing, firewall configuration, 394–95
  - inbound traffic, 385, 389–91, 395, 463–64
  - informational events, 675
  - inheritance, permissions, 445–46, 448–49
  - Initialize Disk Wizard, 236
  - InPrivate Filtering, 631
  - InPrivate Mode, 627–30
  - input locale, 132–33
  - input/output range resources, 200
  - install images, WDS, 74, 100–02, 170–71
  - install pending, 131
  - Install Software Updates, task sequence, 177
  - Install Software, task sequence, 177
  - Install.wim, 119, 170
  - installing
    - case scenario, Windows 7 installation, 49
    - device drivers, 197, 207–08, 210
    - DVD-ROMs, 119
    - failures, 265
    - installers, launching, 265
    - Offline Virtual Machine Servicing Tool, 97
    - packages, considerations, 131
    - post-installation tasks, 139
    - practice
      - clean installation, performing, 19–22
      - downloading, installing and configuring MDT 2010, 181–87
      - Windows AIK, 84–86
    - reference computer, 65–66

- Setup Analysis Tool, 263
  - source preparation, 6–9
  - Sysprep, 77–84
  - update files, manually, 608
  - WDS, 169
  - Windows 7, 9–19
  - Windows Automated Installation Kit (Windows AIK), 56–58
  - Windows Easy Transfer, 36
  - Interactive Logon
    - Require Smart Card, 498
    - Smart Card Removal Behavior, 498
  - interfaces, IPv6, 340–41
  - interfaces, Windows Firewall, 385
  - interference, wireless connections, 364–65
  - internal hard disks, 230–32, 731
  - internal network resources, 526
  - internal private networks, 305
  - international settings, 75, 120, 122, 131–33
  - International Settings Configuration Tool (Intlcfg.exe), 116
  - Internet. *See also* addresses; Internet Explorer
    - connection sharing, 307
    - files temporary, Disk Cleanup, 228–29
    - private IPv4 addresses, 306–07
    - Remote Desktop connections, 403
    - security settings, 609
  - Internet and Corporate Access message, 519
  - Internet Assigned Numbers Authority (IANA), 306–07
  - Internet Control Message Protocol (ICMP), 312–15, 384
  - Internet Explorer. *See also* Internet add-ons and search providers, 630–32
    - case scenario, 644–45
    - certificate errors, 635
    - compatibility test tool, 262
    - Compatibility View, 622–23
    - InPrivate Mode, 627–30
    - pop-up blocker, 632–33
    - practice, InPrivate Mode and add-ons, 636–40
    - security settings, 623–26
    - SmartScreen Filter, 626–27
    - SSL certificates, configuring, 633–36
    - zone rules, 276
  - Internet Options, configuring, 715–16
  - Internet Protocol (IP) addresses, 392
  - Internet Protocol Security (IPSec)
    - connection rules and policies, 342, 394
    - cryptography, 497
    - DirectAccess, 515–16
    - IPv6, advantages of, 333
    - Windows Firewall, 384
  - Internet Protocol Version 4 (TCP/IPv4), 362
  - Internet Protocol Version 4 (TCR/IPv4) Properties, 310–11
  - Internet Protocol Version 6 (TCP/IPv6), 340–41, 362
  - Internet Protocol-Hypertext Protocol Secure (IP-HTTPS), 516
  - Internet zone rules, 276
  - internetwork, 315
  - interrupt request (IRQ), 200, 717
  - interrupt storms, 717
  - Intlcfg, 75
  - intranets, 276, 331–32
  - Intra-Site Automatic Tunneling Addressing Protocol (ISATAP), 337
  - invalid logon attempts, 500
  - invitations, Remote Assistance, 406–07
  - IP addresses, static, 368
  - IP configuration, troubleshooting, 312–15
  - IP routing statistics, 319–21
  - IP Security Policies Management console, 342
  - Ipconfig, 301, 313, 338–39
  - IP-HTTPS, 516, 521
  - IP-HTTPS State, 518
  - IPSec (Internet Protocol Security)
    - connection rules and policies, 342, 394
    - cryptography, 497
    - DirectAccess, 515–16
    - IPv6, advantages of, 333
    - Windows Firewall, 384
  - IPv4
    - addressing, 301–07
    - case scenario, IPv4 connectivity, 377
    - configuring
      - connecting to network, 307–11
      - overview, 300–01
      - practice, configuring network connectivity, 321–24
      - troubleshooting connectivity, 311–21
    - DirectAccess, 515–16, 519
    - network statistics, 319–21
    - Remote Desktop connections, 403
  - Windows Firewall with Advanced Security (WFAS), 392
- IPv6**
- address structure, 328–32
  - advantages of, 333–34
  - case scenario, IPv6 connectivity, 377
  - connectivity, 338–43
  - IPv4 compatibility, 334–37
  - network statistics, 319–21
  - practice, configuring IPv6 connectivity, 343–45
  - Remote Desktop connections, 403
  - Windows Firewall with Advanced Security (WFAS), 392
- IPv6 neighbor Discovery (ND), 333
- IPv6 reverse lookup zone, 334
- ipv6.arpa, 334
- ISATAP (Intra-Site Automatic Tunneling Addressing Protocol), 337
- isolation rules, 393
- J**
- Join Domain or Workgroup, task sequence, 178
- K**
- Kerberos V5 protocol, 393
- kernel debugging, 751
- Kernel Memory, 665
- kernel mode drivers, 263
- kernel trace data, 652
- Key Management Service (KMS), 82
- keyboard layout, 132–33
- keys
  - encryption, 556–57
  - Network Security Key, 355
  - recovery key, 560, 562
  - startup keys, 557, 562
  - Windows Firewall with Advanced Security (WFAS), 393
- Knowledge Base ID, 604–06
- L**
- L2TP/IPsec, 515, 530–31, 535
- LAB deployment point, 168

LAN (local area network), 305–06  
 Language ID, 138  
 language packs, 120, 122, 132–33, 135, 140–43, 164, 191  
 laptop computers.  
   *See also* wireless connections  
   case scenario, offline files, 596–97  
   dialup connections, 540  
   loss of, 555  
   offline files, 574–82  
   power configurations, 582–89  
   shared folders, configuring, 580–81  
   Sync Center, 578–80  
   transparent caching, 577  
 Last Known Good Configuration, 751, 753, 755–56  
 Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPsec), 515  
 LDM (Logical Disk Manager), 236  
 legacy hardware, 206  
 libraries  
   dynamic link libraries (DLLs), 263, 273–74, 279–80, 670  
   sharing, 432–33, 435–38  
   WMI scripting library, 696–97  
 license product key, 82  
 Link-layer Topology Discovery Mapper I/O Driver, 362  
 Link-layer Topology Discovery Responder, 362  
 link-local addresses, 330–32  
 Links folder, 734  
 list items, 139  
 Lite Touch Installation (LTI), 73, 147, 168–69  
 LoadState, 41  
 Local and Internet Access message, 519  
 local area network (LAN), 305–06  
 Local Group Policy Editor, 208, 233–35, 449–51  
 Local Intranet, security settings, 623–24  
 Local Security Policy, 487–88  
 Local Subnet, 392  
 LocalAccountTokenFilterPolicy, 409  
 location-aware printing, 370  
 Lock Workstation, 498  
 lockout policies, accounts, 499–500  
 loctl\_disk\_performance files, 681

logging  
   events, logging and forwarding, 673–80, 689–90, 725  
   managing, 75  
   Sysprep, 83–84  
 Logical Disk Manager (LDM), 236  
 Logman, 655–56  
 logons  
   Credential Manager, 493–95  
   Remote Desktop, 402–03  
 loopback address, 332  
 LTI (Lite Touch Installation), 73, 147, 168–69

## M

MAC (media access control), 305–06, 334, 367  
 Machine OOBE, 64  
 maintenance tasks, disks, 228–35  
 MAK (Multiple Activation Keys), 82  
 malware. *See* User Account Control (UAC)  
 Manage Add-Ons, 632  
 Manage File Encryption Certificates, 502–04  
 Manage Wireless Networks, 357  
 Manage-bde.exe, 567  
 Managed Object Format (.mof), 179  
 managing  
   applications  
     Application Compatibility Diagnostics policies, 264–65  
     Application Compatibility Toolkit (ACT), 260–64  
     AppLocker control policies, overview, 276–77  
     AppLocker rules, 277–83  
     AppLocker, auditing, 285–86  
     AppLocker, configuring  
       exceptions, 283  
       case scenarios, 294–95  
       compatibility, configuring  
         options, 257–60  
       executable rules, 278  
       overview, 255  
       practice, compatibility, 267–69  
       practice, restricting applications, 286–89  
     Software Restriction Policies, 271–76  
     Windows XP Mode, 265–66  
 BitLocker  
   BitLocker To Go, 564–67  
   data recovery agents (DRA), 559–61  
   enabling, 561–63  
   modes, 556–57  
   overview, 555–56  
   practice, BitLocker To Go, 568–71  
   TPM chip, 557  
 certificates, 502–04  
 devices  
   configuring installation policies, 207–08  
   Device Manager, 197–203  
   driver signing and digital signatures, 215–19  
   Driver Verifier Monitor, 214–15  
   File Signature Verification, 218–19  
   installing non-PnP devices, 206  
   installing, Windows Update, 204–06  
   overview, 203–04  
   practice, configuring policy and driver search, 220–25  
   resolving conflicts, 210–14  
   staging device drivers, 205  
   working with drivers, 208–10  
 DirectAccess  
   case scenarios, 550  
   client configuration, 517–21  
   overview, 515–17  
   practice, configuring with Netsh, 526–27  
   server, configuring, 521–26  
   troubleshooting, 519–21  
 disks  
   basic and dynamic disks, 236–38  
   case scenario, managing disk volumes, 252  
   disk volumes, 240–46  
   maintenance, 228–35  
   moving, 239  
   partitions, working with, 235–36  
   practice, configuring policy and disk conversion, 247–48  
   reactivating dynamic disks, 240  
 Internet Explorer, InPrivate Mode, 627–30  
 network connections, 362–63  
 performance  
   CIM Classes, 696  
   CIM Repository, 695–96  
   WMI Administrative Tools, 697–705  
   WMI consumers, 696  
   WMI providers, 694–95

- WMI scripting library, 696–97
- WMI Service, 695
- WMI, CIMOM, 695
- WMI, overview, 689–94
- practice, managing credentials, 504–07
- printers, 434
- remote management
  - BCDEdit, 754–55
  - case scenarios, 419
  - practice, remote management options, 411–15
  - Remote Assistance, 405–08
  - Remote Desktop, 402–04
  - Windows Remote Management, 408–10
- shared resources
  - BranchCache, 461–62
  - BranchCache, configuring clients, 463–67
  - BranchCache, Distributed Cache mode, 463
  - BranchCache, Hosted Cache mode, 462
  - BranchCache, Windows Server 2008, 468–70
  - folders, 431
  - practice, BranchCache configuration, 470–71
- system image deployment
  - applications, adding, 164–66
  - applications, servicing, 125–27
  - case scenarios, 191–92
  - deployment points, 166–68
  - device drivers, adding, 154–55
  - DISM WIM commands, 116–23
  - distribution share, creating, 152–53
  - drivers, servicing, 123–25
  - international settings, 131–33
  - language packs, 164
  - LTI bootable media, 168–69
  - managing and distributing images, overview, 151–52
  - manual installations, 180–81
  - MDT (Microsoft Deployment Toolkit), overview, 146–51
  - offline files, updating, 163–64
  - operating system image, adding, 153–54
  - operating system packages, servicing, 127–30
  - package installation, 131
  - practice, downloading, installing and configuring MDT 2010, 181–87
  - practice, mounting offline image and installing language packs, 140–43
  - SCCM 2007, 175–80
  - task sequences, 155–61
  - unattended servicing, command-line, 137–40
  - updates, adding, 161–63
  - WDS, 169–75
  - Windows editions, managing, 133–35
  - Windows PE, 135–36, 168
  - User Account Control (UAC), 479–80, 482–90
  - user profiles
    - migrating user profile data, 34
    - practice, migrating user data, 43–46
    - User State Migration Tool (USMT), 39–42
    - Windows Easy Transfer, 35–39
  - virtual hard disk files
    - case scenario, working with VHD, 111
    - native VHDs, using, 89–94
    - Offline Virtual Machine Servicing Tool, 96–98
    - practice, creating bootable VHD, 105–08
    - pre-staging client computers, 103–04
    - WDS, online VHD deployment, 98–104
    - Windows Image to Virtual Hard Disk Tool (WIM2VHD), 94–96
  - Windows Firewall, 383–88, 395–98
  - Windows Firewall with Advanced Security (WFAS)
    - overview, 389–95
    - practice, configuring, 395–98
    - wireless networks, 356–57
- map accelerator, 631
- Maximum Password Age, 499
- MBR disks, 235, 241
- MBSA (Microsoft Baseline Security Analyzer), 616
- MDT (Microsoft Deployment Toolkit)
  - applications, adding, 164–66
  - deployment points, 166–68
  - distribution share, creating, 152–53
  - language packs, 164
  - LTI bootable media, 168–69
  - managing and distributing images, overview, 151–52
  - MDT 2010, overview, 73
  - offline files, updating, 163–64
  - operating system image, adding, 153–54
  - overview, 146–51
  - SCCM, integrating, 179–80
  - task sequences, 155–61
  - updates, adding, 161–63
  - Windows PE options, configuring, 168
- Microsoft Baseline Security Analyzer (MBSA), 616
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2), 533
- Microsoft Data Protection Manager, 89
- Microsoft Deployment Toolkit (MDT), 73
  - applications, adding, 164–66
  - deployment points, 166–68
  - distribution share, creating, 152–53
  - language packs, 164
  - LTI bootable media, 168–69
  - managing and distributing images, overview, 151–52
  - offline files, updating, 163–64
  - operating system image, adding, 153–54
  - overview, 146–51
  - SCCM, integrating, 179–80
  - task sequences, 155–61
  - updates, adding, 161–63
  - Windows PE options, configuring, 168
- Microsoft Hyper-V Server, 97
- Microsoft Protected EAP (PEAP), 532–33
- Microsoft Secured Password (EAP-MSCHAP v2), 532
- Microsoft Smart Card or Other Certificate, 532–33
- Microsoft Update, application servicing, 125

- Microsoft Virtual PC, 265
- Microsoft-Windows-Security-Licensing (SLC), 82
- MigApp.xml, 40
- MigDocs.xml, 40
- migration
  - case scenario, migrating user data, 49–50
  - from Windows Vista, 26
  - from Windows XP, 29–30
  - practice, migrating user data, 43–46
  - store types, 42
  - user profile data, 34
  - Windows Easy Transfer, 37–39
- MigUser.xml, 40
- Minimum Password Age, 499
- Minimum Password Length, 499
- mirrored volumes, 237, 239, 243
- MOBIKE, 535
- mobile devices. *See also* virtual private networks (VPN)
  - case scenario, offline files, 596–97
  - offline files, 574–82
  - shared folders, configuring, 580–81
  - Sync Center, 578–80
  - transparent caching, 577
- mobile phone networks, 360
- mobility
  - offline files, 574–82
  - power configurations, 582–89
  - shared folders, configuring, 580–81
  - Sync Center, 578–80
  - transparent caching, 577
- modems, 403, 540–43
- modules, 670
- MOF Generator Wizard, 699
- monitoring systems
  - Action Center, 661–64
  - events, logging and forwarding, 673–80
  - performance monitoring and reporting, 649–58
  - case scenarios, 725–26
  - CIM Classes, 696
  - CIM Repository, 695–96
  - CIMOM, 695
  - networking, configuring, 715–16
  - Performance Options, 709–11
  - practice, Performance Monitor, 680–86
  - practice, Windows performance analysis tools, 719–21
  - troubleshooting, 712–13
- Windows Performance Analysis Toolkit (WPT), 717–18
- WMI Administrative Tools, 697–705
- WMI consumers, 696
- WMI providers, 694–95
- WMI scripting library, 696–97
- WMI Service, 695
- WMI, overview, 689–94
- write caching, configuring, 711–12
- Process Explorer, 670–72
- reliability, stability and performance, 658–61
- Resource Monitor, 667–70
- Services console, 707–09
- System Configuration (MSConfig), 705–07
- Task Manager, 215, 664–67, 714–15
- More Info
  - ACT, 261, 264
  - advanced system tools and command-line utilities, 671
  - answer files, 65, 81
  - AppLocker auditing, 286
  - audit mode and Sysprep, 64
  - audit mode, booting to, 83
  - audit policy, advanced, 451
  - BCD boot options, 755
  - BCD WMI interface, 755
  - BCDBoot, 71, 174
  - BCDEdit, 94
  - Biometrics, 498
  - BitLocker, 556
  - BitLocker DRAs, 561
  - Bluetooth, 356
  - configuration pass, 139
  - custom commands and scripts, adding, 140
  - Data Collector Sets, 654–55
  - Default Local Users Group, 497
  - deployment, 67, 99
  - DirectAccess, 519, 521
  - DirectAccess Executive Overview, 516
  - Disable Driver Signature Enforcement, 217
  - Diskpart, 174, 246
  - Distributed Management Task Force (DMTF), 696
  - driver store and staging, 206
  - Driver Verifier Monitor, 215
  - EAP, 359
  - El Torito boot sector file, 68
  - Encrypting File System (EFS), 452
  - external resolution, 349
  - files and settings, rerouting, 41
  - global unicast addresses, 330
  - Hosted Cache servers, configuring, 462
  - lcacls, 447
  - images, creating, 75
  - internal vs. external resolution, 305
  - Internet connection sharing, 307
  - Internet Explorer enhanced security, 626
  - IPv6 addressing, 330
  - LoadState, 41
  - loctl\_disk\_performance files, 681
  - Logman, 656
  - managing images with WDS, 103
  - MDT (Microsoft Deployment Toolkit), 148
  - Microsoft Baseline Security Analyzer (MBSA), 616
  - Microsoft-Windows-Security-Licensing-SLC, 82
  - migration, 40, 42–43
  - MOF files, compiling, 702
  - NAP, 537
  - Netsh, 341
  - Network Address Translation (NAT), 306
  - network bridges, 313
  - Offline Virtual Machine Servicing Tool and SCVMM, 164
  - Peer Name Resolution Protocol, 334
  - PhysicalDisk %Disk Time counter, 683
  - PnPUtil, 224
  - power management, 584
  - Powercfg.exe, 588
  - pre-staging client computers, 104
  - printer permissions, 435
  - RD (Remote Desktop) Gateway, 537
  - remote access, Windows PowerShell, 410
  - RemoteApp, 540
  - ScanState, 41
  - SCCM 2007 and software update installation, 180, 611
  - SCCM client discovery, 176
  - share permissions and NFS permissions, 432
  - smart cards, 499
  - Software Restriction Policies, 276
  - subnetting and supernetting, 303

Sysprep, Audit mode, 79  
 task sequence actions and variables, 178  
 Task Sequence Editor, 158  
 TCP connection states, 320  
 Teredo addresses, 336  
 transparent caching, 577  
 USMT, 58  
 virtual hard drives (VHDs), 90  
 Virtual PC and Windows XP, 735  
 Wbadadmin, 740  
 WDS, 98–100, 175  
 WDSUTIL, 175  
 Web Proxy Auto Detect, 608  
 WIM2VHD, 96  
 Windows 7 deployment, 71  
 Windows 7 Upgrade Advisor, 27  
 Windows image, state of, 83  
 Windows Update Stand-alone Installer, 608  
 WMI classes, 691  
 WSUS, 612  
 moving files, 448–49  
 MP3 players, 233–35  
 MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2), 533  
 MSConfig (System Configuration), 705–07  
 MS-DOS-style MBR partition tables, 236  
 Msinfo32 (System Information), 212–14  
 multicast, 329, 332  
 multifactor authentication, 498  
 multimedia settings, 586, 716  
 multinetting, 329  
 Multiple Activation Keys (MAK), 82  
 music, 425  
 My Computer, zone rules, 276  
 Mystore, 41

## N

NAP (Network Access Protection), 536–37, 609–10  
 NAT (Network Address Translation), 305–06, 337, 393, 403  
 negative caching, 314–15  
 neighbor cache, 341  
 Net Share command, 431  
 NetBIOS, 310, 409  
 netbook computers, 7

Netsh  
 BranchCache, configuring clients, 463–67  
 DirectAccess, 519  
 IPv4 configuring, 310–11  
 IPv6 configuring, 340–41  
 IPv6 to IPv4 compatibility, 337  
 practice, configuring DirectAccess, 526–27  
 Windows Firewall, 388  
 Windows Firewall with Advanced Security (WFAS), 395  
 Windows Update, 608  
 wireless networks, 352–56  
 Netstat, 319–21, 338  
 Network Access Protection (NAP), 536–37, 609–10  
 Network Address Translation (NAT), 305–06, 337, 393, 403  
 network address, Windows Firewall, 385  
 Network And Sharing Center  
 ad hoc networks, 360  
 connection interfaces, 362  
 dialup connections, 540  
 HomeGroups, 427  
 ICS clients, adding, 308  
 Internet connections, 350  
 Network Location Awareness (NLA), 385  
 sharing resources, 423–25  
 virtual private networks (VPNs), 530–31  
 Windows Network Diagnostics, 316  
 wireless networks, 356  
 network bridges, 313, 363  
 Network Configuration Operators group, 497  
 Network Diagnostics, 675  
 Network Discovery, 176, 425  
 Network Level Authentication, 403–04  
 Network Location Awareness (NLA), 385–87  
 network migration method, 36  
 Network Printer Installation Wizard, 369  
 Network Security Key, 355  
 network share  
 as installation source, 8–9  
 capturing installation images, 68–69  
 deployment, 69–71  
 network-based installation, 99  
 networks. *See also* offline files

ad hoc networks, 360  
 backup storage, 733  
 case scenario  
 IPv4 connectivity, 377  
 IPv6 connectivity, 377  
 wireless networks, 377–78  
 connectivity  
 managing connections, 362–63  
 overview, 348–50  
 setting up connections, 350–52  
 internal wireless adapter security, 357–60  
 IPv4, configuring  
 addressing, 301–07  
 connecting to network, 307–11  
 overview, 300–01  
 practice, configuring, 321–24  
 troubleshooting, 311–21  
 IPv6, configuring  
 addresses, 328–32  
 advantages of IPv6, 333–34  
 connectivity, 338–43  
 IPv4 compatibility, 334–37  
 practice, configuring IPv6 connectivity, 343–45  
 managing, 689–90  
 Network Location Awareness, 385–87  
 network services, 304–06  
 network type, selecting, 14  
 performance monitoring, 652, 715–16  
 practice, creating ad hoc network, 371–73  
 printing enhancements, 368–70  
 wireless, 675  
 wireless computers, adding, 352–56  
 wireless networks  
 managing, 356–57  
 security, 367–68  
 technologies, 361  
 troubleshooting, 363–67  
 zone rules, 276  
 New Application Wizard, 165–66  
 New Connection Security Rule Wizard, 393–94  
 New Deployment Point Wizard, 166–68  
 New Driver Wizard, 154–55  
 New Inbound (or Outbound) Rule Wizard, 389–91  
 New OS Wizard, 153  
 New Task Sequence Wizard, 177  
 NFTS permissions, 432



NLA (Network Location Awareness), 385–87  
 Notify Blocked Drivers, 265  
 NTFS files, 169, 442, 449, 733  
 NTFS permissions, 442, 449, 556  
 NTFS-formatted removable devices, 565  
 NTLMv2, 393

## O

object repository, 695–96  
 octets, 302  
 OEM Activation licenses, 82  
 offline attacks, 555  
 offline dynamic disks, 240  
 offline files, 163–64, 574–82, 596–97. *See also* sharing resources  
 offline images, 123, 129  
 offline migrations, 42–43  
 Offline Settings, 430  
 Offline Virtual Machine Servicing Tool, 128, 163–64  
 offline Web pages, 228–29  
 offlineServicing, 80  
 On/Off Transition Trace Capture (Xbootmgr.exe), 717–18  
 online images, working with, 121–23, 129  
 Only Elevate Executables That Are Signed and Validated, 485–86  
 Only Elevate UIAccess Applications That Are Installed In Secure Locations, 487  
 OOBE (out-of-box experience), 94, 134  
 oobeSystem, 63, 80, 83  
 Operating System (OS) fingerprinting, 384  
 operating system image, adding, 153–54  
 operating system packages, servicing, 127–30  
 operating system, default, 17–19  
 operating systems. *See also* system images, configuring; specific system name  
   Windows Automated Installation Kit (Windows AIK), 56–58  
 optical media, 173  
 Optional Updates, 603  
 orphaned images, 121  
 Osdcmg, 58  
 outbound traffic, 385, 389–91, 395, 463–64  
 out-of-box device drivers, 66, 121–23  
 Out-of-Box Experience (OOBE), 94, 134  
 overlapping networks, 364

## P

Package Manager (Pkgmgr.exe), 75, 116  
 packages, 75, 122, 131, 135  
 page files settings, 710  
 PAP (Password Authentication Protocol), 533  
 parameters, WIM2VHD, 94–95  
 partitions  
   basic and dynamic disks, 236–38  
   disks, working with, 235–36  
   network share deployment, 69  
 Password Authentication Protocol, 533  
 Password Must Meet Complexity Requirements, 499  
 Password Protected Sharing, 425  
 password reset disk, 500  
 passwords  
   account policies, 499–500  
   case scenario, UAC and passwords, 511  
   Credential Manager, 493–95  
   HomeGroup Connections, 425  
   on wakeup, 585  
   practice, managing credentials, 504–07  
   recovery passwords, 559–60  
   remote access, 409–10  
   Remote Assistance, 407  
   removable data drives, 565  
   resolving authentication issues, 500–01  
   Runas, 495–96  
   smart cards, 497–99  
   VPN authentication protocols, 533  
   wireless networks, 367  
 patches, 95, 125–27  
 path rules, 272, 274  
 Pathping tool, 315, 338  
 PCI Express, 586  
 PEAP (Microsoft Protected EAP), 532–33  
 Peer Name Resolution Protocol (PNRP), 334, 406–07  
 Peer-Discovery, 464  
 peer-to-peer environments, 334  
 PEimg, 75  
 pending computers, 99  
 performance  
   Action Center, 661–64  
   booting from VHD, 93  
   case scenarios, 725–26  
   defragmenting disks, 230–32  
   events, logging and forwarding, 673–80  
   monitoring and reporting, 649–58  
   network statistics, 319–21  
   networks, configuring, 715–16  
 Offline Virtual Machine Servicing Tool, 97  
 practice, Performance Monitor, 680–86  
 practice, Windows performance analysis tools, 719–21  
 Process Explorer, 670–72  
 reliability, stability and performance, 658–61  
 Resource Monitor, 667–70  
 Services console, 707–09  
 spanned volumes, 241  
 striped volumes with parity (RAID-5), 243–45  
 System Configuration (MSConfig), 705–07  
 Task Manager, 664–67, 714–15  
 troubleshooting, 712–13  
 Windows Performance Analysis Toolkit (WPT), 717–18  
 WMI  
   CIM Classes, 696  
   CIM Repository, 695–96  
   CIMOM, 695  
   overview, 689–94  
   providers, 694–95  
   WMI Administrative Tools, 697–705  
   WMI consumers, 696  
   WMI scripting library, 696–97  
   WMI Service, 695  
   write caching, configuring, 711–12  
 Performance Analyzer, 718  
 Performance Log Users group, 497  
 Performance Monitor, 215, 650–52, 680–86  
 permissions  
   configuring with Icacls, 446–47  
   Effective Permissions, 447  
   file and folder, 442–49  
   inheriting, 445–46  
   NTFS permissions, 271

- printers, 434–35
- Removable Disk policies, 234–35
- script rules, 279
- shared folders, 428–32
- shared resources, 454–58, 474
- personal identification number (PIN), 556–57
- Personal mode, 359–60
- phishing, 626
- physical machines, image deployment, 89
- Physical Memory, 665
- pictures, 425
- PID (process ID), 320
- PIN (personal identification number), 556–57
- Ping, 312–15, 317–19, 338
- PIV standard, 498
- Pkgmgr.exe, 75
- plug and play (PnP) devices, 81, 197–203
- PNRP (Peer Name Resolution Protocol), 334
- Point-to-Point Tunneling Protocol (PPTP), 515, 530–31, 535, 541–42
- policies. *See also* Group Policy
  - accelerators, 632
  - account lockout policies, 501
  - Application Compatibility Diagnostics policies, 264–65
  - AppLocker
    - auditing, 285–86
    - configuring exceptions, 283
    - practice, restricting applications, 286–89
    - rules, 277–83
  - auditing remote connections, 544
  - Auto-Add, 99, 103–04
  - BitLocker DRAs, 559–60
  - BitLocker To Go, 564–66
  - BranchCache, configuring clients, 463–67
  - case scenario
    - restricting applications, 294–95
  - case scenario, driver signing policy, 252
  - device drivers, 205, 207–08, 216, 220–25
  - DirectAccess, 517–26
  - disk policies, 233–35
  - event subscriptions, 678–79
  - InPrivate, 629–30
  - IPSec, 342
  - location-aware printing, 370
  - offline files, 577–78
  - power settings, 587
  - practice
    - access policy and converting a disk, 247–48
    - BitLocker To Go, 568–71
    - remote access, 409
    - Remote Desktop Gateway, 538–39
    - smart cards, 498
    - Software Restriction Policies, 271–76
    - updates, 611
    - User Account Control (UAC), 482–87
    - user rights, 496–97
    - Windows Update, 612–16
    - write caching, configuring, 711–12
- pop-up blocker, 632–33
- portable computers
  - case scenario, offline files, 596–97
  - dialup connections, 540
  - loss of, 555
  - offline files, 574–82
  - power configurations, 582–89
  - shared folders, configuring, 580–81
  - Sync Center, 578–80
  - transparent caching, 577
- port-based authentication, 358–60
- ports, 319–21, 384, 387–89
- power allocation, 202, 582–92
- Power Management, 199
- Power Users group, 497
- PowerShell, 163–64, 408–10, 414–15
- PPTP (Point-to-Point Tunneling Protocol), 515, 530–31, 535, 541–42
- practice
  - backup, configuring file and folder, 741–43
  - BitLocker To Go, 568–71
  - BranchCache configuration, 470–71
  - clean installation, performing, 19–22
  - compatibility, 267–69
  - credentials, managing, 504–07
  - device drivers, configuring policy and driver search, 220–25
  - DirectAccess, configuring with Netsh, 526–27
  - disks, access policy and covertion, 247–48
  - Internet Explorer, InPrivate Mode and add-ons, 636–40
  - MDT 2010, downloading, installing and configuring, 181–87
  - migrating user data, 43–46
  - mounting offline image and installing language packs, 140–43
  - Performance Monitor, 680–86
  - power plans, managing, 589–92
  - recovering renamed files, 771–75
  - remote connections, configuring, 545–47
  - remote management options, 411–15
  - shared resources, encryption and permissions, 454–58
  - sharing resources, 435–40
  - system protection and restore, 756–60
  - upgrading to Windows 7, 30–31
  - User Account Control (UAC), configuring, 488–90
  - VHD, bootable, 105–08
  - WIM image, creating, 84–86
  - Windows Firewall, 395–98
  - Windows performance analysis tools, 719–21
  - Windows Update, configuring, 617–19
- precedence, 272, 274
- preferred wireless networks, 356–57
- pre-shared key (PSK) mode, 359–60
- Print Management MMC
  - snap-in, 369
- printers, 370, 434–35, 689–90
- printing, Windows 7 enhancements, 368–70
- private addresses, 306–07
- private intranets, 331–32
- private keys, 452
- private networks, 305–06
- privileges
  - case scenario, UAC and passwords, 511
  - elevation of, 479–80
  - User Account Control (UAC) overview, 479–80
  - policies, 482–87
  - practice, configuring, 488–90
  - Secpol and Local Security Policy, 487–88
  - settings, 480–82
- virtual private networks (VPNs), 530
- Problem Devices, 212
- Process Explorer, 267–69, 670–72



## process ID (PID)

- process ID (PID), 320
- Processor Power Management, 586
- processors, 5–6, 265–66, 652, 664–67
- product keys, 82, 133–34
- Program Compatibility troubleshooter, 257–58, 265
- Program Files, 279, 486–87
- Programs and Features, 387–88
- prompts, UAC, 483–84
- Protected Mode, Internet Explorer, 624
- Provide The Unique Identifiers For Your Organization Policy, 565
- proxy servers, 607–08
- PSK (pre-shared key) mode, 359–60
- public addresses, 306–07
- Public Folder Sharing setting, 425
- public key encryption, 452
- Public Networks, 385
- publisher rules, 280–81
- PXE-compliant clients, 147
- PXE-enabled computers, 173

## Q

- Quality of Service (QoS), 333, 362
- Quick Fix Engineering (QFE), 95

## R

- RADIUS (Remote Authentication Dial In User Service), 358–60
- RAID-5 volumes, 237, 239, 243–45
- RAM, 265–66, 664–67, 752
- RAMdisk mode, 135
- read
  - performance, 244
  - permissions, 442–43
  - removable devices, 565
  - Removable Disks policies, 234–35
  - shared folders, 428–32
- Read/Write image, 120
- Read/Write permissions, 428–32
- read-only images, 119
- real-time traffic, 333
- reboots, monitoring, 658–60
- Recommended Updates, 602
- Recovery Agents, 453
- recovery key, 560, 562
- recovery passwords, 559–60

- recovery, data. *See also* backup
  - Advanced Boot Options, 750–53
  - BitLocker protected drives, 566–67
  - boot options, 754–55
  - case scenarios, 779–80
  - file copying and, 730
  - practice, recovering renamed files, 771–75
  - previous versions of files, 766
  - renamed and deleted files, 765–66
  - restoring damaged or deleted files, 762–69
  - system protection and disk usage, configuring, 769–71
  - user profiles, restoring, 767–69
  - Volume Shadow Copy Service (VSS), 766
- recovery, system, 755–60
- Recycle Bin, 228–29, 735, 765–66
- Redirect, 333
- Reduced Functionality Mode (RFM), 82
- reference computers, 59, 65–66
- registry, 486, 689–90, 730, 746–50
- registry keys, 263
- Reliability Monitor, 214, 658–60
- Remember My Credentials, 493
- Remote Assistance, 405–08
- Remote Authentication Dial In User Service (RADIUS), 358–60
- remote computers, Device Manager, 198
- remote connections
  - auditing, 544
  - case scenarios, 550–51
  - dialup connections, 540–43
  - practice, configuring remote connections, 545–47
  - Remote Desktop, 537–40
  - virtual private networks (VPNs)
    - incoming connections, accepting, 541–43
    - NAP remediation, 536–37
    - overview, 530–32
    - VPN Reconnect, 535–36
- Remote Desktop, 402–04, 411–13, 496, 537–40
- Remote Desktop Services, 498
- Remote Desktop Users group, 404, 496–97
- remote management
  - case scenarios, 418–19
  - practice, remote management options, 411–15

- Remote Assistance, 405–08
- Remote Desktop, 402–04
- Windows Remote Management, 408–10
- RemoteApp, 539–40
- removable devices. *See also* USB (universal serial bus) devices
  - booting target drives, 173
  - data drives, 564–66
  - deployment points, 166
  - disk policies, 233–35
  - partitioning, 236
  - policies about, 208
  - practice, write access, 247–48
- Repair Your Computer, 746
- replay protection protocol, 531
- Replicator group, 497
- reports. *See* resources, performance monitoring and reporting
- Res.rwm files, 99
- Reset Account Lockout Counter After, 500
- resetting user account passwords, 500
- resizing volumes, 245–46
- Resource Monitor, 667–70
- resources
  - Device Manager, 200
  - hardware, Msinfo32, 212
  - performance monitoring and reporting
    - Action Center, 661–64
    - case scenarios, 725–26
    - CIM Classes, 696
    - events, logging and forwarding, 673–80
    - networking, configuring, 715–16
    - overview, 649–58
    - Performance Options, 709–11
    - practice, Performance Monitor, 680–86
    - practice, Windows performance analysis tools, 719–21
    - Process Explorer, 670–72
    - reliability, stability and performance, 658–61
    - Resource Monitor, 667–70
    - Task Manager, 215, 664–67, 714–15
    - troubleshooting, 712–13
    - Windows Performance Analysis Toolkit (WPT), 717–18
    - WMI Administrative Tools, 697–705
    - WMI consumers, 696

- WMI providers, 694–95
  - WMI scripting library, 696–97
  - WMI Service, 695
  - WMI, CIMOM, 695
  - WMI, overview, 689–94
  - sharing. *See also* virtual private networks (VPN)
    - auditing, configuring, 449–51
    - BranchCache, configuring clients, 463–67
    - BranchCache, Distributed Cache mode, 463
    - BranchCache, Hosted Cache mode, 462
    - BranchCache, overview, 461–62
    - BranchCache, Windows Server 2008, 468–70
    - case scenarios, 474
    - DirectAccess, 526
    - Encrypting File System (EFS), 451–54
    - file and folder permissions, 442–49
    - libraries, 432–33
    - Network And Sharing Center, 423–25
    - practice, BranchCache configuration, 470–71
    - practice, encryption and permissions, 454–58
    - practice, sharing, 435–40
    - printers, 434–35
    - shared folders, 428–32
    - System Configuration (MSConfig), 705–07
    - usage monitoring, 215
  - Restart Computer,
    - task sequence, 178
  - restore, 493–95, 746–50, 758, 762–69
  - Restore Files Wizard, 763, 767–69
  - Restore My Files, 763
  - Restore Settings, 770
  - Restore Vault, 495
  - Restricted Sites, 276, 624
  - resume, 718
  - reverse lookup, 334
  - roaming profiles, 767
  - Robocopy.exe, 449
  - roll backs, 28, 197, 208, 612
  - Route, command-line tool, 338
  - Router Discovery, 333
  - routers
    - edge devices, 393
    - site-local addresses, 331–32
  - SOHO, Windows Firewall and, 387
  - subnets and supernets, 303–04
  - switching between WAPs, 363–64
  - routing table, IPv6, 333
  - Rule Creation Wizard, 281–82
  - rule scope, 392–93
  - rules, 383, 386
  - Run All Administrators In Admin Approval Mode, 486
  - Run Command Line, task sequence, 177
  - RunSynchronous, 81
- ## S
- Safe Mode, 747, 750
  - Same Service Set Identifier (SSID), 365–68
  - Saved Games, 734
  - scaling, 259
  - ScanState, 41
  - SCCM 2007, 163, 175–80
  - scheduled tasks, 689–90
  - scratch space, 136
  - screen resolution, 259
  - scripts
    - AppLocker, script rules, 279
    - Cscript, 94
    - Deployment Workbench, 148
    - More Info, 140
    - network share deployment, 70
    - rules for, 279
    - WMI scripting library, 696–97
  - SCSI (Small Computer System Interface)
    - defragmenting disks, 232
  - SCVMM (System Center Virtual Machine Manager), 97–98, 128, 147, 163
  - search providers, 630–32
  - Searches folders, 734
  - Secedit.exe, 487–88
  - Secpol, 487–88
  - Secure Desktop, 480, 483–84, 486–87
  - Secure Socket Tunneling Protocol (SSTP), 515, 530–31, 535
  - Secure Sockets Layer (SSL), 531, 626, 633–36
  - security. *See also* remote management; updates; User Account Control (UAC)
    - Action Center, 661–64
    - AppLocker
      - auditing, 285–86
      - configuring exceptions, 283
      - rules, 277–83
    - backup, 737
    - BitLocker
      - BitLocker To Go, 564–67
      - data recovery agents (DRA), 559–61
      - enabling, 561–63
      - modes, 556–57
      - overview, 555–56
      - practice, BitLocker To Go, 568–71
      - TPM chip, 557
    - case scenario, restriction applications, 294–95
    - device drivers, 205
    - DirectAccess, 517–19
    - disk policies, 233–35
    - events, logging and forwarding, 673–80
    - internal wireless adapters, 357–60
    - Internet Explorer settings, 623–26
    - IPv6, advantages of, 333
    - managing, 689–90
    - mobility
      - case scenario, offline files, 596–97
      - offline files, 574–82
      - shared folders, configuring, 580–81
      - Sync Center, 578–80
      - transparent caching, 577
    - network performance and, 716
    - Network Security Key, 355
    - operating system image, adding, 153
    - patches, offline images, 127
    - practice, restricting applications, 286–89
    - pre-staging client computers, 104
    - public and private addresses, 306
    - SCCM 2007, 175–76
    - shared resources
      - configuring auditing, 449–51
      - Encrypting File System (EFS), 451–54
      - file and folder permissions, 442–49
      - practice, encryption and permissions, 454–58
    - Software Restriction Policies, 271–76
    - updates, adding with MDT, 161–63

- virtual private networks (VPNs), 531–33, 536, 544
- Windows Firewall, 383–88, 395–98, 419
- Windows Firewall with Advanced Security (WFAS), 389–98, 419
- wireless networks, 356–57, 365–68
- Security Center, 537, 609–10
- Security Health Validators (SHVs), 536
- Security Levels, 272
- Security Template, 487–88
- self-powered hubs, 202
- Serial Advanced Technology Attachment (SATA) disks, 232
- server message block (SMB), 177
- server-to-server rules, 394
- service set identifier (SSID), 353–54
- Services console, 707–09
- services, event logs, 674
- servicing jobs, 163–64
- Set Network Location, 423
- Set Task Sequence Variable, 178
- settings. *See also* settings, network
  - Action Center, 662–63
  - Advanced Sharing Settings, 423, 434
  - answer file, 59, 64–65
  - devices, 197, 199
  - file copying and recovery, 730
  - international, 75, 131–33
  - Internets Explorer security, 623–26
  - migrating user profile data, 34, 37–39
  - Offline Settings, 430
  - performance
    - CIM Classes, 696
    - CIM Repository, 695–96
    - Performance Options, 709–11
    - WMI Administrative Tools, 697–705
    - WMI consumers, 696
    - WMI providers, 694–95
    - WMI scripting library, 696–97
    - WMI, CIMOM, 695
    - WMI, overview, 689–94
  - power configurations, 582–89
  - system restore, 746–50
  - time and date, 13
  - User Account Control (UAC), 480–82
  - user, compatibility modes, 260
  - Windows Firewall, 388
  - Windows PE images, 135
- settings, network. *See also* settings
  - ad hoc networks, 360
  - case scenario
    - IPv4 connectivity, 377
    - IPv6 connectivity, 377
    - wireless networks, 377–78
  - connectivity
    - managing connections, 362–63
    - overview, 348–50
    - setting up connections, 350–52
  - internal wireless adapter security, 357–60
  - IPv4
    - addressing, 301–07
    - connecting to network, 307–11
    - overview, 300–01
    - practice, configuring, 321–24
    - troubleshooting connectivity, 311–21
  - IPv6
    - advantages of IPv6, 333–34
    - configuring addresses, 328–32
    - connectivity, 338–43
    - IPv4 compatibility, 334–37
    - practice, configuring IPv6 connectivity, 343–45
  - practice, creating ad hoc network, 371–73
  - printing enhancements, 368–70
  - wireless computers, adding, 352–56
  - wireless networks
    - managing, 356–57
    - security, 367–68
    - technologies, 361
    - troubleshooting, 363–67
- Setup Analysis Tool, 263
- setup log files, 228–29
- shadow copies, 762–69
- share permissions, 432
- sharing media, 586
- sharing resources. *See also* virtual private networks (VPN)
  - auditing, configuring, 449–51
  - BranchCache, configuring clients, 463–67
  - BranchCache, Distributed Cache mode, 463
  - BranchCache, Hosted Cache mode, 462
  - BranchCache, overview, 461–62
  - BranchCache, Windows Server 2008, 468–70
  - case scenarios, 474
  - DirectAccess, 526
  - EFS and HomeGroups, 454
  - EFS recovery, 453
  - Encrypting File System (EFS), 451–54
  - file and folder permissions, 442–49
  - folders, 428–32, 580–81, 689–90
  - libraries, 432–33
  - Network And Sharing Center, 423–25
  - practice
    - BranchCache configuration, 470–71
    - encryption and permissions, 454–58
    - sharing resources, 435–40
    - printers, 434–35
  - shim, defined, 262
  - shutdown, 403, 583, 612, 718
  - SHVs (Security Health Validators), 536
  - side-by-side migrations, 29
  - signing, drivers, 215–19
  - Sigverif (File Signature Verification), 218–19
  - single instance storage, 72
  - site IDs, 339
  - site-local addresses, 331–32
  - SkipReam, 82
  - SKU (Stock-Keeping Unit), 94
  - sleep mode, 402–03, 583, 586–87, 718
  - Small Computer System Interface (SCSI), 232
  - small office/home office (SOHO), 387
  - Smart Card or Other Certificate, 533
  - smart cards, 497–99, 532, 539
    - SmartScreen Filter, 626–27
  - SMS (System Management Server), 73
  - snapshots, 766
  - software. *See* applications, managing
  - Software Restriction Policies, 256, 271–76, 286–87, 294–95
  - SOHO (small office/home office) network, 306–07, 350–52, 359–60, 387
  - spanned partitions, 235, 237
  - spanned volumes, 239, 241–42
  - specialize, configuration pass, 80
  - split WIM, 95
  - SQL Server, 147
  - SSID, 353–54, 365–68
  - SSL (Secure Sockets Layer), 531, 626, 633–36

- SSTP (Secure Socket Tunneling Protocol), 515, 530–31, 535
- Stability Chart, 661
- Stability Index, 660–61
- staging device drivers, 205
- standard providers, 695
- Standard User Analyzer, 263–64
- Start Windows Normally, 751
- startup keys, 557, 562
- Startup Repair, 751
- stateful address configuration, 331
- stateless address configuration, 331–32
- static IP addresses, 368
- statistics, network, 319–21
- stealth, 384
- Stock-Keeping Unit (SKU), 3, 94
- STOP errors, 652
- storage. *See also* disks; removable devices; USB (universal serial bus) devices
  - backup, 733, 736
  - defragmenting disks, 230–32
  - file-based, 71
  - ImageX, 68–69
  - migration store types, 42
  - requirements, 5–6
  - write caching, configuring, 711–12
- Store Passwords Using Reversible Encryption, 499
- streaming multimedia, 716
- stress tests, device drivers, 215
- striped partitions, 235, 237
- striped volumes, 239, 242–45
- subnet address, 303
- subnet masks, 300
- subnets, 302–04
- subscriptions, event, 676–77
- supernetting, 303–04
- Switch To The Secure Desktop When Prompting For Elevation, 486
- Switch User, 403
- Sync Center, 575, 578–80
- synchronization, offline files, 574–82
- Sysprep, 64, 77–84, 172
- sysprep/generalize command, 79
- System and Security, 661–64, 731–39
- System Center Virtual Machine Manager (SCVMM), 97–98, 128, 147, 163
- System Check, 563
- system cleanup, 78
- System Configuration (MSConfig), 705–07
- system diagnostics report, 656–58
- System Diagnostics, DCS, 652
- system files, backup and restore, 735, 747
- System Image Recovery, 752
- System Image, backup and restore, 733–34, 739–41, 749–50
- system images, configuring. *See also* system images, deploying
  - case scenario, generating system images, 111
  - Deployment Image Servicing and Management Tool (DISM), 75–77
  - distributing images, 72–75
  - international settings, 131–33
  - Offline Virtual Machine Servicing Tool, 96–98
  - operating system packages, servicing, 127–30
  - overview, 53
  - practice, creating bootable VHD, 105–08
  - practice, creating WIM image, 84–86
  - pre-staging client computers, 103–04
  - reference image, creating, 58–72
  - Sysprep, 77–84
  - VHDs, native, 89–94
  - WDS images, 74–75
  - WDS, online VHD deployment, 98–104
  - Windows Automated Installation Kit (Windows AIK), 56–58
  - Windows Image to Virtual Hard Disk Tool (WIM2VHD), 94–96
  - Windows Preinstallation Environment (WinPE), 58
- system images, deploying. *See also* system images, configuring
  - applications, servicing, 125–27
  - case scenarios, 191–92
  - DISM WIM commands, 116–23
  - drivers, servicing, 123–25
  - manual installations, 180–81
  - MDT (Microsoft Deployment Toolkit)
    - applications, adding, 164–66
    - deployment points, 166–68
    - device drivers, adding, 154–55
    - distribution shares, creating, 152–53
    - language packs, 164
    - LTI bootable media, 168–69
    - managing and distributing images, overview, 151–52
    - offline files, updating, 163–64
    - operating system image, adding, 153–54
    - overview, 146–51
    - program folders, 148
    - task sequences, 155–61
    - updates, adding, 161–63
    - Windows PE options, 168
  - package installation, 131
  - practice, downloading, installing and configuring MDT 2010, 181–87
  - practice, mounting offline image and installing language packs, 140–43
  - SCCM 2007, 175–80
  - unattended servicing, command-line, 137–40
  - WDS, 169–75
  - Windows editions, managing, 133–35
  - Windows PE images, servicing, 135–36
- System Information (Msinfo32), 212–14
- system locale, 132–33
- System Management Server (SMS), 73
- system partitions, network share deployment, 69
- System Performance, DCS, 652
- System Properties, 403–04, 406
- System Protection, 769–71
- system recovery
  - boot options, 754–55
  - practice, system protection and restore, 756–60
  - rolling back drivers, 755–56
  - system restore, 746–50
- System Recovery, 750–53
- System Recovery Options, 751–52
- System Restore Wizard, 746–47
- system settings. *See* settings; settings, network

## T

- target path, 135–36
- Task Manager, 215, 664–67, 714–15
- Task Sequence Editor, 156, 177–79

- tasks
  - attaching to events, 675
  - managing, 689–90
  - Task Scheduler, 739
  - task sequence, 148–49, 155–61
- TCP (Transmission Control Protocol), 320
- TCP/IP, 675
- technician computers, 59
- template files
  - Deployment Workbench, 148
  - Security Template, 487–88
- temporary files, 228–29, 735
- Teredo, 335–36, 516, 519–21
- Teredo Default Qualified policy, 518
- Teredo Server Name policy, 518
- Terminal Services, 537
- Terminal Services Gateway, 403, 498, 537
- themes, visual, 259
- thick images, 150–51, 153
- thin images, 150–53
- thumbnails, 228–29
- time and date settings, 13
- time zones, 133
- timers, wake, 586
- TLS (Transport Layer Security), 626
- Toolbars and Extensions, 630
- TPM (Trusted Platform Module), 556–57, 564
- Trace Capture, Processing, and Command-Line Analysis tool (Xperf.exe), 717–18
- Tracert tool, 315, 338, 342
- traces, kernel trace data, 652
- transaction processing, 146
- translate accelerator, 631
- Transmission Control Protocol (TCP), 320, 384
- Transmission Control Protocol/Internet Protocol (TCP/IP), 497, 675
- transparent caching, 577
- Transport Layer Security (TLS), 626
- troubleshooting
  - Action Center, 609
  - Application Compatibility
    - Diagnostics policies, 264–65
  - boot configuration data, 754–55
  - case scenario, performance, 725
  - device driver conflicts, 212–15
  - Device Manager, 197
  - DirectAccess, 519–21
  - DirectX, 217–18
  - IP configuration, 312–15

- IPv4 network connectivity, 311–21
- IPv6 connectivity, 342–43
- Program Compatibility, 257–58
- System Configuration (MSCConfig), 705–07
- System Performance, DCS, 652
- wireless networks, 363–67
- Trusted Platform Module (TPM), 556–57, 564
- Trusted Publishers certificate store, 215–19
- Trusted Root CA Certification Authorities, 216
- Trusted Sites, 276, 624
- trusts, 409, 485–86
- tunnel rules, 394
- Tzutil, 133

## U

- UAC (User Account Control)
  - Action Center, 609
  - application compatibility, 265
  - case scenario, UAC and passwords, 511
  - overview, 479–80
  - policies, 482–87
  - practice, configuring, 488–90
  - Remote Assistance, 405
  - Secpol and Local Security Policy, 487–88
  - settings, 480–82
- UDP (User Datagram Protocol), 320, 335, 384
- UIAccess Applications, 486–87
- Unattend.xml, 94
- unattended answer files, 134
- unattended installations, 59, 80–81, 83
- Unattended.xml answer files, 127, 137–40
- unblocking, 317
- uncompressed migration stores, 42
- universal serial bus (USB) devices
  - as installation source, 7–8
  - backup storage, 733, 736
  - BitLocker, 563–64
  - booting target drives, 173
  - data migration, 36
  - defragmenting, 230–32
  - deployment points, 166
  - dialup connections, 540
  - discover images, 171–72
  - Encrypting File System (EFS), 451–52
  - network connections, 350–52
  - password reset disks, 500
  - policies, 208, 233–35
  - power settings, 586
  - practice, write access, 247–48
  - security and, 555
  - write caching, configuring, 711–12
- unspecified address, 332
- Update Driver, 208–09
- updates
  - Action Center, 609–10
  - adding, MDT (Microsoft Deployment Toolkit), 161–63
  - applications, servicing, 125–27
  - case scenarios, 644
  - device drivers, 197, 208
  - DirectAccess, 515
  - images, WDS, 102–03
  - Microsoft Baseline Security Analyzer (MBSA), 616
  - offline files, 163–64
  - Offline Virtual Machine Servicing Tool, 96
  - practice, configuring Windows Update, 617–19
  - reliability, stability and performance, 658–61
  - SCCM 2007, 175–76
  - WIM images, 120
  - Windows Server Update Services (WSUS), 610–12
  - adding updates, 163
  - application servicing, 125
  - NAP remediation, 537
  - offline files, 163
  - Offline Virtual Machine Servicing Tool, 96
  - overview, 610–12
- Windows Update
  - Action Center, 661–64
  - case scenario, 644
  - configuring, 601–08
  - device drivers, installing, 204–06
  - policies, 612–16
  - practice, configuring, 617–19
  - smart cards, 498
- upgrades
  - from Windows 7 Editions, 25–26
  - from Windows Vista, 26–28
  - practice, upgrading to Windows 7, 30–31
  - Windows image, 75

USB (universal serial bus) devices  
 as installation source, 7–8  
 backup storage, 733, 736  
 BitLocker, 563–64  
 booting target drives, 173  
 data migration, 36  
 defragmenting, 230–32  
 deployment points, 166  
 dialup connections, 540  
 discover images, 171–72  
 disk policies, 233–35  
 Encrypting File System (EFS),  
 451–52  
 password reset disks, 500  
 policies, 208  
 power settings, 586  
 practice, write access, 247–48  
 security and, 555  
 write caching, configuring, 711–12  
 USB controllers, 203, 350–52  
 USB hubs, power allocation, 202  
 User Account Control (UAC)  
 Action Center, 609  
 application compatibility, 265  
 case scenario, UAC and  
 passwords, 511  
 overview, 479–80  
 policies, 482–87  
 practice, configuring, 488–90  
 Remote Assistance, 405  
 Secpol and Local Security Policy,  
 487–88  
 settings, 480–82  
 user accounts  
 data recovery agent (DRA)  
 accounts, 559  
 HomeGroup Connections, 425  
 shared folders, 428–32  
 User Datagram Protocol (UDP), 320,  
 335, 384  
 User Defined Reports, 656  
 User Interface Accessibility  
 (UIAccess), 486–87  
 user messages, 208  
 user names, 425, 493–95, 497–99  
 user profiles  
 backup, 735  
 case scenario, migrating user data,  
 49–50  
 migrating user profile data, 34,  
 37–39  
 migration, Windows AIK, 56–58  
 practice, migrating user data,  
 43–46  
 restoring, 767–69  
 Windows Easy Transfer, 35–39

user rights, 496–97, 530  
 user settings, compatibility  
 modes, 260  
 User State Migration Tool (USMT),  
 39–42, 56–58  
 user state steps, 178  
 users  
 Remote Desktop Users group, 404  
 Runas, 495–96

## V

validation, 64–65, 205, 485–86, 536  
 verification, 205  
 VHD. *See* virtual hard disks (VHDs)  
 video playback settings, 586  
 video, recovery options, 751  
 video, sharing, 425  
 View Certificates, 633  
 View Update History, 604  
 virtual hard disks (VHDs)  
 attaching and detaching, 91  
 backup storage, 733, 736  
 BitLocker recovery, 566–67  
 boot entry, adding, 93–94  
 booting from, 93  
 case scenario, working with  
 VHDs, 111  
 defragmenting, 230–32  
 dual-boot installations, 17–19  
 image creation, Windows PE, 67  
 LTI bootable media, 168–69  
 native, using, 89–94  
 network share, image storage,  
 68–69  
 offline files, updating, 163–64  
 Offline Virtual Machine Servicing  
 Tool, 96–98  
 operating system packages,  
 servicing, 127–30  
 overview, 513  
 practice, creating bootable VHD,  
 105–08  
 pre-staging client computers,  
 103–04  
 System Image backups, 739–41  
 task sequence, deploy to VHD,  
 159–61  
 updates related to, 53  
 WDS, online VHD deployment,  
 98–104  
 WIM2VHD, 94–96  
 virtual machines, image  
 deployment, 89

Virtual PC, 89–90  
 virtual private networks (VPN)  
 auditing, 544  
 authentication protocols, 533  
 case scenarios, 550–51  
 DirectAccess  
 client configuration, 517–21  
 overview, 515–17  
 practice, configuring with Netsh,  
 526–27  
 server, configuring, 521–26  
 troubleshooting, 519–21  
 incoming connections, accepting,  
 541–43  
 NAP remediation, 536–37  
 overview, 530–32  
 practice, configuring remote  
 connections, 545–47  
 Remote Desktop connections, 403  
 VPN Reconnect, 535–36  
 wireless networks, 356  
 Virtual Server, 89–90, 97  
 Virtualize File and Registry  
 Write Failures To Per  
 User-Locations, 486  
 Visual Effects, 709  
 visual themes, 259  
 Visual Trace Analysis (Xperfview.exe),  
 717–18  
 VMware ESX Server, 97  
 volume licenses, 82  
 Volume Shadow Copy Service  
 (VSS), 766  
 volume status, 239  
 volumes, disk  
 case scenario, managing, 252  
 deleting, 246  
 managing, 240–46  
 resizing, 245–46  
 VPN (virtual private networks).  
*See* virtual private networks  
 (VPN)  
 VPN Reconnect, 532, 535–36  
 VSS (Volume Shadow Copy  
 Service), 766

## W

Wake on LAN, 402–03  
 wake timers, 586  
 wakeup, 585  
 WAN (wide area networks),  
 349, 577  
 WAP, 304–07, 312, 363–64



- Wbadmin, 739
- WCS (Windows Color System), 369
- WDS (Windows Deployment Services)
  - as installation source, 9
  - image deployment, 153, 169–75
  - MMC snap-in
    - boot image, adding, 101
    - capture image, creating, 100
    - discover image, creating, 101
    - exporting image, 102
    - images, 74–75
    - install image, adding, 101–02
    - overview, 99
    - updating an image, 102–03
    - online VHD deployment, 98–104
- WDSUTIL, 99, 102–04, 174–75
- Web Proxy Auto Detect (WPAD), 608
- web sites, certificate errors, 635
- WEP (Wireless Equivalent Privacy), 357–60, 367
- WFAS (Windows Firewall with Advanced Security), 317–19
- wide area network (WAN), 349, 577
- Wi-Fi Protected Access (WPA), 357–60
- wildcards, 274
- WIM (Windows Imaging)
  - command options, 75
  - image mounting, 116–23
  - imaging format, 71–72
  - mounted images, information about, 119–21
  - practice, creating WIM image, 84–86
- WIM2VHD (Windows Image to Virtual Hard Disk Tool), 94–96
- Wimscript.ini, 68, 71
- Windows 2000, compatibility modes, 258
- Windows 7
  - activation, resetting, 82
  - automated installations, Windows AIK, 56–58
  - editions, overview, 3
  - Enterprise, 5, 93, 96, 276–77, 403–04, 451–52, 461, 517, 564, 574, 734
  - hardware requirements, 5–6
  - Home Basic, 4
  - Home Premium, 4
  - installation source, preparing, 6–9
  - installing, 9–19
  - migrating from Windows XP, 29–30
  - practice, performing clean installation, 19–22
  - practice, upgrading to Windows 7, 30–31
  - Professional, 403–04, 451–52, 574 Starter, 4
  - Ultimate, 5, 93, 96, 276–77, 403–04, 451–52, 461, 517, 564, 574, 734
  - upgrading from Windows 7 Editions, 25–26
  - upgrading from Windows Vista, 26–28
- Windows 7 Professional, 4
- Windows 7 Upgrade Advisor, 27
- Windows 95, compatibility modes, 258
- Windows 98, compatibility modes, 258
- Windows AIK (Windows Automated Installation Kit)
  - BCDboot, 173
  - installing and using, 56–58
  - MDT (Microsoft Deployment Toolkit), 147
  - mounting images, 116
  - practice, installing, 84–86
  - USMT (User State Migration Tool), 39–42
  - VHDs, native, 90
- Windows boot manager (Bootmgr.exe), 754–55
- Windows Color System (WCS), 369
- Windows DDNS, 331–32
- Windows Deployment Services (WDS)
  - as installation source, 9
  - MMC snap-in
    - boot image, adding, 101
    - capture image, creating, 100
    - discover image, creating, 101
    - exporting image, 102
    - images, 74–75
    - install image, adding, 101–02
    - overview, 99
    - updating an image, 102–03
    - online VHD deployment, 98–104
- Windows Deployment Services Image Capture Wizard, 74, 173
- Windows Deployment tools, 90
- Windows Deployment Wizard, 168
- Windows Event Collector, 676
- Windows Experience Index, 663–64
- Windows Firewall
  - allowing programs, 387–88
  - case scenario, 419
  - event forwarding, 676
  - Network Location Awareness, 385–87
  - network settings, configuring, 317–19
  - overview, 383–88
  - Ping commands, 341
  - practice, configuring, 395–98
- Windows Firewall with Advanced Security (WFAS)
  - case scenario, 419
  - DirectAccess, 526
  - network settings, configuring, 317–19
  - overview, 389–95
  - practice, configuring, 395–98
- Windows folders, 279, 486
- Windows Image to Virtual Hard Disk Tool (WIM2VHD), 94–96
- Windows Imaging (WIM)
  - command options, 75
  - image mounting, 116–23
  - imaging format, 71–72
  - mounted images, information about, 119–21
  - practice, creating WIM image, 84–86
- Windows Installer (.msi), 123, 125–27, 276, 278
- Windows Internet Naming Service (WINS), 310, 392
- Windows Memory Diagnostic, 752
- Windows Network Diagnostic tool, 315–16, 675
- Windows NT, 258
- Windows operating system loader (Winload.exe), 754–55
- Windows PE
  - boot images, 116
  - bootable medium, creating, 66–68
  - capture image, WDS, 74
  - configuration passes, 79
  - configuring options, 168
  - feature settings, 62
  - images, creating, 56–58
  - images, servicing, 135–36
  - MDT (Microsoft Deployment Toolkit), 148
  - network share, image storage, 68–69

- practice, creating boot DVD, 84–86
- profiling tool, 135
- system images, capturing, 58
- Windows AIK tools, 58
- Windows Performance Analysis Toolkit (WPT), 717–18
- Windows PowerShell, 163–64, 408–10, 414–15
- Windows Preinstallation Environment (WinPE).  
See Windows PE
- Windows RE (Recovery Environment), 749–50, 752
- Windows Recovery Environment (Windows RE), 749–50, 752
- Windows Remote Assistance, 405–08, 486–87
- Windows Remote Management (WinRM), 408–10, 676–77
- Windows Remote Shell (WinRS), 395, 409–10, 414–15
- Windows Resource Protection (WRP), 263
- Windows resume loader (Winresume.exe), 754–55
- Windows Server 2003, 96, 175, 259, 271–76, 461
- Windows Server 2008
  - backward compatibility, 117
  - BranchCache, 461, 468–70
  - change and configuration management, 175
  - DirectAccess, 522
  - discover image, creating, 171
  - MDT (Microsoft Deployment Toolkit), 73, 147
  - Offline Virtual Machine Servicing Tool, 96
  - Remote Assistance, 406–07
  - Remote Desktop, 403
  - SCVMM Administrative Console, 97
  - servicing, 75
  - smart cards, 498
  - Software Restriction Policies, 271–76
  - Teredo address, 335–36
- Windows Server and Certificate Services, 215–19
- Windows Server Backup, 89
- Windows Server Update Services (WSUS)
  - adding updates, 163
  - application servicing, 125
  - NAP remediation, 537
  - offline files, 163
- Offline Virtual Machine Servicing Tool, 96
- overview, 610–12
- Windows Setup, 79–80
- Windows SIM (Windows System Image Manager), 57, 60, 81, 138–39
- Windows System 32 folders, 486–87
- Windows Task Scheduler, 739
- Windows Update
  - Action Center, 661–64
  - case scenario, 644
  - configuring, 601–08
  - device drivers, installing, 204–06
  - policies, 612–16
  - practice, configuring, 617–19
  - smart cards, 498
- Windows Update Stand-alone Installer (.msu), 127–28
- Windows User State Migration Toolkit (USMT), 147
- Windows Vault, 493–95
- Windows Virtual PC, 387–88, 735
- Windows Vista
  - backward compatibility, 117
  - BitLocker, 564
  - compatibility modes, 259
  - connection security and IPsec, 394
  - deploying to VHD, 159–61
  - DirectAccess, 517
  - migrating user profile data, 34, 39
  - practice, upgrading to Windows 7, 30–31
  - Remote Assistance, 406
  - Remote Desktop, 403–04
  - servicing, 75
  - Software Restriction Policies, 271–76
  - Teredo address, 335–36
  - upgrading from, 26–28
  - Windows Easy Transfer, 35–39
  - Windows Firewall, 386–88
- Windows Welcome, 64, 83
- Windows XP
  - compatibility modes, 258
  - connection security and IPsec, 394
  - DirectAccess, 517
  - migrating from, 29–30
  - migrating user profile data, 34, 39
  - Remote Assistance, 405–08
  - Remote Desktop, 403–04
  - ScanState, 41
  - Software Restriction Policies, 271–76
  - Windows Easy Transfer, 35–39
  - Windows XP Mode, 265–66
- WindowsImageBackup folder, 740
- Winload.exe, 754–55
- WinPE (Windows Preinstallation Environment)
  - boot images, 116
  - bootable medium, creating, 66–68
  - capture image, WDS, 74
  - configuration passes, 79
  - configuring options, 168
  - feature settings, 62
  - images, creating, 56–58
  - MDT, 148
  - network share, image storage, 68–69
  - practice, creating boot DVD, 84–86
  - profiling tool, 135
  - system images, capturing, 58
  - Windows AIK tools, 58
- Winresume.exe, 754–55
- WinRM (Windows Remote Management), 408–09, 676–77
- WinRS (Windows Remote Shell), 395, 408–10, 414–15
- wipe-and-load migrations, 30
- Wired Equivalent Privacy (WEP), 357–60, 367
- wired small network, 349
- wireless adapter settings, 585
- wireless connections
  - case scenario, wireless networks, 377–78
  - IPv4 network connections, 309
  - networks, 349, 352–56, 361, 675
  - security, 357–60, 367–68
  - troubleshooting, 363–67
  - Wireless Network Setup Wizard, 355
- wireless devices, 349
- Wireless Network Properties, 355, 364, 367
- Wizards
  - Add Application Wizard, 127
  - Add Features, DirectAccess, 522
  - Add Features, Windows Server 2008, 468
  - Add Hardware Wizard, 206



- Add Printer Wizard, 369
- Automatically Generate Rules, 283
- certificate management, 502
- Create A Basic Task Wizard, 675
- Create A Shared Folder Wizard, 431
- Create New Data Collector Wizard, 655
- Forgotten Password Wizard, 500
- Initialize Disk Wizard, 236
- MOF Generator Wizard, 699
- Network Printer Installation Wizard, 369
- New Application Wizard, 165–66
- New Connection Security Rule Wizard, 393–94
- New Deployment Point Wizard, 166–68
- New Driver Wizard, 154–55
- New Inbound (or Outbound) Rule Wizard, 389–91
- New OS Wizard, 153
- New Task Sequence Wizard, 177
- Restore Files Wizard, 763, 767–69
- Rule Creation Wizard, 281–82
- System Restore Wizard, 746–47
- Windows Deployment Services
  - Image Capture Wizard, 74, 173
- Windows Deployment Wizard, 168

- Wireless Network Setup Wizard, 355
- WMI
  - CIM Classes, 696
  - CIM Repository, 695–96
  - CIM Studio, 697–99
  - Event Registration, 702–03
  - Event Viewer, 703–05
  - Object Browser, 700–02
  - overview, 689–94
  - providers, 694
  - repository, 694
  - Service, 694
  - WMI Administrative Tools, 697–705
  - WMI consumers, 696
  - WMI providers, 694–95
  - WMI scripting library, 696–97
  - WMI Service, 695
- WPA encryption, 367
- WPA2 certifications, 358–60
- WPA2-Enterprise, 359
- WPAD (Web Proxy Auto Detect), 608
- WPA-Enterprise, 359
- WPT (Windows Performance Analysis Toolkit), 717–18
- WQL Query Builder, 699
- write
  - performance, 244
  - permissions, 442–43
  - practice, access to USB devices, 247–48
- Removable Disk policies, 234–35

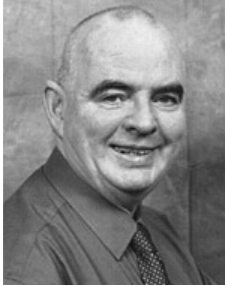
- removable drives, 565
- removable media, 233–35, 565
- User Account Controls (UAC), 486
- write caching, configuring, 711–12
- WRP (Windows Resource Protection), 263
- WSUS (Windows Server Update Services), 610–12
  - adding updates, 163
  - application servicing, 125
  - NAP remediation, 537
  - offline files, updating, 163
  - Offline Virtual Machine Servicing Tool, 96

## X

- Xbootmgr.exe, 717–18
- XML Paper Specification (XPS), 368
- XORing (exclusive ORing), 335
- Xperf.exe, 717–18
- Xperfview.exe, 718

## Z

- Zero Touch Installation (ZTI), 73, 147
- zone ID, 341
- zone rules, 272



**IAN MCLEAN**, MCSE, MCITP, MCT, has over 40 years of experience in industry, commerce, and education. He started his career as an electronics engineer before going into distance learning and then education as a university professor. Currently, he runs his own consultancy company. Ian has written more than 20 books and many papers and technical articles. He has been working with Microsoft operating systems since 1997.



**ORIN THOMAS**, is an author and an MCT. He has written more than a dozen certification textbooks for Microsoft Press. He holds many certifications, including several MCSE and MCITP credentials. He is the convener of the Melbourne Security and Infrastructure Interchange and a Microsoft Security MVP. He lives in Melbourne, Australia, with his wife and son and enjoys traveling around the world speaking at technical conferences like Tech.ED.



# System Requirements

We recommend that you use a test workstation to complete the exercises in each lab. The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. For more information, see the Introduction.

## Hardware Requirements

---

You can complete almost all practice exercises in this book using virtual machines rather than real workstation hardware. The following hardware is required to complete the lab exercises:

- Personal computer with minimum 1GHz (x86) or 1.4GHz (x64) processor (2GHz or faster recommended).
- 1 GB of RAM or more (2 GB recommended; 4 GB enables you to host all the virtual machines specified for all the practice exercises in the book.)
- 40 GB hard disk space of which 15 GB is available (40 GB free hard disk space recommended; 60 GB enables you to host all the virtual machines specified for all the practice exercises in the book.)
- DVD-ROM drive
- A graphics adapter that supports DirectX 9 graphics, has a Windows Display Driver Model (WDDM) driver, supports Pixel Shader 2.0 hardware and 32 bits per pixel, and has 128 MB graphics memory. (256 MB graphics memory recommended.)
- Keyboard and Microsoft mouse or compatible pointing device
- 1 GB or larger USB storage device.

## Software Requirements

---

- Windows 7 Enterprise or Ultimate.
- To perform the practice exercises in Chapter 6, “Network Settings,” you need an additional Windows 7 Workstation. (This can be a virtual machine.)
- To perform the optional exercises in Chapter 14, “Recovery and Backup,” you need an additional hard disk formatted with the NTFS filing system. This hard disk can be internal or external and should have at least 20 GB free hard disk space.
- Windows Media Player. To view the Webcasts on the book’s DVD you will need Windows Media Player. A free download is available at <http://www.microsoft.com/windows/windowsmedia/player/download/download.aspx>.

To minimize the time and expense of configuring physical computers, we recommend that you use virtual machines. To run computers as virtual machines within Windows, you can use Microsoft Virtual PC 2007. You can download Virtual PC 2007 for free from <http://www.microsoft.com/windows/downloads/virtualpc/default.mspx>.