

DON POULTON

Cert Guide

Learn, prepare, and practice for exam success



- ▶ Master every topic on Microsoft's new MCTS 70-640 exam.
- ▶ Assess your knowledge and focus your learning.
- ▶ Get the practical workplace knowledge you need!

MCTS

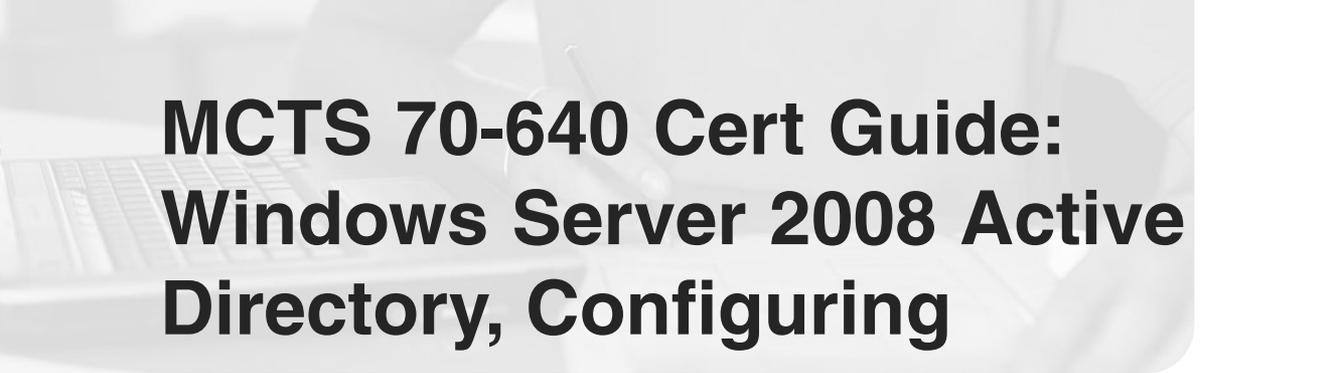
70-640

Windows Server 2008
Active Directory, Configuring



CD INCLUDES
COMPLETE
SAMPLE EXAM

PEARSON



MCTS 70-640 Cert Guide: Windows Server 2008 Active Directory, Configuring

Don Poulton

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

MCTS 70-640 Cert Guide: Windows Server 2008 Active Directory, Configuring

Copyright © 2011 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-4708-2

ISBN-10: 0-7897-4708-1

Library of Congress Cataloging-in-Publication Data:

Poulton, Don.

MCTS 70-640 cert guide : Windows server 2008 Active directory,
configuring / Don Poulton.

p. cm.

ISBN 978-0-7897-4708-2 (hardcover w/CD)

1. Microsoft Windows server--Examinations--Study guides. 2. Operating systems (Computers)--Examinations--Study guides. 3. Directory services (Computer network technology)--Examinations--Study guides. 4. Local area networks (Computer networks)--Management--Examinations--Study guides. 5. Telecommunications engineers--Certification. 6. Electronic data processing personnel--Certification. I. Title. II. Title: Windows server 2008 Active directory, configuring.

QA76.76.O63P6685 2011

005.4'476--dc22

2010043593

Printed in the United States of America

First Printing: December 2010

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419 corpsales@pearsonontechgroup.com

For sales outside of the U.S., please contact

International Sales international@pearson.com

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Associate Publisher

Dave Dusthimer

Acquisitions Editor

Betsy Brown

Development Editor

Box Twelve
Communications, Inc.

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Copy Editor

Mike Henry

Indexer

Erika Millen

Proofreader

Megan Wade

Technical Editor

Chris Crayton

Publishing Coordinator

Vanessa Evans

Multimedia Developer

Dan Scherf

Designer

Gary Adair

Page Layout

Mark Shirar

Contents at a Glance

Introduction	3
Chapter 1	Getting Started with Active Directory 17
Chapter 2	Installing and Configuring DNS for Active Directory 43
Chapter 3	Installing Active Directory Domain Services 73
Chapter 4	Configuring DNS Server Settings and Replication 107
Chapter 5	Global Catalogs and Operations Masters 143
Chapter 6	Configuring Active Directory Sites and Replication 173
Chapter 7	Additional Active Directory Roles 205
Chapter 8	Read-Only Domain Controllers 251
Chapter 9	Active Directory User and Group Accounts 281
Chapter 10	Trust Relationships in Active Directory 321
Chapter 11	Creating and Applying Group Policy Objects 345
Chapter 12	Group Policy Software Deployment 393
Chapter 13	Account Policies and Audit Policies 417
Chapter 14	Monitoring Active Directory 453
Chapter 15	Maintaining Active Directory 515
Chapter 16	Installing and Configuring Certificate Services 559
Chapter 17	Managing Certificate Templates, Enrollments, and Certificate Revocation 587
Practice Exam	629
Answers to Practice Exam	691
Appendix A	Answers to the “Do I Know This Already?” Quizzes 729
Appendix B	Installing Windows Server 2008 R2 763
	Glossary 773
	Index 796
Elements Available on CD	
Appendix C	Memory Tables 3
Appendix D	Memory Tables Answer Key 3

Table of Contents

Introduction 3

Goals and Methods	3
How This Book Is Organized	4
Study and Exam Preparation Tips	7
Learning Styles	7
Study Tips	8
<i>Study Strategies</i>	9
<i>Pretesting Yourself</i>	10
Exam Prep Tips	10
Microsoft 70-640 Exam Topics	12

Chapter 1 Getting Started with Active Directory 17

The Foundation of Active Directory	17
X.500	17
LDAP	18
Naming Standards of X.500 and LDAP	19
<i>Distinguished Names</i>	19
<i>Relative Distinguished Names</i>	20
<i>User Principal Names</i>	21
<i>Globally Unique Identifiers</i>	21
<i>Security Identifiers</i>	21
<i>Active Directory Canonical Names</i>	22
The Building Blocks of Active Directory	22
Namespaces	22
Objects	23
Containers	24
Schemas	24
Global Catalogs	24
Partitions	25
Logical Components of Active Directory	26
Domains	26
Trees	27
Forests	27
Organizational Units	29
Sites	30
Domain Controllers	31

Global Catalog Servers	31
Operations Masters	32
New Features of Active Directory in Windows Server 2008	33
Server Manager	35
<i>Adding Roles and Features</i>	36
<i>Command-Line Server Management</i>	36
Windows Server 2008 R2	37
Summary	40
Chapter 2	Installing and Configuring DNS for Active Directory
	43
“Do I Know This Already?” Quiz	43
The Hierarchical Nature of DNS	48
Installing DNS on Windows Server 2008 R2	49
Configuring DNS Zones	51
DNS Zone Types	52
<i>Primary Zones</i>	53
<i>Secondary Zones</i>	53
<i>Stub Zones</i>	53
<i>Active Directory–Integrated Zones</i>	53
<i>GlobalNames Zones</i>	54
DNS Name Server Roles	55
<i>Primary Name Server</i>	55
<i>Secondary Name Server</i>	55
<i>Caching–Only Server</i>	56
<i>Forwarders</i>	56
Creating DNS Zones	57
<i>Forward Lookup Zones</i>	57
<i>Reverse Lookup Zones</i>	59
DNS Resource Records	61
Configuring DNS Zone Properties	62
<i>Configuring Zone Types</i>	63
<i>Adding Authoritative DNS Servers to a Zone</i>	63
<i>Dynamic, Nondynamic, and Secure Dynamic DNS</i>	64
<i>Zone Scavenging</i>	65
<i>Time to Live</i>	66
<i>Integrating DNS with WINS</i>	68
Command-Line DNS Server Administration	69
Review All the Key Topics	71

Complete the Tables and Lists from Memory 71
Definitions of Key Terms 71

Chapter 3 Installing Active Directory Domain Services 73

“Do I Know This Already?” Quiz 73
Planning the Active Directory Namespace 77
 Subdividing the Active Directory Namespace 77
 Administrative or Geographical Organization of Domains 78
 Use of Multiple Trees 79
 Best Practices 80
Creating Forests and Domains 81
 Requirements for Installing Active Directory Domain Services 81
 Installing Active Directory Domain Services 82
 New Forests 83
 New Domains in Existing Forests 88
 Existing Domains 89
 Performing Unattended Installations of Active Directory 90
 Server Core Domain Controllers 92
 Removing Active Directory 92
Interoperability with Previous Versions of Active Directory 93
 Forest and Domain Functional Levels 94
 Upgrading Domain and Forest Functional Levels 95
 The Adprep Utility 96
 Running the Adprep /forestprep Command 96
 Running the Adprep /domainprep Command 97
 Upgrading a Windows Server 2003 Domain Controller 97
Additional Forest and Domain Configuration Tasks 98
 Verifying the Proper Installation of Active Directory 98
 Active Directory Migration Tool v.3.1 100
 Alternative User Principal Name Suffixes 101
Review All the Key Topics 103
Complete the Tables and Lists from Memory 103
Definitions of Key Terms 104

Chapter 4 Configuring DNS Server Settings and Replication 107

“Do I Know This Already?” Quiz 107
Configuring DNS Server Settings 112
 Forwarding 112
 Conditional Forwarders 114

Root Hints	116
Configuring Zone Delegation	117
Debug Logging	119
Event Logging	121
DNS Security Extensions	121
Advanced Server Options	123
<i>Server Options</i>	123
<i>Round Robin</i>	124
<i>Disable Recursion</i>	125
<i>Name Checking</i>	125
<i>Loading Zone Data</i>	126
<i>Server Scavenging</i>	126
Monitoring DNS	127
Configuring Zone Transfers and Replication	128
Replication Scope	128
Types of Zone Transfers	130
<i>Full Zone Transfer</i>	130
<i>Incremental Zone Transfer</i>	131
<i>Configuring Zone Transfers</i>	132
<i>Configuring DNS Notify</i>	133
Secure Zone Transfers	134
Configuring Name Servers	136
Application Directory Partitions	138
<i>Installing and Configuring Application Directory Partitions</i>	138
<i>Creating Application Directory Partition Replicas</i>	139
<i>Application Directory Partition Reference Domains</i>	139
Review All the Key Topics	140
Complete the Tables and Lists from Memory	140
Definitions of Key Terms	140
Chapter 5 Global Catalogs and Operations Masters	143
“Do I Know This Already?” Quiz	143
Configuring Global Catalog Servers	148
Planning the Placement of Global Catalog Servers	148
Promoting Domain Controllers to Global Catalog Servers	150
Using Universal Group Membership Caching	151
Using Partial Attribute Sets	152

Configuring Operations Masters	153
Schema Master	153
<i>Configuring the Schema</i>	154
<i>Extending the Schema</i>	155
<i>Deactivating Schema Objects</i>	159
Domain Naming Master	160
PDC Emulator	160
<i>Time Service</i>	161
Infrastructure Master	162
RID Master	162
Placement of Operations Masters	163
Transferring and Seizing of Operations Master Roles	164
<i>Transferring Operations Master Roles</i>	165
<i>Seizing Operations Masters Roles</i>	167
Review All the Key Topics	169
Complete the Tables and Lists from Memory	169
Definitions of Key Terms	170

Chapter 6 Configuring Active Directory Sites and Replication 173

“Do I Know This Already?” Quiz	173
The Need for Active Directory Sites	178
Configuring Sites and Subnets	179
Creating Sites	180
Adding Domain Controllers	181
Creating and Using Subnets	182
Site Links, Site Link Bridges, and Bridgehead Servers	184
The Need for Site Links and Site Link Bridges	184
Configuring Site Links	185
Site Link Bridges	185
Site Link Costs	186
Sites Infrastructure	189
<i>Knowledge Consistency Checker</i>	189
<i>Intersite Topology Generator</i>	189
Configuring Active Directory Replication	189
Concepts of Active Directory Replication	190
<i>Intersite and Intrasite Replication</i>	191
<i>Distributed File System</i>	192
<i>One-Way Replication</i>	193

<i>Bridgehead Servers</i>	193
<i>Replication Protocols</i>	194
<i>Ports Used for Intersite Replication</i>	195
Replication Scheduling	196
<i>Intersite Replication Scheduling</i>	196
<i>Intrasite Replication Scheduling</i>	198
<i>Forcing Intersite Replication</i>	200

Review All the Key Topics	201
Complete the Tables and Lists from Memory	202
Definitions of Key Terms	202

Chapter 7 Additional Active Directory Roles 205

“Do I Know This Already?” Quiz	205
New Server Roles and Features	210
Active Directory Lightweight Directory Services	211
Installing AD LDS	213
<i>Installing the AD LDS Role</i>	213
<i>Installing AD LDS Instances</i>	214
Configuring Data Within AD LDS	217
<i>Using the ADSI Edit Snap-in</i>	217
<i>Using Ldp.exe</i>	218
<i>Using the Active Directory Schema Snap-in</i>	220
<i>Using the Active Directory Sites and Services Snap-in</i>	221
Migrating to AD LDS	221
Configuring an Authentication Server	222
<i>Creating AD LDS User Accounts and Groups</i>	222
<i>Binding to an AD LDS Instance with an AD LDS User</i>	224
Using AD LDS on Server Core	224
Active Directory Rights Management Services	225
Installing AD RMS	226
Certificate Request and Installation	228
Self-Enrollments	230
Delegation	230
Active Directory Metadirectory Services	231
Active Directory Federation Services	231
Installing the AD FS Server Role	233
Configuring Trust Policies	236
User and Group Claim Mapping	237

Configuring Federation Trusts 238

Creating Claims 239

Creating Account Stores 240

Enabling Applications 241

Creating Federation Trusts 242

Windows Server 2008 R2 Virtualization 244

Review All the Key Topics 247

Complete the Tables and Lists from Memory 247

Definitions of Key Terms 248

Chapter 8 Read-Only Domain Controllers 251

“Do I Know This Already?” Quiz 251

Installing a Read-Only Domain Controller 254

Planning the Use of RODCs 254

Installing RODCs 256

Prestaging an RODC 257

Managing a Read-Only Domain Controller 259

Unidirectional Replication 260

Administrator Role Separation 261

Read-Only DNS 262

BitLocker 263

Preparing Your Computer to Use BitLocker 265

Enabling BitLocker 265

Managing BitLocker 269

Replication of Passwords 270

Planning a Password Replication Policy 271

Configuring a Password Replication Policy 272

Credential Caching 273

Administering the RODC's Authentication Lists 275

syskey 276

Review all the Key Topics 278

Definitions of Key Terms 278

Chapter 9 Active Directory User and Group Accounts 281

“Do I Know This Already?” Quiz 281

Creating User and Group Accounts 286

Introducing User Accounts 286

Introducing Group Accounts 287

Creating User, Computer, and Group Accounts 288

Use of Template Accounts	290
Using Bulk Import to Automate Account Creation	291
<i>Csvde</i>	292
<i>Ldifde</i>	293
<i>Dsadd</i>	294
<i>Additional Command-Line Tools</i>	295
<i>Scripts</i>	296
Configuring the UPN	296
<i>UPN Suffixes</i>	296
<i>Adding or Removing UPN Suffixes</i>	297
Configuring Contacts	298
Creating Distribution Lists	299
Managing and Maintaining Accounts	300
Creating Organizational Units	301
Configuring Group Membership	304
AGDLP/AGUDLP	306
Account Resets	308
Deny Domain Local Group	308
Protected Admin	309
Local Versus Domain Groups	310
Deprovisioning Accounts	312
Delegating Administrative Control of Active Directory Objects	313
Review All the Key Topics	317
Complete the Tables and Lists from Memory	318
Definitions of Key Terms	318
Chapter 10 Trust Relationships in Active Directory	321
“Do I Know This Already?” Quiz	321
Types of Trust Relationships	325
Transitive Trusts	325
Forest Trusts	326
External Trusts and Realm Trusts	326
Shortcut Trusts	327
Creating and Configuring Trust Relationships	328
Creating a Forest Trust Relationship	329
Creating External Trust Relationships	335
Creating Realm Trust Relationships	336
Creating Shortcut Trust Relationships	337

Managing Trust Relationships	338
Validating Trust Relationships	338
Authentication Scope	338
SID Filtering	340
Removing a Cross-forest Trust Relationship	341
Review All the Key Topics	343
Complete the Tables and Lists from Memory	343
Definitions of Key Terms	343
Chapter 11 Creating and Applying Group Policy Objects	345
“Do I Know This Already?” Quiz	345
Overview of Group Policy	351
Components of Group Policy	351
<i>Group Policy Containers</i>	352
<i>Group Policy Templates</i>	352
New Features of Group Policy in Windows Server 2008 and Windows Server 2008 R2	354
Creating and Applying GPOs	355
Managing GPOs	359
<i>Linking GPOs</i>	360
<i>Managing GPO Links</i>	361
<i>Deleting a GPO</i>	362
<i>Delegating Control of GPOs</i>	362
<i>Specifying a Domain Controller</i>	365
Configuring GPO Hierarchy and Processing Priority	365
<i>OU Hierarchy</i>	367
<i>Enforced</i>	367
<i>Block Inheritance</i>	369
<i>Modifying the Sequence of GPO Application</i>	370
<i>Disabling User Objects</i>	370
Group Policy Filtering	371
<i>Security Filtering of GPOs</i>	371
<i>Windows Management Instrumentation</i>	374
<i>Windows PowerShell</i>	374
Configuring GPO Templates	376
Group Policy Loopback Processing	377
User Rights	378
ADMX Central Store	379
Administrative Templates	380

	Restricted Groups	384
	Starter GPOs	385
	Shell Access Policies	387
	Review All the Key Topics	389
	Complete the Tables and Lists from Memory	389
	Definitions of Key Terms	390
Chapter 12	Group Policy Software Deployment	393
	“Do I Know This Already?” Quiz	393
	Types of Software Deployment	398
	Assigning and Publishing Software	399
	<i>Assigning Software to Users</i>	399
	<i>Assigning Software to Computers</i>	399
	<i>Publishing Software to Users</i>	399
	Deploying Software Using Group Policy	400
	ZAP Files	402
	Software Installation Properties	403
	Software Package Properties	405
	Upgrading Software	407
	Use of Transform Files to Modify Software Packages	409
	Redeployment of Upgraded Software	411
	Removal of Software	413
	Review All the Key Topics	414
	Complete the Tables and Lists from Memory	414
	Definitions of Key Terms	414
Chapter 13	Account Policies and Audit Policies	417
	“Do I Know This Already?” Quiz	417
	Use of Group Policy to Configure Security	422
	Configuring Account Policies	422
	<i>Domain Password Policies</i>	423
	<i>Account Lockout</i>	426
	<i>Unlocking an Account</i>	427
	<i>Kerberos Policy</i>	428
	Fine-Grained Password Policies	428
	<i>Password Settings Precedence</i>	429
	<i>Configuring Fine-Grained Password Policies</i>	430
	<i>Managing Fine-Grained Password Policies</i>	435
	<i>Viewing the Resultant PSO</i>	435

Security Options	436
Using Additional Security Configuration Tools	439
Auditing of Active Directory Services	441
New Features of Active Directory Auditing	441
Using GPOs to Configure Auditing	442
<i>Available Auditing Categories</i>	442
<i>Configuring Basic Auditing Policies</i>	443
<i>Configuring Advanced Audit Policies</i>	446
Using Auditpol.exe to Configure Auditing	447
Review All the Key Topics	449
Complete the Tables and Lists from Memory	450
Definitions of Key Terms	450

Chapter 14 Monitoring Active Directory 453

“Do I Know This Already?” Quiz	453
Tools Used to Monitor Active Directory	459
Network Monitor	459
Task Manager	463
<i>Configuring Application Priority</i>	465
Event Viewer	466
<i>Customizing Event Viewer</i>	468
<i>Customizing Event Viewer Detail</i>	470
Reliability and Performance Monitor	471
<i>Resource Monitor</i>	473
<i>Reliability Monitor</i>	473
<i>Performance Monitor</i>	476
<i>Data Collector Sets</i>	479
Windows System Resource Manager	484
Server Performance Advisor	486
Monitoring and Troubleshooting Active Directory Replication	487
replmon	487
repadmin	491
<i>replicate</i>	491
<i>showmeta</i>	492
<i>showreps</i>	492
<i>add</i>	492
<i>sync</i>	493
<i>syncall</i>	493

<i>showconn</i>	493
<i>replsummary</i>	494
<i>dcdiag</i>	494
Troubleshooting the Application of Group Policy Objects	496
Resultant Set of Policy	496
<i>Planning Mode/Group Policy Modeling</i>	497
<i>Logging Mode/Group Policy Results</i>	501
<i>Using the Delegation of Control Wizard</i>	509
<i>gpresult</i>	509
Review All the Key Topics	512
Complete the Tables and Lists from Memory	513
Definitions of Key Terms	513

Chapter 15 Maintaining Active Directory 515

“Do I Know This Already?” Quiz	515
Backing Up and Recovering Active Directory	520
Backup Permissions	521
Use of Windows Server Backup	521
<i>Installing Windows Server Backup</i>	521
<i>Backing Up Critical Volumes of a Domain Controller</i>	522
<i>The wbadmin Command</i>	525
<i>Scheduling a Backup</i>	526
<i>Using Removable Media</i>	527
Recovering Active Directory	528
<i>Directory Services Restore Mode</i>	528
<i>Performing a Nonauthoritative Restore</i>	529
<i>Using the wbadmin Command to Recover Your Server</i>	534
<i>Performing an Authoritative Restore</i>	536
<i>Recovering Back-Links of Authoritatively Restored Objects</i>	537
<i>Performing a Full Server Recovery of a Domain Controller</i>	538
<i>Linked-Value Replication and Authoritative Restore of Group Memberships</i>	539
The Active Directory Recycle Bin	540
<i>Enabling the Active Directory Recycle Bin</i>	541
<i>Using the Active Directory Recycle Bin to Restore Deleted Objects</i>	543
Backing Up and Restoring GPOs	545
<i>Backing Up GPOs</i>	545
<i>Restoring GPOs</i>	545
<i>Importing GPOs</i>	547
<i>Using Scripts for Group Policy Backup and Restore</i>	548

Offline Maintenance of Active Directory	549
Restartable Active Directory	549
Offline Defragmentation and Compaction	550
<i>Online Defragmentation</i>	551
<i>Offline Defragmentation</i>	551
Active Directory Database Storage Allocation	553
Review All the Key Topics	555
Complete the Tables and Lists from Memory	556
Definitions of Key Terms	556

Chapter 16 Installing and Configuring Certificate Services 559

“Do I Know This Already?” Quiz	559
What’s New with Certificate Services in Windows Server 2008?	563
New Features of Active Directory Certificate Services in Windows Server 2008 R2	564
Installing Active Directory Certificate Services	565
Configuring Certificate Authority Types and Hierarchies	565
Installing Root CAs	567
Installing Subordinate CAs	571
Understanding Certificate Requests	571
Using Certificate Practice Statements	572
Configuring Certificate Authority Server Settings	573
Installing the Certificates Snap-in	573
Working with Certificate Stores	575
<i>Using Group Policy to Import Certificates</i>	575
<i>Backing Up Certificates and Keys</i>	576
<i>Restoring Certificates and Keys</i>	577
<i>Using Group Policy to Enable Credential Roaming</i>	578
Backing Up and Restoring Certificate Databases	580
Assigning Administration Roles	581
<i>Configuring Certificate Server Permissions</i>	582
Review All the Key Topics	583
Complete the Tables and Lists from Memory	584
Definitions of Key Terms	584

Chapter 17 Managing Certificate Templates, Enrollments, and Certificate Revocation 587

“Do I Know This Already?” Quiz	587
Managing Certificate Templates	592

Understanding Certificate Template Types	592
Configuring Certificate Templates	593
<i>Securing Template Permissions</i>	595
<i>Enabling the Use of Templates</i>	597
Managing Different Certificate Template Versions	597
Archiving Keys	599
Configuring Key Recovery Agents	599
Managing Certificate Enrollments	602
Understanding Network Device Enrollment Services	602
Enabling Certificate Autoenrollment	605
Configuring Web Enrollment	606
Configuring Smart Card Enrollment	609
Creating Enrollment Agents	610
<i>Using Group Policy to Require Smart Cards for Logon</i>	614
Managing Certificate Revocation	616
Configuring Certificate Revocation Lists	617
<i>Configuring a CRL Distribution Point</i>	619
<i>Troubleshooting CRLs</i>	620
Configuring Online Responders	621
<i>Configuring Responder Properties</i>	622
<i>Adding a Revocation Configuration</i>	623
<i>Configuring Arrays</i>	624
Configuring Authority Information Access	624
Review All the Key Topics	625
Complete the Tables and Lists from Memory	626
Definitions of Key Terms	626
Practice Exam	629
Answers to Practice Exam	691
Appendix A Answers to the “Do I Know This Already?” Quizzes	729
Appendix B Installing Windows Server 2008 R2	763
Glossary	773
Index	796
Elements Available on CD	
Appendix C Memory Tables	3
Appendix D Memory Tables Answer Key	3

About the Author

Don Poulton (A+, Network+, Security+, MCSA, MCSE) is an independent consultant who has been involved with computers since the days of 80-column punch cards. After a career of more than 20 years in environmental science, Don switched careers and trained as a Windows NT 4.0 MCSE. He has been involved in consulting with a couple of small training providers as a technical writer, during which time he wrote training and exam prep materials for Windows NT 4.0, Windows 2000, and Windows XP. Don has written or contributed to several titles, including *Security+ Lab Manual* (Que, 2004); *MCSA/MCSE 70-299 Exam Cram 2: Implementing and Administering Security in a Windows 2003 Network (Exam Cram 2)* (Que, 2004); *MCSE 70-294 Exam Prep: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure* (Que, 2006); *MCTS 70-620 Exam Prep: Microsoft Windows Vista, Configuring* (Que, 2008); and *MCTS 70-680 Cert Guide: Microsoft Windows 7, Configuring* (Que, 2011).

In addition, he has worked on programming projects, both in his days as an environmental scientist and more recently with Visual Basic to update an older statistical package used for multivariate analysis of sediment contaminants.

When not working on computers, Don is an avid amateur photographer who has had his photos displayed in international competitions and published in magazines such as *Michigan Natural Resources Magazine* and *National Geographic Traveler*. Don also enjoys traveling and keeping fit.

Don lives in Burlington, Ontario, with his wife, Terry.

Dedication

I would like to dedicate this book to my wife Terry, who has stood by my side and supported me throughout the days spent writing this book. This project would not have been possible without her love and support.

Acknowledgments

I would like to thank all the staff at Pearson and in particular Betsy Brown for making this project possible. My sincere thanks goes out to Chris Crayton for his helpful technical suggestions, as well as Jeff Riley, development editor, and Mike Henry, copy editor, for their improvements to the manuscript.

—Don Poulton

About the Technical Reviewer

Christopher A. Crayton is an author, technical editor, technical consultant, security consultant, trainer, and SkillsUSA state-level technology competition judge. Formerly, he worked as a computer and networking instructor at Keiser College (2001 Teacher of the Year); as network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak Headquarters as a computer and network specialist. Chris has authored several print and online books, including *The A+ Exams Guide, Second Edition* (Cengage Learning, 2008); *Microsoft Windows Vista 70-620 Exam Guide Short Cut* (O'Reilly, 2007); *CompTIA A+ Essentials 220-601 Exam Guide Short Cut* (O'Reilly, 2007); *The A+ Exams Guide* (Charles River Media, 2008); *The A+ Certification and PC Repair Handbook* (Charles River Media, 2005); *The Security+ Exam Guide* (Charles River Media, 2003); and *A+ Adaptive Exams* (Charles River Media, 2002). He is also coauthor of the *How to Cheat at Securing Your Network* (Syngress, 2007). As an experienced technical editor, Chris has provided many technical edits/reviews for several major publishing companies, including Pearson Education, McGraw-Hill, Cengage Learning, Wiley, O'Reilly, Syngress, and Apress. He holds MCSE, A+, and Network+ certifications.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson Publishing, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Dave Dusthimer
Associate Publisher
Pearson Education
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonITcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.



Introduction

MCTS Windows Server 2008 Active Directory, Configuring Cert Guide (Exam 70-640) is designed for network administrators, network engineers, and consultants who are pursuing the Microsoft Certified Technology Specialist (MCTS) or Microsoft Certified IT Professional (MCITP) certifications for Windows Server 2008. This book covers the “TS: Microsoft Windows Server 2008 Active Directory, Configuring” exam (70-640), which earns you the Microsoft Certified Technology Specialist: Windows Server 2008 Active Directory, Configuration certification. The exam is designed to measure your skill and ability to implement, administer, and troubleshoot Active Directory running on Windows Server 2008. Microsoft not only tests you on your knowledge of Active Directory, but it has purposefully developed questions on the exam to force you to problem-solve in the same way that you would when presented with a real-life error. Passing this exam demonstrates your competency in administration.

This book covers all the objectives that Microsoft has established for exam 70-640. It doesn’t offer end-to-end coverage of Active Directory in Windows Server 2008; rather, it helps you develop the specific core competencies that you need to master as an Active Directory administrator. You should be able to pass the exam by learning the material in this book, without taking a class.

Goals and Methods

The number-one goal of this book is a simple one: to help you get ready to take—and pass—Microsoft Certification Exam 70-640, “TS: Windows Server 2008 Active Directory, Configuring.” You will find information within this book that will help ensure your success as you pursue this Microsoft exam and the Technology Specialist or IT Professional certification.

Because Microsoft certification exams stress problem-solving abilities and reasoning more than memorization of terms and facts, our goal is to help you master and understand the required objectives for the 70-640 exam.

To aid you in mastering and understanding the MCTS certification objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics to be covered in the chapter; it also lists the corresponding 70-640 exam objectives.
- **Do I Know This Already Quizzes:** At the beginning of each chapter is a quiz. The quizzes, and answers/explanations (found in Appendix A), are meant to gauge your knowledge of the subjects. If the answers to the questions don't come readily to you, be sure to read the entire chapter.
- **Foundation Topics:** The heart of the chapter. Explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. The chapters are broken down into several topics each.
- **Key Topics:** The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table form at the end of the chapter.
- **Memory Tables:** These can be found on the DVD within Appendix C, "Memory Tables." Use them to help memorize important information.
- **Key Terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the complete key terms in the glossary.

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and enable you to easily move between chapters and sections of chapters to cover just the material that you need more work with. If you do intend to read all the chapters, the order in the book is an excellent sequence to use.

Chapter 1, "Getting Started with Active Directory," is an introductory chapter that presents the concepts around which Active Directory is built. It serves as a reference to the material that follows and eases users who are new to Active Directory into the book. If you have worked with Active Directory in Windows 2000 or Windows Server 2003, you might want to start with Chapter 2; however, you should take a look at the overview presented here of new capabilities of Active Directory in Windows Server 2008 and its R2 update.

The core chapters, Chapters 2 through 17, cover the following topics:

- **Chapter 2, “Installing and Configuring DNS for Active Directory”:** This chapter focuses on the concepts of Domain Name System (DNS) required for setting up an Active Directory domain. You learn about how to install DNS on your server and how to set up and configure DNS zones.
- **Chapter 3, “Installing Active Directory Domain Services”:** This chapter shows you how to set up your first domain. It then continues to discuss creating additional domain controllers in this domain and child domain controllers. It also discusses the requirements that must be met when upgrading domains based on older Windows server versions to allow them to operate in Windows Server 2008 with complete functionality.
- **Chapter 4, “Configuring DNS Server Settings and Replication”:** This chapter builds on Chapter 2 to delve into additional items that you must configure in server settings, zone transfers, and DNS replication.
- **Chapter 5, “Global Catalogs and Operations Masters”:** Proper operation of global catalog servers and operations masters is vital to the day-to-day functioning of your domain and forest. This chapter focuses on the configuration and troubleshooting steps necessary with these specialized domain controllers.
- **Chapter 6, “Configuring Active Directory Sites and Replication”:** Active Directory divides forests and domains on a geographical basis by using sites. To function properly, Active Directory depends on data replication among all its domain controllers. This chapter shows you how to set up sites and ensure that all directory objects are located in the site corresponding to their locations. It then continues with configuring replication, both on an intrasite and intersite basis.
- **Chapter 7, “Additional Active Directory Roles”:** This chapter takes care of other Active Directory roles including Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS), and Active Directory Rights Management Service (AD RMS). AD LDS is designed to provide additional directory services where an additional domain and its domain controllers are not required. AD RMS enhances security in your domain by enabling the creation of rights-protected files and folders that can be accessed only by authorized users. AD FS provides a single sign-on capability for authenticating users to multiple web-based applications.
- **Chapter 8, “Read-Only Domain Controllers”:** This chapter discusses how to set up a read-only domain controller (RODC) and configure its interaction with

other (writable) domain controllers in your forest. An RODC is useful in a situation such as a branch office where physical security of the domain controller might be of concern.

- **Chapter 9, “Active Directory User and Group Accounts”:** This chapter shows you how to create user and group accounts in Active Directory, including methods for bulk creation of large numbers of accounts. It introduces the various types and scopes of groups available in Active Directory and the recommended methods of nesting these groups to facilitate the provision of access to resources in your forest. It also looks at account properties, creation of organizational units (OUs), and delegation of control.
- **Chapter 10, “Trust Relationships in Active Directory”:** By default, all domains in a forest trust each other. However, you might need to access objects located in another forest, and this chapter talks about methods you might use to provide and troubleshoot such access. Windows Server 2008 provides several types of trust relationships that can be used for meeting different requirements.
- **Chapter 11, “Creating and Applying Group Policy Objects”:** Group Policy is at the heart and soul of resource management in Active Directory. This chapter shows you how to set up Group Policy objects and configure them to apply to users, groups, and OUs as required. The hierarchy of GPO application and the methods to modify this hierarchy are also discussed.
- **Chapter 12, “Group Policy Software Deployment”:** This chapter shows you how to use Group Policy for deploying software to large numbers of users so that they have the applications they need to perform their jobs. You also learn how to upgrade software when new editions and features become available and how to remove software when it is no longer required by users.
- **Chapter 13, “Account Policies and Audit Policies”:** This chapter expands the coverage of Group Policy to include policies that govern the safety and security of accounts in your domain and audit access to Active Directory objects and components so that you can meet the increasingly complex regulatory requirements.
- **Chapter 14, “Monitoring Active Directory”:** This chapter focuses on the tools you can use to monitor the functionality of Active Directory. You also learn about the tools and methods used for monitoring Active Directory replication as well as the tools and techniques you can use to monitor and troubleshoot the application of Group Policy.
- **Chapter 15, “Maintaining Active Directory”:** This chapter shows you how to back up, recover, restart, and troubleshoot Active Directory and its components.

You learn how to perform nonauthoritative and authoritative restore of Active Directory and how to use the new Windows Server 2008 R2 Active Directory Recycle Bin.

- **Chapter 16, “Installing and Configuring Certificate Services”:** A system of certificates is vital to carrying out secure business, especially when an Internet presence is required. This chapter shows you how to set up a hierarchy of certificate servers within Active Directory and back up, restore, and archive your certificates and keys.
- **Chapter 17, “Managing Certificate Templates, Enrollments, and Certificate Revocation”:** Certificates issued by your servers require management to ensure that users requiring certificates can obtain them, and that compromised certificates are revoked and cannot be used by unauthorized parties. This chapter looks at these topics and helps you to ensure the security of your certificate hierarchy.

In addition to the 17 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The CD includes the glossary, practice test, and memory tables that you can work through to verify your knowledge of the subject matter.

Study and Exam Preparation Tips

It’s a rush of adrenaline during the final day before an exam. If you’ve scheduled the exam on a workday, or following a workday, you will find yourself cursing the tasks you normally cheerfully perform because the back of your mind is telling you to read just a bit more, study another scenario, practice another skill so that you will be able to get this exam out of the way successfully.

The way that Microsoft has designed its tests lately does not help. I remember taking Microsoft exams many years ago and thoroughly understanding the term *paper certified*. Nowadays, you can’t get through a Microsoft exam without knowing the material so well that when confronted with a problem, whether a scenario or real-life situation, you can handle the challenge. Instead of trying to show the world how many MCSEs are out there, Microsoft is trying to prove how difficult it is to achieve a certification, including the newly created MCTS and MCITP as well as the MCSE and MCSA, thereby making those who are certified more valuable to their organizations.

Learning Styles

To best understand the nature of preparation for the test, it is important to understand learning as a process. You are probably aware of how you best learn new

material. You might find that outlining works best for you, or, as a visual learner, you might need to “see” things. Or, as a person who studies kinesthetically, the hands-on approach serves you best. Whether you need models or examples, or you just like exploring the interface, or whatever your learning style, solid test preparation works best when it takes place over time. Obviously, you shouldn’t start studying for a certification exam the night before you take it; it is very important to understand that learning is a developmental process. Understanding learning as a process helps you focus on what you know and what you have yet to learn.

People study in a combination of different ways: by doing, by seeing, and by hearing and writing. This book’s design fulfills all three of these study methods. For the kinesthetic, there are key topics scattered throughout each chapter. You will also discover step-by-step procedural instructions that walk you through the skills you need to master Active Directory in Windows Server 2008. The visual learner can find plenty of screen shots explaining the concepts described in the text. The auditory learner can reinforce skills by reading out loud and copying down key concepts and exam tips scattered throughout the book. You can also practice writing down the meaning of the key terms defined in each chapter, and in completing the memory tables for most chapters found on the accompanying DVD. While reading this book, you will realize that it stands the test of time. You will be able to turn to it over and over again.

Thinking about how you learn should help you recognize that learning takes place when you are able to match new information to old. You have some previous experience with computers and networking. Now you are preparing for this certification exam. Using this book, software, and supplementary materials will not just add incrementally to what you know; as you study, the organization of your knowledge actually restructures as you integrate new information into your existing knowledge base. This leads you to a more comprehensive understanding of the tasks and concepts outlined in the objectives and of computing in general. Again, this happens as a result of a repetitive process rather than a singular event. If you keep this model of learning in mind as you prepare for the exam, you will make better decisions concerning what to study and how much more studying you need to do.

Study Tips

There are many ways to approach studying, just as there are many different types of material to study. However, the tips that follow should work well for the type of material covered on Microsoft certification exams.

Study Strategies

Although individuals vary in the ways they learn information, some basic principles of learning apply to everyone. You should adopt some study strategies that take advantage of these principles. One of these principles is that learning can be broken into various depths. Recognition (of terms, for example) exemplifies a rather surface level of learning in which you rely on a prompt of some sort to elicit recall. Comprehension or understanding (of the concepts behind the terms, for example) represents a deeper level of learning than recognition. The ability to analyze a concept and apply your understanding of it in a new way represents further depth of learning.

Your learning strategy should enable you to know the material at a level or two deeper than mere recognition. This will help you perform well on the exams. You will know the material so thoroughly that you can go beyond the recognition-level types of questions commonly used in fact-based multiple-choice testing. You will be able to apply your knowledge to solve new problems.

Macro and Micro Study Strategies

One strategy that can lead to deep learning includes preparing an outline that covers all the objectives and subobjectives for the particular exam you are planning to take. You should delve a bit further into the material and include a level or two of detail beyond the stated objectives and subobjectives for the exam. Then you should expand the outline by coming up with a statement of definition or a summary for each point in the outline.

An outline provides two approaches to studying. First, you can study the outline by focusing on the organization of the material. You can work your way through the points and subpoints of your outline, with the goal of learning how they relate to one another. For example, you should be sure you understand how each of the main objective areas for Exam 70-640 is similar to and different from another. Then you should do the same thing with the subobjectives; you should be sure you know which subobjectives pertain to each objective area and how they relate to one another.

Next, you can work through the outline, focusing on learning the details. You should memorize and understand terms and their definitions, facts, rules and tactics, advantages and disadvantages, and so on. In this pass through the outline, you should attempt to learn detail rather than the big picture (the organizational information that you worked on in the first pass through the outline).

Research has shown that attempting to assimilate both types of information at the same time interferes with the overall learning process. If you separate your studying into these two approaches, you will perform better on the exam.

Active Study Strategies

The process of writing down and defining objectives, subobjectives, terms, facts, and definitions promotes a more active learning strategy than merely reading the material does. In human information-processing terms, writing forces you to engage in more active encoding of the information. Simply reading over the information leads to more passive processing. Using this study strategy, you should focus on writing down the items that are highlighted in the book—bulleted or numbered lists, key topics, notes, cautions, and review sections, for example.

You need to determine whether you can apply the information you have learned by attempting to create examples and scenarios on your own. You should think about how or where you could apply the concepts you are learning. Again, you should write down this information to process the facts and concepts in an active fashion.

Common-Sense Strategies

You should follow common-sense practices when studying: You should study when you are alert, reduce or eliminate distractions, and take breaks when you become fatigued.

Pretesting Yourself

Pretesting allows you to assess how well you are learning. One of the most important aspects of learning is what has been called *meta-learning*. Meta-learning has to do with realizing when you know something well or when you need to study some more. In other words, you recognize how well or how poorly you have learned the material you are studying.

For most people, this can be difficult to assess. Memory tables, practice questions, and practice tests are useful in that they reveal objectively what you have learned and what you have not learned. You should use this information to guide review and further studying. Developmental learning takes place as you cycle through studying, assessing how well you have learned, reviewing, and assessing again until you feel you are ready to take the exam.

You might have noticed the practice exam included in this book. You should use it as part of the learning process. The Exam Gear test-simulation software included on this book's CD-ROM also provides you with an excellent opportunity to assess your knowledge.

You should set a goal for your pretesting. A reasonable goal would be to score consistently in the 90% range.

Exam Prep Tips

After you have mastered the subject matter, the final preparatory step is to understand how the exam will be presented. Make no mistake: An MCTS exam challenges

both your knowledge and your test-taking skills. Preparing for the 70-640 exam is a bit different from preparing for those old Microsoft exams. The following is a list of things that you should consider doing:

- **Combine your skill sets into solutions:** In the past, exams would test whether you knew to select the right letter of a multiple choice answer. Today, you need to know how to resolve a problem that may involve different aspects of the material covered. For example, on exam 70-640 you could be presented with a problem that requires you to understand how to configure Group Policy to apply to a specific set of users and not to other users, and to troubleshoot this policy if it is not properly applied. The skills themselves are simple. Being able to zero in on what caused the problem and then to resolve it for a specific situation is what you need to demonstrate. In fact, you should not only be able to select one answer, but also multiple parts of a total solution.
- **Delve into excruciating details:** The exam questions incorporate a great deal of information in the scenarios. Some of the information is ancillary: It will help you rule out possible issues, but not necessarily resolve the answer. Some of the information simply provides you with a greater picture, as you would have in real life. Some information is key to your solution. For example, you might be presented with a question that lists the components of an Active Directory domain such as the number of server and client computers, the organizational unit (OU) structure, and so on. When you delve further into the question, you realize that the OU structure is the problem. Other times, you will find that the OU structure simply eliminates one or more of the answers that you could select. If you don't pay attention to what you can eliminate, the answer can elude you completely. And other times, the hardware configuration simply lets you know that the hardware is adequate.
- **Microsoft likes to quiz exam takers on the latest modifications of its technology:** From time to time, Microsoft seeds new questions into its exam database and beta tests these questions on exam takers. During the beta period for each question, its answer is not taken into account in computing the final score. However, when Microsoft is satisfied with the question's performance, it becomes live and is scored appropriately. You can expect to see questions that test your knowledge of the latest changes in Active Directory technology, including the enhancements introduced in 2009 with Windows Server 2008 R2.
- **It's a GUI test:** Microsoft has expanded its testing criteria into interface recognition. You should be able to recognize each dialog box, properties sheet, options, and defaults. You will be tested on how to perform typical configuration actions in Active Directory. In fact, Microsoft has begun to include performance-based questions on its exams that instruct you to perform a given task and presents

you with a live version of some Active Directory tool. You must complete the required actions and no others; otherwise, your response will be scored as incorrect.

- **Practice with a time limit:** The tests have always been time restricted, but it takes more time to read and understand the scenarios now and time is a whole lot tighter. To get used to the time limits, test yourself with a timer. Know how long it takes you to read scenarios and select answers.

Microsoft 70-640 Exam Topics

Table I-1 lists the exam topics for the Microsoft 70-640 exam. This table also lists the book parts in which each exam topic is covered.

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
1	The Foundation of Active Directory The Building Blocks of Active Directory New Features of Active Directory in Windows Server 2008	(n/a)
2	The Hierarchical Nature of DNS Installing DNS on Windows Server 2008 Configuring DNS Zones	Configuring Domain Name System (DNS) for Active Directory ■ Configure Zones
3	Planning the Active Directory Namespace Creating Forests and Domains Upgrading Older Versions of Active Directory Additional Forest and Domain Configuration Tasks	Configuring the Active Directory Infrastructure ■ Configure a forest or a domain
4	Configuring DNS Server Settings Configuring Zone Transfers and Replication	Configuring Domain Name System (DNS) for Active Directory ■ Configure DNS Server Settings ■ Configure DNS Zone Transfers and Replication

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
5	Configuring Global Catalog Servers Configuring Operations Masters	Configuring the Active Directory Infrastructure <ul style="list-style-type: none"> ■ Configure the global catalog ■ Configure operations masters
6	The Need for Active Directory Sites Configuring Sites and Subnets Site Links, Site Link Bridges, and Bridgehead Servers Configuring Active Directory Replication	Configuring the Active Directory Infrastructure <ul style="list-style-type: none"> ■ Configure sites ■ Configure Active Directory replication
7	New Server Roles and Features Active Directory Lightweight Directory Services (AD LDS) Active Directory Rights Management Services (AD RMS) Active Directory Federation Services (AD FS) Windows Server 2008 R2 Virtualization	Configuring Additional Active Directory Server Roles <ul style="list-style-type: none"> ■ Configure Active Directory Lightweight Directory Services (AD LDS) ■ Configure Active Directory Rights Management Service (AD RMS) ■ Configure Active Directory Federation Services (AD FS)
8	Installing a Read-Only Domain Controller Managing a Read-Only Domain Controller	Configuring Additional Active Directory Server Roles <ul style="list-style-type: none"> ■ Configure the read-only domain controller (RODC)
9	Creating User and Group Accounts Managing and Maintaining Accounts	Creating and Maintaining Active Directory Objects <ul style="list-style-type: none"> ■ Automate creation of Active Directory accounts ■ Maintain Active Directory accounts
10	Types of Trust Relationships Creating and Configuring Trust Relationships Managing Trust Relationships	Configuring the Active Directory Infrastructure <ul style="list-style-type: none"> ■ Configure trusts

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
11	Overview of Group Policy Creating and Applying GPOs Configuring GPO Templates	Creating and Maintaining Active Directory Objects <ul style="list-style-type: none"> ■ Create and apply Group Policy objects (GPOs) ■ Configure GPO templates
12	Types of Software Deployment Deploying Software Using Group Policy Upgrading Software Removal of Software	Creating and Maintaining Active Directory Objects <ul style="list-style-type: none"> ■ Configure software deployment GPOs
13	Use of Group Policy to Configure Security Auditing of Active Directory Services	Creating and Maintaining Active Directory Objects <ul style="list-style-type: none"> ■ Configure account policies ■ Configure audit policy by using GPOs
14	Tools Used to Monitor Active Directory Monitoring and Troubleshooting Active Directory Replication Troubleshooting the Application of Group Policy Objects	Maintaining the Active Directory Environment <ul style="list-style-type: none"> ■ Monitor Active Directory
15	Backing Up and Recovering Active Directory Offline Maintenance of Active Directory	Maintaining the Active Directory Environment <ul style="list-style-type: none"> ■ Configure backup and recovery ■ Perform offline maintenance
16	What's New with Certificate Services in Windows Server 2008? Installing Active Directory Certificate Services Configuring Certificate Authority Server Settings	Configuring Active Directory Certificate Services <ul style="list-style-type: none"> ■ Install Active Directory Certificate Services ■ Configure CA server settings

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
17	Managing Certificate Templates Managing Certificate Enrollments Managing Certificate Revocation	Configuring Active Directory Certificate Services <ul style="list-style-type: none">■ Manage certificate templates■ Manage enrollments■ Manage certificate revocation



This chapter covers the following subjects:

- **Planning the Active Directory Namespace:** This section provides a basic introduction to best practices you should follow in planning and designing an Active Directory namespace that will serve your company properly both now and in the years to come.
- **Creating Forests and Domains:** In this section, you learn how to create your first domain controller in a new Active Directory forest. You then learn how to add additional domain controllers to your forest and create child domains.
- **Interoperability with Previous Versions of Active Directory:** Many organizations are using Active Directory domains based on Windows 2000 and Windows Server 2003. This section takes you through the preparatory tasks you must perform before you can add a Windows Server 2008 R2 domain controller as well as the actual upgrading of older domain controllers. In addition, it introduces you to the concept of forest and domain functional levels, as well as the benefits of the newest Windows Server 2008 R2 functional levels.
- **Additional Forest and Domain Configuration Tasks:** After you have installed and configured your first domain, you should perform several additional tasks. This section discusses verifying your Active Directory installation, using the Active Directory Migration tool (ADMT), and creating alternative user principal name (UPN) suffixes.

Installing Active Directory Domain Services

In Chapter 1, “Getting Started with Active Directory,” you were introduced to the basic building blocks of the logical Active Directory structure: forests, trees, domain, and organizational units (OUs). You were also introduced to the concept of sites for distinguishing portions of the network separated physically by slow WAN links. Now you begin to create an actual Active Directory forest and domain structure.

The act of installing Active Directory on a server is conceptually very simple. You need only run the Active Directory Domain Services (AD DS) Installation Wizard from the Add Roles Wizard of Server Manager and provide answers to the questions the wizard asks. The actual act of installing AD DS, however, can be thought of as the tip of the iceberg. Before you install AD DS, you need to plan how Active Directory will fit into your company’s corporate and geographical structure as well as your expectations for future growth and the potential for acquiring other companies. This chapter serves only as a basic introduction to the topic of planning.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read this entire chapter or simply jump to the “Exam Preparation Tasks” section for review. If you are in doubt, read the entire chapter. Table 3-1 outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

Table 3-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions Covered in This Section
Planning the Active Directory Namespace	1
Creating Forests and Domains	2–7
Interoperability with Previous Versions of Active Directory	8–9
Additional Forest and Domain Configuration Tasks	10–11

1. Which of the following are best practices that you should follow when planning an AD DS domain structure? (Choose all that apply.)
 - a. Employ a test lab
 - b. Prepare thorough documentation
 - c. Keep everyone, including top managers, informed
 - d. Understand thoroughly the network's TCP/IP infrastructure
 - e. Develop and adhere to an adequate security policy
 - f. Know the capabilities of your WAN links

2. On which of the following editions of Windows Server 2008 R2 can you install the AD DS role? (Choose all that apply.)
 - a. Web
 - b. Foundation
 - c. Standard
 - d. Enterprise
 - e. Datacenter

3. Which of the following tools can you use to install AD DS on a server running Windows Server 2008 R2? (Choose two.)
 - a. The `dcpromo.exe` command
 - b. The Manage Your Server tool
 - c. The Configure Your Server tool
 - d. The Add Roles Wizard
 - e. The Add Features Wizard

4. Which of the following conditions would represent a problem when you are attempting to install the first domain controller in your domain?
 - a. A DHCP server is not present.
 - b. A DNS server is not present.
 - c. The server's hard disk is formatted with the FAT32 file system.
 - d. The server's hard disk has only 10 GB free space available.

5. Which of the following is a new AD DS administrative tool included with Windows Server 2008 R2 and was not present in older versions of Windows Server?
 - a. Active Directory Users and Computers
 - b. Active Directory Administrative Center
 - c. Active Directory Sites and Services

- d. Active Directory Domains and Trusts
 - e. User Manager for Domains
6. Your computer is running the Server Core edition of Windows Server 2008 R2. You want to promote this server to domain controller. What should you do?
- a. Use Server Manager to run the Add Roles Wizard.
 - b. Use the Initial Configuration Tasks window to run the Add Roles Wizard.
 - c. Use `dcpromo.exe` and specify the required parameters when prompted.
 - d. Use `dcpromo.exe` together with an answer file that provides the required parameters.
 - e. You cannot promote this server to domain controller without reinstalling Windows Server 2008 as a full edition server.
7. You are the administrator of DC1, which is a Windows Server 2008 R2 domain controller in your company's domain. You are experiencing problems with DC1 and decide to run the Active Directory Installation Wizard again on this machine. What happens?
- a. A new copy of the AD DS software is installed.
 - b. Two copies of the AD DS software will exist side-by-side.
 - c. The domain controller is demoted to a member server.
 - d. You receive an error message informing you that the wizard cannot be run again.
8. Which of the following is not a valid domain or forest functional level for a domain controller running Windows Server 2008 R2?
- a. Windows 2000 mixed
 - b. Windows 2000 native
 - c. Windows Server 2003 native
 - d. Windows Server 2008 native
 - e. Windows Server 2008 R2 native
9. You have installed Windows Server 2008 R2 on a brand-new server and want to promote this server to domain controller in your domain, which has domain controllers running Windows Server 2003 and operates at the Windows Server 2003 native domain functional level. What should you do first?
- a. Run `adprep /forestprep` and then run `adprep /domainprep`.
 - b. Run `adprep /domainprep` and then run `adprep /forestprep`.
 - c. Raise the domain functional level to Windows Server 2008 R2.
 - d. Raise the forest functional level to Windows Server 2008 R2.

- 10.** Your company has acquired another company, and both companies operate an AD DS forest with a single domain. The CIO has decided that all users of the acquired company are to be moved into your company's domain so that the other company's forest and domain can be decommissioned. What tool should you use to assist you in this action?

 - a.** Active Directory Users and Computers
 - b.** Active Directory Administrative Center
 - c.** Active Directory Migration Tool (ADMT)
 - d.** User State Migration Tool (USMT)

- 11.** You are the administrator for the `sales.que.com` domain. You are configuring an implicit user principal name (UPN) suffix user named Sharon. Which of the following is a valid implicit UPN?

 - a.** `Sharon@sales.que.com`
 - b.** `Sharon@sales`
 - c.** `Sales.que.com\Sharon`
 - d.** `Sales\Sharon`

Foundation Topics

Planning the Active Directory Namespace

As discussed in Chapter 1, “Getting Started with Active Directory,” the domain is the primary administrative unit within an Active Directory namespace. Windows Server 2008 uses the concept of domains to separate available resources among registered users. It is also the basic security unit, as you will see throughout this book, because many of the security requirements in Active Directory are focused at the domain level. Therefore, it is important to begin the process of planning any company’s Active Directory Domain Services (AD DS) namespace from the viewpoint of the domain structure.

All planning starts from the name of your company’s root domain. Recall in Chapter 1 that each tree has a root domain that is located at the top of the inverted tree structure. All subdomains contain this root domain name in their own domain names. In addition, the first domain in the entire forest is not only a root domain, it is also the forest root. Also, the top-level domain names used on the Internet and defined in the DNS hierarchy are included. The latter is not an absolute requirement if you are planning a domain that has no Internet representation whatsoever, but what company these days does not have a presence on the Internet?

Therefore, it makes sense that your root domain can take the same name as your Internet domain name as registered with InterNIC (Internet Network Information Center). Consider a fictional company with an Internet domain name of `mycompany.biz`. Although you can use this name as your AD DS root domain name, it creates a risk of revealing your company’s AD DS structure to the public Internet. Consequently, you might want to keep the internal name separate and use something like `mycompany.local` for the AD DS root domain name of the same fictional company.

Subdividing the Active Directory Namespace

You can subdivide your namespace within Active Directory in two ways:

- Separate domains
- Organizational units (OUs)

In many instances, the use of separate domains or OUs would serve just as well as the other. In larger companies, the use of separate domains often arose from the limitations of the Security Accounts Manager (SAM) database in Windows NT. Because the AD DS database can hold millions of objects, this limitation is seldom of importance in AD DS design. For this reason, and because a single domain structure is the easiest type of structure to administer, this method is the best means of organizing your company’s namespace if possible. There is no specific need to create separate domains for administrative functions, geographical sites, or departments in the

company. Logically, you can handle this function by setting up a system of OUs. An internal system of OUs provides the following additional advantages:

- It can be administered either centrally or locally. The concept of delegation of control in AD DS facilitates the assignment of individuals as local administrators.
- User authentication is simpler and faster within a single domain environment, regardless of where a user is located.
- It is far simpler to modify when needed—for example, if your company is reorganized.
- It is flexible and can include an internal hierarchy of departments, sections, work units, and so on.

There are, however, reasons for using separate domains for discrete divisions of your company:

- This approach can facilitate decentralized administration of network resources.
- In the case of multiple Internet domain names, the domain can be built to mirror the Internet functionality.
- Multiple domains representing different geographical locations might reduce the amount of replication traffic across low wide area network (WAN) links.
- User account requirements that vary among departments or locations, such as password complexity, are more easily handled with separate domains.
- International legal and language needs might be handled more easily by using separate domains.
- Very massive organizations can be broken down into a domain structure.

Administrative or Geographical Organization of Domains

You can organize a series of domains along either administrative or geographical means. For example, Figure 3-1 shows `mycompany.biz` organized along three administrative divisions—Accounting, Products, and Advertising—all reporting to a Management group, contrasted with the company's main offices located in San Francisco, Dallas, Toronto, and Atlanta.

You need to take into account conditions that favor either the administrative or geographical model. This can include the following factors:

- Plans for future offices in additional cities
- Projected growth of each of the company's divisions
- Potential for reorganization of the company along new departmental lines
- Requirements for centralized or decentralized administration of the company

Figure 3-1 Administrative and geographical divisions of **mycompany.biz**.

- Needs for different security levels in either certain departments or certain offices
- Current or future use of one or more Internet DNS namespaces

Such factors suggest the best domain organization for your company's AD DS namespace.

Use of Multiple Trees

Within the AD DS forest, you can have one or more trees. As outlined in Chapter 1, the main difference between trees and forests is that domains within a tree share a contiguous namespace, whereas domains located in different trees in the same forest have a disjointed namespace. Thus, `que.com` and `examcram.com` are root domains in two separate trees of the same forest.

In almost all multiple domain enterprises, it makes sense to employ a single tree. The major exception occurs when two companies merge and want to maintain their separate identities. Their identities, and indeed their Internet namespaces, are best served by having more than one tree in the forest.

NOTE Another way of designing a multidomain forest is to employ an empty forest root domain with a series of child domains representing administrative or geographical divisions of the company. The root domain contains only a small number of objects, and you can readily control membership in the Enterprise Admins and Schema Admins groups. The impact of business decisions, such as the spin-off or

renaming of subsidiary companies, can be handled more readily. On the other hand, you must ensure that the forest root domain controllers are carefully secured and protected against disaster because their loss effectively destroys the entire forest structure.

Best Practices

Planning the AD DS domain structure is an act that has far-reaching implications. This process is something that cannot simply be decided by a few network administrators sitting down with a few diagrams of the network and company business structures. Rather, it must involve the company's senior and middle management as well as business strategy specialists and representatives from remote offices. If you use internally developed applications, representatives of the development team should be involved. The following guidelines will help you make your AD DS implementation proceed smoothly:

Key Topic

- **Know everything there is to know about the network:** Although this guideline might sound intuitive for senior administrators who have built the network from the ground up, those who have come on the scene more recently need to gather information about everything that must be accounted for in an AD DS plan.
- **Employ a test lab:** The lab should contain representative domain controllers, member servers, and client computers. Set up a mini version of your complete network and engage the assistance of a representative set of users to test all facets of the implementation thoroughly.
- **Prepare thorough documentation:** This point can never be understated. Use tools such as Microsoft Visio to prepare diagrams of different levels of company detail, from the major administrative units down to the smallest workgroups. Visio is a tool that is specifically designed for preparing administrative diagrams such as those required in this scenario. This exercise also helps in optimizing communication between technical individuals and top management.
- **Use an email distribution list to keep everyone informed:** When all concerned individuals have full access to the latest developments, unpleasant surprises are minimized.
- **Keep all employees informed:** Although the regular workers might not understand the details of what is happening, they should be informed of the summary points of any planned changes. They will then be much more able to cope with the changes. In addition, they could provide valuable feedback.
- **Ensure that all top managers know what's happening:** This point also can never be understated. This helps prevent unpleasant surprises and the need to redo portions of the planning process.

- **Understand thoroughly the network's TCP/IP infrastructure:** Your understanding helps in designing the network and DNS configuration that is the foundation of the AD DS infrastructure. It is especially true in developing the proper site structure, as will be discussed in Chapter 6, “Configuring Active Directory Sites and Replication.”
- **Develop and adhere to an adequate security policy:** Thoroughly review any security policy that your company already has in place. Apply the policy's constraints to the proper design of your company's domain structure. Make any appropriate changes as you develop the AD DS infrastructure.
- **Know the capabilities of your WAN links:** If your network includes slow WAN links, test and monitor the use of these links before and during the AD DS implementation to ensure that you have the optimum configuration.

Creating Forests and Domains

After you have created a comprehensive plan for your organization's AD DS structure, you are almost ready to begin the installation. The first task that you must perform is to install the first domain controller for the forest root domain.

Requirements for Installing Active Directory Domain Services

Before you can install AD DS, you must have at least one server that meets the following requirements:

Key Topic

- **Operating system:** The server must be running the Foundation, Standard, Enterprise, or Datacenter edition of Windows Server 2008 R2. Note that a server running the Web edition cannot act as a domain controller.
- **Adequate hard disk space:** Beyond the space used for installing Windows Server 2008 R2, the server must have a minimum of 500 MB of disk space for the Active Directory database and SYSVOL folder, plus at least 100 MB for the transaction log files. The larger the proposed network, the more disk space is necessary. And in practical terms, you should have several gigabytes of available space at a minimum. In Windows Server 2008 R2, you should have additional disk space for the following reasons:
 - The online defragmentation process is changed in Windows Server 2008 R2.
 - Windows Server 2008 R2 domain controllers have additional indices on the large link table.
 - The Active Directory Recycle Bin in Windows Server 2008 R2 holds deleted objects and their attributes until cleared.
- **A disk volume formatted with the NTFS file system:** This ensures security of the database; furthermore, it is required for the SYSVOL folder. Windows Server 2008 R2 creates an NTFS partition by default when installed.

TIP It is strongly recommend that you use a fault-tolerant disk volume such as RAID-1 (disk mirroring) or RAID-5 (disk striping with parity) for the Active Directory files. This enables the domain controller to function in the event of a disk failure, until the failed disk can be replaced. However, fault-tolerant disks are no substitute for regular backups of Active Directory. Backups are discussed in Chapter 15, “Maintaining Active Directory.”

- **A DNS server:** Active Directory requires that a DNS server that supports service (SRV) resource records be present. This can be any server running Windows 2000 or later or a UNIX server running Berkeley Internet Name Domain (BIND) 4.9.7 or later. If you want to integrate the DNS database with Active Directory, you should install DNS on the same server that you install AD DS. If the Active Directory Installation Wizard cannot find a suitable DNS server, you will be prompted to install one. DNS is discussed in Chapter 2, “Installing and Configuring DNS for Active Directory,” and Chapter 4, “Configuring DNS Server Settings and Replication.”
- **Administrative privileges:** You must be logged on with an account that has the appropriate administrative privileges. For the first domain controller, this is a local administrator. To add a domain to an existing forest, you must be a member of the Enterprise Admins group in this forest; to add a domain controller to an exiting domain, you must be a member of the Domain Admins or Enterprise Admins group in this domain. Group memberships are discussed in Chapter 9, “Active Directory User and Group Accounts.”

Installing Active Directory Domain Services

As in Windows 2000 and Windows Server 2003, Active Directory provides the Active Directory Installation Wizard (`dcpromo.exe`) that handles all aspects of installing or removing Active Directory. Windows Server 2008 is different from previous Windows Servers in that you install AD DS first and then install a domain controller. You can install AD DS without installing a domain controller if you are configuring your server for a directory-related application such as Exchange Server. This section looks at the use of this wizard for installing different types of domain controllers.

You can start the Active Directory Installation Wizard from the Add Roles Wizard in Server Manager or directly from the `dcpromo.exe` command. The following sections describe the use of the Add Roles Wizard for installing AD DS.

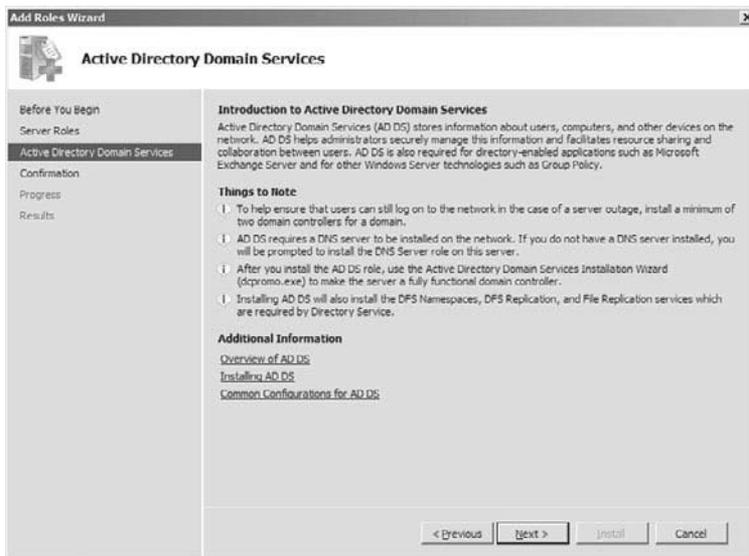
NOTE If you run `dcpromo.exe` without having first installed AD DS, Windows installs this service before starting the Active Directory Installation Wizard.

New Forests

As already noted, the first domain installed is the root domain in its forest. You must be a local administrator on the server on which you install Active Directory to proceed. The following procedure describes the installation of the first domain:

- Step 1.** In the Add Roles Wizard, select **Active Directory Domain Services** and then click **Next**.
- Step 2.** If you receive a message box labeled Add features required for Active Directory Domain Services and asking you to install .NET Framework 3.5.1, click **Add Required Features**.
- Step 3.** The wizard displays the Introduction to Active Directory Domain Services page shown in Figure 3-2. Make note of the points displayed by this page. If you want additional details regarding installation of Active Directory, click any of the links provided. When finished, click **Next**.

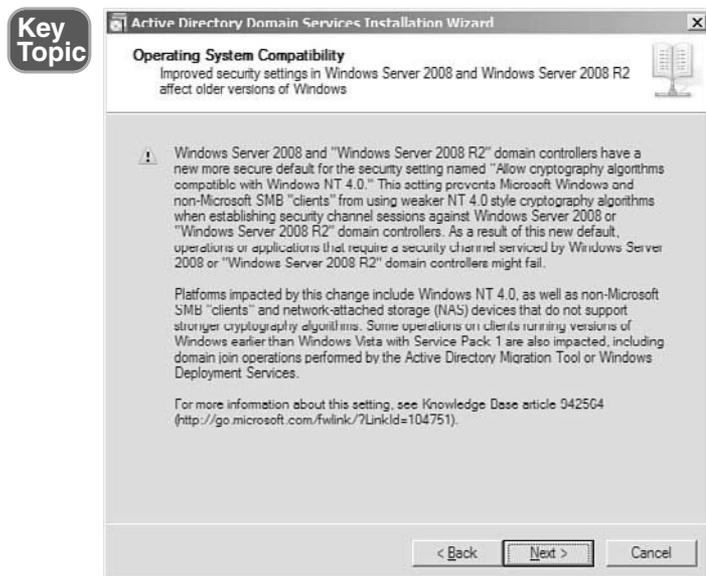
Figure 3-2 You can use the Add Roles Wizard to begin the installation of AD DS.



- Step 4.** Note the information provided on the Confirm Installation Selections page and then click **Install** to begin installing Active Directory.
- Step 5.** The wizard displays an Installation Progress page that charts the progress of installation. After a few minutes, it informs you that the AD DS role has been installed successfully and that you need to launch the Active Directory Domain Services Installation Wizard (dcpromo.exe). Click **Close** to exit the wizard and return to Server Manager.

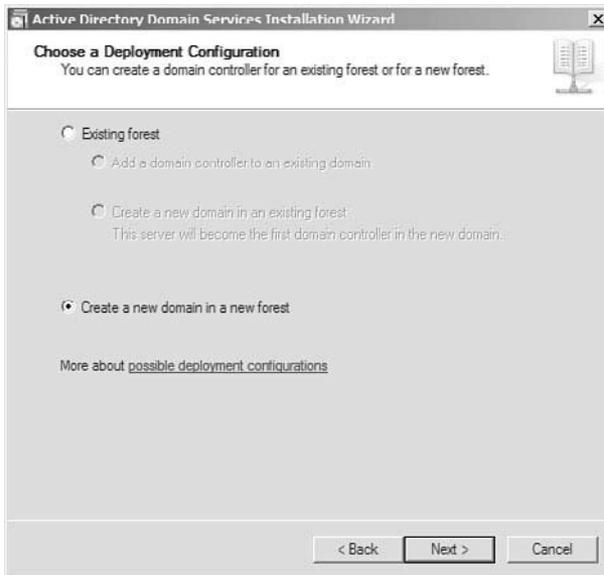
- Step 6.** Scroll down to the Roles Summary section of Server Manager. Note that Active Directory Domain Services is shown as having been installed. A message marked with a red X indicates the number of system services that are not running.
- Step 7.** Click this message. You are informed that the server is not yet running as a domain controller. Click the link provided to start the AD DS Installation Wizard.
- Step 8.** This wizard opens with a Welcome page. Click **Next**.
- Step 9.** The Operating System Compatibility page shown in Figure 3-3 informs you that Windows Server 2008 R2 security settings affect how older versions of Windows communicate with the domain controller. Access the Knowledge Base article quoted for more information. Click **Next** to proceed with AD DS installation.

Figure 3-3 You are informed about security settings that prevent some older Windows clients or non-Windows systems from logging on to the Windows Server 2008 R2 domain controller.



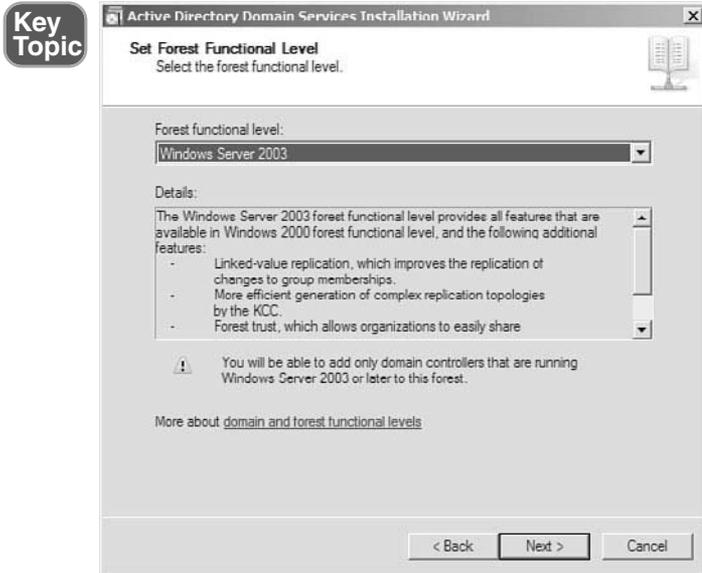
- Step 10.** On the Choose a Deployment Configuration page shown in Figure 3-4, select **Create a new domain in a new forest** and then click **Next**. On this page, you would select the **Existing forest** option when creating a new domain in an existing forest or adding a domain controller to an existing domain. These options are discussed later in this chapter.
- Step 11.** Type the full DNS name of the forest root domain and then click **Next**.

Figure 3-4 The wizard provides options for installing a domain controller in an existing forest or a new one.



NOTE Windows Server 2008 R2 no longer supports the creation of single-label domain names; however, you can still upgrade existing single-label domains to Windows Server 2008 R2. For more information, refer to “Information about configuring Active Directory domains by using single-label DNS names” at <http://support.microsoft.com/kb/300684>.

- Step 12.** The wizard verifies the forest and NetBIOS names and then displays the Set Forest Functional Level page shown in Figure 3-5. Select the appropriate forest functional level and then click **Next**. The available domain and forest functional levels are discussed later in this chapter.
- Step 13.** Select a domain functional level and then click **Next**.
- Step 14.** The Additional Domain Controller Options page provides the following additional options that you can install for the domain controller. Ensure that **DNS Server** is selected and then click **Next**.
- DNS Server:** Installs DNS on this server. This option is selected by default when first installing AD DS because DNS is required for Active Directory.
 - Global Catalog:** Installs a Global Catalog server. This option is not available but selected when installing the first domain controller in any domain because this server must be a global catalog server.

Figure 3-5 The wizard enables you to select from four forest functional levels.

—**Read-Only Domain Controller (RODC)**: Installs an RODC. This option is not available because the first domain controller cannot be an RODC. Installing an RODC is discussed in Chapter 8, “Read-Only Domain Controllers.”

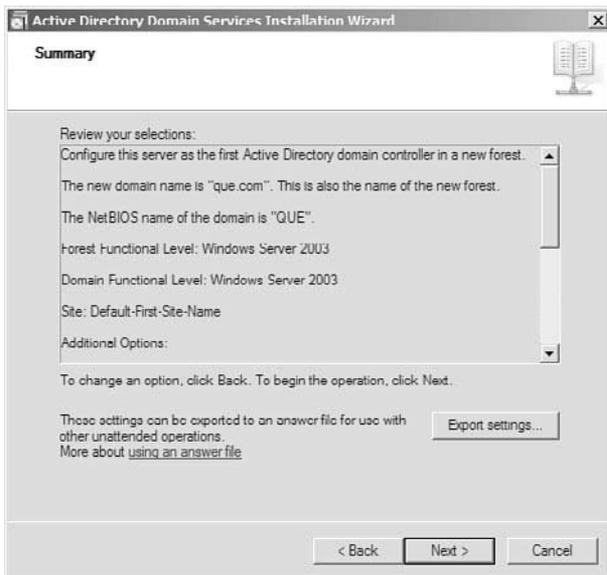
- Step 15.** If the server does not have a statically assigned IP address, you are informed of this fact. A domain controller (and in particular, one that is configured as a DNS server) should always have a statically assigned IP address to ensure that client computers can always reach it. Select **Yes**, **open the IP properties so that I can assign a static IP address to the network adapter**, and then configure an appropriate IP address, subnet mask, default gateway, and default DNS server address.
- Step 16.** If you receive a message informing you that a delegation for the DNS server will not be created, click **Yes** to continue. You might receive this message if you are installing DNS on this server. If so, you should manually create this delegation later.
- Step 17.** Confirm the locations provided for the database, log files, and SYSVOL folders. If you want to change any of these locations, type the desired path or click **Browse**. When finished, click **Next**.

TIP When setting up a domain controller on a production network, it is advisable to place the database and log folders on a separate drive from the SYSVOL folder.

The reason for doing so is to improve only I/O performance; this does not improve security or fault tolerance, as an exam question might lead you to believe.

- Step 18.** On the Directory Services Restore Mode Administrator Password page, type and confirm a secure password. Make a careful note of the password you typed in case you need to use it later and then click **Next**.
- Step 19.** The wizard provides a Summary page as shown in Figure 3-6. Review the information provided on the Summary page. If you want to change any settings, click **Back** and make the appropriate changes. If you want to export information to an answer file, click **Export settings** and provide an appropriate path and filename. Then click **Next** to configure AD DS. This process takes several minutes.

Figure 3-6 The wizard provides a summary page that enables you to review the settings you've specified.



- Step 20.** When the completion page appears, click **Finish** and then click **Restart Now** to reboot your server. To reboot the server automatically, select the **Reboot on Completion** check box.

NOTE The Welcome page of the Active Directory Installation Wizard also contains an Advanced mode option. Select the check box provided to perform any of the following actions:

- Installing a domain controller from backup media created on an existing domain controller
- Modifying the NetBIOS name generated by default
- Selecting a source domain controller when installing an additional domain controller in the domain
- Defining a password replication policy that specifies the passwords cached on a read-only domain controller (RODC)

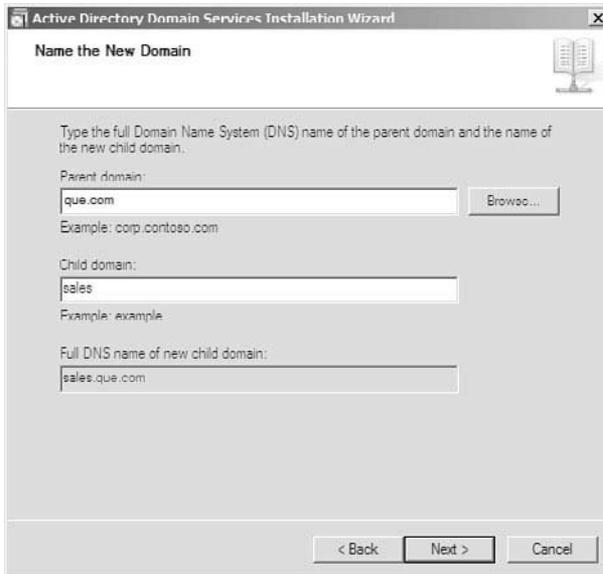
You can also invoke the Advanced mode directly from the `dcpromo` command by including the `/adv` parameter with this command.

New Domains in Existing Forests

After you have installed the forest root domain, you can add additional child domains or domain trees to the forest. Either procedure is similar to the procedure already outlined for creating a forest root domain, as follows:

- Step 1.** Follow the procedure to install AD DS and start the Active Directory Installation Wizard as described in the previous section until you receive the Choose a Deployment Configuration page previously shown in Figure 3-4.
- Step 2.** On this page, select **Existing forest**, and then select **Create a new domain in an existing forest**. Then click **Next**.
- Step 3.** On the Network Credentials page, type the name of the parent domain in which you want to install a child domain. Then click **Set** and specify the username and password of an account with the appropriate privileges described earlier in this chapter and click **Next**.
- Step 4.** On the Name the New Domain page shown in Figure 3-7, type the name of the parent and child domains in the spaces provided. The new domain will be created as a child domain or new tree automatically depending on the name you provide. Then click **Next**.
- Step 5.** On the Set Domain Functional Level page, select the required functional level and then click **Next**. Domain functional levels are discussed later in this chapter.
- Step 6.** On the Select a Site page, select an appropriate site and then click **Next**. Sites are discussed in Chapter 6.
- Step 7.** Complete the installation of the domain controller according to steps 14–20 of the previous procedure.

Figure 3-7 You create a child domain name from the name of the parent domain and the new top-level name on the Name the New Domain page.



Existing Domains

Installing additional domain controllers in an existing domain is important for the following reasons:

Key Topic

- Doing so adds fault tolerance and load balancing to the domain. In other words, additional domain controllers help share the load and improve performance.
- Users logging on to the domain can connect to any available domain controller for authentication.
- Users at a remote location can connect to a domain controller at their site rather than making a slow connection across a WAN link.
- If a domain controller should become unavailable because of a network or hardware failure, users can still log on to the domain.

To install an additional domain controller in an existing domain, follow the same procedure as in the previous section, except select the **Add a domain controller to an existing domain** option shown in Figure 3-4. Then select the proper domain from the Select a Domain page (this page will display all available domains in the forest). The remainder of the procedure is the same as that for creating a new domain in an existing forest, except that the Set Domain Functional Level page does not appear.

Performing Unattended Installations of Active Directory

Key Topic

Windows Server 2008 R2 enables you to specify parameters for Active Directory installation in an answer file that you can use to facilitate the installation of multiple domain controllers. This file is formatted as a simple text file containing the statement [DCINSTALL] on the first line followed by statements in the form *option=value*. Table 3-2 describes several of the more common options you can use in this file:

Table 3-2 Several Options Used for Unattended Domain Controller Installation

Option	Value	Meaning
UserName	Username of administrative user	Installs the domain controller in the context of this user.
Password	User's password *	Specifies the password of the user installing the domain controller. Use * to prompt for the password.
ReplicaOrNewDomain	Domain Replica ReadOnlyReplica	Specifies whether to install a new domain, an additional domain controller (replica) in an existing domain, or an RODC in an existing domain.
ReplicaDomainDNSName	Existing domain name	Specifies the fully qualified domain name (FQDN) of the domain in which you are installing an additional domain controller.
NewDomain	Forest Tree Child	Specifies whether to install a new forest, a new tree in an existing forest, or a child domain.
NewDomainDNSName	Domain name to be created	Specifies the FQDN for a new domain.
ParentDomainDNSName	Parent domain name	Specifies the FQDN of the parent domain when creating a child domain.
ChildName	Child domain name	Specifies the top-level DNS name of the child domain. This name is prefixed to the parent name to create the FQDN of the child domain.

Table 3-2 Several Options Used for Unattended Domain Controller Installation

Option	Value	Meaning
ForestLevel	0 2 3 4	Specifies the forest functional level of a new forest: 0 = Windows 2000 2 = Windows Server 2003 3 = Windows Server 2008 4 = Windows Server 2008 R2
DomainLevel	0 2 3 4	Specifies the domain functional level of a new domain. Parameters have the same meaning as just described.
InstallDNS	Yes No	Specifies whether a DNS server is installed.
ConfirmGC	Yes No	Specifies whether the domain controller is installed as a global catalog server.
DatabasePath	Path to database folder	Default is %systemroot%\NTDS.
LogPath	Path to log folder	Default is %systemroot%\NTDS.
SysvolPath	Path to SYSVOL folder	Default is %systemroot%\SYSVOL.
RebootOnCompletion	Yes No	Specifies whether to restart the computer on completion, regardless of success.

Many additional options are available, including options specific to the demotion of domain controllers. For additional information, consult “Appendix of Unattended Installation Parameters” at [http://technet.microsoft.com/en-us/library/cc732086\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc732086(W.S.10).aspx).

To perform an unattended installation of a domain controller, open a command prompt and type the following command:

```
dcpromo /answer:path_to_answer_file
```

where *path_to_answer_file* specifies the complete path to the unattended answer file containing the parameters specified in Table 3-2. You can also include any of these parameters in the command line by prefixing each of them with the “/” character. The output to the command prompt will track the progress of the

promotion, and then the server will automatically reboot if the `RebootOnCompletion` parameter has been specified.

Server Core Domain Controllers

You cannot use Server Manager or a simple execution of `dcpromo` to promote a Server Core machine to a domain controller. You must use an unattended installation answer file in a similar manner to that described in the previous section. This file must include the information required to identify the domain being joined, including the username and password for a domain administrator account.

NOTE For further information on the use of Server Core, including its use as a domain controller, refer to “Server Core Installation Option of Windows Server 2008 Step-by-Step Guide” at [http://technet.microsoft.com/en-us/library/cc753802\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc753802(W.S.10).aspx).

Removing Active Directory

The Active Directory Installation Wizard also enables you to remove Active Directory from a domain controller, thereby demoting it to a member server. Proceed as follows:

- Step 1.** Click **Start > Run**, type **dcpromo**, and then press **Enter**.
- Step 2.** Windows checks whether Active Directory Domain Services is installed and then displays the Welcome page. Click **Next**.
- Step 3.** If you receive a message warning you of the effects of removing a global catalog server, click **OK**.
- Step 4.** You receive the Delete the Domain page shown in Figure 3-8. Note all the warnings displayed about the effects of removing a domain. Select the check box only if you are removing the last domain controller from its domain and then click **Next**.
- Step 5.** You receive the Application Directory Partitions page if the server holds the last replica of any application directory partitions. Click **Next**, select the check box labeled **Delete all application directory partitions on this Active Directory domain controller**, and then click **Next** again to remove the application directory partitions.
- Step 6.** Type and confirm a password for the local Administrator account on the server, and then click **Next**.
- Step 7.** Read the information provided on the Summary page. If you need to make any changes, click **Back**. When ready, click **Next** to demote the server.

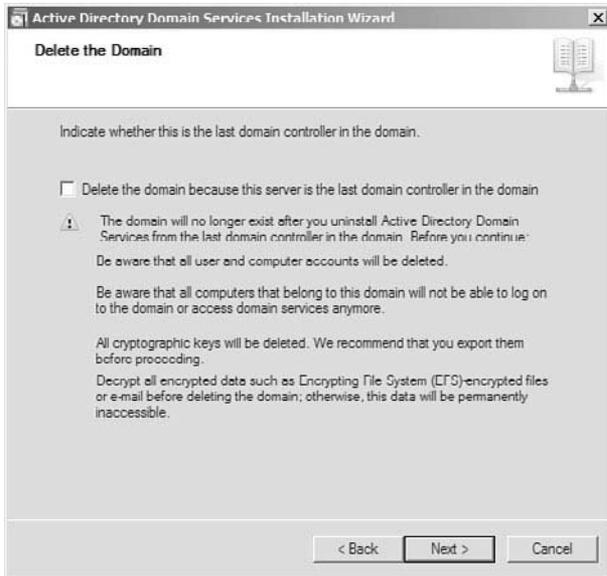


Figure 3-8 When you demote a domain controller, you are warned of the effects of deleting the domain.

- Step 8.** When the demotion is finished, click **Finish** and then click **Restart now** to restart the server. To reboot the server automatically, select the **Reboot on Completion** check box.

NOTE Although this procedure demotes the computer to a member server, it does not remove AD DS. If you want to remove AD DS after demoting the server, use the Remove Roles Wizard available from Server Manager after restarting the server.

Interoperability with Previous Versions of Active Directory

Many organizations have created Active Directory domains based on Windows 2000 or Windows Server 2003 domain controllers and are now in a position to take advantage of the new features of Windows Server 2008 and Windows Server 2008 R2 Active Directory. You can add new Windows Server 2008 domain controllers to an existing older Active Directory forest or upgrade all domain controllers in the forest to Windows Server 2008.

As summarized in Chapter 1, Active Directory in Windows Server 2008 and Windows Server 2008 R2 introduces numerous additional features not supported by previous versions of Windows Server. Many of these features limit the interoperability of Windows Server 2008 with previous versions, and Microsoft has

extended the concept of domain and forest functional levels to define the actions that can be done on a network that includes older domain controllers.

This section looks at these functional levels and the tools used for upgrading an older Active Directory network to Windows Server 2008.

Forest and Domain Functional Levels

As you noticed when installing your first domain controller (refer to Figure 3-5), Table 3-3 summarizes the forest and domain functional levels supported by Active Directory in Windows Server 2008.



Table 3-3 Forest and Domain Functional Levels in Windows Server 2008 R2 Active Directory

Forest Functional Level	Domain Functional Levels Supported	Domain Controllers Supported
Windows 2000 native	Windows 2000 native	Windows 2000
	Windows Server 2003 native	Windows Server 2003
	Windows Server 2008 native	Windows Server 2008
	Windows Server 2008 R2 native	Windows Server 2008 R2
Windows Server 2003 native	Windows Server 2003 native	Windows Server 2003
	Windows Server 2008 native	Windows Server 2008
	Windows Server 2008 R2 native	Windows Server 2008 R2
Windows Server 2008 native	Windows Server 2008 native	Windows Server 2008
	Windows Server 2008 R2 native	Windows Server 2008 R2
Windows Server 2008 R2 native	Windows Server 2008 R2 native	Windows Server 2008 R2

To make use of the functionality provided by Windows Server 2008 Active Directory, you must upgrade all domain controllers to Windows Server 2008 and upgrade the functional levels accordingly. A domain running at the Windows Server 2008 domain functional level located in a forest running at a lower functional level supports domain-based Windows Server 2008 Active Directory features but not forest-based ones.

Furthermore, to make use of the newest Active Directory features in Windows Server 2008 R2, you must upgrade all domain controllers to Windows Server 2008 R2 and upgrade the domain and forest functional levels accordingly.

NOTE You can deploy an RODC to a domain in which the domain and forest functional levels are set to Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

Windows Server 2008 does not support the Windows 2000 mixed functional level previously found in older Active Directory networks. If you still have any domain controllers running Windows NT 4.0, you must upgrade or remove these domain controllers before introducing a Windows Server 2008 or Windows Server 2008 R2 domain controller on your network.

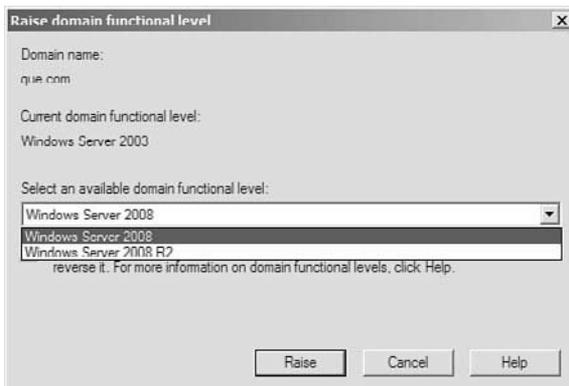
Upgrading Domain and Forest Functional Levels

To raise the forest functional level, you must first raise the functional level of all domains in the forest to the same or higher domain functional level. To raise the domain functional level, perform any of the following three actions:

- Open the Active Directory Administrative Center snap-in, right-click your domain, and then choose **Raise the domain functional level**.
- Open the Active Directory Users and Computers snap-in. Right-click **Active Directory Users and Computers** and choose **All Tasks > Raise domain functional level**.
- Open the Active Directory Domains and Trusts snap-in, right-click your domain, and choose **Raise domain functional level**.

In the dialog box shown in Figure 3-9, select the appropriate functional level and click **Raise**. Then click **OK** to accept the warning that is displayed.

Figure 3-9 Raising the domain functional level.



To raise the forest functional level, access the Active Directory Domains and Trusts snap-in. Right-click **Active Directory Domains and Trusts** and select **Raise forest functional level**. Select the appropriate functional level, click **Raise**, and then click **OK** to accept the warning that is displayed. You can also right-click your domain name in the Active Directory Administrative Center and choose **Raise the forest functional level** and then follow the same procedure described here.

WARNING It is important to remember that raising forest and domain functional levels is a one-way operation. You cannot go back to a lower functional level. In addition, you cannot introduce an older domain controller after you have raised the domain functional level.

NOTE For additional information on domain and forest functional level upgrades, refer to “Identifying Your Functional Level Upgrade” at [http://technet.microsoft.com/en-us/library/cc754209\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc754209(WS.10).aspx).

**Key
Topic**

The **Adprep** Utility

Microsoft provides the **Adprep** utility to prepare a down-level Active Directory domain for receiving Windows Server 2008 and Windows Server 2008 R2 domain controllers. Found in the `\sources\adprep` folder of the installation DVD-ROM, this tool prepares the forest and domain by extending the Active Directory schema and updating several required permissions.

Running the **Adprep /forestprep** Command

You must run the `Adprep /forestprep` command on the schema master of the forest first. It extends the schema to receive the new Windows Server 2008 enhancements, including the addition of directory descriptors for certain objects including granular password policies. You have to run this command and let its changes replicate throughout the forest before you run the `Adprep /domainprep` command. To run this command, you must be a member of the Enterprise Admins, Schema Admins, and Domain Admins groups in the forest root domain.

WARNING Before running this command, ensure that any Windows 2000 domain controllers are upgraded to SP2 or later, or at least to SP1 with hotfix QFE265089. Refer to Microsoft Knowledge Base article 331161 for more information.

Running the **Adprep /domainprep** Command

Run the `Adprep /domainprep` command on the infrastructure master of each domain in which you plan to introduce Windows Server 2008 domain controllers. It adjusts access control lists (ACLs) on Active Directory objects and on the `sysvol` shared folder for proper access by Windows Server 2008 domain controllers. To run this command, you must be a member of the Domain Admins group in the respective domain and the domain must be operating at the Windows 2000 Server native mode or higher.

You can also run the `Adprep /domainprep /prep` command to include updates required for enabling Resultant Set of Policy (RSOP) planning mode functionality.

TIP Remember that you must run `adprep /forestprep` on the schema master and that you must run this command before you run `adprep /domainprep`. Also remember that you must run `adprep /domainprep` on the infrastructure master of each domain in which you want to introduce a Windows Server 2008 domain controller and that you must complete these commands before promoting or upgrading an existing domain controller.

Upgrading a Windows Server 2003 Domain Controller

You can also upgrade an existing Windows Server 2003 domain controller to Windows Server 2008. See Appendix B, “Installing Windows Server 2008 R2,” for information on upgrading Windows Server 2003 computers; the procedure outlined in this chapter automatically upgrades AD DS to Windows Server 2008. However, you cannot upgrade a Windows 2000 domain controller to Windows Server 2008 directly; you must first upgrade to Windows Server 2003 and then to Windows Server 2008.

Note that to upgrade a Windows Server 2003 domain controller to Windows Server 2008, you must first run the `Adprep` utility as already discussed to upgrade the schema for accepting Windows Server 2008 domain controllers.

You can upgrade a Windows Server 2003 domain controller to Windows Server 2008 R2, provided the server meets the hardware requirements discussed in Appendix B.

Before upgrading the first Windows Server 2003 domain controller, ensure that you have run the `Adprep /forestprep` and `Adprep /domainprep` commands and that these commands have completed without error. Then select the **Install now** command from the Welcome screen displayed by the Windows Server 2008 R2 DVD-ROM, and follow the instructions provided by the Installation Wizard and summarized in Appendix B, “Memory Tables”.

Additional Forest and Domain Configuration Tasks

This section introduces two additional configuration tasks specified in the Exam 70-640 objectives for configuring a forest or domain: use of the Active Directory Migration Tool (ADMT) v.3.1 and the alternative user principal name (UPN) suffix. Before introducing these tasks, we take a quick look at some procedures that verify that AD DS has been properly installed and, in doing so, introduce some of the administrative tools included with AD DS.

Verifying the Proper Installation of Active Directory

After you have installed Active Directory, there are several steps you should perform to verify that the proper components have been installed. Click **Start > Administrative Tools**. On a Windows Server 2008 R2 computer, you should see links to five Active Directory management tools: Active Directory Administrative Center, Active Directory Domains and Trusts, Active Directory Module for Windows PowerShell, Active Directory Sites and Services, and Active Directory Users and Computers. You should also see a link to the DNS snap-in unless you have specified another server as the DNS server for your domain.

Open Active Directory Users and Computers. You should see the default containers Builtin, Computers, ForeignSecurityPrincipals, Managed Service Accounts, and Users under the domain you have created. You should also see a default Domain Controllers OU. Select this OU and verify that computer accounts for all domain controllers in the domain are present, as shown in Figure 3-10.

On a Windows Server 2008 R2 computer, open Active Directory Administrative Center. As shown in Figure 3-11, this new MMC snap-in enables you to perform a large range of administrative tasks on your domain, including the following:

- Creating and managing user, group, and computer accounts
- Creating and managing OUs and other Active Directory containers
- Managing other trusted AD DS domains
- Using query-building searches to filter AD DS data

Uses of this tool will be discussed throughout this *Cert Guide* as appropriate, together with references to tools used on Windows Server 2008 computers that are not running R2.

Figure 3-10 After installing Active Directory, you should see a default set of containers in the Active Directory Users and Computers, together with domain controller computer accounts in the Domain Controllers OU.

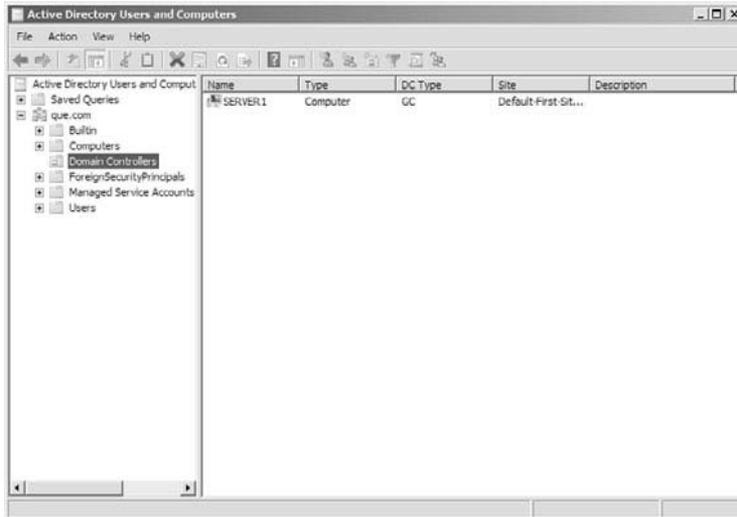


Figure 3-11 Windows Server 2008 R2 adds the Active Directory Administrative Center to the suite of tools provided for administering AD DS.



NOTE In this discussion and elsewhere in this book, the term *Windows Server 2008* is taken to include both the original and R2 versions unless otherwise noted. The term *Windows Server 2008 R2* is used when referring to new features added with this version of the server software.

The Active Directory Administrative Center is installed automatically when you install the AD DS server role in Windows Server 2008 R2. You can also install this tool on a Windows Server 2008 R2 member server or a Windows 7 computer by installing the Remote Server Administration Tools (RSAT) feature. You cannot, however, install Active Directory Administrative Center on a computer running the original version of Windows Server 2008 or on older versions of Windows Server.

NOTE For an overview of the capabilities of the Active Directory Administrative Center, refer to “What’s New in AD DS: Active Directory Administrative Center” at [http://technet.microsoft.com/en-us/library/dd378856\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd378856(Ws.10).aspx).

Active Directory Migration Tool v.3.1

ADMT v.3.1 is the most recent version of a utility, available for download from the Microsoft website, which assists you in migrating objects such as users, groups, and computers between Active Directory domains in the same forest or in different forests. This tool assists you in the potentially difficult task of restructuring your AD DS forest structure; for example, when changes in your organization’s business structure occur because of mergers, acquisitions, or divestitures. You can migrate these objects from a source domain running at any functional level of Windows 2000 native or higher to a target domain running at any functional level of Windows 2000 native or higher. If the source and target domains are in different forests, you must configure trust relationships between the domains in use to ensure data security during the migration process.

Actions performed by ADMT include the following:

- Ensures security of objects being migrated by using 128-bit encryption with the Passport Export Server (PES) service
- Preserves the SID history of objects being migrated
- Enables migration of user profiles
- Migrates computer accounts including domain controllers
- Enables the restructuring of Active Directory domains between forests
- Enables you to use a preconfigured SQL database to hold migration information
- Enables you to perform test migrations so that you can ensure the actual migration will run properly
- Provides a log file that you can check for migration errors and other problems
- Provides for rollback options in the event that the migration does not proceed properly
- Facilitates the decommissioning of old domains in forests to be removed

NOTE If you are migrating from or restructuring Windows NT 4.0 domains to Active Directory, you should use the 3.0 version of ADMT. You can use version 3.0 when restructuring a series of Windows NT 4.0 domains (such as account and resource domains structured into a multiple trust model) into a single Active Directory domain. Version 3.0 runs on Windows 2000 and Windows Server 2003 computers only; it does not run on Windows Server 2008 computers.

ADMT 3.1 runs on a server running the original edition of Windows Server 2008 only; it does not run on Windows Server 2008 R2. To use ADMT 3.1, navigate to <http://www.microsoft.com/downloads/details.aspx?familyid=AE279D01-7DCA-413C-A9D2-B42DFB746059&displaylang=en> and click the **Download** button. Then follow the instructions provided to download and save the `admtsetup31.exe` file to an appropriate location on your computer. Double-click the file, click **Run**, and then follow the instructions provided to install ADMT 3.1.

NOTE For more information on ADMT 3.1, refer to “ADMT v3.1 Guide: Migrating and Restructuring Active Directory Domains” at <http://www.microsoft.com/downloads/en/confirmation.aspx?familyId=6d710919-1ba5-41ca-b2f3-c11bcb4857af&displayLang=en>. For information on use of ADMT 3.1 in domains with Windows Server 2008 R2 domain controllers, refer to “Known issues that may occur when you use ADMT 3.1 to migrate to a domain that contains Windows Server 2008 R2 domain controllers” at <http://support.microsoft.com/kb/976659>.

Alternative User Principal Name Suffixes

As mentioned earlier in this chapter, a UPN is a logon name specified in the format of an email address such as `user@examcram.com`. It is a convenient means of logging on to a domain from a computer located in another domain in the forest or a trusted forest. Two types of UPNs are available:

- **Implicit UPN:** This UPN is always in the form `user@domain`, such as `peter@sales.que.com`. It is defined on the Account tab of a user’s Properties dialog box in Active Directory Users and Computers.
- **Explicit UPN:** This UPN is in the form `string1@string2`, where an administrator can define values for each string. For example, a user named Peter in the `sales.que.com` domain could have an explicit UPN in the form `peter@sales`. Using explicit UPNs is practical when an organization does not want to reveal its internal domain structure.

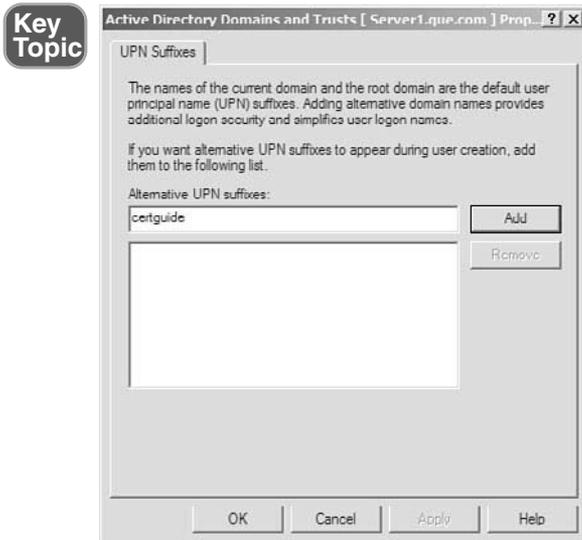
Windows Server 2008 supports the principle of the UPN suffix, first introduced in Windows Server 2003. This is the portion of the UPN to the right of the at (@) character. By default, the UPN suffix is the DNS domain name of the domain in which the user account is located.

Adding an alternative UPN suffix provides several advantages:

- You can use a common UPN suffix across all users in a forest. This is especially useful if some users have long domain names.
- The UPN suffix enables you to conceal the actual domain structure of the forest from external users.
- You can use separate UPN suffixes in situations where different divisions of a company have separate email domain names, thereby enabling users to log on with a name that matches their email address.

To define an alternative UPN suffix, access Active Directory Domains and Trusts from the Administrative Tools folder. Right-click **Active Directory Domains and Trusts** and click **Properties**. From the Properties dialog box shown in Figure 3-12, type the name of the alternative UPN suffix desired, click **Add**, and then click **OK**. After you have done this, the alternative UPN suffix is available when you are configuring new or existing user accounts. For more information on configuring user accounts, see Chapter 9.

Figure 3-12 You can configure alternative UPN suffixes from the Active Directory Domains and Trusts Properties dialog box.



Exam Preparation Tasks

Review All the Key Topics



Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 3-4 lists a reference of these key topics and the page numbers on which each is found.

Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
List	Lists important guidelines you should follow in preparing to install AD DS	80
List	Summarizes requirements for installing AD DS	81
Figure 3-2	You use the Add Roles Wizard to begin the installation of AD DS	83
Figure 3-3	Displays important security considerations when installing AD DS	84
Figure 3-5	Selecting a forest functional level	86
List	Summarizes important reasons for installing multiple domain controllers in a domain	89
Paragraph	Describes the methods of performing unattended installations of AD DS	90
Table 3-3	Summarizes available forest and domain functional levels in Windows Server 2008 R2	94
Paragraph	Describes the adprep utility used for preparing forests and domains for upgrade	96
Figure 3-12	Specifying additional UPN suffixes	102

Complete the Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

Definitions of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary.

Active Directory Migration Tool (ADMT), Active Directory Administrative Center, Adprep, dcpromo, domain controller (DC), domain functional level, forest functional level, forest root, read-only domain controller (RODC), Server Core, universal principal name (UPN), universal principal name (UPN) suffix

This page intentionally left blank



Index

A

A and AAAA (host) resource records, 61

AboveNormal priority level, 465

access

denying, 308–309

shell access policies, 387

account lockout policy, 426–427

account partners, 231

account policies, 422

account lockout policy, 426–427

“Do I Know This Already?” quiz, 417–421

domain password policies, 423, 425

exam preparation task, 449–450

Kerberos policy, 428

unlocking accounts, 427

“Account Policies” (article), 428

account stores, creating, 240–241

accounts

account lockout policy, 426–427

AD LDS accounts, creating, 222–223

delegating administrative control, 313–316

group accounts

configuring group membership, 304–305

creating manually, 288–290

creating with Cvsde tool, 292–293

creating with Dsadd tool, 294–295

creating with Ldifde tool, 293–294

creating with scripts, 296

denying access, 308–309

deprovisioning, 313

“Do I Know This Already?” quiz, 281–285

exam preparation tasks, 317–318

explained, 287

local versus domain groups, 310–312

nesting with AGDLP/AGUDLP, 306–307

template accounts, 290–291

unlocking, 427

user accounts

contact, 298–299

creating manually, 288–290

creating with Cvsde tool, 292–293

creating with Dsadd tool, 294–295

creating with Ldifde tool, 293–294

creating with scripts, 296

deprovisioning, 312–313

distribution lists, 299–300

“Do I Know This Already?” quiz, 281–285

exam preparation tasks, 317–318

explained, 286

Protected Admin accounts, 309–310

resetting, 308

UPNs (user principal names), 296–298

Active Directory

AD CS (Active Directory Certificate Services). *See* AD CS

AD DS (Active Directory Domain Services). *See* AD DS

- AD FS (Active Directory Federation Service). *See* AD FS
- AD LDS (Active Directory Lightweight Directory Service). *See* AD LDS
- AD MDS (Active Directory Metadirectory Services), 231
- AD RMS (Active Directory Rights Management Service), *See* AD RMS
- audits
 - configuring with Auditpol.exe*, 447, 449
 - configuring with GPOs*, 442–447
 - “Do I Know This Already?” quiz*, 417–421
 - exam preparation task*, 449–450
 - new features*, 441–442
- backing up
 - backup permissions*, 521
 - critical volumes of domain controllers*, 522–524
 - GPOs (Group Policy Objects)*, 545, 548
 - to removable media*, 527
 - scheduling backups*, 526–527
 - wbadmin utility*, 525
 - Windows Server 2008 versus Windows Server 2008 R2*, 520–521
 - Windows Server Backup installation*, 521–522
- classes. *See* classes
- containers, explained, 24
- domains
 - administrative and geographical organization of*, 78–79
 - application directory partition reference domains*, 139
 - benefits of multiple domains*, 26–27
 - best practices*, 80–81
 - domain controllers*, 26, 31, 33
 - explained*, 26, 31
 - forests*, 27
 - functional levels*, 94–96
 - installing domain controllers in existing domains*, 89
 - installing new domains in existing forests*, 88
 - multiple trees*, 79
 - ntds.dit files*, 26
 - offline domain join*, 38
 - RODCs (read-only domain controllers)*, 33
 - trees*, 27
- flexible single-master operations (FSMO) servers, 32–33
- forests
 - functional levels*, 94–96
 - installation*, 83–87
 - installing new domains in*, 88
- foundations
 - LDAP (Lightweight Directory Access Protocol)*, 18–19
 - X.500*, 17–18
- GC (global catalog) servers
 - features*, 148
 - partial attribute sets*, 152–153
 - placement*, 148–150
 - promoting domain controllers to*, 150
 - removing*, 151
 - UGMC (Universal Group Membership Caching)*, 151
- global catalogs
 - “Do I Know This Already?” quiz*, 143–147
 - exam preparation tasks*, 169–170
 - explained*, 24–25, 31
 - global catalog servers*, 31–32
- group accounts
 - configuring group membership*, 304–305
 - creating manually*, 288–290
 - creating with Csvde tool*, 292–293
 - creating with Dsadd tool*, 294–295
 - creating with Ldifde tool*, 293–294
 - creating with scripts*, 296
 - delegating administrative control*, 313–316

- denying access*, 308–309
- deprovisioning*, 313
- “Do I Know This Already?” quiz*, 281–285
- exam preparation tasks*, 317–318
- explained*, 287
- local versus domain groups*, 310–312
- nesting with AGDLP/AGUDLP*, 306–307
- Group Policy, 34
- installation, 82
 - Active Directory Migration Tool (ADMT) v.3.1*, 100–101
 - alternative UPN (user principal name) suffixes*, 101–102
 - “Do I Know This Already?” quiz*, 73–76
 - domain controllers in existing domains*, 89
 - domains*, 78–81, 88
 - exam preparation tasks*, 103–104
 - namespaces*, 77–78
 - new forests*, 83–87
 - requirements*, 81–82
 - Server Core domain controllers*, 92
 - unattended installations*, 90–92
 - verifying*, 98, 100
- interoperability with previous versions of Active Directory, 93
 - Adprep utility*, 96–97
 - forest and domain functional levels*, 94–96
 - upgrading Windows Server 2003 domain controllers*, 97
- namespaces
 - contiguous namespaces*, 23
 - disjointed namespaces*, 23
 - explained*, 22
 - flat namespaces*, 23
 - hierarchical namespaces*, 23
 - planning*, 77
 - subdividing*, 77–78
- naming standards
 - canonical names*, 22
 - DNs (distinguished names)*, 19–20
 - GUIDs (globally unique identifiers)*, 21
 - RDNs (relative distinguished names)*, 20–21
 - SIDs (security identifiers)*, 21–22
 - UPNs (user principal names)*, 21
- new features in Windows Server 2008, 33–34
- objects. *See* objects
- operations masters, 153
 - “Do I Know This Already?” quiz*, 143–147
 - domain naming masters*, 160
 - exam preparation tasks*, 169–170
 - failures*, 164–165
 - infrastructure masters*, 162
 - PDC emulators*, 160–162
 - placement*, 163–164
 - RID masters*, 162
 - schema masters*, 153–160
 - seizing operations master roles*, 167–168
 - transferring operations master roles*, 165–167
- OUs (organizational units), explained, 29–30
- partitions
 - application partitions*, 25
 - configuration partitions*, 25
 - domain partitions*, 25
 - explained*, 25
 - schema partitions*, 25
- passwords, 34
- recovering. *See also* Recycle Bin
 - authoritative restore*, 536–537
 - authoritative restore of group memberships*, 539
 - Directory Services Restore Mode (DSRM)*, 528–529
 - explained*, 528
 - full-server recovery of domain controllers*, 538–539
 - GPOs (Group Policy Objects)*, 545, 547–548
 - linked-value replication*, 539

- nonauthoritative restore*, 529–534
- recovering back-links of authoritatively restored objects*, 537
- wbadmin command*, 534–535
- Recycle Bin, 37
 - enabling*, 541–543
 - explained*, 540–541
 - restoring deleted objects*, 543–545
- removing, 92–93
- replication
 - bridgehead servers*, 193–194
 - DFS (Distributed File System)*, 192–193
 - “Do I Know This Already?” quiz, 173–177
 - exam preparation tasks*, 201–202
 - explained*, 190–191
 - forcing*, 200–201
 - intersite replication*, 191, 195–201
 - intrasite replication*, 191, 198–199
 - multi-master replication*, 190
 - one-way replication*, 193
 - ports*, 195
 - replication protocols*, 194–195
 - scheduling*, 196–199
- restarting, 549–550
- schemas, 24
- security enhancements, 34
- Server Core, 33
- Server Manager
 - adding roles and features*, 36
 - capabilities*, 36
 - command-line server management*, 36
 - opening*, 35
- server roles, 33. *See also* specific roles
 - “Do I Know This Already?” quiz, 205–209
 - exam preparation tasks*, 247–248
 - installing*, 211
 - removing*, 211
 - role services*, 210
- sites
 - benefits of*, 178–179
 - creating*, 180–181
 - “Do I Know This Already?” quiz, 173–177
 - domain controllers, adding*, 181
 - exam preparation tasks*, 201–202
 - explained*, 30, 178
 - ISTG (Intersite Topology Generator)*, 189
 - KCC (Knowledge Consistency Checker)*, 189
 - planning*, 179
 - site link bridges*, 185
 - site links*, 184–188
 - subnets*, 182–184
- trust relationships
 - authentication scope*, 338–340
 - defined*, 325
 - “Do I Know This Already?” quiz, 321–324
 - exam preparation tasks*, 343
 - external trusts*, 326, 335–336
 - forest trusts*, 326, 329–330, 332–335
 - prerequisites*, 328–329
 - realm trusts*, 326, 336
 - removing cross-forest trust relationships*, 341–342
 - shortcut trusts*, 327, 337
 - SID filtering*, 340–341
 - table of trust types*, 328
 - transitive trusts*, 325–326
 - validating*, 338
- user accounts
 - contact*, 298–299
 - creating manually*, 288–290
 - creating with Csvde tool*, 292–293
 - creating with Dsadd tool*, 294–295
 - creating with Ldifde tool*, 293–294
 - creating with scripts*, 296
 - delegating administrative control*, 313–316
 - deprovisioning*, 312–313
 - distribution lists*, 299–300
 - “Do I Know This Already?” quiz, 281–285
 - exam preparation tasks*, 317–318
 - explained*, 286
 - Protected Admin accounts*, 309–310

- resetting*, 308
- template accounts*, 290–291
- UPNs (user principal names)*, 296–298
- Windows Server 2008 R2 virtualization, 244–246
- zones
 - configuring zone transfers*, 132–133
 - DNS notify*, 133–134
 - full zone transfer (AXFR)*, 130
 - incremental zone transfer (IXFR)*, 131
 - replication scope*, 128–130
 - secure zone transfer*, 134–136
- Active Directory Administrative Center (ADAC)**, 38
- “Active Directory Backup and Restore in Windows Server 2008” (article)**, 526
- Active Directory Certificate Services.**
See AD CS
- Active Directory Domain Services Installation Wizard**, 258–259
- Active Directory Federation Service.**
See AD FS
- “Active Directory Federation Services Role” (article)**, 233
- Active Directory Installation Wizard**, 82
 - installing domain controllers in existing domains, 89
 - installing new domains in existing forests, 88
 - installing new forests, 83–87
- Active Directory Lightweight Directory Service.** *See AD LDS*
- Active Directory Management Pack**, 38
- Active Directory Metadirectory Services (AD MDS)**, 231
- Active Directory Migration Tool (ADMT) v.3.1**, 100–101
- “Active Directory Recycle Bin Step-by-Step Guide” (article)**, 545
- “Active Directory Replication over Firewalls” (article)**, 195
- Active Directory Rights Management Service.** *See AD RMS*
- “Active Directory Rights Management Services Overview” (article)**, 226
- Active Directory Schema snap-in**, 220
- Active Directory Sites and Services snap-in**, 179, 221
 - adding domain controllers, 181
 - creating sites, 180–181
 - creating subnets, 182–184
- Active Directory Web Services**, 38
- AD CS (Active Directory Certificate Services)**, 34
 - certificate practice statements, 572–573
 - certificate requests, 571–572
 - certificate revocation
 - Authority Information Access (AIA)*, 624–625
 - certificate revocation lists (CRLs)*, 617, 619–621
 - explained*, 616–617
 - online responders*, 621–624
 - certificate stores, 575
 - certificate templates
 - archiving keys*, 599
 - configuring*, 593–595
 - defined*, 592
 - duplicating*, 597–598
 - enabling*, 597
 - key recovery agents (KRAs)*, 599–602
 - permissions*, 595–597
 - template types*, 592
- Certification Authority Web Enrollment**
 - configuring smart card enrollment*, 609–610
 - configuring Web enrollment*, 606–607
 - creating enrollment agents*, 610–613

- enabling certificate autoenrollment, 605–606*
- Network Device Enrollment Services (NDES), 602–604*
- configuration
 - assigning administration roles, 581–582*
 - assigning certificate server permissions, 582–583*
 - backing up and restoring certificate databases, 580–581*
 - backing up certificates and keys, 576–577*
 - enabling credential roaming, 578–580*
 - importing certificates, 575–576*
 - restoring certificates and keys, 577–578*
- “Do I Know This Already?” quiz, 559–562, 587–591
- exam preparation tasks, 583–584, 625–626
- explained, 210
- installation, 565
 - certificate authority types and hierarchies, 565–567*
 - Certificates snap-in, 573–574*
 - root CAs, 567–568, 570–571*
 - subordinate CAs, 571*
- new features, 563–565
- “AD CS: Restricted Enrollment Agent” (article), 614**
- AD DS (Active Directory Domain Services)**
 - database storage allocation, 553–554
 - defragmentation
 - offline defragmentation, 551–552*
 - online defragmentation, 551*
 - monitoring. *See* monitoring Active Directory
 - restarting, 549–550
- “AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide” (article), 436**
- AD DS Installation Wizard, 256–257**
- AD FS (Active Directory Federation Service)**
 - explained, 210, 231–232
 - federation trust configuration, 238
 - account stores, 240–241*
 - claims, 239*
 - creating federation trusts, 242–243*
 - enabling applications, 241–242*
 - installing, 233–236
 - role services, 232–233
 - trust policy configuration, 236–237
 - user and group claim mapping, 237–238
 - Web agents, 233
- “AD FS in Windows Server 2008 R2 Step-by-Step Guide” (article), 243**
- AD LDS (Active Directory Lightweight Directory Service), 34**
 - AD LDS security principal, 223
 - binding to AD LDS instances, 222, 224
 - configuration, 217
 - with Active Directory Schema snap-in, 220*
 - with Active Directory Sites and Services snap-in, 221*
 - with ADSI Edit snap-in, 217–218*
 - with Ldp.exe, 218–220*
 - creating AD LDS user accounts and groups, 222–223
 - explained, 210–213
 - installation, 213
 - AD LDS instances, 214–216*
 - AD LDS roles, 213*
 - migrating to, 221
 - on Server Core, 224–225
- AD LDS Administrators page (Lightweight Directory Services Setup Wizard), 215**
- “AD LDS Getting Started Step-by-Step Guide” (article), 217**

- AD MDS (Active Directory Metadirectory Services), 231**
- AD RMS (Active Directory Rights Management Service), 34**
 - benefits of, 225–226
 - certificate request and installation, 228–230
 - delegation, 230–231
 - enhancements to, 226
 - explained, 210
 - installing, 226–228
 - self-enrollments, 230
- AD RMS Auditors administrative role, 230**
- AD RMS Enterprise Administrators administrative role, 230**
- “AD RMS Prerequisites” (article), 228**
- “AD RMS Step-by-Step Guide” (article), 228**
- AD RMS Template Administrators administrative role, 230**
- ADAC (Active Directory Administrative Center), 38**
- Add Counters dialog box, 477, 479**
- Add Items dialog box, 524**
- Add Monitored Server Wizard, 487, 489–491**
- add nc replica command, 139**
- Add or Remove Snap-ins dialog box, 574**
- add parameter (repadmin utility), 492–493**
- Add Revocation Configuration Wizard, 623**
- Add Role Services Wizard, 603**
- Add Roles Wizard, 36, 83**
 - installing CAs with, 567–571
- Add Upgrade Package dialog box, 407–408**
- Additional Domain Controller Options page (Active Directory Domain Services Installation Wizard), 259**
- Additional Domain Controller Options page (Active Directory Installation Wizard), 85**
- administration**
 - authentication lists, 275–276
 - DNS servers, 69–70
- administration roles, assigning, 581–582**
- administrative control, delegating, 313–316**
- administrative organization of domains, 78–79**
- “Administrative Template Settings” (article), 384**
- administrative templates, 380–384**
- administrator role separation, 261–262**
- ADMIT (Active Directory Migration Tool) v.3.1, 100–101**
- ADMX central store, 379–380**
- ADMX format, 354**
- Adprep utility, 96**
 - Adprep /domainprep command, 97
 - Adprep /forestprep command, 96
 - Adprep /rodcprep command, 255
- ADSI Edit snap-in, 217–218**
- Advanced Password Replication Policy dialog box, 275–276**
- “Advanced Security Audit Policy Settings” (article), 447**
- Advanced Security Settings dialog box, 316**
- Advanced tab (Properties dialog box), 123**
 - Disable Recursion setting, 125
 - Enable automatic scavenging of stale records setting, 126

- Loading Zone Data setting, 126
- Name Checking setting, 125–126
- Round Robin setting, 124–125
- Server Options, 123–124
- Advanced tab (Software Installation Properties dialog box), 404**
- Advertising test (dcdiag utility), 495**
- AGDLP strategy, 306–307**
- agents, creating enrollment agents, 610–613**
- AGUDLP strategy, 306–307**
- AIA (Authority Information Access), configuring, 624–625**
- allocating database storage, 553–554**
- alternative UPN (user principal name) suffixes, 101–102**
- Answer files, 770**
- answers to “Do I Know This Already?” quizzes**
 - chapter 2, 729–731
 - chapter 3, 731–732
 - chapter 4, 732–734
 - chapter 5, 735–736
 - chapter 6, 737–739
 - chapter 7, 739–741
 - chapter 8, 741–743
 - chapter 9, 743–745
 - chapter 10, 745–747
 - chapter 11, 747–749
 - chapter 12, 749–751
 - chapter 13, 751–753
 - chapter 14, 754–756
 - chapter 15, 756–758
 - chapter 16, 758–759
 - chapter 17, 759–761
- answers to practice exam, 691–727**
- Application Directory Partition page (Lightweight Directory Services Setup Wizard), 215**
- application directory partitions, 25, 138–139**
 - application directory partition reference domains, 139
 - creating application directory partition replicas, 139
 - installing and configuring, 138–139
- application priority, configuring, 465**
- archiving keys, 599**
- arrays, configuring, 624**
- assigning**
 - administration roles, 581–582
 - certificate server permissions, 582–583
 - software to computers/users, 399
- attributes, 23, 154**
- Auditpol.exe, 447, 449**
- audits**
 - configuring with Auditpol.exe, 447, 449
 - configuring with GPOs, 442
 - advanced auditing policies, 446–447*
 - available auditing categories, 442–443*
 - basic auditing policies, 443–445*
 - “Do I Know This Already?” quiz, 417–421
 - exam preparation tasks, 449–450
 - new features, 441–442
- authentication**
 - scope, 338–340
 - smart cards, implementing, 609–610, 612–615
- authentication lists, administration, 275–276**
- authentication servers, configuration**
 - binding to AD LDS instances, 222, 224
 - creating AD LDS user accounts and groups, 222–223
- authoritative restore, 536–537**

authoritative restore of group memberships, 539
 authoritative secondary servers, adding to zones, 63
 Authority Information Access (AIA), configuring, 624–625
 autoenrollment, 605–606
 automating Windows Server 2008 R2 installation, 770–771
 AXFR (full zone transfer), 130

B

Back Up Group Policy Object dialog box, 545
 back-links of authoritatively restored objects, recovering, 537
 BackupAllGPOS.wsf, 548
 BackupGPO.wsf, 548
 backups

- backup permissions, 521
- of certificate databases, 580–581
- of certificates and keys, 576–577
- critical volumes of domain controllers, 522–524
- GPOs (Group Policy Objects), 545, 548
- to removable media, 527
- scheduling, 526–527
- wbadmin utility, 525
- Windows Server 2008 versus Windows Server 2008 R2, 520–521
- Windows Server Backup installation, 521–522

 batch files, 296
 BelowNormal priority level, 465
 Berkeley Internet Name Domain (BIND), 124
 best practices, domain structure, 80–81

Best Practices Analyzer (BPA), 38
 BIND (Berkeley Internet Name Domain), 124
 binding to AD LDS (Active Directory Lightweight Directory Service) instances, 222, 224

BitLocker

- enabling, 265–269
- explained, 263–264
- managing, 269–270
- preparing for, 265
- turning off, 269

Block Inheritance setting (GPOs), 369

boot option (Gpupdate), 511

BPA (Best Practices Analyzer), 38

BranchCache, 39

bridgehead servers, 193–194

bulk import, creating accounts with, 291–292

- Csvde tool, 292–293

- Dsadd tool, 294–295

- Ldifde tool, 293–294

- scripts, 296

C

c parameter (dcdiag utility), 495

cache.dns file, 117

caching, credential caching, 273–275

caching-only servers, 56

canonical names, 22

CAs (Certificate Authorities)

- Certification Authority Web Enrollment

- configuring smart card enrollment, 609–610*

- configuring Web enrollment, 606–607*

- creating enrollment agents, 610–613*

enabling certificate autoenrollment,
605–606
Network Device Enrollment Services
(NDES), 602–604

enterprise CAs, 565
intermediate CAs, 566
issuing CAs, 566
root CAs, 566
standalone CAs, 566
subordinate CAs, installing, 571
three-tier CA hierarchy, 566
two-tier CA hierarchy, 566

catalogs. *See* **global catalogs**

Categories tab

Software Installation Properties dialog
box, 405
Software Package Properties dialog
box, 406

CDPs (CRL distribution points), configuring, 619–620

Certificate Authorities. *See* **CAs**

certificate databases, backing up and restoring, 580–581

Certificate Export Wizard, 576–577

Certificate Import Wizard, 577–578

certificate practice statements,
572–573

certificate requests, 571–572

certificate revocation

Authority Information Access (AIA),
624–625
certificate revocation lists (CRLs)
CDPs (CRL distribution points),
619–620
configuring, 617, 619
troubleshooting, 620–621
explained, 616–617
online responders, 621–624

certificate server permissions, assigning, 582–583

Certificate Services. *See* **AD CS**
(**Active Directory Certificate**
Services)

certificate stores, 575

certificate templates

archiving keys, 599
configuring, 593–595
defined, 592
duplicating, 597–598
enabling, 597
key recovery agents (KRAs), 599–602
permissions, 595–597
template types, 592

certificates, request and installation,
228–230

Certificates snap-in, installing,
573–574

Certification Authority Backup
Wizard, 580–581

Certification Authority Restore
Wizard, 581

Certification Authority Web
Enrollment

configuring smart card enrollment,
609–610
configuring Web enrollment, 606–607
creating enrollment agents, 610–613
enabling certificate autoenrollment,
605–606
Network Device Enrollment Services
(NDES), 602–604

Change Domain Controller dialog
box, 166

Change Zone Replication Scope dialog
box, 129–130

“Changes in Functionality from
Windows Server 2008 to Windows
Server 2008 R2” (article), 434

Check Replication Topology option
(*replmon* utility), 490

checking names, 125–126

ChildName option (Active Directory installation), 90

Choose a Deployment Configuration page (Active Directory Installation Wizard), 84

claims

creating, 239

user and group claim mapping, 237–238

Claims-aware agents, 233

classes, 23, 154

CLC (Client Licensor certificate), 229

Clear Log option (replmon utility), 490

clearcache command (dnscmd), 70

Client Licensor certificate (CLC), 229

cmdlets,

Enable-ADOptionalFeature, 541

CNAME (alias) resource record, 61

command-line DNS server administration, 69–70

command-line server management, 36

commands. *See also* utilities

add nc replica, 139

Adprep /domainprep, 97

Adprep /forestprep, 96

depromo, 91–92

dnscmd, 113–114, 118–119, 125, 137–138

dsmgmt, 262

ldifde, 221

net start ntds, 550

net stop ntds, 550

netdom, 341

netdom trust, 335

remove nc replica, 139

repadmin /prp, 274

syskey, 276–277

Windows Server Core commands, 768–769

comments for Group Policy settings, 354

“Compact the directory database file (offline defragmentation)” (article), 553

Computer Management snap-in, 36

computers, assigning software to, 399

conditional forwarders, 114–115

config command (dnscmd), 70

configurable credential caching, 273

configuration

accounts. *See* accounts

Active Directory

bridgehead servers, 193–194

DFS (Distributed File System), 192–193

forcing, 200

one-way replication, 193

ports, 195

replication, 191–200

replication protocols, 194–195

scheduling, 196–199

Active Directory sites

adding domain controllers, 181

creating sites, 180–181

creating subnets, 182–184

ISTG (Intersite Topology Generator), 189

KCC (Knowledge Consistency Checker), 189

site link bridges, 185

site links, 184–188

AD LDS (Active Directory Lightweight Directory Service), 217

with Active Directory Schema snap-in, 220

with Active Directory Sites and Services snap-in, 221

with ADSI Edit snap-in, 217–218

with Ldp.exe, 218–220

- application priority, 465
- arrays, 624
- Authority Information Access (AIA), 624–625
- CDPs (CRL distribution points), 619–620
- certificate templates, 593–595
- contacts, 298–299
- CRLs (certificate revocation lists), 617, 619
- DNS (Domain Name System)
 - authoritative secondary servers*, 63
 - “Do I Know This Already?” quiz*, 43–47
 - Dynamic DNS (DDNS)*, 64
 - exam preparation tasks*, 71
 - integrating with WINS*, 68–69
 - name server roles*, 55
 - Nondynamic DNS (NDDNS)*, 64
 - overview*, 51–52
 - resource records*, 61
 - Secure Dynamic DNS (SDDNS)*, 65
 - time to live (TTL)*, 66–68
 - zone creation*, 57–60
 - zone properties*, 62
 - zone scavenging*, 65–66
 - zone types*, 52–55, 63
- DNS server
 - application directory partitions*, 138–139
 - debug logging*, 119–121
 - DNS monitoring*, 127–128
 - DNS notify*, 133–134
 - DNS Security Extensions (DNSSEC)*, 121–123
 - “Do I Know This Already?” quiz*, 107–111
 - event logging*, 121
 - exam preparation tasks*, 140
 - forwarding*, 112–115
 - loading zone data*, 126
 - name checking*, 125–126
 - name servers*, 136–138
 - replication scope*, 128–130
 - recursion*, 125
 - root hints*, 116–117
 - round robin*, 124–125
 - server options*, 123–124
 - server scavenging*, 126
 - zone delegation*, 117–119
 - zone transfer*, 130–136
- federation trusts, 238
 - account stores*, 240–241
 - claims*, 239
 - creating federation trusts*, 242–243
 - enabling applications*, 241–242
- fine-grained password policies, 430–434
- GC (global catalog) servers, 148
 - partial attribute sets*, 152–153
 - placement*, 148–150
 - promoting domain controllers to*, 150
 - removing*, 151
 - UGMC (Universal Group Membership Caching)*, 151
- GPO hierarchy and processing priority, 365, 367
 - Block Inheritance setting*, 369
 - disabling user objects*, 370
 - Enforced setting*, 367–368
 - modifying sequence of GPO application*, 370
 - OU hierarchy*, 367
- group membership, 304–305
- online responders, 621–624
- operations masters
 - domain naming masters*, 160
 - failures*, 164–165
 - infrastructure masters*, 162
 - PDC emulators*, 160–162
 - placement*, 163–164
 - RID masters*, 162
 - seizing operations master roles*, 167–168
 - transferring operations master roles*, 165–167
- password replication policy, 272–273

- schema masters
 - configuring schema*, 154–155
 - deactivating schema objects*, 159–160
 - extending schema*, 155–158
 - schema definitions*, 153–154
 - smart card enrollment, 609–610
 - trust policies, 236–237
 - Web enrollment, 606–607
 - configuration partitions, 25
 - Configure a DNS Server Wizard**, 117
 - “Configure the Network Device Enrollment Service”** (article), 604
 - “Configuring SID Filter Quarantining on External Trusts”** (article), 341
 - Confirm Incoming Trust page (New Trust Wizard)**, 334
 - Confirm Outgoing Trust page (New Trust Wizard)**, 334
 - ConfirmGC option (Active Directory installation)**, 91
 - Connection Settings dialog box**, 430
 - contacts, configuring, 298–299
 - containers
 - defined, 153
 - explained, 24
 - GPCs (Group Policy Containers), 352
 - contiguous namespaces, 23
 - control of GPOs (Group Policy Objects), delegating, 362, 364
 - CopyAllGPOs.wsf**, 548
 - CopyGPO.wsf**, 548
 - costs, site link, 186–188
 - counters, 477, 479
 - “Create an LDIF file for recovering back-links for authoritatively restored objects”** (article), 538
 - Create Custom View dialog box**, 469
 - Create New Attribute dialog box**, 156–157
 - Create New Data Collector Set Wizard**, 480–481
 - Create Object dialog box**, 222, 431
 - Create Organizational Unit dialog box**, 303
 - CreateGPO.wsf**, 548
 - “Creating External Trusts”** (article), 336
 - “Creating Realm Trusts”** (article), 337
 - credential caching, 273–275
 - credential roaming, enabling, 578–580
 - CRL distribution points (CDPs)**, 619–620
 - CRLs (certificate revocation lists)**
 - CDPs (CRL distribution points), 619–620
 - configuring, 617, 619
 - troubleshooting, 620–621
 - cross-forest trust relationships**, removing, 341–342
 - cscript scregedit.wsf command**, 768
 - .csv extension**, 292
 - Csvde tool**, 292–293
 - customizing Event Viewer**, 468–471
- ## D
- data collector sets**, 479–484
 - database storage allocation**, 553–554
 - DatabasePath option (Active Directory installation)**, 91
 - databases**
 - certificate databases, backing up and restoring, 580–581
 - database storage allocation, 553–554
 - SAM (Security Accounts Manager) database, 77
 - dcdiag tool**, 189, 494–496
 - dcpromo command**, 91–92, 769

- DDNS (Dynamic DNS), 64**
- deactivating schema objects, 159–160
- debug logging, 119–121
- Debug Logging tab (Properties dialog box), 120**
- default schemas, 24
- defragmentation
 - offline defragmentation, 551–552
 - online defragmentation, 551
- delegating**
 - AD RMS, 230–231
 - administrative control, 313–316
 - control of GPOs (Group Policy Objects), 362, 364
 - zones, 117–119
- Delegation of Control Wizard, 364, 509**
- Delegation of RODC Installation and Administration page (Active Directory Domain Services Installation Wizard), 259**
- Delete option (replmon utility), 490**
- deleted objects, restoring, 543–545
- deleting GPOs (Group Policy Objects), 362
- denying access, 308–309
- Deploy Software dialog box, 401, 410**
- deployment of software. *See* software deployment
- Deployment tab (Software Package Properties dialog box), 405**
- deprovisioning accounts, 312–313
- DFS (Distributed File System), 192–193**
- DFS Management snap-in, 193**
- “DFS Step-by-Step Guide for Windows Server 2008” (article), 193**
- dialog box, 219, 224. *See also names of specific dialog boxes*
- DIB (Directory Information Base), 18**
- differentiating VHDs (virtual hard disks), 246
- DirectAccess, 39**
- Direction of Trust page (New Trust Wizard), 331–332**
- Directory Information Base (DIB), 18**
- Directory Services Restore Mode (DSRM), 528–530**
- Directory Services Restore Mode Administrator Password page (Active Directory Installation Wizard), 87**
- Disable Recursion setting (DNS server), 125**
- disabling**
 - recursion, 125
 - user objects, 370
- disjointed namespaces, 23**
- distinguished names (DNs), 19–20**
- Distributed File System (DFS), 192–193**
- distribution lists, creating, 299–300**
- distribution points, 400**
- DNs (distinguished names), 19–20**
- DNS (Domain Name System)**
 - command-line DNS server administration, 69–70
 - DNS server. *See* DNS server
 - “Do I Know This Already?” quiz, 43–47
 - domain namespaces, 48
 - Dynamic DNS (DDNS), 64
 - exam preparation tasks, 71
 - hierarchical nature of, 48–49
 - hostnames, 49
 - installing on Windows Server 2008 R2, 49–51
 - integrating with WINS, 68–69

- monitoring, 127–128
- Nondynamic DNS (NDDNS), 64
- read-only DNS, 262–263
- resource records, 61
- root-level domains, 49
- second-level domains, 49
- Secure Dynamic DNS (SDDNS), 65
- server roles
 - caching-only servers*, 56
 - forwarders*, 56–57
 - primary name servers*, 55
 - secondary name servers*, 55–56
- top-level domains, 49
- zones
 - adding authoritative secondary servers to*, 63
 - configuring zone properties*, 62
 - configuring zone types*, 63
 - creating*, 57–60
 - forward lookup zones*, 57–58
 - GlobalNames zones*, 54–55
 - integrated zones*, 53–54
 - primary zones*, 53
 - reverse lookup zones*, 59–60
 - secondary zones*, 53
 - stub zones*, 53
 - time to live (TTL)*, 66–68
 - zone scavenging*, 65–66

DNS notify, 133–134

DNS Security Extensions (DNSSEC), 121–123

DNS server, configuration

- application directory partitions, 138–139
- debug logging, 119–121
- DNS monitoring, 127–128
- DNS notify, 133–134
- DNS Security Extensions (DNSSEC), 121–123
- “Do I Know This Already?” quiz, 107–111

- event logging, 121
- exam preparation tasks, 140
- forwarding, 112–115
- loading zone data, 126
- name checking, 125–126
- name servers, 136–138
- recursion, 125
- replication scope, 128–130
- root hints, 116–117
- round robin, 124–125
- server options, 123–124
- server scavenging, 126
- zone delegation, 117–119
- zone transfer, 130–136

dns.log file, 119

dnscmd command, 113–114, 118–119, 125, 137–138

Dnscmd.exe utility, 69–70

DNSSEC (DNS Security Extensions), 121–123

“Do I Know This Already?” quiz

- account policies and auditing, 417–421
- Active Directory installation, 73–76
- Active Directory maintenance, 515–519
- AD CS (Active Directory Certificate Services), 559–562, 587–591

answers

- chapter 2*, 729–731
- chapter 3*, 731–732
- chapter 4*, 732–734
- chapter 5*, 735–736
- chapter 6*, 737–739
- chapter 7*, 739–741
- chapter 8*, 741–743
- chapter 9*, 743–745
- chapter 10*, 745–747
- chapter 11*, 747–749
- chapter 12*, 749–751
- chapter 13*, 751–753
- chapter 14*, 754–756

- chapter 15, 756–758*
- chapter 16, 758–759*
- chapter 17, 759–761*
- DNS installation and configuration, 43–47
- DNS server configuration, 107–111
- global catalogs and operations masters, 143–147
- GPOs (Group Policy Objects), 345–350
- Group Policy software deployment, 393–397
- monitoring, 453–458
- RODCs (read-only domain controllers), 251–253
- server roles, 205–209
- sites and replication, 173–177
- trust relationships, 321–324
- user and group accounts, 281–285
- “Domain Controller and Member Server Policy Settings” (article), 438**
- domain controllers, 26**
 - adding to sites, 181
 - backing up critical volumes of, 522–524
 - bridgehead servers, 193–194
 - explained, 31
 - full-server recovery of, 538–539
 - installing in existing domains, 89
 - promoting to GC (global catalog) servers, 150
 - RODCs (read-only domain controllers), 33
 - administrator role separation, 261–262*
 - BitLocker, 263–270*
 - “Do I Know This Already?” quiz, 251–253*
 - exam preparation tasks, 278*
 - installing, 256–257*
 - password replication, 270–276*
 - planning use of, 254–255*
 - preparing for, 255–256*
 - prestaging, 257–259*
 - read-only DNS, 262–263*
 - syskey utility, 276–277*
 - unidirectional replication, 260–261*
- Server Core domain controllers, 92
- specifying, 365
- Windows Server 2003 domain controllers, upgrading, 97
- domain groups, 310–312**
- Domain Name System. See DNS**
- domain namespaces, 48**
- domain naming masters, 160**
- domain partitions, 25**
- domain password policies, 423, 425**
- domain-wide authentication, 339**
- DomainDnsZones, 138**
- DomainLevel option (Active Directory installation), 91**
- domains**
 - administrative and geographical organization of, 78–79
 - application directory partition reference domains, 139
 - benefits of multiple domains, 26–27
 - best practices, 80–81
 - domain controllers. *See* domain controllers
 - domain password policies, 423, 425
 - explained, 26
 - forests, 27
 - installation, 83–87*
 - functional levels
 - table of, 94–95*
 - upgrading, 95–96*
 - installation
 - installing domain controllers in existing domains, 89*
 - installing new domains in existing forests, 88*

- multiple trees, 79
- ntds.dit files, 26
- offline domain join, 38
- root-level domains, 49
- second-level domains, 49
- top-level domains, 49
- trees, 27
- Dsadd tool, 223, 294–295**
- dsget, 295**
- dsmgmt utility, 262**
- dsmod, 295**
- dsmove, 295**
- dsquery, 295**
- dsrcm, 295**
- DSRM (Directory Services Restore Mode), 528–529**
- dual-factor authentication, 609**
- Duplicate Template dialog box, 605**
- duplicating certificate templates, 597–598**
- DVD-ROM, installing Windows Server 2008 R2 from, 764–766**
- Dynamic DNS (DDNS), 64**
- dynamic VHDs (virtual hard disks), 245**

E

- Edit Forwarders dialog box, 113–114**
- Edit Name Server Record dialog box, 117, 137**
- “11 Essential Tools for Managing Active Directory” (article), 295**
- Enable automatic scavenging of stale records setting (DNS server), 126**
- Enable Certificate Templates dialog box, 597–598**
- “Enable Clients to Locate a Domain Controller in the Next Closest Site” (article), 263**

- Enable-ADOptionalFeature cmdlet, 541**
- enabling**
 - AD FS applications, 241–242
 - BitLocker, 265–269
 - certificate autoenrollment, 605–606
 - certificate templates, 597
 - credential roaming, 578–580
 - Recycle Bin, 541–543
- Enforced setting (GPOs), 367–368**
- enrollment. *See* Certification Authority Web Enrollment**
- enrollment agents, creating, 610–613**
- enterprise CAs (certificate authorities), 565**
- Enterprise PKI (PKIView), 564**
- enumzones command (dnscmd), 70**
- Establish Restricted Enrollment Agents’ (article), 614**
- event logging, 121**
- Event Logging tab (Properties dialog box), 121**
- Event Viewer, 466–471**
 - replication monitoring, customizing, 470–471
- exam. *See* practice exam**
- exam preparation tasks**
 - account policies and auditing, 449–450
 - Active Directory installation, 103–104
 - Active Directory maintenance, 555–556
 - AD CS (Active Directory Certificate Services), 583–584, 625–626
 - DNS (Domain Name System) installation and configuration, 71
 - DNS server configuration, 140
 - global catalogs and operations masters, 169–170
 - GPOs (Group Policy Objects), 389–390
 - Group Policy software deployment, 414

- monitoring, 512–513
- RODCs (read-only domain controllers), 278
- server roles, 247–248
- sites and replication, 201–202
- trust relationships, 343
- user and group accounts, 317–318

Expires After setting (SOA records), 68

explicit UPNs (user principal names), 101

extending schema, 155–158

external trusts

- creating, 335–336
- explained, 326

F

f parameter (dcdiag utility), 495

failed replication, monitoring tools, 470–471

failures, operations master failures, 164–165

fault tolerance, 31

features, adding, 36

Federation Service. *See* AD FS (Active Directory Federation Service)

Federation Service Proxy, 233

federation trusts

- configuring, 238
 - account stores, 240–242*
 - claims, 239*
- creating, 242–243

ferr parameter (dcdiag utility), 495

File Extensions tab (Software Installation Properties dialog box), 404

File Locations page (Lightweight Directory Services Setup Wizard), 215

File Replication Service (FRS), 192

files

- cache.dns, 117
- dns.log, 119
- Gpt.ini., 353
- .msi files, 412
- Registry.pol, 353
- transform files
 - compared to patches, 411*
 - modifying software packages with, 409–410*
- virtual hard disk (VHD) files, 245–246
- Zero Administration Package (ZAP) files, 402–403

Filter Current Log dialog box, 470

filtering

- Group Policy, 371
 - Security Filtering, 371–372*
 - Windows Management Instrumentation (WMI), 374*
 - Windows PowerShell, 374–376*
- SID filtering, 340–341

fine-grained password policies

- configuring, 430–434
- explained, 428–429
- managing, 435
- password settings precedence, 429
- viewing resultant PSO, 435–436

fixed VHDs (virtual hard disks), 245

flat namespaces, 23

flexible single-master operations (FSMO) servers, 32–33

folders, SYSVOL, replication, 261

force option (Gpupdate), 511

forcing intersite replication, 200–201

forest trusts

- creating, 329–330, 332–335
- explained, 326

forest-wide authentication, 339

ForestDnsZones, 138

ForestLevel option (Active Directory installation), 91

forests

explained, 27

functional levels

table of, 94–95

upgrading, 95–96

installation, 83–87

installing new domains in, 88

forward lookup zones, 57–58

forwarders, 56–57

Forwarders tab (Properties dialog box), 113

forwarding

conditional forwarders, 114–115

explained, 112–113

specifying forwarders, 113–114

foundations of Active Directory

LDAP (Lightweight Directory Access Protocol), 18–19

X.500, 17–18

Freesysvol test (dcdiag utility), 496

FRS (File Replication Service), 192

Frsevent test (dcdiag utility), 496

FSMO (flexible single-master operations) servers, 32–33

full zone transfer (AXFR), 130

full-server recovery of domain controllers, 538–539

G

GC (global catalog) servers, 31–32

features, 148

partial attribute sets, 152–153

placement, 148–150

promoting domain controllers to, 150

removing, 151

UGMC (Universal Group Membership Caching), 151

General tab

Software Installation Properties dialog box, 403

Software Package Properties dialog box, 405

geographical organization of domains, 78–79

global catalogs

“Do I Know This Already?” quiz, 143–147

exam preparation tasks, 169–170

explained, 24–25, 31

GC (global catalog) servers, 31–32

features, 148

partial attribute sets, 152–153

placement, 148–150

promoting domain controllers to, 150

removing, 151

UGMC (Universal Group Membership Caching), 151

globally unique identifiers (GUIDs), 21, 352

GlobalNames zones, 54–55

GPCs (Group Policy Containers), 352

gpedit.msc, 134

GPMC (Group Policy Management Console), 34

creating GPOs, 355–359

explained, 354

GPOs (Group Policy Objects)

administrative templates, 380–384

ADMX central store, 379–380

backing up, 545, 548

creating, 355–359

delegating control of, 362, 364

deleting, 362

- “Do I Know This Already?” quiz, 345–350
- filtering, 371
 - Security Filtering*, 371–372
 - Windows Management Instrumentation (WMI)*, 374
 - Windows PowerShell*, 374–376
- hierarchy and processing priority, 365, 367
 - Block Inheritance setting*, 369
 - disabling user objects*, 370
 - Enforced setting*, 367–368
 - modifying sequence of GPO application*, 370
 - OU hierarchy*, 367
- importing, 547–548
- linking, 360
- loopback processing, 377–378
- managing GPO links, 361–362
- restoring, 545, 547–548
- restricted groups, 384–385
- RSoP (Resultant Set of Policy)
 - Delegation of Control Wizard*, 509
 - explained*, 496–497
 - Gpresult*, 509–510
 - Gpupdate*, 511
 - logging mode*, 501–508
 - planning mode*, 497–501
 - saving RSoP data*, 508–509
- shell access policies, 387
- specifying domain controllers, 365
- Starter GPOs, 385–387
- user rights, 378
- Gpresult**, 509–510
- Gpt.ini file**, 353
- GPTs (Group Policy Templates)**, 352–353
- Gpupdate**, 511
- group accounts**
 - configuring group membership, 304–305
 - creating
 - with Csvde tool*, 292–293
 - with Dsadd tool*, 294–295
 - with Ldifde tool*, 293–294
 - manually*, 288–290
 - with scripts*, 296
 - delegating administrative control, 313–316
 - denying access, 308–309
 - deprovisioning, 313
 - “Do I Know This Already?” quiz, 281–285
 - exam preparation tasks, 317–318
 - explained, 287
 - local versus domain groups, 310–312
 - nesting with AGDLP/AGUDLP, 306–307
- Group Policy, 34**
 - account policies, 422
 - account lockout policy*, 426–427
 - “Do I Know This Already?” quiz*, 417–421
 - domain password policies*, 423, 425
 - exam preparation task*, 449–450
 - Kerberos policy*, 428
 - unlocking accounts*, 427
 - additional security-related policy settings, 436–439
 - administrative templates, 380–384
 - ADMX central store, 379–380
 - audits, configuring, 442
 - advanced auditing policies*, 446–447
 - Auditpol.exe*, 447, 449
 - available auditing categories*, 442–443
 - basic auditing policies*, 443–445
 - explained, 351–352
 - filtering, 371
 - Security Filtering*, 371–372
 - Windows Management Instrumentation (WMI)*, 374
 - Windows PowerShell*, 374–376

- fine-grained password policies
 - configuring*, 430–434
 - explained*, 428–429
 - managing*, 435
 - password settings precedence*, 429
 - viewing resultant PSO*, 435–436
 - GPCs (Group Policy Containers), 352
 - GPMC (Group Policy Management Console)
 - creating GPOs*, 355–359
 - explained*, 354
 - GPOs. *See* GPOs (Group Policy Objects)
 - GPTs (Group Policy Templates), 352–353
 - importing certificates with, 575–576
 - loopback processing, 377–378
 - new features, 354–355
 - overview, 352
 - restricted groups, 384–385
 - RSoP (Resultant Set of Policy)
 - Delegation of Control Wizard*, 509
 - explained*, 496–497
 - Gpresult*, 509–510
 - Gpupdate*, 511
 - logging mode*, 501–508
 - planning mode*, 497–501
 - saving RSoP data*, 508–509
 - shell access policies, 387
 - software, redeploying, 413
 - software deployment
 - assigning software*, 399
 - benefits of*, 398
 - “Do I Know This Already?” quiz*, 393–397
 - exam preparation tasks*, 414
 - explained*, 400–401
 - modifying software packages with transform files*, 409–410
 - publishing software*, 399
 - redeploying upgraded software*, 411–412
 - removing software*, 413
 - software installation properties*, 403–405
 - software lifecycle*, 398–399
 - software package properties*, 405–407
 - upgrading software*, 407–409
 - ZAP files*, 402–403
 - software package properties, 405
 - user rights, 378
 - Group Policy Containers (GPCs), 352**
 - Group Policy Management Console (GPMC), 34**
 - creating GPOs, 355–359
 - explained, 354
 - “Group Policy Management Console Scripting Samples” (article), 549**
 - Group Policy Objects. *See* GPOs**
 - “Group Policy Settings Reference for Windows and Windows Server” (article), 384**
 - Group Policy Templates (GPTs), 352–353**
 - groups**
 - AD LDS groups, creating, 222–223
 - authoritative restore of group memberships, 539
 - restricted groups, 384–385
 - GTIMESERV, 161**
 - GUIDs (globally unique identifiers), 21, 352**
- ## H
- h parameter (dcdiag utility), 495**
 - hardware requirements for Windows Server 2008 R2, 763–764**
 - Help command, 769**
 - hierarchical namespaces, 23**
 - hierarchical nature of DNS (Domain Name System), 48–49**
 - hierarchy (GPOs), 365, 367**

High priority level, 465

hostnames, 49

“How to rebuild the SYSVOL tree and its content in a domain” (article), 261

Hyper-V, 38, 244–246

I–J

“Implement Role-Based Administration” (article), 583

implicit UPNs (user principal names), 101

Import Settings Wizard, 547–548

ImportGPO.wsf, 548

importing

certificates, 575–576

GPOs (Group Policy Objects), 547–548

Importing LDIF Files page (Lightweight Directory Services Setup Wizard), 215

incremental zone transfer (IXFR), 131

info command (dnscmd), 70

infrastructure masters, 162

installation

Active Directory, 82

Active Directory Migration Tool (ADMT) v.3.1, 100–101

alternative UPN (user principal name) suffixes, 101–102

“Do I Know This Already?” quiz, 73–76

domain controllers in existing domains, 89

domains, 78–81, 88

exam preparation tasks, 103–104

namespaces, 77–78

new forests, 83–87

requirements, 81–82

Server Core domain controllers, 92

unattended installations, 90–92

verifying installation, 98, 100

AD CS (Active Directory Certificate Services), 565

certificate authority types and hierarchies, 565–567

root CAs, 567–568, 570–571

subordinate CAs, 571

AD FS (Active Directory Federation Service), 233–236

AD LDS (Active Directory Lightweight Directory Service), 213

AD LDS instances, 214–216

AD LDS roles, 213

AD RMS (Active Directory Rights Management Service), 226–228

application directory partitions, 138–139

certificate request and installation, 228–230

DNS (Domain Name System)

“Do I Know This Already?” quiz, 43–47

exam preparation tasks, 71

on Windows Server 2008 R2, 49–51

Hyper-V, 245–246

Network Monitor, 460–461

RODCs (read-only domain controllers), 254

AD DS Installation Wizard, 256–257

planning use of, 254–255

preparation, 255–256

prestaging, 257–259

server roles, 211

software installation properties, 403–405

Windows Server 2008 R2

automated installation, 770–771

complete server installation, 765

complete server installation from DVD-ROM, 764–766

upgrading Windows Server 2003 or 2008 computers, 769–770

- Windows Server Core commands*, 768–769
 - Windows Server Core computers*, 767–768
 - Windows Server Backup, 521–522
 - WSRM (Windows System Resource Manager), 484
 - Installation Progress page (Add Roles Wizard)**, 83
 - InstallDNS option (Active Directory installation)**, 91
 - Installing AD LDS page (Lightweight Directory Services Setup Wizard)**, 216
 - Instance Name page (Lightweight Directory Services Setup Wizard)**, 214
 - integrated zones, 53–54
 - integrating DNS (Domain Name System) with WINS, 68–69
 - intermediate CAs (certificate authorities), 566
 - Internet Server Application Programming Interface (ISAPI) filters**, 602
 - Internet Society (ISOC)**, 49
 - interoperability with previous versions of Active Directory**, 93
 - Adprep utility, 96
 - Adprep /domainprep command*, 97
 - Adprep /forestprep command*, 96
 - forest and domain functional levels
 - table of*, 94–95
 - upgrading*, 95–96
 - upgrading Windows Server 2003 domain controllers, 97
 - intersite replication**, 191, 195
 - forcing, 200–201
 - scheduling, 196–198
 - Intersite Topology Generator (ISTG)**, 189
 - intrasite replication**, 191
 - scheduling, 198–199
 - Introduction to Active Directory Domain Services page (Add Roles Wizard)**, 83
 - ISAPI (Internet Server Application Programming Interface) filters**, 602
 - ISOC (Internet Society)**, 49
 - Issue and Manage Certificates permissions**, 582
 - issuing CAs (certificate authorities)**, 566
 - ISTG (Intersite Topology Generator)**, 189
 - IXFR (incremental zone transfer)**, 131
- ## K
- KCC (Knowledge Consistency Checker)**, 189
 - Kccevent test (dcdiag utility)**, 496
 - KDC (Kerberos Key Distribution Center)**, 428
 - Kerberos policy**, 428
 - key recovery agents (KRAs)**, 599–602
 - keys
 - archiving, 599
 - backing up, 576–577
 - key recovery agents (KRAs), 599–602
 - restoring, 577–578
 - Knowledge Consistency Checker (KCC)**, 189
 - KnowsOfRoleHolders test (dcdiag utility)**, 495
 - KRAs (key recovery agents)**, 599–602
- ## L
- LDAP (Lightweight Directory Access Protocol)**, 18–19
 - ldifde command**, 221, 293–294, 434

Ldp.exe, 218–220, 541–544

Lightweight Directory Access Protocol (LDAP), 18–19

Lightweight Directory Service. *See* **AD LDS (Active Directory Lightweight Directory Service)**

Lightweight Directory Services Setup Wizard, 214–216

linked-value replication, 539

linking GPOs (Group Policy Objects), 360

links, GPO links

- creating, 360
- managing, 361–362

lists

- authentication lists, administration, 275–276
- distribution lists, creating, 299–300

load balancing, 31

loading zone data, 126

Loading Zone Data setting (DNS server), 126

local groups, 310–312

lockout, account lockout policy, 426–427

logging

- debug logging, 119–121
- directory service information, Event Viewer and, 468
- event logging, 121

logging mode (RSoP), 501–508

logoff option (Gpupdate), 511

LogPath option (Active Directory installation), 91

lookup zones

- forward lookup zones, 57–59
- overview, 57
- reverse lookup zones, 59–60

loopback processing mode (Group Policy), 377–378

Low priority level, 465

M

Machine certificate, 229

MachineAccount test (dcdiag utility), 496

mail exchanger (MX) resource record, 61

Manage Backups dialog box, 546

Manage CA permissions, 583

Managed Service Accounts, 39

managing

- BitLocker, 269–270

- fine-grained password policies, 435

- GPO (Group Policy Object) links, 361–362

- trust relationships

- authentication scope*, 338–340

- SID filtering*, 340–341

- validating relationships*, 338

mapping user and group claims, 237–238

Maximum Tolerance for Computer Clock Synchronization policy setting, 428

MDT (Microsoft Deployment Toolkit) 2010, 771

Microsoft Simple Certificate Enrollment Protocol, 563

“Microsoft® Hyper-V Server 2008 R2” (article), 246

migrating to AD LDS (Active Directory Lightweight Directory Service), 221

Modifications tab (Software Package Properties dialog box), 407

modifying

- schemas, 24

software packages with transform files,
409–410

monitoring Active Directory

data collector sets, 479–484

“Do I Know This Already?” quiz,
453–458

Event Viewer, 466–471

exam preparation tasks, 512–513

Network Monitor, 459–461, 463

Performance Monitor, 476–479

Reliability Monitor, 473, 475

replication

dcdiag, 494–496

Event Viewer, 470–471

repadmin, 491–494

replmon, 487–491

Resource Monitor, 473–474

Server Performance Advisor, 486

Task Manager, 463–465

Windows System Resource Manager
(WSRM), 484–486

monitoring DNS (Domain Name System), 127–128

Monitoring tab

DNS server, 127–128

Properties dialog box, 127–128

Move Server dialog box, 181

.msi files, 412

.msp extension, 411

.mst extension, 411

multi-master replication, 190

Multibyte (UTFB), 126

multimaster replication, 26

**multiple domains, benefits of,
26–27**

multiple trees, 79

**MX (mail exchanger) resource
record, 61**

N

n parameter (dcdiag utility), 495

**Name Checking setting (DNS server),
125–126**

name server (NS) resource record, 61

name servers

caching-only servers, 56

configuration, 136–138

forwarders, 56–57

primary name servers, 55

secondary name servers, 55–56

**Name the New Domain page (Active
Directory Installation Wizard), 88**

names

hostnames, 49

name checking, 125–126

namespaces, 23

contiguous namespaces, 23

disjointed namespaces, 23

domain namespaces, 48

explained, 22

flat namespaces, 23

hierarchical namespaces, 23

planning, 77

subdividing, 77–78

naming standards

canonical names, 22

DNs (distinguished names), 19–20

GUIDs (globally unique identifiers), 21

RDNs (relative distinguished names),
20–21

SIDs (security identifiers), 21–22

UPNs (user principal names), 21

NCSecDesc test (dcdiag utility), 495

NDDNS (Nondynamic DNS), 64

**NDES (Network Device Enrollment
Services), 602–604**

nesting group accounts, 306–307
net start ntds command, 550
net stop ntds command, 550
netdom command, 341
netdom join command, 768
netdom trust command, 335
“Netdom trust” (article), 341
NetLogons test (dcdiag utility), 495
netsh advfirewall command, 769
netsh interface IPv4 command, 769
Network Credentials page
 Active Directory Domain Services
 Installation Wizard, 258
 Active Directory Installation
 Wizard, 88
**Network Device Enrollment Services
 (NDES), 602–604**
**Network Location Awareness
 (NLA), 354**
Network Monitor, 459–461, 463
**New Connection Security Rule
 Wizard, 134–136**
New Delegation Wizard, 118
**new features of Active Directory,
 33–34**
New Group dialog box, 311
**New Name Server Record dialog box,
 63, 117–118, 136–137**
New Object - Contact dialog box, 299
**New Object - Organizational Unit dia-
 log box, 303**
New Object - Site dialog box, 180
**New Object - Site Link Bridge dialog
 box, 186**
**New Object - Site Link dialog
 box, 185**
New Object - Subnet dialog box, 182
New Object - User dialog box, 288
New Starter GPO dialog box, 386

New Trust Wizard
 external trusts, creating, 335–336
 forest trusts, creating, 329–330,
 332–335
 realm trusts, creating, 336
 shortcut trusts, creating, 337
**NewDomain option (Active Directory
 installation), 90**
**NewDomainDNSName option (Active
 Directory installation), 90**
**NLA (Network Location
 Awareness), 354**
nmcap.exe, 463
Non RFC (ANSI), 126
nonauthoritative restore, 529–534
Nondynamic DNS (NDDNS), 64
Normal priority level, 465
normal restore, 529–534
notifications, DNS notify, 133–134
Notify dialog box, 133
NS (name server) resource record, 61
**NTDS Settings Properties
 dialog box, 150**
ntds.dit files, 26
ntdsutil utility, 167–168, 529

O

objectGUID, 21
objects
 attributes, explained, 23
 defined, 23, 153
 GPOs. *See* GPOs (Group Policy
 Objects)
 objectGUID, 21
 Password Settings Container, 429
**ObjectsReplicated test (dcdiag
 utility), 496**
oclist command, 768

ocsetup command, 769

OCSP (Online Certificate Status Protocol), 563

offline defragmentation, 551–552

one-way replication, 193

Online Certificate Status Protocol (OCSP), 563

online defragmentation, 551

Online Responder Installation, Configuration, and Troubleshooting Guide, 621

Online Responder Properties dialog box, 622

online responders, 621–624

opening Server Manager, 35

Operating System Compatibility page

- Active Directory Domain Services Installation Wizard, 258
- Active Directory Installation Wizard, 84

operations masters, 32–33, 153

- “Do I Know This Already?” quiz, 143–147
- domain naming masters, 160
- exam preparation tasks, 169–170
- failures, 164–165
- infrastructure masters, 162
- PDC emulators, 160–162
- placement, 163–164
- RID masters, 162
- schema masters
 - configuring schema, 154–155*
 - deactivating schema objects, 159–160*
 - extending schema, 155–158*
 - schema definitions, 153–154*
- seizing operations master roles, 167–168
- transferring operations master roles, 165–167

Operations Masters dialog box, 166

OUs (organizational units)

- creating, 301–304
- explained, 29–30
- hierarchy, 367

P

p parameter (dcdiag utility), 495

packages

- modifying with transform files, 409–410
- software package properties, 405–407

ParentDomainDNSName option (Active Directory installation), 90

partial attribute sets, 152–153

partitions

- application directory partitions, 25, 138–139
 - application directory partition reference domains, 139*
 - creating application directory partition replicas, 139*
 - installing and configuring, 138–139*
- configuration partitions, 25
- domain partitions, 25
- explained, 25
- schema partitions, 25

Password option (Active Directory installation), 90

“Password Replication Policy” (article), 272

Password Settings Container, 429

Password Settings Objects. See PSOs

passwords, 34

- domain password policies, 423, 425
- fine-grained password policies
 - configuring, 430–434*
 - explained, 428–429*
 - managing, 435*

- password settings precedence*, 429
- viewing resultant PSO*, 435–436
- replication
 - authentication list administration*, 275–276
 - configuring*, 272–273
 - credential caching*, 273–275
 - explained*, 270–271
 - planning*, 271–272
- patches, compared to transform files, 411
- PDC emulators, 160–162
- “Performance and Reliability Monitoring Step-by-Step Guide for Windows Server 2008” (article), 472, 484
- Performance Logs and Alerts. *See* data collector sets
- Performance Monitor, 476–479
- “Performance Monitor Getting Started Guide,” 479
- “Performing Authoritative Restore of Active Directory Objects” (article), 540
- permissions
 - backup permissions, 521
 - certificate server permissions, assigning, 582–583
 - certificate template permissions, 595–597
- placement
 - of GC (global catalog) servers, 148–150
 - of operations masters, 163–164
- planning
 - Active Directory sites, 179
 - namespaces, 77
 - password replication policy, 271–272
 - RODCs (read-only domain controllers), 254–255
- “Planning for Active Directory Forest Recovery” (article), 528
- planning mode (RSoP), 497–501
- pointer (PTR) resource record, 61
- policies
 - Group Policy. *See* Group Policy management, 34
 - password replication policy
 - authentication list administration*, 275–276
 - configuring*, 272–273
 - credential caching*, 273–275
 - planning*, 271–272
 - trust policy configuration, 236–237
- ports for intersite replication, 195
- Ports page (Lightweight Directory Services Setup Wizard), 214
- PowerShell, 296, 374–376
- PowerShell 2.0, 37
- practice exam, 629–689
 - answers, 691–727
- preparing
 - for BitLocker, 265
 - for RODCs (read-only domain controllers), 255–256
- prestaging RODCs (read-only domain controllers), 257–259
- primary name servers, 55
- Primary Server setting (SOA records), 68
- primary zones, 53
- priority of applications, configuring, 465
- processing priority (GPOs), 365, 367
- promoting domain controllers to global catalog servers, 150
- properties
 - software packages, Group Policy and, 405
 - zone properties
 - authoritative secondary servers*, 63

- configuring*, 62
- Dynamic DNS (DDNS)*, 64
- Nondynamic DNS (NDDNS)*, 64
- Secure Dynamic DNS (SDDNS)*, 65
- time to live (TTL)*, 66–68
- zone scavenging*, 65–66
- zone types*, 63

Properties dialog box (DNS server), 112

Advanced tab, 123

- Disable Recursion setting*, 125
- Enable automatic scavenging of stale records setting*, 126
- Loading Zone Data setting*, 126
- Name Checking setting*, 125–126
- Round Robin setting*, 124–125
- Server Options*, 123–124

Debug Logging tab, 120

Event Logging tab, 121

Forwarders tab, 113–114

Monitoring tab, 127–128

Root Hints tab, 116

Trust Anchors tab, 122

Properties of New Template dialog box, 605

Properties option (replmon utility), 491

Protected Admin accounts, 309–310 protocols

LDAP (Lightweight Directory Access Protocol), 18–19

Remote Procedure Call (RPC) over IP, 184

replication protocols, 194–195

SMTP (Simple Mail Transfer Protocol), 184

X.500, 17–18

PSOs (Password Settings Objects)

defined, 429

viewing, 435–436

PTR (pointer) resource record, 61

Publishing license, 229

publishing software to users, 399

Q

q parameter (dcdiag utility), 495

quizzes. *See* “Do I Know This Already?” quiz

R

r option (Gpresult), 509

RAC (Rights account certificate), 229

RDNs (relative distinguished names), 20–21

RDS (Remote Desktop Services), 38

Read permissions, 582

read-only DNS, 262–263

read-only domain controllers. *See* RODCs

Ready to Install page (Lightweight Directory Services Setup Wizard), 216

realm trusts

creating, 336

explained, 326

Realtime priority level, 465

RebootOnCompletion option (Active Directory installation), 91

recovery. *See also* Recycle Bin

authoritative restore, 536–537

authoritative restore of group memberships, 539

Directory Services Restore Mode (DSRM), 528–529

explained, 528

full-server recovery of domain controllers, 538–539

GPOs (Group Policy Objects), 545, 547–548

- linked-value replication, 539
- nonauthoritative restore, 529–534
- recovering back-links of authoritatively restored objects, 537
- wbadmin command, 534–535
- Recovery Wizard, 531–534**
- recursion, disabling, 125**
- Recycle Bin**
 - enabling, 541–543
 - explained, 540–541
 - restoring deleted objects, 543–545
- redeploying upgraded software, 411–412**
- Refresh Interval setting (SOA records), 68**
- Registry.pol file, 353**
- REG_DWORD value, 195**
- relationships, trust**
 - authentication scope, 338–340
 - defined, 325
 - “Do I Know This Already?” quiz, 321–324
 - exam preparation tasks, 343
 - external trusts, 326, 335–336
 - forest trusts, 326, 329–330, 332–335
 - prerequisites, 328–329
 - realm trusts, 326, 336
 - removing cross-forest trust relationships, 341–342
 - shortcut trusts, 327, 337
 - SID filtering, 340–341
 - table of trust type, 328
 - transitive trusts, 325–326
 - validating, 338
- relative distinguished names (RDNs), 20–21**
- Reliability and Performance Monitor console, 472**
- Reliability Monitor, 473, 475**
- Remote Desktop Services (RDS), 38**
- Remote Procedure Call (RPC) over IP, 184**
- removable media, 527**
- remove nc replica command, 139**
- Remove Software dialog box, 413**
- removing**
 - Active Directory, 92–93
 - cross-forest trust relationships, 341–342
 - GC (global catalog) servers, 151
 - server roles, 211
 - software, 413
- repadmin, 491**
 - /add parameter, 492–493
 - /replicate parameter, 491
 - /replsummary parameter, 494
 - /showconn parameter, 493
 - /showmeta parameter, 492
 - /showreps parameter, 492
 - /sync parameter, 493
 - /syncall parameter, 493
- repadmin /prp command, 274**
- repadmin tool, 189**
- ReplicaDomainDNSName option (Active Directory installation), 90**
- ReplicaOrNewDomain option (Active Directory installation), 90**
- replicas, application directory partition replicas, 139**
- replicate parameter (repadmin utility), 491**
- Replicate this attribute to the Global Catalog option, 154**
- replication**
 - bridgehead servers, 193–194
 - DFS (Distributed File System), 192–193

- “Do I Know This Already?” quiz, 173–177
- Event Viewer, customizing, 470–471
- exam preparation tasks, 201–202
- explained, 190–191
- forcing, 200–201
- intersite replication, 191, 195
 - forcing*, 200–201
 - scheduling*, 196–198
- intrasite replication, 191
 - scheduling*, 198–199
- linked-value replication, 539
- monitoring
 - dcdiag*, 494–496
 - repadmin*, 491–494
 - replmon*, 487–491
- multi-master replication, 190
- one-way replication, 193
- password replication
 - authentication list administration*, 275–276
 - configuring*, 272–273
 - credential caching*, 273–275
 - explained*, 270–271
 - planning*, 271–272
- replication protocols, 194–195
- scheduling
 - intersite replication*, 196–198
 - intrasite replication*, 198–199
- scope, 128–130
- unidirectional replication, 260–261
- Replications test (dcdiag utility), 495**
- replmon, 189, 487–491**
- replsum.exe, 38**
- replsummary parameter (repadmin utility), 494**
- Report Options dialog box, 489**
- Report Status dialog box, 490**
- Request Certificates permissions, 583**
- “Request Handling” (article), 595**
- resetting user accounts, 308**
- resilient software, 398**
- Resource Monitor, 473–474**
- resource partners, 231**
- resource records (DNS), 61**
- Responsible Person setting (SOA records), 68**
- restarting Active Directory, 549–550**
- restore options. *See also* Recycle Bin**
 - authoritative restore, 536–537
 - authoritative restore of group memberships, 539
 - Directory Services Restore Mode (DSRM), 528–529
 - explained, 528
 - full-server recovery of domain controllers, 538–539
 - GPOs (Group Policy Objects), 545, 547–548
 - linked-value replication, 539
 - nonauthoritative restore, 529–534
 - recovering back-links of authoritatively restored objects, 537
 - wbadmin command, 534–535
- RestoreAllGPOs.wsf, 548**
- RestoreGPO.wsf, 548**
- restoring**
 - authoritative, 536
 - certificate databases, 580–581
 - certificates and keys, 577–578
- restricted groups, 384–385**
- Resultant Set of Policy. *See* RSoP**
- Retry Interval setting (SOA records), 68**
- reverse lookup zones, 59–60**
- Revoked Certificates Properties dialog box, 618**

revoking certificates

Authority Information Access (AIA),
624–625

certificate revocation lists (CRLs)

CDPs (CRL distribution points),
619–620

configuring, 617, 619

troubleshooting, 620–621

explained, 616–617

online responders, 621–624

RID masters, 162

RidManager test (dcdiag utility), 495

Rights account certificate (RAC), 229

**Rights Management Service. See AD
RMS (Active Directory Rights
Management Service)**

**RODCs (read-only domain con-
trollers), 33, 52**

administrator role separation, 261–262

BitLocker

enabling, 265–269

explained, 263–264

managing, 269–270

preparing for, 265

turning off, 269

“Do I Know This Already?” quiz,
251–253

exam preparation tasks, 278

installing, 256–257

password replication

authentication list administration,
275–276

configuring, 272–273

credential caching, 273–275

explained, 270–271

planning, 271–272

planning use of, 254–255

preparing for, 255–256

prestaging, 257–259

read-only DNS, 262–263

syskey utility, 276–277

unidirectional replication, 260–261

role services, 210

role-based administration, 581

roles, 33. See also server roles

adding, 36

administration roles, assigning,
581–582

role-based administration, 581

root CAs (certificate authorities)

defined, 566

installing, 567–568, 570–571

root hints, 116–117

**Root Hints tab (Properties dialog
box), 116**

root-level domains, 49

**Round Robin setting (DNS server),
124–125**

RSoP (Resultant Set of Policy)

Delegation of Control Wizard, 509

explained, 496–497

Gpresult, 509–510

Gpupdate, 511

logging mode, 501–508

planning mode, 497–501

saving RSoP data, 508–509

S

s option (Gpresult), 509

s parameter (dcdiag utility), 495

**SAM (Security Accounts Manager)
database, 77**

**Save Filter to Custom View dialog
box, 470**

**saving RSoP (Resultant Set of Policy)
data, 508–509**

scavenging, 65–66, 126

**SCEP (Simple Certificate Enrollment
Protocol), 602**

Schedule for (site link name) dialog box, 197

Schedule for dialog box, 199

scheduling

backups, 526–527

replication

forcing replication, 200–201

intersite replication, 196–198

intrasite replication, 198–199

Schema Admins group, 154

schema masters

configuring schema, 154–155

deactivating schema objects, 159–160

extending schema, 155–158

schema definitions, 153–154

schema partitions, 25

schemas

configuring, 154–155

deactivating schema objects, 159–160

default schemas, 24

explained, 24

extending, 155–158

modifying, 24

scope, replication scope, 128–131

scope option (Gpresult), 510

scripts

backup and restore scripts, 548

creating accounts with, 296

SDDNS (Secure Dynamic DNS), 65

second-level domains, 49

secondary name servers, 55–56

secondary zones, 53

Secure Dynamic DNS (SDDNS), 65

security, 34. *See also* backups

account policies

account lockout policy, 426–427

domain password policies, 423, 425

Kerberos policy, 428

unlocking accounts, 427

AD LDS security principal, 223

additional security-related policy

settings, 436–439

audits

configuring with Auditpol.exe, 447, 449

configuring with GPOs, 442–447

“Do I Know This Already?” quiz, 417–421

exam preparation task, 449–450

new features, 441–442

backup permissions, 521

fine-grained password policies

configuring, 430–434

explained, 428–429

managing, 435

password settings precedence, 429

viewing resultant PSO, 435–436

secure zone transfer, 134–136

security configuration tools, 439–441

user authentication, smart cards,

609–610, 612–615

Security Accounts Manager (SAM) database, 77

Security Configuration and Analysis snap-in, 439

Security Configuration Wizard, 439

Security Filtering (GPOs), 371–372

security identifiers (SIDs), 21–22

“Security Options” (article), 438

Security Settings dialog box, 372

Security tab (Software Package Properties dialog box), 407

Security Templates snap-in, 439

seizing operations master roles, 167–168

Select a Domain page (Active Directory Installation Wizard), 89

Select a Site page (Active Directory Installation Wizard), 88**Select Schema Object dialog box, 157, 159****selective authentication, 339****self-enrollments (AD RMS), 230****Serial Number setting (SOA records), 68****Server Core, 33**

AD LDS (Active Directory Lightweight Directory Service) on, 224–225

domain controllers, 92

Server Licensor certificate (SLC), 229**Server Manager**

adding roles and features, 36

capabilities, 36

command-line server management, 36

opening, 35

Server Options (DNS server), 123–124**Server Performance Advisor, 486****server roles. *See also names of specific roles***

AD CS (Active Directory Certificate Services), 210

AD FS (Active Directory Federation Service)

explained, 210, 231–232
federation trust configuration, 238–243

installing, 233–236

role services, 232–233

trust policy configuration, 236–237
user and group claim mapping, 237–238

Web agents, 233

AD LDS (Active Directory Lightweight Directory Service)

AD LDS security principal, 223

binding to AD LDS instances, 222, 224

configuration, 217–221

creating AD LDS user accounts and groups, 222–223

explained, 210–213

installation, 213–216

migrating to, 221

on Server Core, 224–225

AD MDS (Active Directory Metadirectory Services), 231

AD RMS (Active Directory Rights Management Service)

benefits of, 225–226

certificate request and installation, 228–230

delegation, 230–231

enhancements to, 226

explained, 210

installing, 226–228

self-enrollments, 230

“Do I Know This Already?” quiz, 208–209

installing, 211

removing, 211

role services, 210

server scavenging, 126**“Server Security Policy Management in Windows Server 2008” (article), 441****ServerManagerCmd command, 36, 769****servers**

bridgehead servers, 193–194

DNS servers. *See* DNS servers

flexible single-master operations (FSMO) servers, 32–33

GC (global catalog) servers, 31–32

features, 148

partial attribute sets, 152–153

placement, 148–150

promoting domain controllers to, 150
removing, 151

UGMC (Universal Group Membership Caching), 151

- name servers, configuration, 136–138
- roles, 33
 - adding*, 36
 - “Do I Know This Already?” quiz*, 205–207
 - exam preparation tasks*, 247–248
- Server Core, 33
- Server Manager
 - adding roles and features*, 36
 - capabilities*, 36
 - command-line server management*, 36
 - opening*, 35
- Windows Server. *See* Windows Server 2008 R2
- service (SRV) resource record, 61
- Service Account Selection Partition page (Lightweight Directory Services Setup Wizard), 215
- Services test (dcdiag utility), 496
- Set Domain Functional Level page (Active Directory Installation Wizard), 88
- Set Forest Functional Level page (Active Directory Installation Wizard), 85
- Setting Up Certificate Enrollment Web Services’ (article), 609
- Setup Options page (Lightweight Directory Services Setup Wizard), 214
- shell access policies, 387
- shortcut trusts
 - creating, 337
 - explained, 327
- Show Attribute Meta-Data for Active Directory Object option (replmon utility), 490
- Show Bridgehead Servers option (replmon utility), 490
- Show Current Performance Data option (replmon utility), 490
- Show Domain Controllers in Domain option (replmon utility), 490
- Show Global Catalog Servers in Enterprise option (replmon utility), 490
- Show Group Policy Object Status option (replmon utility), 490
- Show Replication Topologies option (replmon utility), 490
- Show Trust Relationships option (replmon utility), 490
- showconn parameter (repladmin utility), 493
- showmeta parameter (repladmin utility), 492
- showreps parameter (repladmin utility), 492
- SID filtering, 340–341
- “SID Filtering Dialog box—Securing External Trusts” (article), 341
- SIDs (security identifiers), 21–22
- signing certificates, obtaining, 610
- Simple Certificate Enrollment Protocol (SCEP), 602
- Simple Mail Transfer Protocol (SMTP), 184
- site link bridges, 185
- site links
 - configuring, 185–186
 - costs, 186–188
 - explained, 184
- sites
 - benefits of, 178–179
 - creating, 180–181
 - “Do I Know This Already?” quiz*, 173–177
 - domain controllers, adding, 181
 - exam preparation tasks, 201–202
 - explained, 30, 178

- ISTG (Intersite Topology Generator), 189
- KCC (Knowledge Consistency Checker), 189
- planning, 179
- site link bridges, 185
- site links
 - configuring, 185–186*
 - costs, 186–188*
 - explained, 184*
 - subnets, creating, 182–184
- skip parameter (dcdiag utility), 495**
- SLC (Server Licensor certificate), 229**
- Slides of Trust page (New Trust Wizard), 332**
- smart card authentication strategy, implementing, 609–610, 612–615**
- smart card enrollment, configuring, 609–610**
- SMTP (Simple Mail Transfer Protocol), 184**
- snap-ins**
 - Active Directory Schema, 220
 - Active Directory Sites and Services, 179, 221
 - adding domain controllers, 181*
 - creating sites, 180–181*
 - creating subnets, 182–184*
 - ADSI Edit, 217–218
 - Certificates, installing, 573–574
 - DFS Management, 193
 - Security Configuration and Analysis, 439
 - Security Templates, 439
- SOA (start of authority) resource record, 61, 68**
- software**
 - package properties, 405
 - redeploying, Group Policy and, 413
- software deployment**
 - assigning software
 - to computers, 399*
 - to users, 399*
 - benefits of, 398
 - “Do I Know This Already?” quiz, 393–397
 - exam preparation tasks, 414
 - with Group Policy
 - explained, 400–401*
 - software installation properties, 403–405*
 - software package properties, 405–407*
 - ZAP files, 402–403*
 - modifying software packages with transform files, 409–410
 - publishing software to users, 399
 - redeploying upgraded software, 411–412
 - removing software, 413
 - software lifecycle, 398–399
 - upgrading software, 407–409
- Software Installation and Maintenance**
 - assigning software, 399
 - publishing software, 399
- Software Installation Properties dialog box, 403, 405**
- Software Package Properties dialog box, 405–407**
- solution accelerators, 771**
- “Specify CRL Distribution Points” (article), 620**
- Specify the Computer Name page (Active Directory Domain Services Installation Wizard), 258**
- SRV (service) resource record, 61**
- staging environments, 548**
- standalone CAs (certificate authorities), 566**

start of authority (SOA) resource record, 61, 68

Starter GPOs, 385–387

statistics command (dnscmd), 70

Stop Other Services dialog box, 550

Strict RFC (ANSI), 125

stub zones, 53

subdividing namespaces, 77–78

subnets, creating, 182–184

subordinate CAs (certificate authorities), installing, 571

Summary page (Active Directory Installation Wizard), 87

Support Tools, Event Viewer, customizing, 470–471

sync parameter (repadmin utility), 493

syncall parameter (repadmin utility), 493

Synchronize Each Directory Partition with All Servers option (replmon utility), 490

syskey utility, 276–277

Sysprep, 771

system keys, 276–277

System Recovery Options dialog box, 538

Systemlog test (dcdiag utility), 496

SYSVOL folder, replication, 261

SysvolPath option (Active Directory installation), 91

T

target option (Gpupdate), 511

Task Manager, 463–465

template accounts, 290–291

templates

- administrative templates, 380–384
- certificate templates
 - archiving keys*, 599

- configuring*, 593–595
- defined*, 592
- duplicating*, 597–598
- enabling*, 597
- key recovery agents (KRAs)*, 599–602
- permissions*, 595–597
- template types*, 592

GPTs (Group Policy Templates), 352–353

- template accounts, 290–291

test parameter (dcdiag utility), 495

three-tier CA hierarchy, 566

Time Service (W32time), 161–162

time to live (TTL), 66–68

top-level domains, 49

TPM (Trusted Platform Module), 263–264

transfer, zone transfer

- configuration, 132–133
- full zone transfer (AXFR), 130
- incremental zone transfer (IXFR), 131
- secure zone transfer, 134–136

transferring operations master roles, 165–167

transform files

- compared to patches, 411
- modifying software packages with, 409–410

transitive trusts, 325–326

trees

- explained, 27
- multiple trees, 79

troubleshooting

- certificate revocation lists (CRLs), 620–621
- Group Policy with RSoP
 - Delegation of Control Wizard*, 509
 - explained*, 496–497
 - Gpresult*, 509–510
 - Gpupdate*, 511

- logging mode*, 501–508
 - planning mode*, 497–501
 - saving RSoP data*, 508–509
 - Trust Anchors tab (Properties dialog box)**, 122
 - Trust Creation Complete page (New Trust Wizard)**, 333
 - Trust Name page (New Trust Wizard)**, 330–331
 - trust policies, configuring**, 236–237
 - trust relationships**
 - authentication scope, 338–340
 - defined, 325
 - “Do I Know This Already?” quiz, 321–324
 - exam preparation tasks, 343
 - external trusts
 - creating*, 335–336
 - explained*, 326
 - forest trusts
 - creating*, 329–330, 332–335
 - explained*, 326
 - prerequisites, 328–329
 - realm trusts
 - creating*, 336
 - explained*, 326
 - removing cross-forest trust relationships, 341–342
 - shortcut trusts
 - creating*, 337
 - explained*, 327
 - SID filtering, 340–341
 - table of trust type, 328
 - transitive trusts, 325–326
 - validating, 338
 - Trust Selections Complete page (New Trust Wizard)**, 333
 - Trust Type page (New Trust Wizard)**, 330–331
 - Trusted Platform Module (TPM)**, 263–264
 - trusts, federation trusts**
 - account stores, 240–241
 - claims, 239
 - configuring, 238–241
 - configuring/enabling applications, 241–242
 - creating, 242–243
 - TTL (time to live)**, 66–68
 - turning off BitLocker**, 269
 - two-tier CA hierarchy**, 566
- ## U
- u option (Gpresult)**, 510
 - u parameter (dcdiag utility)**, 495
 - UGMC (Universal Group Membership Caching)**, 151
 - unattend.xml file**, 770
 - unattended installations of Active Directory**, 90–92
 - “Understanding AD FS Role Services” (article)**, 233
 - “Understanding AD RMS Certificates” (article)**, 230
 - “Understanding Claims” (article)**, 238
 - “Understanding User Accounts” (article)**, 286
 - “Understanding When to Create a Shortcut Trust” (article)**, 337
 - unidirectional replication**, 260–261
 - Universal Group Membership Caching (UGMC)**, 151
 - unlocking accounts**, 427
 - Update Status option (replmon utility)**, 490
 - Upgrades tab (Software Package Properties dialog box)**, 406
 - upgrading**
 - domain and forest functional levels, 95–96

- software, 407–409
 - Windows Server 2003 domain controllers, 97
 - Windows Server 2003 or 2008 computers, 769–770
- UPNs (user principal names), 21, 101–102, 296–298**
- Use license, 230**
- “Use the Network Device Enrollment Service” (article), 604**
- user accounts**
 - contact, 298–299
 - creating
 - with Csvde tool, 292–293*
 - with Dsadd tool, 294–295*
 - with Ldifde tool, 293–294*
 - manually, 288–290*
 - with scripts, 296*
 - delegating administrative control, 313–316
 - deprovisioning, 312–313
 - distribution lists, 299–300
 - “Do I Know This Already?” quiz, 281–285
 - exam preparation tasks, 317–318
 - explained, 286
 - Protected Admin accounts, 309–310
 - resetting, 308
 - template accounts, 290–291
 - UPNs (user principal names), 296–298
- user authentication, smart cards, implementing, 609–610, 612–615**
- user objects, disabling, 370**
- user option (Gpresult), 509**
- user principal names (UPNs), 21, 101–102, 296–298**
- user rights (Group Policy), 378**
- UserName option (Active Directory installation), 90**
- users**
 - administrator role separation, 261–262
 - assigning software to, 399
 - publishing software to, 399
- “Using Identity Federation with Active Directory Rights Management Services Step-by-Step Guide” (article), 237**
- utilities**
 - Adprep, 96–97
 - Adprep /rodcp, 255
 - Auditpol.exe, 447, 449
 - Csvde, 292–293
 - dcdiag, 494–496
 - dnscmd, 137–138
 - Dsadd, 223, 294–295
 - dsget, 295
 - dsmgmt, 262
 - dsmod, 295
 - dsmove, 295
 - dsquery, 295
 - dsrm, 295
 - Event Viewer, 466–471
 - Gpresult, 509–510
 - Gpupdate, 511
 - Ldifde, 293–294, 434
 - Ldp.exe, 218–220, 541–544
 - Network Monitor, 459–461, 463
 - nmcap.exe, 463
 - ntdsutil, 529
 - Performance Monitor, 476–479
 - Reliability Monitor, 473, 475
 - repadmin, 491
 - /add parameter, 492–493*
 - /replicate parameter, 491*
 - /replsummary parameter, 494*
 - /showconn parameter, 493*
 - /showmeta parameter, 492*

/showreps parameter, 492

/sync parameter, 493

/syncall parameter, 493

replmon, 487–491

Resource Monitor, 473–474

Server Performance Advisor, 486

syskey, 276–277

Task Manager, 463–465

wbadmin, 525, 534–535

Windows System Resource Manager (WSRM), 484–486

V

v option (Gpresult), 510

v parameter (dcdiag utility), 495

validating trust relationships, 338

verifying Active Directory installation, 98, 100

VerifyReferences test (dcdiag utility), 496

VHD (virtual hard disk) files, 245–246

viewing PSOs, 435–436

virtual hard disk (VHD) files, 245–246

virtualization, Windows Server 2008 R2, 244–246

W

W32time, 161–162

wait option (Gpupdate), 511

wbadmin command, 525, 534–535

WDS (Windows Deployment Services), 771

Web agents (AD FS), 233

Welcome page (Active Directory Installation Wizard), 87

“What’s New in AD DS: Active Directory Recycle Bin” (article), 545

“What’s New in Group Policy” (article), 355

Windows Deployment Services (WDS), 771

Windows Installer, 412

Windows Management Instrumentation (WMI), 374

Windows Memory Diagnostic tool, 764

Windows PowerShell, 296, 374–376

Windows PowerShell 2.0, explained, 37

Windows Script Host (WSH), 296

Windows Server 2003

Support Tools, Event Viewer, 470–471
upgrading, 769–770

Windows Server 2003 domain controllers, upgrading, 97

Windows Server 2008

Active Directory. *See* Active Directory certificate services. *See* AD CS (Active Directory Certificate Services)
security configuration tools, 439–441

upgrading, 769–770

Windows Server 2008 R2

features, 211

hardware requirements, 763–764

installation

automated installation, 770–771

complete server installation from DVD-ROM, 764–766

upgrading Windows Server 2003 or 2008 computers, 769–770

Windows Server Core commands, 768–769

Windows Server Core computers, 767–768

installing DNS (Domain Name System) on, 49–51

new features, 37–39

virtualization, 244–246

“Windows Server 2008 Restartable AD DS Step-by-Step Guide” (article), 550

Windows Server Backup

- backing up critical volumes of domain controllers, 522–524
- backup permissions, 521
- installing, 521–522
- to removable media, 527
- restore options. *See also* Recycle Bin
 - authoritative restore, 536–537*
 - authoritative restore of group memberships, 539*
 - Directory Services Restore Mode (DSRM), 528–529*
 - explained, 528*
 - full-server recovery of domain controllers, 538–539*
 - GPOs (Group Policy Objects), 545, 547–548*
 - linked-value replication, 539*
 - nonauthoritative restore, 529–534*
 - recovering back-links of authoritatively restored objects, 537*
 - wbadmin command, 534–535*
- scheduling backups, 526–527
- wbadmin utility, 525
- Windows Server 2008 versus Windows Server 2008 R2, 520–521

Windows Server Core

- commands, 768–769
- installation, 767–768

Windows Server Migration Tools, 39

Windows System Resource Manager (WSRM), 484–486

Windows Time Service (W32time), 161–162

Windows token-based agents, 233

WINS, integrating with DNS (Domain Name System), 68–69

wizards

- Active Directory Installation Wizard, 82
 - installing domain controllers in existing domains, 89*
 - installing new domains in existing forests, 88*
 - installing new forests, 83–87*
- AD DS Installation Wizard, 256–257
- Add Monitored Server Wizard, 487, 489–491
- Add Revocation Configuration Wizard, 623
- Add Role Services Wizard, 603
- Add Roles Wizard, 36, 83
 - installing CAs with, 567–568, 570–571*
- Certificate Export Wizard, 576–577
- Certificate Import Wizard, 577–578
- Certification Authority Backup Wizard, 580–581
- Certification Authority Restore Wizard, 581
- Configure a DNS Server Wizard, 117
- Create New Data Collector Set Wizard, 480–481
- Delegation of Control Wizard, 364, 509
- Import Settings Wizard, 547–548
- Lightweight Directory Services Setup Wizard, 214–216
- New Connection Security Rule Wizard, 134–136
- New Delegation Wizard, 118
- New Trust Wizard
 - creating external trusts, 335–336*
 - creating forest trusts, 329–330, 332–335*
 - creating realm trusts, 336*
 - creating shortcut trusts, 337*

Recovery Wizard, 531–534
 Security Configuration Wizard, 439
WMI (Windows Management Instrumentation), 374
“Work with WMI Filters” (article), 374
WSH (Windows Script Host), 296
WSRM (Windows System Resource Manager), 484–486

X-Z

X.500, 17–18

z option (Gpresult), 510

ZAP (Zero Administration Package) files, 402–403

zoneadd command (dnscmd), 70

zonedelete command (dnscmd), 70

zoneexport command (dnscmd), 70

zoneinfo command (dnscmd), 70

zones (DNS)

adding authoritative secondary servers to, 63

configuring zone properties, 62

configuring zone types, 63

creating, 57–60

DNS notify, 133–134

forward lookup zones, 57–58

GlobalNames zones, 54–55

integrated zones, 53–54

loading zone data, 126

primary zones, 53

replication scope, 128–130

reverse lookup zones, 59–60

secondary zones, 53

stub zones, 53

time to live (TTL), 66–68

zone delegation, 117–119

zone scavenging, 65–66

zone transfer

configuration, 132–133

full zone transfer (AXFR), 130

incremental zone transfer

(IXFR), 131

secure zone transfer, 134–136

This page intentionally left blank

Try Safari Books Online FREE

Get online access to 5,000+ Books and Videos



Safari[®]
Books Online

FREE TRIAL—GET STARTED TODAY!
www.informit.com/safaritrial



Find trusted answers, fast

Only Safari lets you search across thousands of best-selling books from the top technology publishers, including Addison-Wesley Professional, Cisco Press, O'Reilly, Prentice Hall, Que, and Sams.



Master the latest tools and techniques

In addition to gaining access to an incredible inventory of technical books, Safari's extensive collection of video tutorials lets you learn from the leading video training experts.

WAIT, THERE'S MORE!



Keep your competitive edge

With Rough Cuts, get access to the developing manuscript and be among the first to learn the newest technologies.



Stay current with emerging technologies

Short Cuts and Quick Reference Sheets are short, concise, focused content created to get you up-to-speed quickly on new and cutting-edge technologies.



Adobe Press



Cisco Press



IBM Press



Microsoft Press



O'REILLY



que



SAMS



Your Publisher for IT Certification

Pearson IT Certification is the leader in technology certification learning and preparation tools.

Visit pearsonITcertification.com today to find

- **CERTIFICATION EXAM** information and guidance for IT certifications, including



- **EXAM TIPS AND TRICKS** by reading the latest articles and sample chapters by Pearson IT Certification's expert authors and industry experts, such as

- Mark Edward Soper and David Prowse – CompTIA
- Wendell Odom – Cisco
- Shon Harris – Security
- Thomas Erl – SOACP



- **SPECIAL OFFERS** (pearsonITcertification.com/promotions)
- **REGISTRATION** for your Pearson IT Certification products to access additional online material and receive a coupon to be used on your next purchase

Be sure to create an account on **pearsonITcertification.com** and receive member's-only offers and benefits.

Pearson IT Certification is a publishing imprint of Pearson



Connect with Pearson IT Certification

pearsonITcertification.com/newsletters



twitter.com/pearsonITCert



facebook.com/pearsonitcertification



youtube.com/pearsonITCert



pearsonitcertification.com/rss/

This page intentionally left blank

