

Microsoft

EXAM 70-640

Covers Windows
Server 2008

R2

Configuring Windows Server® 2008 Active Directory®



Dan Holme
Nelson Ruest
Danielle Ruest
Jason Kellington

SECOND EDITION

Training Kit

Exam 70-640: Windows Server 2008 Active Directory, Configuring (2nd Edition)

OBJECTIVE	LOCATION IN BOOK
CONFIGURING DOMAIN NAME SYSTEM (DNS) FOR ACTIVE DIRECTORY	
Configure zones.	Chapter 9, Lesson 1
Configure DNS server settings.	Chapter 9, Lesson 2
Configure zone transfers and replication.	Chapter 9, Lesson 2
CONFIGURING THE ACTIVE DIRECTORY INFRASTRUCTURE	
Configure a forest or a domain.	Chapter 1, Lessons 1, 2 Chapter 10, Lessons 1, 2 Chapter 12, Lessons 1, 2
Configure trusts.	Chapter 12, Lesson 2
Configure sites.	Chapter 11, Lessons 1, 2
Configure Active Directory replications.	Chapter 8, Lesson 3 Chapter 10, Lesson 3 Chapter 11, Lesson 3
Configure the global catalog.	Chapter 11, Lesson 2
Configure operations masters.	Chapter 10, Lesson 2
CONFIGURING ADDITIONAL ACTIVE DIRECTORY SERVER ROLES	
Configure Active Directory Lightweight Directory Service (AD LDS).	Chapter 14, Lessons 1, 2
Configure Active Directory Rights management Service (AD RMS).	Chapter 16, Lessons 1, 2
Configure the read-only domain controller (RODC).	Chapter 8, Lesson 3
Configure Active Directory Federation Services (AD FS).	Chapter 17, Lessons 1, 2
CREATING AND MAINTAINING ACTIVE DIRECTORY OBJECTS	
Automate creation of Active Directory accounts.	Chapter 3, Lessons 1, 2 Chapter 4, Lessons 1, 2 Chapter 5, Lessons 1, 2
Maintain Active Directory accounts.	Chapter 2, Lessons 1, 2, 3 Chapter 3, Lessons 1, 2, 3 Chapter 4, Lessons 1, 2, 3 Chapter 5, Lessons 1, 2, 3 Chapter 8, Lesson 4
Create and apply Group Policy objects (GPOs).	Chapter 6, Lessons 1, 2, 3
Configure GPO templates.	Chapter 6, Lessons 1, 2, 3 Chapter 7, Lessons 1, 2, 3
Configure software deployment GPOs.	Chapter 7, Lesson 3
Configure account policies.	Chapter 8, Lesson 1
Configure audit policy by using GPOs.	Chapter 7, Lesson 4 Chapter 8, Lesson 2
MAINTAINING THE ACTIVE DIRECTORY ENVIRONMENT	
Configure backup and recovery.	Chapter 13, Lesson 2
Perform offline maintenance.	Chapter 13, Lesson 1
Monitor Active Directory.	Chapter 6, Lesson 3 Chapter 11, Lesson 3 Chapter 13, Lesson 1
CONFIGURING ACTIVE DIRECTORY CERTIFICATE SERVICES	
Install Active Directory Certificate Services.	Chapter 15, Lesson 1
Configure CA server settings.	Chapter 15, Lesson 2
Manage certificate templates.	Chapter 15, Lesson 2
Manage enrollments.	Chapter 15, Lesson 2
Manage certificate revocations	Chapter 15, Lesson 2

Exam Objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning Web site for the most current listing of exam objectives: <http://www.microsoft.com/learning/en/us/Exam.aspx?ID=70-640>.

**Self-Paced Training
Kit (Exam 70-640):
Configuring Windows
Server® 2008 Active
Directory® (2nd Edition)**

Dan Holme
Danielle Ruest
Nelson Ruest
Jason Kellington

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

Copyright © 2011 by Dan Holme, Nelson Ruest, Danielle Ruest, and Jason Kellington

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

Library of Congress Control Number: 2011929710
ISBN: 978-0-7356-5193-7

Printed and bound in the United States of America.

7 8 9 10 11 12 13 14 15 QG 8 7 6 5 4 3

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

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

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

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

Acquisitions Editor: Jeff Koch

Developmental Editor: Karen Szall

Project Editor: Rosemary Caperton

Editorial Production: Tiffany Timmerman, S4Carlisle Publishing Services

Technical Reviewer: Kurt Meyer; Technical Review services provided by Content Master, a member of CM Group, Ltd.

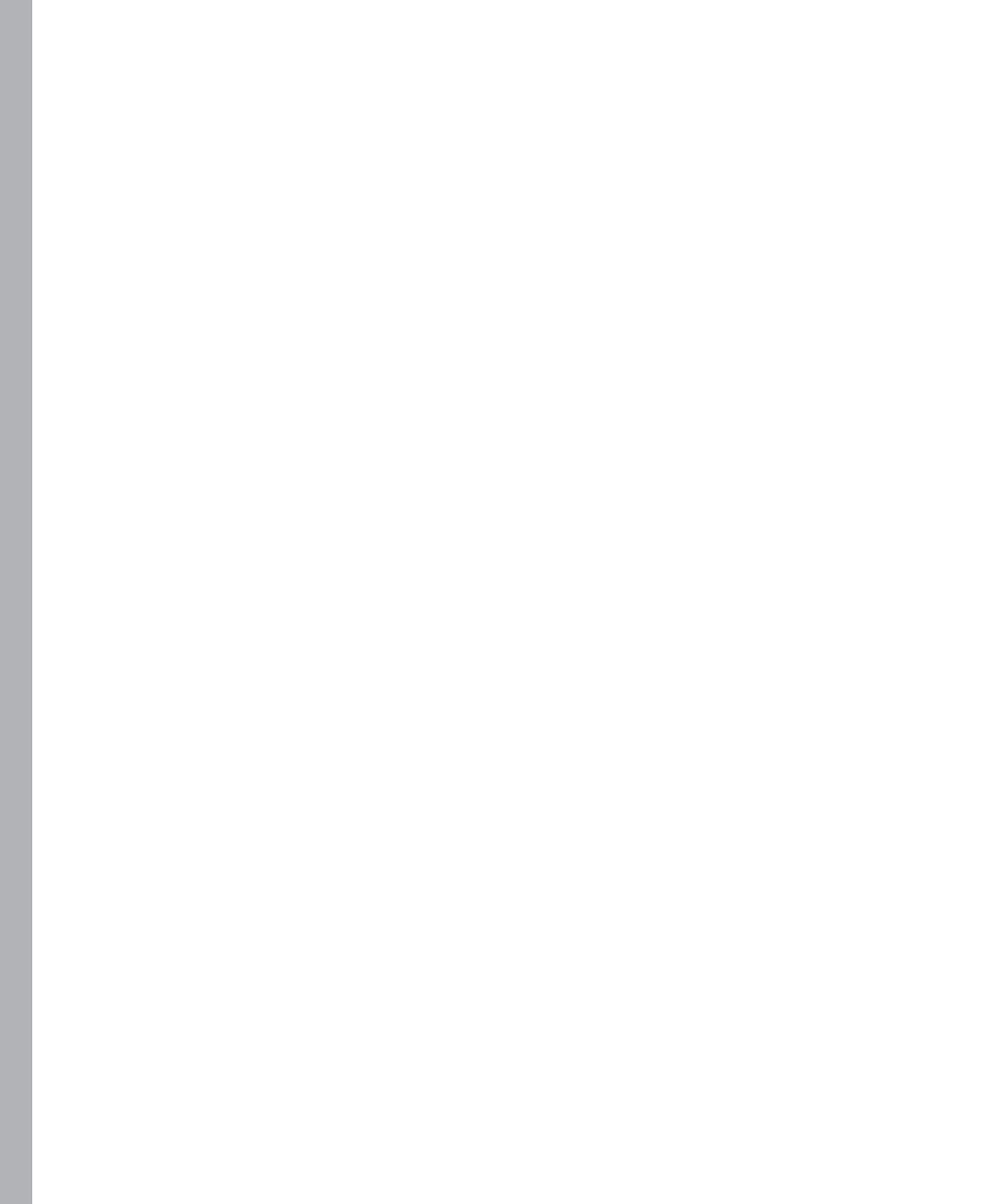
Copyeditor: Crystal Thomas

Indexer: Maureen Johnson

Cover: Twist Creative • Seattle

Contents at a Glance

	<i>Introduction</i>	<i>xxvii</i>
CHAPTER 1	Creating an Active Directory Domain	1
CHAPTER 2	Administering Active Directory Domain Services	35
CHAPTER 3	Administering User Accounts	87
CHAPTER 4	Managing Groups	149
CHAPTER 5	Configuring Computer Accounts	205
CHAPTER 6	Implementing a Group Policy Infrastructure	247
CHAPTER 7	Managing Enterprise Security and Configuration with Group Policy Settings	317
CHAPTER 8	Improving the Security of Authentication in an AD DS Domain	389
CHAPTER 9	Integrating Domain Name System with AD DS	439
CHAPTER 10	Administering Domain Controllers	507
CHAPTER 11	Managing Sites and Active Directory Replication	557
CHAPTER 12	Managing Multiple Domains and Forests	605
CHAPTER 13	Directory Business Continuity	655
CHAPTER 14	Active Directory Lightweight Directory Services	731
CHAPTER 15	Active Directory Certificate Services and Public Key Infrastructures	771
CHAPTER 16	Active Directory Rights Management Services	833
CHAPTER 17	Active Directory Federation Services	879
	<i>Answers</i>	<i>921</i>
	<i>Index</i>	<i>963</i>



Contents

Introduction	xxvii
System Requirements	xxvii
Hardware Requirements	xxviii
Software Requirements	xxix
Using the Companion CD	xxx
How to Install the Practice Tests	xxx
How to Use the Practice Tests	xxx
How to Uninstall the Practice Tests	xxxii
Acknowledgments	xxxii
Support & Feedback	xxxii
Errata	xxxiii
We Want to Hear from You	xxxiii
Stay in Touch	xxxiii

Chapter 1 Creating an Active Directory Domain	1
Before You Begin	2
Lesson 1: Installing Active Directory Domain Services	3
Active Directory, Identity and Access	3
Beyond Identity and Access	8
Components of an Active Directory Infrastructure	9
Preparing to Create a New Windows Server 2008 Forest	12
Adding the AD DS Role Using the Windows Interface	12
Creating a Domain Controller	13
Lesson Summary	21
Lesson Review	22

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Lesson 2: Active Directory Domain Services on Server Core	23
Understanding Server Core	23
Installing Server Core	24
Performing Initial Configuration Tasks	25
Server Configuration	26
Adding AD DS to a Server Core Installation	27
Removing Domain Controllers	27
Lesson Summary	30
Lesson Review	30
Chapter Review	32
Chapter Summary	32
Key Terms	32
Case Scenario	33
Case Scenario: Creating an Active Directory Forest	33
Take a Practice Test	33

Chapter 2 Administering Active Directory Domain Services 35

Before You Begin	35
Lesson 1: Working with Active Directory Snap-ins	37
Understanding the Microsoft Management Console	37
Active Directory Administration Tools	39
Finding the Active Directory Administrative Tools	39
Adding the Administrative Tools to Your Start Menu	40
Creating a Custom Console with Active Directory Snap-ins	40
Running Administrative Tools with Alternate Credentials	41
Saving and Distributing a Custom Console	42
Lesson Summary	47
Lesson Review	48
Lesson 2: Creating Objects in Active Directory	49
Creating an Organizational Unit	49
Creating a User Object	51
Creating a Group Object	53
Creating a Computer Object	55
Finding Objects in Active Directory	57

Understanding DNs, RDNs, and CNs	63
Finding Objects by Using Dsquery	63
Lesson Summary	70
Lesson Review	71
Lesson 3: Delegation and Security of Active Directory Objects	72
Understanding Delegation	72
Viewing the ACL of an Active Directory Object	73
Property Permissions, Control Access Rights, and Object Permissions	75
Assigning a Permission Using the Advanced Security Settings Dialog Box	76
Understanding and Managing Permissions with Inheritance	76
Delegating Administrative Tasks with the Delegation Of Control Wizard	77
Reporting and Viewing Permissions	78
Removing or Resetting Permissions on an Object	78
Understanding Effective Permissions	79
Designing an OU Structure to Support Delegation	80
Lesson Summary	82
Lesson Review	83
Chapter Review	84
Chapter Summary	84
Key Terms	84
Case Scenario	84
Case Scenario: Managing Organizational Units and Delegation	84
Suggested Practices	85
Maintain Active Directory Accounts	85
Take a Practice Test	86

Chapter 3 Administering User Accounts 87

Before You Begin	88
Lesson 1: Automating the Creation of User Accounts	89
Creating Users with Templates	89
Using Active Directory Command-Line Tools	91

Creating Users with DSAdd	92
Exporting Users with CSVDE	92
Importing Users with CSVDE	93
Importing Users with LDIFDE	94
Lesson Summary	100
Lesson Review	100
Lesson 2: Administering with Windows PowerShell and Active Directory Administrative Center	102
Introducing Windows PowerShell	102
Preparing to Administer Active Directory Using Windows PowerShell	103
cmdlets	105
Parameters	107
Get-Help	107
Objects	108
Variables	108
Pipeline	109
Aliases	111
Namespaces, Providers, and PSDrives	112
The Active Directory PowerShell Provider	113
Creating a User with Windows PowerShell	113
Populating User Attributes	115
Importing Users from a Database with Windows PowerShell	116
The Active Directory Administrative Center	117
Lesson Summary	123
Lesson Review	124
Lesson 3: Supporting User Objects and Accounts	125
Managing User Attributes with Active Directory Users And Computers	125
Managing User Attributes with DSMod and DSGet	129
Managing User Attributes with Windows PowerShell	131
Understanding Name and Account Attributes	131
Administering User Accounts	135
Lesson Summary	143
Lesson Review	143

Chapter Review	145
Chapter Summary.....	145
Key Terms.....	145
Case Scenario.....	145
Case Scenario: Import User Accounts	146
Suggested Practices	146
Automate the Creation of User Accounts	146
Maintain Active Directory Accounts	146
Use the Active Directory Administrative Console	147
Take a Practice Test.....	147

Chapter 4 Managing Groups 149

Before You Begin.....	149
Lesson 1: Managing an Enterprise with Groups	151
Understanding the Importance of Groups	151
Defining Group Naming Conventions	157
Understanding Group Types	159
Understanding Group Scope	160
Converting Group Scope and Type	165
Managing Group Membership	166
Developing a Group Management Strategy	169
Lesson Summary	173
Lesson Review	173
Lesson 2: Automating the Creation and Management of Groups.....	175
Creating Groups with DSAdd	175
Importing Groups with CSVDE	176
Importing Groups with LDIFDE	177
Retrieving Group Membership with DSGet	178
Changing Group Membership with DSMod	179
Copying Group Membership	179
Moving and Renaming Groups with DSMove	179
Deleting Groups with DSRm	180
Managing Groups with Windows PowerShell	181

Lesson Summary	184
Lesson Review	185
Lesson 3: Administering Groups in an Enterprise	186
Best Practices for Group Attributes	186
Protecting Groups from Accidental Deletion	188
Delegating the Management of Group Membership	189
Understanding Shadow Groups	193
Default Groups	194
Special Identities	196
Lesson Summary	199
Lesson Review	199
Chapter Review	201
Chapter Summary	201
Key Terms	201
Case Scenario	202
Case Scenario: Implementing a Group Strategy	202
Suggested Practices	202
Automate Group Membership and Shadow Groups	202
Take a Practice Test.	203

Chapter 5 Configuring Computer Accounts 205

Before You Begin	206
Lesson 1: Creating Computers and Joining the Domain	207
Understanding Workgroups, Domains, and Trusts	207
Identifying Requirements for Joining a Computer to the Domain	208
The Computers Container and OUs	208
Delegating Permission to Create Computers	210
Prestaging a Computer Account	210
Joining a Computer to the Domain	211
Secure Computer Creation and Joins	214
Offline Domain Join	217
Lesson Summary	223
Lesson Review	224

Lesson 2: Automating the Creation of Computer Objects	225
Importing Computers with CSVDE	225
Importing Computers with LDIFDE	226
Creating Computers with DSAdd	227
Creating Computers with NetDom	227
Creating Computers with Windows PowerShell	228
Lesson Summary	230
Lesson Review	230
Lesson 3: Supporting Computer Objects and Accounts	232
Configuring Computer Properties	232
Moving a Computer	233
Managing a Computer from the Active Directory Users And Computers Snap-In	234
Understanding the Computer's Logon and Secure Channel	234
Recognizing Computer Account Problems	234
Resetting a Computer Account	235
Renaming a Computer	236
Disabling and Enabling Computer Accounts	238
Deleting Computer Accounts	238
Recycling Computer Accounts	239
Lesson Summary	241
Lesson Review	241
Chapter Review	243
Chapter Summary	243
Key Term	243
Case Scenarios	243
Case Scenario 1: Creating Computer Objects and Joining the Domain	244
Case Scenario 2: Automating the Creation of Computer Objects	244
Suggested Practices	244
Create and Maintain Computer Accounts	244
Take a Practice Test	245

Chapter 6	Implementing a Group Policy Infrastructure	247
	Before You Begin	248
	Lesson 1: Implementing Group Policy	249
	What Is Configuration Management?	249
	An Overview and Review of Group Policy	250
	Group Policy Objects	256
	Policy Settings	262
	Registry Policies in the Administrative Templates Node	265
	Lesson Summary	275
	Lesson Review	276
	Lesson 2: Managing Group Policy Scope	278
	GPO Links	278
	GPO Inheritance and Precedence	280
	Using Security Filtering to Modify GPO Scope	285
	WMI Filters	288
	Enabling or Disabling GPOs and GPO Nodes	290
	Targeting Preferences	291
	Group Policy Processing	292
	Loopback Policy Processing	294
	Lesson Summary	299
	Lesson Review	300
	Lesson 3: Supporting Group Policy	301
	Understanding When Settings Take Effect	301
	Resultant Set Of Policy	303
	Troubleshooting Group Policy with the Group Policy Results Wizard and Gpresult.exe	306
	Performing What-If Analyses with the Group Policy Modeling Wizard	306
	Examining Policy Event Logs	307
	Lesson Summary	311
	Lesson Review	311
	Chapter Review	313
	Chapter Summary	313
	Key Terms	313

Case Scenario.	313
Case Scenario: Implementing Group Policy	314
Suggested Practices	314
Create and Apply GPOs	314
Take a Practice Test.	315

Chapter 7 Managing Enterprise Security and Configuration with Group Policy Settings 317

Before You Begin.	317
Lesson 1: Delegating the Support of Computers	319
Understanding Restricted Groups Policies	319
Delegating Administration Using Restricted Groups Policies with the Member Of Setting	322
Delegating Administration Using Restricted Groups Policies with the Members Of This Group Setting	322
Lesson Summary	327
Lesson Review	327
Lesson 2: Managing Security Settings.	330
What Is Security Policy Management?	330
Configuring the Local Security Policy	331
Managing Security Configuration with Security Templates	333
The Security Configuration Wizard	339
Settings, Templates, Policies, and GPOs	345
Lesson Summary	351
Lesson Review	352
Lesson 3: Managing Software with Group Policy	353
Understanding Group Policy Software Installation	353
Preparing an SDP	356
Creating a Software Deployment GPO	356
Managing the Scope of a Software Deployment GPO	358
Maintaining Applications Deployed with Group Policy	359
GPSI and Slow Links	360
Understanding AppLocker	361
Lesson Summary	364
Lesson Review	365

Lesson 4: Implementing an Audit Policy	367
Audit Policy	367
Auditing Access to Files and Folders	370
Auditing Directory Service Changes	374
Lesson Summary	379
Lesson Review	380
Chapter Review	382
Chapter Summary	382
Key Terms	382
Case Scenarios	383
Case Scenario 1: Installing Software with Group Policy Software Installation	383
Case Scenario 2: Configuring Security	383
Suggested Practices	384
Configure Restricted Groups	384
Manage Security Configuration	386
Take a Practice Test	387

Chapter 8 Improving the Security of Authentication in an AD DS Domain 389

Before You Begin	390
Lesson 1: Configuring Password and Lockout Policies	392
Understanding Password Policies	392
Understanding Account Lockout Policies	394
Configuring the Domain Password and Lockout Policy	395
Fine-Grained Password and Lockout Policy	395
Understanding Password Settings Objects	397
PSO Precedence and Resultant PSO	398
PSOs and OUs	398
Lesson Summary	402
Lesson Review	403
Lesson 2: Auditing Authentication	404
Account Logon and Logon Events	404
Configuring Authentication-Related Audit Policies	405

Scoping Audit Policies	406
Viewing Logon Events	407
Lesson Summary	408
Lesson Review	408
Lesson 3: Configuring Read-Only Domain Controllers	410
Authentication and Domain Controller Placement in a Branch Office	410
Read-Only Domain Controllers	411
Deploying an RODC	412
Password Replication Policy	416
Administering RODC Credentials Caching	418
Administrative Role Separation	419
Lesson Summary	422
Lesson Review	423
Lesson 4: Managing Service Accounts	425
Understanding Managed Accounts	425
Requirements for Managed Service Accounts	426
Creating and Configuring a Managed Service Account	427
Installing and Using a Managed Service Account	427
Managing Delegation and Passwords	428
Lesson Summary	432
Lesson Review	432
Chapter Review	434
Chapter Summary	434
Key Terms	434
Case Scenarios	435
Case Scenario 1: Increasing the Security of Administrative Accounts	435
Case Scenario 2: Increasing the Security and Reliability of Branch Office Authentication	435
Suggested Practices	436
Configure Multiple Password Settings Objects	436
Recover from a Stolen Read-Only Domain Controller	436
Take a Practice Test	437

Chapter 9 Integrating Domain Name System with AD DS	439
Before You Begin.....	441
Lesson 1: Understanding and Installing	
Domain Name System	444
DNS and IPv6	445
The Peer Name Resolution Protocol	446
DNS Structures	448
The Split-Brain Syndrome	449
Understanding DNS	452
Windows Server 2008 R2 DNS Features	459
Integration with AD DS	461
New DNS Features in Windows Server 2008 R2	463
Lesson Summary	478
Lesson Review	478
Lesson 2: Configuring and Using	
Domain Name System	480
Configuring DNS	480
Forwarders vs. Root Hints	488
Single-Label Name Management	490
DNS and DHCP Considerations	492
Working with Application Directory Partitions	494
Administering DNS Servers	497
Lesson Summary	501
Lesson Review	502
Chapter Review	504
Chapter Summary.....	504
Key Terms.....	505
Case Scenario.....	505
Case Scenario: Blocking Specific DNS Names	505
Suggested Practices	505
Work with DNS	505
Take a Practice Test.....	506

Chapter 10 Administering Domain Controllers 507

Before You Begin.	508
Lesson 1: Deploying Domain Controllers.	509
Installing a Domain Controller with the Windows Interface	509
Unattended Installation Options and Answer Files	510
Installing a New Windows Server 2008 R2 Forest	512
Installing Additional Domain Controllers in a Domain	513
Installing a New Windows Server 2008 Child Domain	516
Installing a New Domain Tree	517
Staging the Installation of an RODC	518
Installing AD DS from Media	520
Removing a Domain Controller	521
Lesson Summary	525
Lesson Review	526
Lesson 2: Managing Operations Masters	527
Understanding Single Master Operations	527
Forest-Wide Operations Master Roles	529
Domain-Wide Operations Master Roles	529
Optimizing the Placement of Operations Masters	532
Identifying Operations Masters	533
Transferring Operations Master Roles	535
Recognizing Operations Master Failures	536
Seizing Operations Master Roles	536
Returning a Role to Its Original Holder	538
Lesson Summary	541
Lesson Review	541
Lesson 3: Configuring DFS Replication of SYSVOL	543
Raising the Domain Functional Level	543
Understanding Migration Stages	544
Migrating SYSVOL Replication to DFS-R	545
Lesson Summary	551
Lesson Review	551
Chapter Review	553
Chapter Summary.	553

Key Term.....	553
Case Scenario.....	553
Case Scenario: Upgrading a Domain	554
Suggested Practices	554
Upgrade a Windows Server 2003 Domain	554
Take a Practice Test.....	555

Chapter 11 Managing Sites and Active Directory Replication 557

Before You Begin.....	558
Lesson 1: Configuring Sites and Subnets	559
Understanding Sites	559
Planning Sites	560
Creating Sites	562
Managing Domain Controllers in Sites	565
Understanding Domain Controller Location	566
Lesson Summary	570
Lesson Review	570
Lesson 2: Configuring the Global Catalog and Application Directory Partitions	572
Reviewing Active Directory Partitions	572
Understanding the Global Catalog	573
Placing Global Catalog Servers	573
Configuring a Global Catalog Server	574
Universal Group Membership Caching	574
Understanding Application Directory Partitions	576
Lesson Summary	579
Lesson Review	579
Lesson 3: Configuring Replication	581
Understanding Active Directory Replication	581
Connection Objects	582
The Knowledge Consistency Checker	583
Intrasite Replication	584
Site Links	586
Bridgehead Servers	588

Configuring Intersite Replication	590
Monitoring Replication	594
Lesson Summary	598
Lesson Review	598
Chapter Review	601
Chapter Summary	601
Key Terms	601
Case Scenario	602
Case Scenario: Configuring Sites and Subnets	602
Suggested Practices	603
Monitor and Manage Replication	603
Take a Practice Test	604

Chapter 12 Managing Multiple Domains and Forests 605

Before You Begin	605
Lesson 1: Configuring Domain and Forest	
Functional Levels	607
Understanding Functional Levels	607
Domain Functional Levels	608
Forest Functional Levels	611
Lesson Summary	616
Lesson Review	616
Lesson 2: Managing Multiple Domains and Trust Relationships	618
Defining Your Forest and Domain Structure	618
Moving Objects Between Domains and Forests	623
Understanding Trust Relationships	627
How Trusts Work	629
Manual Trusts	632
Shortcut Trusts	636
Administering Trusts	639
Resource Access for Users from Trusted Domains	640
Lesson Summary	649
Lesson Review	650

Chapter Review	652
Chapter Summary	652
Case Scenario	653
Case Scenario: Managing Multiple Domains and Forests	653
Suggested Practices	653
Configure a Forest or Domain	653
Take a Practice Test	654

Chapter 13 Directory Business Continuity 655

Before You Begin	656
Lesson 1: Proactive Directory Maintenance and Data Store Protection	658
Twelve Categories of AD DS Administration	660
Performing Online Maintenance	667
Performing Offline Maintenance	669
Relying on Built-in Directory Protection Measures	669
Relying on Windows Server Backup to Protect the Directory	678
Performing Proactive Restores	687
Protecting DCs as Virtual Machines	697
Lesson Summary	705
Lesson Review	706
Lesson 2: Proactive Directory Performance Management	707
Managing System Resources	707
Working with Windows System Resource Manager	718
Lesson Summary	727
Lesson Review	727
Chapter Review	728
Chapter Summary	728
Key Terms	729
Case Scenario	729
Case Scenario: Working with Lost and Found Data	729
Suggested Practices	729
Practice Proactive Directory Maintenance	729
Take a Practice Test	730

Chapter 14 Active Directory Lightweight Directory Services 731

Before You Begin	733
Lesson 1: Understanding and Installing AD LDS	736
Understanding AD LDS	736
AD LDS Scenarios	738
New AD LDS Features in Windows Server 2008 R2	740
Installing AD LDS	741
Lesson Summary	745
Lesson Review	746
Lesson 2: Configuring and Using AD LDS	747
Working with AD LDS Tools	747
Creating AD LDS Instances	749
Working with AD LDS Instances	755
Lesson Summary	766
Lesson Review	766
Chapter Review	767
Chapter Summary	767
Key Terms	767
Case Scenario	768
Case Scenario: Determining AD LDS Instance Prerequisites	768
Suggested Practices	768
Work with AD LDS Instances	768
Take a Practice Test	769

Chapter 15 Active Directory Certificate Services and Public Key Infrastructures 771

Before You Begin	775
Lesson 1: Understanding and Installing Active Directory Certificate Services	778
Understanding AD CS	779
New AD CS Features in Windows Server 2008 R2	788
Installing AD CS	791
Lesson Summary	801
Lesson Review	802

Lesson 2: Configuring and Using Active Directory	
Certificate Services	804
Finalizing the Configuration of an Issuing CA	804
Finalizing the Configuration of an Online Responder	810
Considerations for the Use and Management of AD CS	814
Working with Enterprise PKI	816
Protecting Your AD CS Configuration	818
Lesson Summary	826
Lesson Review	827
Chapter Review	828
Chapter Summary	828
Key Terms	829
Case Scenario	829
Case Scenario: Managing Certificate Revocation	829
Suggested Practices	830
Work with AD CS	830
Take a Practice Test	831

Chapter 16 Active Directory Rights Management Services 833

Before You Begin	835
Lesson 1: Understanding and Installing Active Directory	
Rights Management Services	837
Understanding AD RMS	837
Installing Active Directory Rights Management Services	844
Lesson Summary	860
Lesson Review	860
Lesson 2: Configuring and Using Active Directory Rights	
Management Services	862
Configuring AD RMS	863
Lesson Summary	873
Lesson Review	874
Chapter Review	875
Chapter Summary	875
Key Terms	876

Case Scenario	876
Case Scenario: Preparing to Work with an External AD RMS Cluster	876
Suggested Practices	876
Work with AD RMS	876
Take a Practice Test	877

Chapter 17 Active Directory Federation Services 879

The Purpose of a Firewall	880
Active Directory Federation Services	881
Before You Begin	883
Lesson 1: Understanding Active Directory Federation Services	885
Working with AD FS Designs	886
Understanding AD FS Components	888
Installing Active Directory Federation Services 2.0	897
Lesson Summary	902
Lesson Review	903
Lesson 2: Configuring and Using Active Directory Federation Services	904
Finalizing the Configuration of AD FS	904
Using and Managing AD FS	905
Lesson Summary	915
Lesson Review	915
Chapter Review	917
Chapter Summary	917
Key Terms	917
Case Scenario	918
Case Scenario: Choosing the Right AD Technology	918
Suggested Practices	918
Prepare for AD FS	918
Take a Practice Test	919
Answers	921
Index	963

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Introduction

This training kit is designed for IT professionals who support or plan to support Microsoft Active Directory (AD) on Windows Server 2008 R2 and who also plan to take the 70-640 examination. It is assumed that you have a solid foundation-level understanding of Microsoft Windows client and server operating systems and common Internet technologies. The exam, and this book, assume that you have at least one year of experience administering AD technologies.

NOTE WINDOWS SERVER 2008 CERTIFICATION

Exam 70-640 is one of three required exams for MCSA: Windows Server 2008 certification. For a limited time, it is also valid for the MCTS certification, which will be retired. Please visit the Microsoft Learning website for the most current information about Microsoft certifications: <http://www.microsoft.com/learning/>

The material covered in this training kit and on exam 70-640 builds on your understanding and experience to help you implement AD technologies in distributed environments, which can include complex network services and multiple locations and domain controllers. The topics in this training kit cover what you need to know for the exam, as described on the Skills Measured tab for the exam, which is available at <http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-640&locale=en-us#tab2>.

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

- Deploy Active Directory Domain Services, Active Directory Lightweight Directory Services, Active Directory Certificate Services, Active Directory Federation Services, and Active Directory Rights Management Services in a forest or domain.
- Upgrade existing domain controllers, domains, and forests to Windows Server 2008 R2.
- Efficiently administer and automate the administration of users, groups, and computers.
- Manage the configuration and security of a domain by using Group Policy, fine-grained password policies, directory services auditing, and the Security Configuration Wizard.
- Implement effective name resolution with the domain name system (DNS) on Windows Server 2008 R2.
- Plan, configure, and support the replication of Active Directory data within and between sites.
- Add, remove, maintain, and back up domain controllers.
- Enable authentication between domains and forests.
- Implement new capabilities and functionality offered by Windows Server 2008 R2.

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

System Requirements

Practice exercises are a valuable component of this training kit. They allow you to experience important skills directly, reinforce material discussed in lessons, and even introduce new concepts.

Each lesson and practice describes the requirements for exercises. Although many lessons require only one computer, configured as a domain controller for a sample domain named contoso.com, some lessons require additional computers acting as a second domain controller in the domain, as a domain controller in another domain in the same forest, as a domain controller in another forest, or as a server performing other roles.

The chapters that cover AD DS (Chapters 1–13) require, at most, three machines running simultaneously. Chapters covering other Active Directory roles require up to four machines running simultaneously to provide a comprehensive experience with the technology.

Chapter 1, “Creating an Active Directory Domain,” includes setup instructions for the first domain controller in the contoso.com domain, which is used throughout this training kit. Lessons that require additional computers provide guidance regarding the configuration of those computers.

Hardware Requirements

You can perform exercises on physical computers. Each computer must meet the minimum hardware requirements for Windows Server 2008 R2, published at <http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx>. Windows Server 2008 R2 can run comfortably with 512 megabytes (MB) of memory in small test environments such as the sample contoso.com domain. However, when you begin to work with other AD technologies, such as AD Rights Management Services, AD Certificate Services, or AD Federation Services, your computers should be configured with at least 1024 MB of RAM. Although Windows Server 2008 R2 Standard edition is sufficient for most chapters, later chapters require the Enterprise edition, and we recommend installing that edition when setting up servers for Chapters 14 through 17.

To minimize the time and expense of configuring the several computers required for this training kit, it’s recommended that you create virtual machines by using Hyper-V—a feature of Windows Server 2008 and Windows Server 2008 R2—or other virtualization software, such as VMware Workstation or Oracle VirtualBox. Note that although the book calls for a number of machines, you never use more than four machines together at the same time. Refer to the documentation of your selected virtualization platform for hardware and software requirements, for instructions regarding host setup and configuration, and for procedures to create virtual machines for Windows Server 2008 R2.

If you choose to use virtualization software, you can run more than one virtual machine on a host computer. Each virtual machine must be assigned at least 512 MB or 1024 MB of RAM as required and must meet the minimum processor and disk space requirements for Windows

Server 2008 R2. The host computer must have sufficient RAM for each virtual machine that you will run simultaneously on the host. If you plan to run all virtual machines on a single host, the host must have at least 4.0 GB of RAM. For example, one of the most complex configurations you will need is two domain controllers, each using 512 MB of RAM, and two member servers, each using 1024 MB of RAM. On a host computer with 4 GB of RAM, this would leave 1 GB for the host. Note that each time you run a machine with the Enterprise edition of Windows Server 2008 R2, you should assign 1024 MB of RAM to it.

If you encounter performance bottlenecks while running multiple virtual machines on a single physical host, consider running virtual machines on more than one physical host.

Ensure that all machines—virtual or physical—that you use for exercises can network with each other. It is highly recommended that the environment be totally disconnected from your production environment. Refer to the documentation of your virtualization platform for network configuration procedures.

We recommend that you preserve each of the virtual machines you create until you have completed the training kit. After each chapter, create a backup of the virtual machines used in that chapter so that you can reuse them, as required in later exercises.

Finally, you must have a physical computer with a CD-ROM drive with which to read the companion media.

Software Requirements

Windows Server 2008 R2 with SP1 is required to perform the practice exercises in this training kit.

You can download evaluation versions of the product from the TechNet Evaluation Center at <http://technet.microsoft.com/evalcenter>. If you use evaluation versions of the software, pay attention to the expiration date of the product. The evaluation version of Windows Server 2008 R2 with SP1, for example, can be used for up to 60 days before it expires, but it can be rearmed up to three times, giving you up to 180 days to use the evaluation.

If you have a TechNet or an MSDN subscription, you can download the products from the subscriber downloads center. These versions do not expire. If you are not a TechNet or MSDN subscriber, it is recommended that you subscribe so that you can access benefits such as product downloads.

If you will install Windows Server 2008 R2 on a physical computer, you need software that allows you to burn the .iso file that you download to a DVD, and you need hardware that supports DVD recording.

To use the companion media, you need a web browser such as Internet Explorer 8, and an application that can display PDF files, such as Adobe Acrobat, which can be downloaded from <http://www.adobe.com>.

Using the Companion CD

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

- **Practice Tests** You can reinforce your understanding of the topics covered in this training kit by using electronic practice tests that you customize to meet your needs. You can run a practice test that is generated from the pool of Lesson Review questions in this book. Alternatively, you can practice for the 70-640 certification exam by using tests created from a pool of over 200 realistic exam questions, which give you many practice exams to ensure that you are prepared.
- **Links to References** The CD includes links to references given in this book. Use these links to go directly to references that supplement the text.
- **An eBook** An electronic version (eBook) of this book is included for when you do not want to carry the printed book with you.

How to Install the Practice Tests

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

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

NOTE IF THE CD MENU DOES NOT APPEAR

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

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

How to Use the Practice Tests

To start the practice test software, follow these steps:

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

NOTE LESSON REVIEWS VS. PRACTICE TESTS

Select the (70-640) TS: Windows Server 2008 Active Directory, Configuring lesson review to use the questions from the “Lesson Review” sections of this book. Select the (70-640) TS: Windows Server 2008 Active Directory, Configuring practice test to use a pool of 200 questions similar to those that appear on the 70-640 certification exam.

Lesson Review Options

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

After you click OK, your lesson review starts.

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

Practice Test Options

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

- **Certification Mode** Closely resembles the experience of taking a certification exam. The test has a set number of questions. It is timed, and you cannot pause and restart the timer.
- **Study Mode** Creates an untimed test during which you can review the correct answers and the explanations after you answer each question.
- **Custom Mode** Gives you full control over the test options so that you can customize them as you like.

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

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

How to Uninstall the Practice Tests

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

NOTE COMPANION CONTENT FOR DIGITAL BOOK READERS

If you bought a digital edition of this book, you can enjoy select content from the print edition’s companion CD. Visit <http://go.microsoft.com/FWLink/?LinkId=218370> to get your downloadable content.

Acknowledgments

The authors’ names appear on the cover of a book, but we are only part of a much larger team. Jeff Koch gave us the opportunity to update the first edition of this training kit and guided it through the business. Karen Szall and Rosemary Caperton, with whom we worked closely, were a dream team as always! And each of the editors did a phenomenal job of adding value to this training kit. Kurt Meyer, our technical reviewer, was extremely helpful and thorough. We are very grateful to the entire team and to everyone’s efforts at making this training kit an indispensable resource to the community. We look forward to working with each of you again in the future!

Support & Feedback

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

Errata

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

<http://go.microsoft.com/fwlink/?LinkID=219768>

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

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

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

We Want to Hear from You

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

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

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

Stay in Touch

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

Preparing for the Exam

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

Managing Groups

Although users and computers, and even services, change over time, business roles and rules tend to remain more stable. Your business probably has a finance role, which requires certain capabilities in the enterprise. The user or users who perform that role will change, but the role will remain. For that reason, it is not practical to manage an enterprise by assigning rights and permissions to individual user, computer, or service identities. Management tasks should be associated with groups. In this training kit, you will learn to use groups to identify administrative and user roles, to filter Group Policy, to assign unique password policies, to assign rights and permissions, and more. To prepare you for those tasks, this lesson demonstrates how to create, modify, delete, and support group objects in an Active Directory Domain Services (AD DS) domain.

Exam objectives in this chapter:

- Automate creation of Active Directory accounts.
- Maintain Active Directory accounts.

Lessons in this chapter:

- Lesson 1: Managing an Enterprise with Groups **151**
- Lesson 2: Automating the Creation and Management of Groups **175**
- Lesson 3: Administering Groups in an Enterprise **186**

Before You Begin

This chapter applies Windows PowerShell, Csvde.exe, and Ldifde.exe to the task of automating computer account creation. Read Lesson 1, "Automating the Creation of User Accounts," and Lesson 2, "Administering with Windows PowerShell and Active Directory Administrative Center," of Chapter 3, "Administering User Accounts," prior to reading this chapter.

In addition, to perform exercises in this chapter, you must have created a domain controller named SERVER01 in a domain named contoso.com. See Chapter 1, "Creating an Active Directory Domain," for detailed steps of this task.



REAL WORLD

Dan Holme

Efficient and effective group management is a tremendous enabler for security, consistency, and productivity in an IT environment. As a consultant, I spend a lot of time with clients, aligning technology with their business needs. In the case of Microsoft Windows technologies, this entails defining and implementing business roles and rules so that administration can be defined, documented, and automated. And that process often requires improving clients' group management knowledge, technologies, and processes. Many IT professionals have come into Windows Server 2008 R2 Active Directory with practices developed in previous versions of Windows that do not take advantage of groups as fully as possible. In fact, I've seen so much wasted productivity and decreased security due to poor group management that I dedicated two chapters of my book, *Windows Administration Resource Kit: Productivity Solutions for IT Professionals* (Microsoft Press, 2008), to improving and automating group management. In this lesson, you learn what you need to know for the certification exam, and I share with you a few of the tips and best practices that you'll need to make the most of groups in a production environment. I highly recommend reading the resource kit for more information, guidance, and fantastic tools related to group management.

Lesson 1: Managing an Enterprise with Groups

You are certainly familiar with the purpose of groups: to collect items and manage them as a single entity. The implementation of group management in Active Directory is not intuitive; Active Directory is designed to support large, distributed environments, so it includes seven types of groups: two types of domain groups with three scopes each, plus local security groups. In this lesson, you learn the purpose of each of these groups, as well as how to align your business requirements with the potentially complex options that Active Directory provides.

After this lesson, you will be able to:

- Understand the role of groups in managing an enterprise.
- Define group naming conventions.
- Create groups by using the Active Directory Users And Computers snap-in.
- Understand, manage, and convert group type and scope.
- Identify group membership and nesting possibilities.
- Manage group membership.
- Develop a group management strategy.

Estimated lesson time: 45 minutes

Understanding the Importance of Groups

Groups are an important class of object because they collect users, computers, and other groups to create a single point of management.

The most straightforward and common use of a group is to grant permissions to a shared folder. A security group is a security principal with a security identifier (SID) and a *member* attribute that identifies members—users, computers, and other groups. If a group has Read access to a folder, for example, any of the group's members can read the folder. You do not have to grant Read access to each individual member—you can manage access to the folder simply by adding and removing members of the group.

Challenges of Managing Without Groups

- Imagine that all of the 100 users in the sales department require Read-level access to a shared folder called Sales on a server. Assigning permissions to each user individually is not a manageable solution. When new salespeople are hired, you must add the new accounts to the access control list (ACL) of the folder. When accounts are deleted, you must remove the permissions from the ACL to avoid an Account Unknown entry on the

ACL (as shown in Figure 4-1), which results from a SID on the ACL that refers to an account that cannot be resolved.

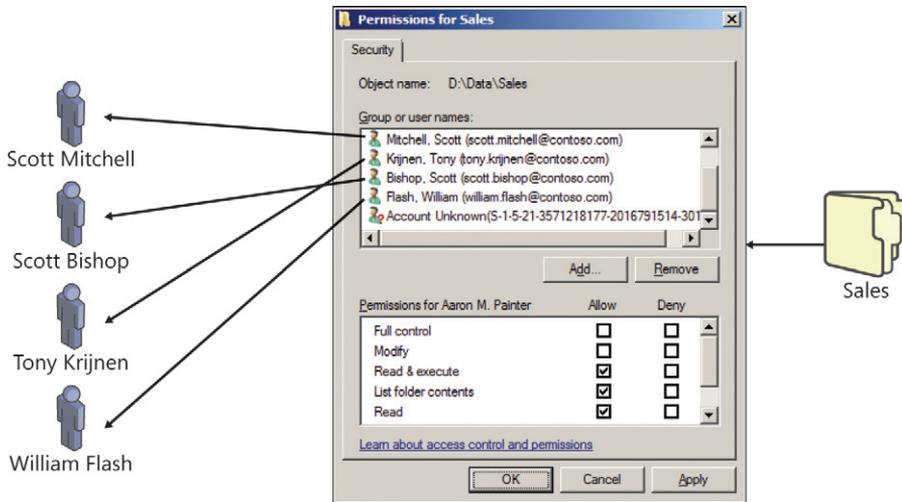


FIGURE 4-1 Access management without groups

- Imagine now that all of the 100 users in the sales department require Read access to three shared folders on three different servers; the management difficulty just increased significantly. How many permissions would you have to apply just to configure access to three folders on three different servers for 100 users? 300!

When you manage permissions by adding and removing identities to and from an ACL, it becomes difficult to answer the question, “Who can read the Sales folder?” To answer the question, you must reverse engineer the ACL. And, in the broader example, if the Sales folders are distributed across three servers, you would have to evaluate three separate ACLs to answer the question.

Groups Add Manageability

The example presented in the previous section may seem extreme, because you have no doubt learned that although assigning permissions to a resource for an individual identity—user or computer—is possible, the best practice is to assign a single permission to a group and then manage access to the resource simply by changing the membership of the group.

So, to continue the example, you could create a group called Sales and assign the group Allow Read permission on the Sales folder. This implementation is shown in Figure 4-2.

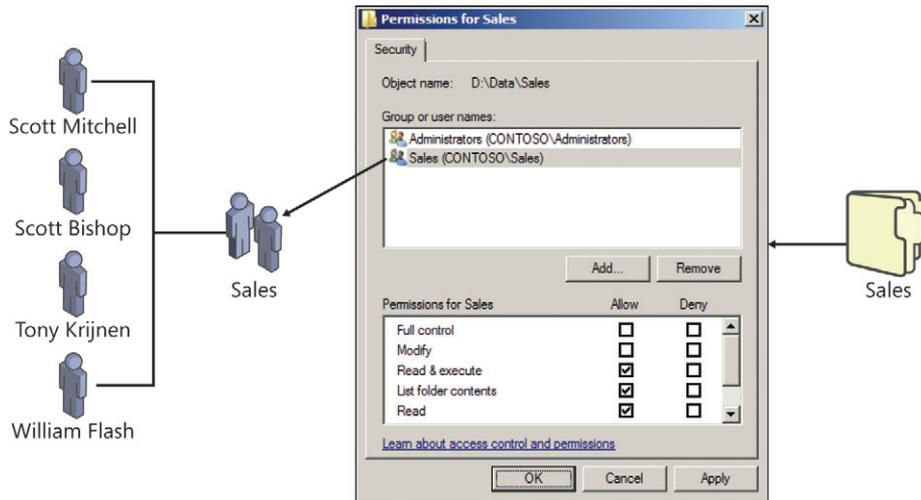


FIGURE 4-2 Assigning Allow Read permission to a group; groups add manageability

You now have a single point of management. The Sales group effectively manages access to the shared folder. You can add new sales users to the group, and they will gain access to the shared folder. When you delete an account, it is automatically deleted from the group, so you will not have irresolvable SIDs on your ACL. It is also easier to answer the question, “Who can read the Sales folder?” You can simply enumerate the membership of the Sales group. The Sales group has become the focus of access management tasks.

There’s an extra benefit: Your ACL remains stable because the Sales group has Allow Read permission, so your backups will be easier. When you change the ACL of a folder, the ACL propagates to all child files and folders, setting the Archive flag and thereby requiring a backup of all files, even if the contents of the files have not changed.

Groups Add Scalability

If the sales users require Read access to three folders on three separate servers, you could assign the Sales group Allow Read permission on each of the three folders. After you assign the three permissions, the Sales group provides a single point of management for resource access, as shown in Figure 4-3.

The Sales group effectively manages access to all three shared folders. You can add new sales users to the group, and they will gain access to the three shared folders on the three servers. When you delete an account, it is automatically deleted from the group, so you will not have irresolvable SIDs on your ACLs.

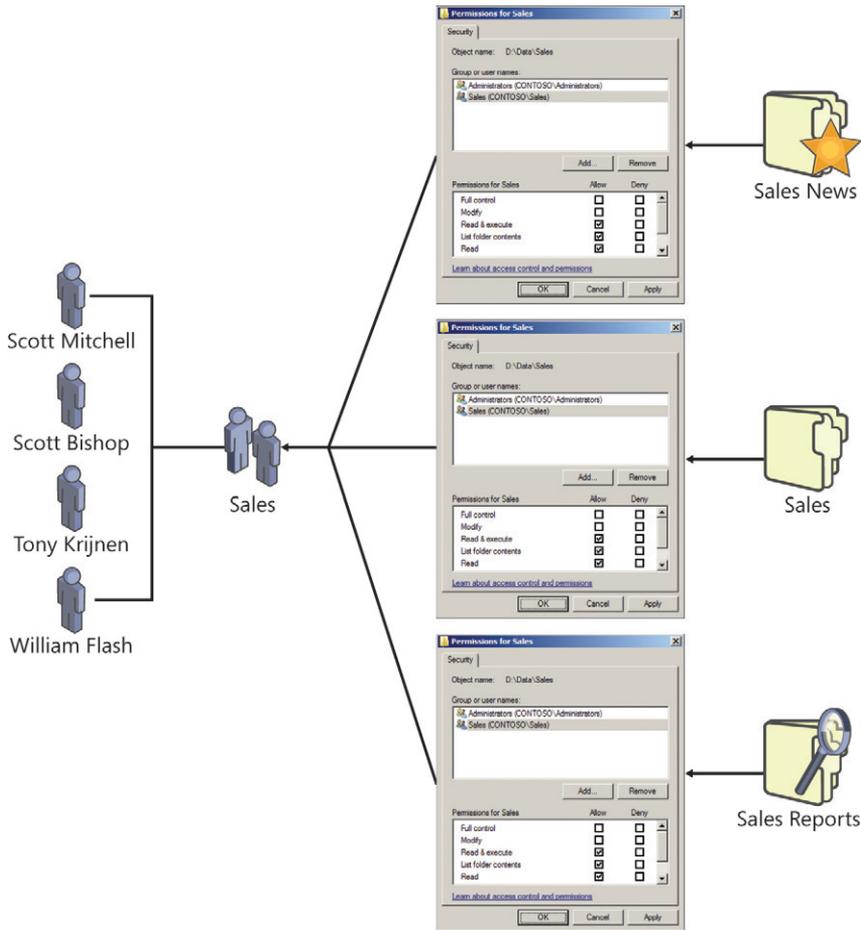


FIGURE 4-3 Assigning Allow Read permission on three folders; groups add scalability

One Type of Group Is Not Enough

Imagine now that it is not only salespeople who require Read access to the folders. The executives, the marketing department employees, and the sales consultant hired by your organization also require Read permission to the same folders.

You could add those groups to the ACL of the folders, granting each of them Allow Read permission, but soon you would have an ACL with multiple permissions, this time assigning the Allow Read permission to multiple groups instead of multiple users. This is shown in Figure 4-4.

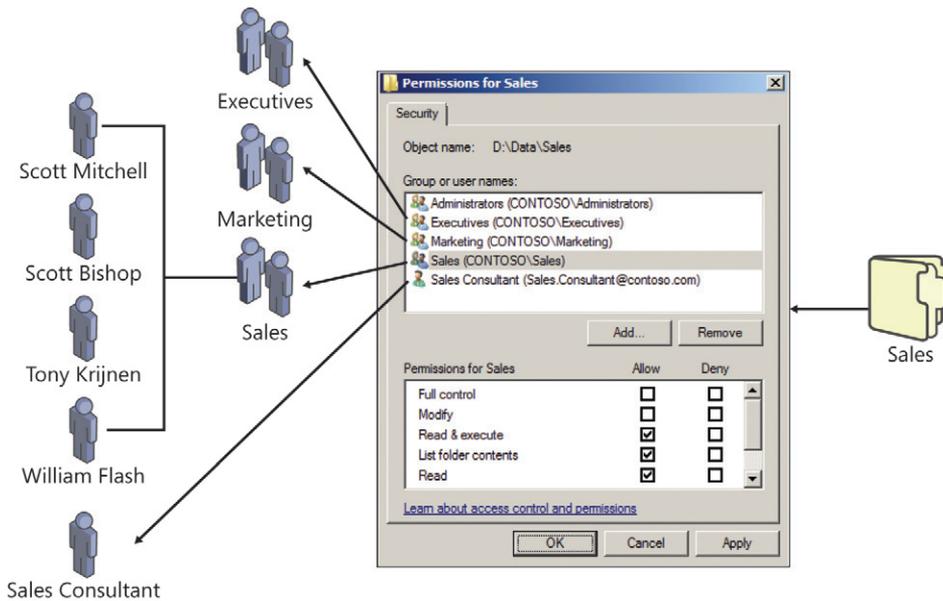


FIGURE 4-4 One kind of group is not enough to efficiently manage permissions

To give the three groups and one user permission to the three folders on the three servers, you would have to add 12 permissions! The next group that required access would require three more changes to grant permissions to the ACLs of the three shared folders.

What if eight users who are not salespeople, marketing employees, or executives have a business need for Read access to the three folders? Do you add their individual user accounts to the ACLs? If so, that's 24 more permissions to add and manage!

You can see that using only one type of group—a role group that defines the business roles of users—quickly becomes an ineffective way of enabling management of access to the three folders. If the management rule suggests that three roles and nine additional users require access to the resource, you are assigning a total of 36 permissions on ACLs. It becomes very difficult to maintain compliance and to audit. Even simple questions such as, “Can you tell me every user who can read the Sales folders?” become difficult to answer.

Role-Based Management: Role Groups and Rule Groups

The solution is to recognize that you must address two management tasks to effectively manage this scenario: You must manage the users as collections, based on their business roles, and, separately, you must manage access to the three folders.

The three folders are also a collection of items: They are a single resource—a collection of Sales folders—that just happens to be distributed across three folders on three servers. And you are trying to manage Read access to that resource. You need a single point of management with which to manage access to the resource.

This requires another group—a group that represents Read access to the three folders on the three servers. Imagine that you create a group called ACL_Sales Folders_Read. This group will be assigned the Allow Read permission on the three folders. The Sales, Marketing, and Executives groups, along with the individual users, will all be members of the ACL_Sales Folders_Read group. You assign only three permissions: one on each folder, granting Read access to the ACL_Sales Folders_Read group. This is shown in Figure 4-5.

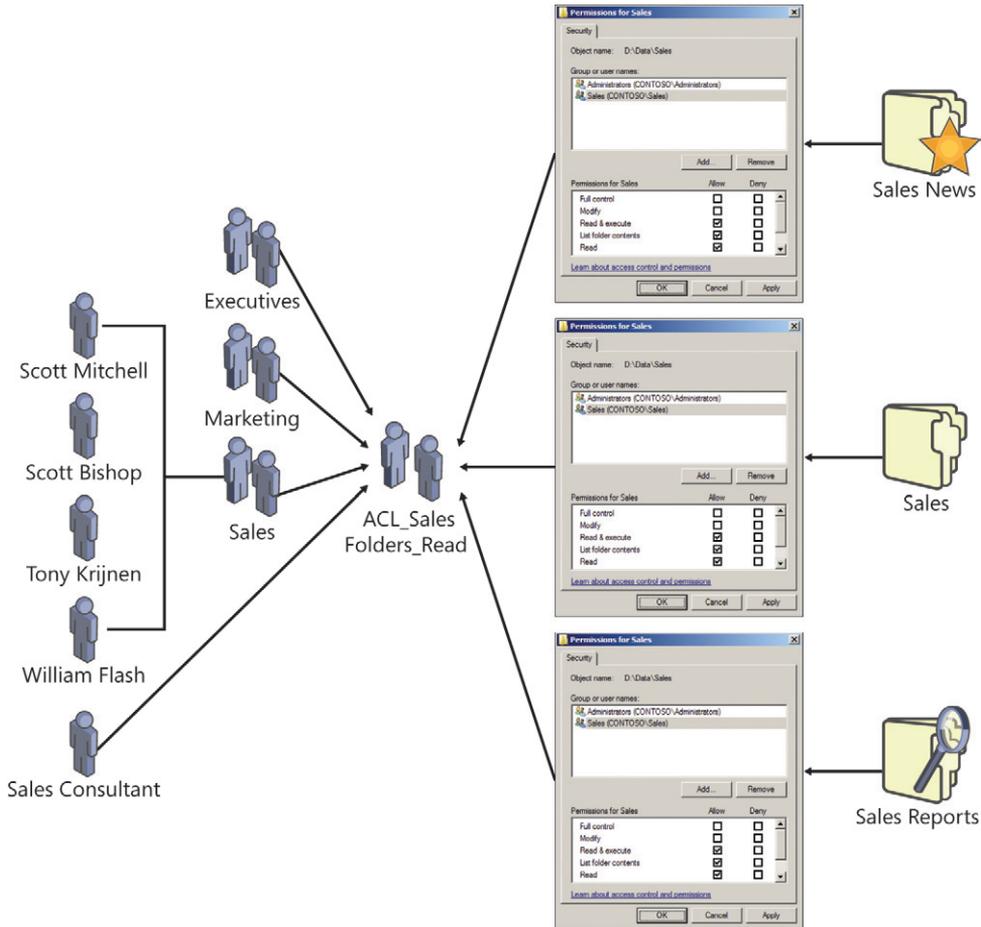


FIGURE 4-5 Role-based management uses role groups and rule groups to efficiently manage access to folders

The ACL_Sales Folders_Read group becomes the focus of access management. As additional groups or users require access to the folders, you add them to that group. It also becomes much easier to report who has access to the folders. Instead of having to examine the ACLs on each of the three folders, you simply examine the membership of the ACL_Sales Folders_Read group.

To effectively manage even a slightly complex enterprise, you need groups that perform two distinct purposes:

- **Groups that define roles** These groups, referred to as *role groups*, contain users, computers, and other role groups based on common business characteristics such as location and job type.
- **Groups that define management rules** These groups, referred to as *rule groups*, define how an enterprise resource is managed.

This approach to managing the enterprise with groups is called *role-based management*. You define roles of users based on business characteristics (for example, department or division affiliation such as sales, marketing, and executives), and you define management rules (for example, the rule that manages which roles and individuals can access the three folders).

You can achieve both management tasks by using groups in a directory. Roles are represented by groups that contain users, computers, and other roles. That's right, roles can include other roles—for example, a Managers role might include the Sales Managers, Finance Managers, and Production Managers roles. Management rules, such as the rule that defines and manages Read access to the three folders, are represented by groups as well. Rule groups contain roles and, occasionally, individual users or computers such as the sales consultant and eight other users in the example.

The key takeaway is that groups serve two distinct purposes: one group defines the role, and another defines how a resource is managed.

To achieve manageability of an enterprise of any size or complexity, you must manage groups effectively and have an infrastructure of groups that provide single points of management for roles and rules. That means, technically, that you will need groups that can include as members users, computers, other groups, and, possibly, security principals from other domains.

For more information about role-based management, see *Windows Administration Resource Kit: Productivity Solutions for IT Professionals*.

Defining Group Naming Conventions

To create a group by using the Active Directory Users And Computers snap-in, simply right-click the organizational unit (OU) in which you want to create a group, point to New, and then click Group. The New Object – Group dialog box, shown in Figure 4-6, lets you specify fundamental properties of the new group.

The following name properties can be configured here:

- **Group name** *cn* attribute of group object; must be unique only within OU
- **Group name (Pre-Windows 2000)** *sAMAccountName* attribute of group; unique in domain

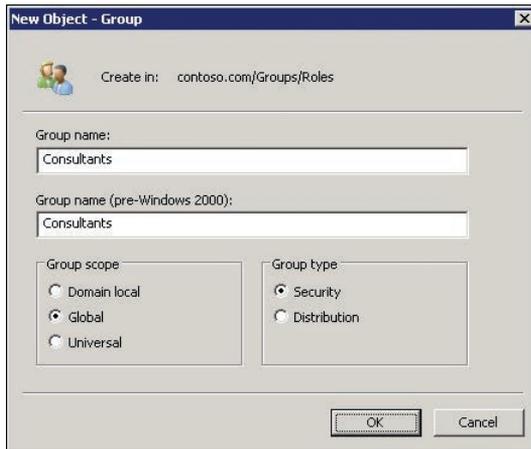


FIGURE 4-6 The New Object – Group dialog box

The first properties you must configure are the group’s names. A group, like a user or computer, has several names. The first, shown in the Group Name box in Figure 4-6, is used by Windows 2000 and later systems to identify the object—it becomes the *cn* and *name* attributes of the object. The second, the pre-Windows 2000 name, is the *sAMAccountName* attribute, used to identify the group to some applications and devices such as network attached storage (NAS) devices running non-Microsoft operating systems. The *cn* and *name* attributes must be unique only within the container—the OU—in which the group exists. The *sAMAccountName* must be unique in the entire domain. Technically, the *sAMAccountName* could be a different value than the *cn* and *name*, but this is highly discouraged. Choose a name that is unique in the domain, and use it in both name boxes in the New Object – Group dialog box.

BEST PRACTICE GROUP NAMES

Use the same name (unique in the domain) for both group name properties.

The following naming conventions are recommended:

- **Role groups.** Simple, unique name, such as Sales or Consultants
- **Management groups.** For example, ACL_Sales Folders_Read
 - **Prefix** This identifies the management purpose of group, such as ACL for groups managing access permissions to shared resources.
 - **Resource identifier** This is a unique identifier for what is being managed.
 - **Suffix** For resource access groups, this is the type of access the group manages.
 - **Delimiter** This should be a consistently used marker separating prefix, identifier, and suffix, such as an underscore (_). Do not use the delimiter elsewhere in the name—use it only as a delimiter.

The name you choose should help you manage the group and your enterprise on a day-to-day basis. It is recommended to follow a naming convention that identifies the type of group and the purpose of the group.

The example in the previous section used a group name, `ACL_Sales Folders_Read`. Let's examine how the recommendations listed earlier apply to the group name.

- **Prefix** The prefix identifies the management purpose of the group. In this case, it is a group used to manage access permissions to a folder. It is used on access control lists, so the prefix `ACL` is used.
- **Resource identifier** The main part of the name uniquely identifies the resource that is being managed with the group—in this example, `Sales Folders`.
- **Suffix** The suffix further defines what is being managed by the group. In the case of resource access management groups, the suffix defines the level of access provided to members of the group. In our example, that is `Read`.
- **Delimiter** A delimiter—in this case, an underscore—is used to separate parts of the name. Note that the delimiter is not used between the words *Sales* and *Folder*. Spaces are acceptable in group names—you just need to enclose such group names in quotes when you refer to them in commands or scripts. You can create scripts that use the delimiter to deconstruct group names to facilitate auditing and reporting.

Remember that role groups that define user roles are often used by non-technical users. For example, you might email-enable the `Sales` group so that it can be used as an email distribution list. Therefore, your naming convention for role groups should be simple and straightforward. In other words, do not use prefixes, suffixes, or delimiters when naming role groups—just use a descriptive user-friendly name.

For more information about managing groups effectively, see *Windows Administration Resource Kit: Productivity Solutions for IT Professionals*.

Understanding Group Types

There are two types of groups: security and distribution. When you create a group, you select the group type in the `New Object – Group` dialog box.

Distribution groups are used primarily by email applications. These groups are not security enabled so they cannot be given permission to resources. Sending a message to a distribution group sends the message to all members of the group.

Security groups are security principals with SIDs. These groups can therefore be used in permission entries in ACLs to control security for resource access. Security groups can also be used as distribution groups by email applications. If a group will be used to manage security, it must be a security group.

Because security groups can be used for both resource access and email distribution, many organizations use only security groups. However, if a group will be used only for email distribution, you should create the group as a distribution group. Otherwise, the group is

assigned a SID and the SID is added to the user's security access token, which can lead to unnecessary bloat of the security token.

Understanding Group Scope

Groups have members: users, computers, and other groups; groups can be members of other groups, and groups can be referred to by ACLs, Group Policy object (GPO) filters, and other management components. *Group scope* affects each of these characteristics of a group: what it can contain, what it can belong to, and where it can be used. There are four group scopes: local, domain local, global, and universal.

The characteristics that define each scope fall into these categories:

- **Replication** Where is the group defined and to what systems is the group replicated?
- **Membership** What types of security principals can the group contain as members? Can the group include security principals from trusted domains? In Chapter 12, "Managing Multiple Domains and Forests," you learn about trust relationships, or *trusts*. A trust allows a domain to refer to another domain for user authentication, to include security principals from the other domain as group members, and to assign permissions to security principals in the other domain. The terminology used can be confusing. If Domain A trusts Domain B, then Domain A is the *trusting* domain and Domain B is the *trusted* domain. Domain A accepts the credentials of users in Domain B. It forwards requests by Domain B users to authenticate to a domain controller in Domain B because it *trusts* the identity store and authentication service of Domain B. Domain A can add Domain B's security principals to groups and ACLs in Domain A. See Chapter 12 for more detail.
- **Availability** Where can the group be used? Is the group available to add to another group? Is the group available to add to an ACL?

Keep these broad characteristics in mind as you explore the details of each group scope.



EXAM TIP

In the context of group membership, remember that if Domain A trusts Domain B, Domain B is *trusted*, and its users and global groups can be members of domain local groups in Domain A. Additionally, Domain B's users and global groups can be assigned permissions to resources in Domain A.

Local Groups

Local groups are truly local—defined on and available to a single computer. Local groups are created in the security accounts manager (SAM) database of a domain member computer—both workstations and servers have local groups.

Local groups have the following characteristics:

- **Replication** A local group is defined only in the local SAM database of a domain member server. The group and its membership are not replicated to any other system.
- **Membership** A local group can include as members:
 - Any security principals from the domain: users, computers, global groups, or domain local groups
 - Users, computers, and global groups from any domain in the forest
 - Users, computers, and global groups from any trusted domain
 - Universal groups defined in any domain in the forest
- **Availability** A local group has only computer-wide scope. It can be used in ACLs on the local computer only. A local group cannot be a member of any other group.

BEST PRACTICE DO NOT MANAGE WITH LOCAL GROUPS

In a workgroup, you use local groups to manage security of resources on a system. In a domain, however, managing the local groups of individual computers becomes unwieldy and is, for the most part, unnecessary. It is not recommended to create custom local groups on domain members. In fact, the Users and Administrators local groups are the only local groups that you should be concerned with managing in a domain environment.

Domain Local Groups

Domain local groups are used primarily to manage permissions to resources. For example, the ACL_Sales Folder_Read group discussed earlier in the lesson would be created as a domain local group. Domain local groups have the following characteristics:

- **Replication** A domain local group is defined in the domain naming context. The group object and its membership (the *member* attribute) are replicated to every domain controller in the domain.
- **Membership** A domain local group can include as members:
 - Any security principals from the domain: users, computers, global groups, or other domain local groups
 - Users, computers, and global groups from any domain in the forest
 - Users, computers, and global groups from any trusted domain
 - Universal groups defined in any domain in the forest
- **Availability** A domain local group can be added to ACLs on any resource on any domain member. Additionally, a domain local group can be a member of other domain local groups or even computer local groups.

The membership capabilities of a domain local group are identical to those of local groups, but the replication and availability of the domain local group make it useful across the entire domain.

BEST PRACTICE MANAGE ACCESS TO RESOURCES WITH DOMAIN LOCAL GROUPS

Domain local groups are well suited for defining business management rules, such as resource access rules, because the group can be applied anywhere in the domain, and it can include members of any type within the domain as well as members from trusted domains. For example, a domain local security group named `ACL_Sales Folders_Read` might be used to manage Read access to a collection of folders that contain sales information on one or more servers.

Global Groups

Global groups are used primarily to define collections of domain objects based on business roles. Role groups, such as the Sales and Marketing groups mentioned earlier, as well as roles of computers such as a Sales Laptops group, would be created as global groups. Global groups have the following characteristics:

- **Replication** A global group is defined in the domain naming context. The group object, including the *member* attribute, is replicated to all domain controllers in the domain.
- **Membership** A global group can include as members users, computers, and other global groups in the same domain only.
- **Availability** A global group is available for use by all domain members as well as by all other domains in the forest and all trusting external domains. A global group can be a member of any domain local or universal group in the domain or in the forest. It can also be a member of any domain local group in a trusting domain. Finally, a global group can be added to ACLs in the domain, in the forest, or in trusting domains.

As you can see, global groups have the most limited membership (only users, computers, and global groups from the same domain) but the broadest availability across the domain, the forest, and trusting domains.

BEST PRACTICE DEFINE ROLES WITH GLOBAL GROUPS

Global groups are well suited to defining roles, because roles are generally collections of objects from the same directory. For example, global security groups named `Consultants` and `Sales` might be used to define users who are consultants and salespeople, respectively.

Universal Groups

Universal groups have the following characteristics:

- **Replication** A universal group is defined in a single domain in the forest but is replicated to the global catalog. You will learn more about the global catalog in Chapter 12. Objects in the global catalog are readily accessible across the forest.
- **Membership** A universal group can include as members users, global groups, and other universal groups from any domain in the forest.
- **Availability** A universal group can be a member of a universal group or domain local group anywhere in the forest. Additionally, a universal group can be used to manage resources—for example, to assign permissions—anywhere in the forest and in trusting forests.

Universal groups are useful in multidomain forests. They let you define roles, or manage resources, that span more than one domain.

The best way to understand universal groups is through an example. Trey Research has a forest with three domains: Americas, Asia, and Europe. Each domain has user accounts and a global group called Regional Managers that includes the managers of that domain's region. Remember that global groups can contain only users from the same domain. A universal group called Trey Research Regional Managers is created, and the three Regional Managers groups are added as members. The Trey Research Regional Managers group therefore defines a role for the entire forest. As users are added to any one of the Regional Managers groups, they will, through group nesting, be members of the Trey Research Regional Managers group.

Trey Research is planning to release a new product that requires collaboration across its regions. Resources related to the project are stored on file servers in each domain. To define who has the ability to modify files related to the new product, a universal group is created called *ACL_New Product_Modify*. That group is assigned the Allow Modify permission to the shared folders on each of the file servers in each of the domains. The Trey Research Regional Managers group is made a member of the *ACL_New Product_Modify* group, as are various global groups and a handful of users from each of the regions.

BEST PRACTICE MANAGE ROLES AND RULES ACROSS DOMAINS IN A FOREST WITH UNIVERSAL GROUPS

As you can see from the example in this section, universal groups can help you represent and consolidate roles that span domains in a forest and define rules that can be applied across the forest.

Summarizing Group Membership Possibilities

For both the certification examinations and day-to-day administration, it is important that you are completely familiar with the membership characteristics of each group scope.

Table 4-1 summarizes the objects that can be members of each group scope.

TABLE 4-1 Group Scope and Members

GROUP SCOPE	MEMBERS FROM THE SAME DOMAIN	MEMBERS FROM ANOTHER DOMAIN IN THE SAME FOREST	MEMBERS FROM A TRUSTED EXTERNAL DOMAIN
Local	Users	Users	Users
	Computers	Computers	Computers
	Global groups	Global groups	Global groups
	Universal groups	Universal groups	groups
	Domain local groups Local users defined on the same computer as the local group		
Domain Local	Users	Users	Users
	Computers	Computers	Computers
	Global groups	Global groups	Global groups
	Universal groups	Universal groups	groups
	Domain local groups		
Universal	Users	Users	N/A
	Computers	Computers	
	Global groups	Global groups	
	Universal groups	Universal groups	
Global	Users	N/A	N/A
	Computers		
	Global groups		

 **Quick Check**

- Which types of objects can be members of a global group in a domain?

Quick Check Answer

- Global groups can contain only users, computers, and other global groups from the same domain.

Converting Group Scope and Type

If, after creating a group, you determine that you need to modify the group's scope or type, you can do so. Open the Properties dialog box of an existing group and, on the General tab, shown in Figure 4-7, you see the existing scope and type. At least one more scope and type are available for selection.

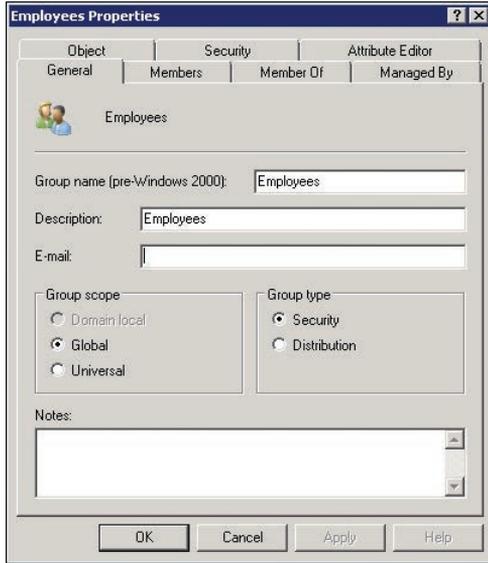


FIGURE 4-7 The General tab of a group's Properties dialog box

You can convert the group type at any time by changing the selection in the Group Type section of the General tab. Be cautious, however. When you convert a group from security to distribution, any resources to which the group had been assigned permission will no longer be accessible in the same way. After the group becomes a distribution group, users who log on to the domain will no longer include the group's SID in their security access tokens.

You can change the group scope in the following ways:

- Global to universal
- Domain local to universal
- Universal to global
- Universal to domain local

The only scope changes that you cannot make directly are from global to domain local or domain local to global. However, you can make these changes indirectly by first converting to universal scope, then converting to the desired scope. So all scope changes are possible.

Remember, however, that a group's scope determines the types of objects that can be members of the group. If a group already contains members or is a member of another group that would violate the new scope, you would be prevented from changing scope. For example, if a global group is a member of another global group, you cannot change the first group to universal scope, because a universal group cannot be a member of a global group. An explanatory error message, such as that shown in Figure 4-8, appears. You must correct the group's membership conflicts before you can change the group's scope.



FIGURE 4-8 The error produced when a group's membership will not allow a change of scope

The `DSMod` command, introduced in Chapter 3, can be used to change group type and scope by using the following syntax:

```
dsmod group GroupDN -secgrp { yes | no } -scope { l | g | u }
```

The *GroupDN* is the distinguished name of the group to modify. The following two parameters affect group scope and type:

- `-secgrp { yes | no }` specifies group type: security (*yes*) or distribution (*no*).
- `-scope { l | g | u }` determines the group scope: domain local (*l*), global (*g*), or universal (*u*).

Managing Group Membership

You can add or remove members of a group by using one of several methods.

The Members Tab

You can open the group's Properties dialog box and click the Members tab. To manage group membership using the group's Members tab:

1. Open the group's Properties dialog box.
2. Click the Members tab.
3. To remove a member, simply select the member and click Remove.
4. To add a member, click Add. The Select Users, Contacts, Computers, Or Groups dialog box appears, as shown in Figure 4-9.

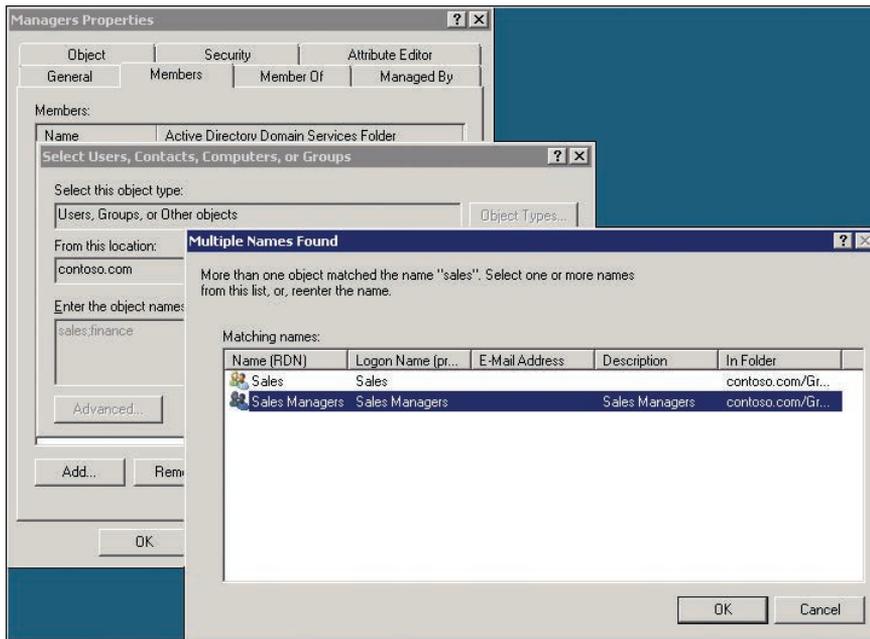


FIGURE 4-9 Adding a member to a group

There are several tips worth mentioning about this process:

- In the Select dialog box, in the Enter The Object Names box, you can type multiple accounts separated by semicolons. For example, in Figure 4-9, both *sales* and *finance* are entered, separated by a semicolon.
- You can type partial names of accounts—you do not need to type the full name. Windows searches Active Directory for accounts that begin with the name you entered. If there is only one match, Windows selects it automatically. If multiple accounts match, the Multiple Names Found dialog box appears, in which you can select the object you want. This shortcut—typing partial names—can save time when adding members to groups and can help when you don't remember the exact name of a member.
- By default, Windows searches only for users and groups that match the names you enter in the Select dialog box. If you want to add computers to a group, you must click Object Types and select Computers.
- By default, Windows searches only domain accounts. If you want to search local accounts, click Locations in the Select dialog box.
- If you cannot find the member you want to add, click Advanced in the Select dialog box. A more powerful query window appears, giving you more options for searching Active Directory.

The Member Of Tab

To manage group membership using the member object's Member Of tab:

1. Open the properties of the member object, and then click its Member Of tab.
2. To remove the object from a group, select the group and then click Remove.
3. To add the object to a group, click Add and select the group.

The Add To A Group Command

To manage group membership using the Add To A Group command:

1. Right-click one or more selected objects in the Active Directory Users And Computers details pane.
2. Click Add To A Group.
3. Use the Select dialog box to specify the group.

The *Member* and *MemberOf* Attributes

When you add a member to a group, you change the group's *member* attribute. The *member* attribute is a multivalued attribute. Each member is a value represented by the distinguished name (DN) of the member. If the member is moved or renamed, Active Directory automatically updates the *member* attributes of groups that include the member.

When you add a member to a group, the member's *memberOf* attribute is also updated, indirectly. The *memberOf* attribute is a special type of attribute called a *backlink*. It is updated by Active Directory when a forward link attribute, such as *member*, refers to the object.

When you add a member to a group, you are always changing the group's *member* attribute. Therefore, when you use the Member Of tab of an object to add to a group, you are actually changing the group's *member* attribute, and Active Directory updates the member's *memberOf* attribute automatically.

Helping Membership Changes Take Effect Quickly

When you add a user to a group, the membership does not take effect immediately. Group membership is evaluated at logon for a user (at startup for a computer). Therefore, a user must log off and log on before the membership change becomes a part of the user's token.

Additionally, there can be a delay while the group membership change replicates. Replication is discussed in Chapter 11, "Managing Sites and Active Directory Replication." This is particularly true if your enterprise has more than one Active Directory site. You can facilitate the speed with which a change affects a user by making the change on a domain controller in the user's site. Right-click the domain in the Active Directory Users And Computers snap-in and choose Change Domain Controller.

Developing a Group Management Strategy

Adding groups to other groups—a process called *nesting*—can create a hierarchy of groups that support your business roles and management rules. Now that you have learned the business purposes and technical characteristics of groups, it is time to align the two in a strategy for group management.

Earlier in this lesson, you learned which types of objects *can* be members of each group scope. Now it is time to identify which types of objects *should* be members of each group scope. This leads to the best practice for group nesting, known as *IGDLA*:

- **I**dentities (user and computer accounts) are members of
- **G**lobal groups that represent business roles. Those role groups (global groups) are members of
- **D**omain **L**ocal groups that represent management rules—for example, managing who has Read permission to a specific collection of folders. These rule groups (domain local groups) are granted
- **A**ccess to resources. In the case of a shared folder, for example, access is granted by adding the domain local group to the folder's ACL, with a permission that provides the appropriate level of access.

A multidomain forest also contains universal groups that fit in between global and domain local groups. Global groups from multiple domains are members of a single universal group. That universal group is a member of domain local groups in multiple domains. You can remember the nesting as *IGUDLA*.

NOTE IGDLA VS. UGDLA

Some texts abbreviate the group nesting strategy as *UGDLA*: *Users go into Global groups, which go into Domain Local groups, which are given Access to resources*. This text, and others, changes the abbreviation to *IGDLA*. Although users are members of groups, so are computers. For example, to deploy software to a collection of computers, you can make them members of a group that is used as a deployment target by your software distribution tools. Therefore, *identities* is more accurate than *users*. In addition, the change allows *U* to be used for *Universal groups* in multidomain forest group nesting.

This best practice for implementing group nesting translates well even in multidomain scenarios. Consider Figure 4-10.

Figure 4-10 represents a group implementation that reflects not only the technical view of group management best practices (IGDLA) but also the business view of role-based, rule-based management.

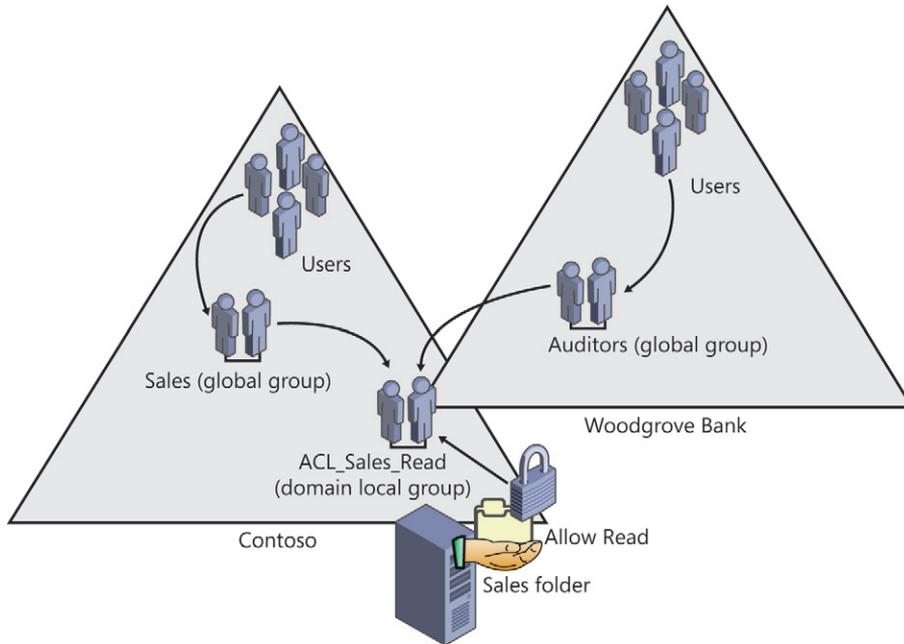


FIGURE 4-10 A group management implementation

Consider the following scenario. The sales force at Contoso, Ltd., has just completed their fiscal year. Sales files from the previous year are in a folder called Sales. The sales force needs Read access to the Sales folder. Additionally, a team of auditors from Woodgrove Bank, a potential investor, requires Read access to the Sales folder to perform an audit. The steps to implement the security required by this scenario are as follows:

1. Assign users with common job responsibilities or other business characteristics to role groups implemented as global security groups.

This happens separately in each domain. Salespeople at Contoso are added to a Sales role group. Auditors at Woodgrove Bank are added to an Auditors role group.

2. Create a group to represent the business rule regarding who can access the Sales folder with Read permission.

This is implemented in the domain that is managing the business rule. In this case, the business rule is Read-level access to the Sales folder, and the Contoso domain (in which the Sales folder resides) manages the access. The resource access management rule group is created as a domain local group, ACL_Sales Folders_Read.

3. Add the role groups to the resource access management rule group ACL_Sales Folders_Read to represent the management rule.

The role groups you add can come from any domain in the forest or from a trusted domain such as Woodgrove Bank. Global groups from trusted external domains, or from any domain in the same forest, can be members of a domain local group.

4. Assign to the rule group the permission that implements the required level of access.
In this case, grant the Allow Read permission to the domain local group ACL_Sales Folders_Read.

This strategy results in single points of management, reducing the management burden. One point of management defines who is in Sales, and one defines who is an Auditor. Those roles, of course, are likely to have a variety of permissions to resources beyond simply the Contoso domain's Sales folder. Another single point of management determines who has Read access to the Sales folder. And, of course, the Sales folder might not just be a single folder on a single server: It could be a collection of folders across multiple servers, each of which assigns Allow Read permission to the single domain local group.

NOTE ROLE-BASED MANAGEMENT

Role-based management is a concept used throughout information technology and information protection, and it can be attained with out-of-the-box capabilities of Active Directory. IGDLA is the implementation of role-based management using Active Directory groups.

PRACTICE Creating and Managing Groups

In this practice, you create groups, experiment with group membership, and convert group type and scope. Before performing the exercises in this practice, you must create the following objects in the contoso.com domain:

- A first-level OU named Groups
- A first-level OU named User Accounts
- User objects in the User Accounts OU for David Jones, Jeff Ford, and Tony Krijnen

EXERCISE 1 Create Groups

In this exercise, you create groups of different scopes and types.

1. Log on to SERVER01 as Administrator. Open the Active Directory Users And Computers snap-in and click the Groups OU in the tree pane.
If the Sales group already exists, delete the group.
2. Right-click the Groups OU, point to New, and then click Group.
3. In the Group Name box, type **Sales**.
4. Select the Global group scope and Security group type. Click OK.
5. Right-click the Sales group and choose Properties.
6. On the Members tab, click Add. Type **Jeff; Tony** and click OK. Click OK to close the Properties dialog box.

7. Repeat steps 2–4 to create two global security groups named Marketing and Consultants.
8. Repeat steps 2–4 to create a domain local security group named ACL_Sales Folder_Read.
9. Open the properties of the ACL_Sales Folder_Read group.
10. On the Members tab, click Add. Type **Sales;Marketing;Consultants** and click OK.
11. Click Add. Type **David** and click OK. Click OK to close the Properties dialog box.
12. Open the Properties dialog box of the Marketing group.
13. On the Members tab, click Add.
14. Type **ACL_Sales Folder_Read** and click OK.
You are unable to add a domain local group to a global group.
15. Close all open dialog boxes.
16. Create a folder named Sales on the C drive.
17. Right-click the Sales folder, click Properties, and then click the Security tab.
18. Click Edit, and then click Add.
19. Click Advanced, and then click Find Now.
Notice that by using a prefix for group names, such as the *ACL_* prefix for resource access groups, you can find them quickly, grouped together at the top of the list.
20. Close all open dialog boxes.
21. Switch to Active Directory Users And Computers, right-click the Groups OU, click New, and then click Group.
22. In the Group Name box, type **Employees**.
23. Select the Domain Local group scope and the Distribution group type. Click OK.

EXERCISE 2 Convert Group Type and Scope

In this exercise, you learn how to convert group type and scope.

1. Right-click the Employees group and choose Properties.
2. Change the group type to Security. Click Apply.
Consider: Can you change the group scope from Domain Local to Global? How?
3. Change the group scope to Universal. Click Apply.
4. Change the group scope to Global. Click Apply.
5. Click OK to close the Properties dialog box.

Lesson Summary

- There are two types of groups: security and distribution. Security groups can be assigned permissions and can be mail-enabled. Distribution groups are used primarily as email distribution lists—they cannot be assigned permissions to resources.
- In addition to local groups, which are maintained only in the local SAM database of a domain member server, there are three domain group scopes: global, domain local, and universal.
- The group scope affects the group's replication, the types of objects that can be members of the group, and the group's availability to be a member of another group or to be used for management tasks such as assigning permissions.
- You can convert group type and scope after creating the group.
- An enterprise group management strategy involves defining user roles as global security groups, and then creating groups that enable you to manage rules. For example, to manage access to a resource at a particular level, such as Read, you create a domain local security group, and then assign that group Read permission to the resource. The result is that user and computer identities become members of global groups, which are then nested into domain local groups, which are given access to resources. This group nesting strategy is abbreviated as *IGDLA*.

Lesson Review

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

NOTE ANSWERS

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

1. A new project requires that users in your domain and in the domain of a partner organization have access to a shared folder on your file server. Which type of group should you create to manage the access to the shared folder?
 - A. Universal security group
 - B. Domain local security group
 - C. Global security group
 - D. Domain local distribution group

2. Your domain includes a global distribution group named Company Update. It has been used to send company news by email to its members. You have decided to allow all members to contribute to the newsletter by creating a shared folder on a file server. What must you do to allow group members access to the shared folder?
- A. Change the group scope to domain local
 - B. Change the group scope to universal
 - C. Add the group to the Domain Users group
 - D. Use DSMod with the *-secgrp yes* parameter
3. You have created a global security group in the contoso.com domain named Corporate Managers. Which members can be added to the group? (Choose all that apply.)
- A. Sales Managers, a global group in the fabrikam.com domain, a trusted domain of a partner company
 - B. Sales Managers, a global group in the tailspintoys.com domain, a domain in the contoso.com forest
 - C. Linda Mitchell, a user in the tailspintoys.com domain, a domain in the contoso.com forest
 - D. Jeff Ford, a user in the fabrikam.com domain, a trusted domain of a partner company
 - E. Mike Danseglio, a user in the contoso.com domain
 - F. Sales Executives, a global group in the contoso.com domain
 - G. Sales Directors, a domain local group in the contoso.com domain
 - H. European Sales Managers, a universal group in the contoso.com forest

Lesson 2: Automating the Creation and Management of Groups

In Lesson 1 you learned the steps for creating groups, choosing group scope and type, and configuring group membership, using the Active Directory Users And Computers snap-in. When you need to create more than one group at a time, or when you want to automate group creation, you must use other tools. Chapter 3 introduced you to command-line and automation tools, including CSVDE, LDIFDE, DSAdd, and Windows PowerShell. These tools can also be used to automate the creation and management of group objects. In this lesson, you'll learn how to manage the life cycle of group objects, from beginning to end, by using command-line and automation tools.

After this lesson, you will be able to:

- Create groups with DSAdd, CSVDE, and LDIFDE.
- Manage group membership with DSMod, LDIFDE, and Windows PowerShell.
- Enumerate group membership with DSGet.
- Move and delete groups with DSMove and DSRm.
- Copy group membership.

Estimated lesson time: 45 minutes

Creating Groups with DSAdd

The DSAdd command, introduced in Chapter 3, lets you add objects to Active Directory. To add a group, type the following command:

```
dsadd group GroupDN
```

where *GroupDN* is the distinguished name (DN) of the group, such as "CN=Finance Managers, OU=Groups,DC=contoso,DC=com." Be certain to surround the DN with quotes if the DN includes spaces.

For example, to create a new global security group named Marketing in the Groups OU of the contoso.com domain, the command would be:

```
dsadd group "CN=Marketing,OU=Groups,DC=contoso,DC=com" -samid Marketing -secgrp yes -scope g
```

You can also provide the *GroupDN* parameter in one of the following ways:

- By piping a list of DNs from another command such as DSQuery.
- By typing each DN on the command line, separated by spaces.

- By leaving the DN parameter empty, at which point you can type the DNs one at a time at the keyboard console of the command prompt. Press Enter after each DN. After the last DN, press Ctrl+Z, and then press Enter.

Each of these three options allows you to generate multiple groups simultaneously with DSAdd. You can also use the DSAdd command with more than one *GroupDN* on the command line, each separated by a space, to generate multiple groups.

The DSAdd command can also configure attributes of the groups you create with the following optional parameters:

- **-secgrp { yes | no }** Specifies group type: security (*yes*) or distribution (*no*).
- **-scope { l | g | u }** Determines the group scope: domain local (*l*), global (*g*), or universal (*u*).
- **-samid *Name*** Specifies the *sAMAccountName* of the group. If not specified, the name of the group from its DN is used. It is recommended that the *sAMAccountName* and the group name be the same, so you do not need to include this parameter when using DSAdd.
- **-desc *Description*** Configures the group's description.
- **-members *MemberDN*** Adds members to the group. Members are specified by their DNs in a space-separated list.
- **-member of *GroupDN ...*** Makes the new group a member of one or more existing groups. The groups are specified by their DNs in a space-separated list.

Importing Groups with CSVDE

Chapter 3 also introduced you to Comma-Separated Values Data Exchange (CSVDE), which imports data from comma-separated values (.csv) files. It also exports data to a .csv file. The following example shows a .csv file that will create a group, Marketing, and populate the group with two initial members, Linda Mitchell and Scott Mitchell.

```
objectClass,sAMAccountName,DN,member
group,Marketing,"CN=Marketing,OU=Groups,DC=contoso,DC=com",
  "CN=Linda Mitchell,OU=User Accounts,DC=contoso,DC=com;
  CN=Scott Mitchell,OU=User Accounts,DC=contoso,DC=com"
```

The .csv file is two lines. The first line contains the attribute names, and the second line contains the values for the new group, *Marketing*. The second line is wrapped for presentation in this text.

Take note of the use of quotation marks in the preceding example. Quotation marks are required when an attribute includes a comma; without quotation marks, the comma would be interpreted as a delimiter. The DN of the group includes commas, so it must be surrounded by quotation marks. In the case of a multivalued attribute such as *member*, each value is separated by a semicolon—there are two values in *member* in the example. The entire *member* attribute is surrounded by quotation marks, not each individual value of the *member* attribute.

You can import this file into Active Directory by using the command:

```
csvde -i -f "filename" [-k]
```

The *-i* parameter specifies import mode. Without it, CSVDE uses export mode. The *-f* parameter precedes the filename, and the *-k* parameter ensures that processing continues even if errors are encountered, such as if the object already exists or the member cannot be found.



EXAM TIP

CSVDE can be used to create objects, but not to modify existing objects. You cannot use CSVDE to import members to existing groups.

Importing Groups with LDIFDE

LDAP Data Interchange Format Data Exchange (LDIFDE), as you learned in Chapter 3, is a tool that imports and exports files in the Lightweight Directory Access Protocol Data Interchange Format (LDIF) format. LDIF files are text files within which operations are specified by a block of lines separated by a blank line. Each operation begins with the DN of the object that is the target of the operation. The next line, *changeType*, specifies the type of operation: *add*, *modify*, or *delete*.

The following LDIF file creates two groups, Finance and Research, in the Groups OU of the contoso.com domain:

```
DN: CN=Finance,OU=Groups,DC=contoso,DC=com
changeType: add
CN: Finance
description: Finance Users
objectClass: group
sAMAccountName: Finance
```

```
DN: CN=Research,OU=Groups,DC=contoso,DC=com
changeType: add
CN: Research
description: Research Users
objectClass: group
sAMAccountName: Research
```

Convention would suggest saving the file with an *.ldf* extension—for example, *Groups.ldf*. To import the groups into the directory, issue the *Ldifde.exe* command, as shown here:

```
ldifde -i -f groups.ldf -k
```

The *-i* parameter specifies import mode. Without it, LDIFDE uses export mode. The *-f* parameter precedes the filename, and the *-k* parameter ensures that processing continues even if errors are encountered, such as if the object already exists.

Modifying Group Membership with LDIFDE

LDIFDE can also be used to modify existing objects in Active Directory, using LDIF operations with a *changeType* of *modify*. To add two members to the Finance group, the LDIF file would be:

```
dn: CN=Finance,OU=Groups,DC=contoso,DC=com
changeType: modify
add: member
member: CN=April Stewart,OU=User Accounts,dc=contoso,dc=com
member: CN=Mike Fitzmaurice,OU=User Accounts,dc=contoso,dc=com
-
```

The *changeType* is set to *modify*, and then the change operation is specified: *add* objects to the *member* attribute. Each new member is then listed on a separate line that begins with the *member* attribute name. The change operation is terminated with a line containing a single dash. Changing the third line to the following would remove the two specified members from the group:

```
delete: member
```

Retrieving Group Membership with DSGet

The DSMod and DSGet commands discussed in Chapter 3 are particularly helpful for managing the membership of groups. There is no option in the Active Directory Users And Computers snap-in to list all the members of a group including nested members. You can see only direct members of a group on the group's Members tab. Similarly, there is no way to list all the groups to which a user or computer belongs, including nested groups. You can see only direct membership on the user's or computer's Member Of tab.

The DSGet command lets you retrieve a complete list of a group's membership, including nested members, with the following syntax:

```
dsgget group "GroupDN" -members [-expand]
```

The *-expand* parameter performs the magic of expanding nested groups' members.

Similarly, the DSGet command can be used to retrieve a complete list of groups to which a user or computer belongs, again by using the *-expand* parameter in the following commands:

```
dsgget user "UserDN" -memberof [-expand]
dsgget computer "ComputerDN" -memberof [-expand]
```

The *-memberof* parameter returns the value of the user's or computer's *memberOf* attribute, showing the groups to which the object directly belongs. When you add the *-expand* parameter, those groups are searched recursively, producing an exhaustive list of all groups to which the object belongs in the domain.

Changing Group Membership with DSMod

The DSMod command was applied in Lesson 1 to modify the scope and type of a group. The command's basic syntax is:

```
dsmod group "GroupDN" [options]
```

You can use options such as *-samid* and *-desc* to modify the *sAMAccountName* and *description* attributes of the group. Most useful, however, are the options that allow you to modify a group's membership:

- **-addmbr "Member DN"** Adds members to the group
- **-rmmbr "Member DN"** Removes members from the group

As with all DS commands, *Member DN* is the distinguished name of another Active Directory object, surrounded by quotes if the DN includes spaces. Multiple *Member DN* entries can be included, separated by spaces. For example, to add Mike Danseglio to the Research group, the DSMod command would be:

```
dsmod group "CN=Research,OU=Groups,DC=contoso,DC=com"  
-addmbr "CN=Mike Danseglio,OU=User Accounts,DC=contoso,DC=com"
```

Copying Group Membership

You can use DSGet in combination with DSMod to copy group membership. In the following example, the DSGet command is used to get information about all the members of the Sales group, and then, by piping that list to DSMod, add those users to the Marketing group:

```
dsget group "CN=Sales,OU=Groups,DC=contoso,DC=com" -members |  
dsmod group "CN=Marketing,OU=Groups,DC=contoso,DC=com" -addmbr
```

Notice the use of piping. The "output" of DSGet (distinguished names of members of the first group) is piped, using the pipe symbol ("`|`"), to act as the input for the DNs that are omitted after the *-addmbr* parameter.

Similarly, the DSGet and DSMod commands can work together to copy the group membership of one object, such as a user, to another object:

```
dsget user "Source User DN" -memberof | dsmod group -addmbr "Target User DN"
```

Moving and Renaming Groups with DSMove

You can move and rename groups in Active Directory Users And Computers by right-clicking the group and then clicking the Move or the Rename command.

The DSMove command, also discussed in Chapter 3, enables you to move or rename an object within a domain. You cannot use it to move objects between domains. Its basic syntax is:

```
dsmove ObjectDN [-newname NewName] [-newparent TargetOUDN]
```

The object is specified by using its distinguished name in the *ObjectDN* parameter. To rename the object, specify its new common name as the value of the *-newname* parameter. To move an object to a new location, specify the distinguished name of the target container as the value of the *-newparent* parameter.

For example, to change the name of the Marketing group to Public Relations, type:

```
dsmove "CN=Marketing,OU=Groups,DC=contoso,DC=com" -newname "Public Relations"
```

To then move that renamed group to the Marketing OU, type:

```
dsmove "CN=Public Relations,OU=Groups,DC=contoso,DC=com" -newparent  
"OU=Marketing,DC=contoso,DC=com"
```

NOTE YOU'RE NOT LIMITED TO THE COMMAND LINE

You can also move or rename a group in the Active Directory Users And Computers snap-in by right-clicking the group and choosing Move or Rename from the context menu.

Deleting Groups with DSRm

DSRm can be used to delete a group or any other Active Directory object. The basic syntax of DSRm is:

```
dsrm ObjectDN ... [-subtree [-exclude]] [--noprompt] [-c]
```

The object is specified by its distinguished name in the *ObjectDN* parameter. You are prompted to confirm the deletion of each object unless you specify the *-noprompt* parameter. The *-c* parameter puts DSRm into continuous operation mode, in which errors are reported, but the command keeps processing additional objects. Without the *-c* switch, processing halts on the first error.

The *-subtree* parameter causes DSRm to delete the object and all child objects. The *-subtree -exclude* option deletes all child objects, but not the object itself.

To delete the Public Relations group, type:

```
dsrm "CN=Public Relations,OU=Marketing,DC=contoso,DC=com"
```

You can also delete a group in the Active Directory Users And Computers snap-in by right-clicking the group and choosing the Delete command.

NOTE KNOW THE IMPACT BEFORE DELETING A GROUP

When you delete a group, you are removing a point of management in your organization. Be certain that you have evaluated the environment to verify that no permissions or other resources rely on the group. Deleting a group is a serious action with potentially significant consequences. When you delete a group, you remove its SID. Re-creating the group with the same name does not restore permissions, because the new group's SID is different from that of the original group.

It is recommended that, before you delete a group, you record its membership and remove all members for a period of time to determine whether the members lose access to any resources. If anything goes wrong, simply re-add the members. If the test succeeds, delete the group.

Managing Groups with Windows PowerShell

Windows PowerShell makes it easy to manage groups. The following cmdlets work with Active Directory group objects:

- **New-ADGroup** Creates a group.
- **Remove-ADGroup** Deletes a group.
- **Get-ADGroup** Retrieves an object reference to a group.
- **Set-ADGroup** Configures properties of a group.
- **Add-ADGroupMember** Adds a member to a group.
- **Remove-ADGroupMember** Removes a member from a group.
- **Get-ADGroupMember** Enumerates the members of a group. The *-recursive* parameter enumerates members of nested groups.

As you learned in Chapter 3, you can use the *Get-Help* cmdlet to learn more about these cmdlets. You use Windows PowerShell to create groups in the Practice for this lesson.

PRACTICE Automating the Creation and Management of Groups

In this practice, you use DS commands, CSVDE, LDIFDE, and Windows PowerShell to perform group management tasks. Before performing the exercises in this practice, you need to create the following objects in the contoso.com domain:

- A first-level OU named Groups
- A first-level OU named User Accounts
- User objects in the User Accounts OU for Linda Mitchell, Scott Mitchell, Jeff Ford, Mike Fitzmaurice, Mike Danseglio, April Stewart, and Tony Krijnen

In addition, *delete* any groups with the following names: Finance, Accounting.

EXERCISE 1 Manage Groups with Windows PowerShell

In this exercise, you use Windows PowerShell to create a group.

1. Log on to SERVER01 as Administrator.
2. Open Active Directory Module For Windows PowerShell. Type the following command on one line:

```
New-ADGroup -Path "OU=Groups,DC=contoso,DC=com" -Name "PowerShell Experts"
-sAMAccountName "PowerShell Experts" -GroupCategory Security -GroupScope Global
```

3. Open the Active Directory Users And Computers snap-in. Select the Groups OU and confirm that the PowerShell Experts group was created.
4. Switch to Windows PowerShell. Type the following command on one line:

```
Add-ADGroupMember -Identity "PowerShell Experts"
  -Members "CN=Mike Danseglio,OU=User Accounts,DC=contoso,DC=com"
```

5. Type the following command:

```
Get-ADGroupMember -Identity "PowerShell Experts"
```

6. Type the following command:

```
Get-Command *ADGroup*
```

EXERCISE 2 Create a Group with DSAdd

In this exercise, you use DSAdd to create a group. DSAdd can create a group, and even populate its membership, with a single command.

1. Type the following command on one line. Then press Enter.

```
dsadd group "CN=Finance,OU=Groups,DC=contoso,DC=com" -samid Finance -secgrp
yes -scope g
```

2. Open the Active Directory Users And Computers snap-in and confirm that the group was created successfully. If the Active Directory Users And Computers snap-in was open prior to performing step 2, refresh the view.

EXERCISE 3 Import Groups with CSVDE

1. Open Notepad and type the following two lines. Note that the second line is wrapped for readability in this text.

```
objectClass,sAMAccountName, DN, member
group,Accounting, "CN=Accounting,OU=Groups,DC=contoso,DC=com",
  "CN=Linda Mitchell,OU=User Accounts,DC=contoso,DC=com;
  CN=Scott Mitchell,OU=User Accounts,DC=contoso,DC=com"
```

2. Save the file to your Documents folder with the name **"Importgroups.csv"** (including the quotes so that Notepad doesn't add a .txt extension).
 3. Open Command Prompt, and type the following command:
- ```
csvde -i -f "%userprofile%\documents\importgroups.csv"
```
4. Switch to the Active Directory Users And Computers snap-in, refresh the view of the Groups OU, and check to confirm that the group was created successfully.

## EXERCISE 4 Modify Group Membership with LDIFDE

CSVDE cannot modify the membership of existing groups, but LDIFDE can. In this exercise, you use LDIFDE to modify the group membership of the Accounting group you imported in Exercise 3, "Import Groups with CSVDE."

1. Open Notepad and type the following lines:

```
dn: CN=Accounting,OU=Groups,DC=contoso,DC=com
changetype: modify
add: member
member: CN=April Stewart,OU=User Accounts,dc=contoso,dc=com
member: CN=Mike Fitzmaurice,OU=User Accounts,dc=contoso,dc=com
-
```

```
dn: CN= Accounting,OU=Groups,DC=contoso,DC=com
changetype: modify
delete: member
member: CN=Linda Mitchell,OU=User Accounts,dc=contoso,dc=com
-
```

Be sure to include the dashes after each block and the blank line between the two blocks.

2. Save the file to your Documents folder as "**MembershipChange.ldf**" (including the quotes so that Notepad doesn't add a .txt extension).
3. Switch to Command Prompt.
4. Type the following command and press Enter:  

```
ldifde -i -f "%userprofile%\documents\membershipchange.ldf"
```
5. Using the Active Directory Users And Computers snap-in, confirm that the membership of the Accounting group changed according to the instructions of the LDIF file. It should now include April Stewart, Mike Fitzmaurice, and Scott Mitchell.

## EXERCISE 5 Modify Group Membership with DSMod

In this exercise, you add a user and a group to the Finance group, using the DSMod command.

1. Switch to Command Prompt.
2. Type the following command on one line to change the membership of the Finance group:

```
dsmod group "CN=Finance,OU=Groups,DC=contoso,DC=com"
-addmbr "CN=Tony Krijnen,OU=User Accounts,DC=contoso,DC=com"
"CN=Accounting,OU=Groups,DC=contoso,DC=com"
```

3. In the Active Directory Users And Computers snap-in, confirm that the membership of the Finance group consists of Tony Krijnen and the Accounting group.

## EXERCISE 6 Confirm Group Membership with DSGet and Windows PowerShell

Evaluating effective group membership is difficult with the Active Directory Users And Computers snap-in but easy with the DSGet command in Windows PowerShell. In this exercise, you look at both the full membership of a group and the group memberships of a user.

1. Switch to Command Prompt.
2. List the direct members of the Accounting group by typing the following command and then pressing Enter:

```
dsget group "CN=Accounting,OU=Groups,DC=contoso,DC=com" -members
```

3. List the direct members of the Finance group by typing the following command and then pressing Enter:

```
dsget group "CN=Finance,OU=Groups,DC=contoso,DC=com" -members
```

4. List the full list of members of the Finance group by typing the following command and then pressing Enter:

```
dsget group "CN=Finance,OU=Groups,DC=contoso,DC=com" -members -expand
```

5. List the direct group membership of Scott Mitchell by typing the following command and then pressing Enter:

```
dsget user "CN=Scott Mitchell,OU=User Accounts,DC=contoso,DC=com" -memberof
```

6. List the full group membership of Scott Mitchell by typing the following command and then pressing Enter:

```
dsget user "CN=Scott Mitchell,OU=User Accounts,DC=contoso,DC=com" -memberof -expand
```

7. Switch to Active Directory Module For Windows PowerShell, type the following command, and then press Enter:

```
Get-ADGroupMember "Finance" -recursive | Select sAMAccountName
```

*Select* is an alias for the *Select-Object* cmdlet, which takes the objects in the pipeline and selects one or more properties of the objects. Used here, it makes the output of the *Get-ADGroupMember* cmdlet more readable. Try it without the pipe and the *Select* cmdlet to see the difference.

## Lesson Summary

- You can create groups with DSAdd, CSVDE, LDIFDE, and Windows PowerShell.
- LDIFDE, DSMOD, and Windows PowerShell can modify the membership of existing groups.
- The DSGet command and Windows PowerShell can list the full membership of a group, including nested groups.

## Lesson Review

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

### **NOTE ANSWERS**

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

1. Which of the following can be used to remove members from a group? (Choose all that apply.)
  - A. Remove-Item
  - B. DSRm
  - C. DSMod
  - D. LDIFDE
  - E. CSVDE
2. You are using DSMod to add a domain local group named GroupA to a global group named GroupB. You are receiving errors. Which command will solve the problem so that you can add GroupA to GroupB? (Choose all that apply.)
  - A. Dsrms.exe
  - B. Dsmode.exe
  - C. Dsquery.exe
  - D. Dsget.exe
3. Your management has asked you to produce a list of all users who belong to the Special Project group, including those users belonging to groups nested into Special Project. Which of the following can you use? (Choose all that apply.)
  - A. *Get-ADGroupMember*
  - B. Dsquery.exe
  - C. LDIFDE
  - D. Dsget.exe

## Lesson 3: Administering Groups in an Enterprise

---

Lessons 1 and 2 prepared you to perform daily administrative tasks related to groups in Active Directory. You learned to create, modify, and delete groups, using a variety of tools and procedures. This lesson rounds out your exploration of groups by preparing you to take advantage of useful group attributes for documenting groups, delegate the management of group membership to specific administrative teams or individuals, and break away from reliance on some of the Active Directory and Windows default groups.

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

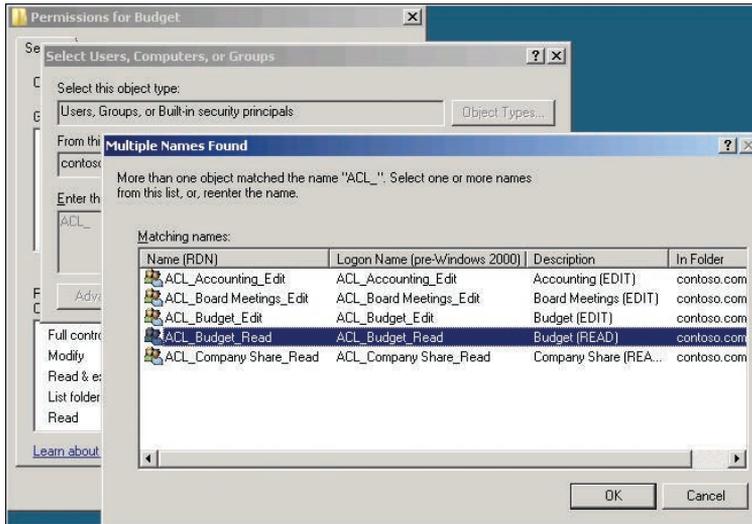
- Document the purpose of a group by using the group's attributes.
- Protect a group from accidental deletion.
- Delegate group membership management using the Managed By tab.
- Create a shadow group.
- Understand default (Builtin) groups.
- Assign permissions to special identities.

**Estimated lesson time: 45 minutes**

## Best Practices for Group Attributes

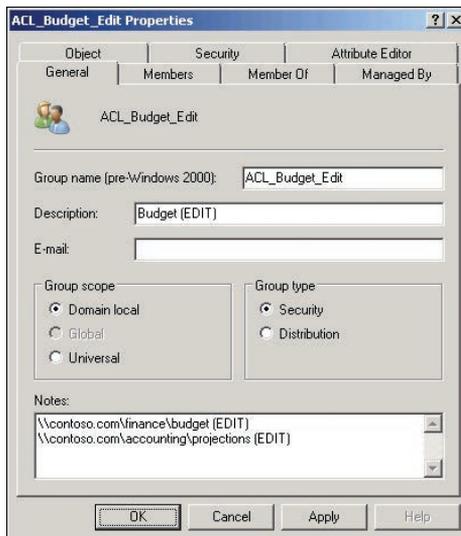
Creating a group in Active Directory is easy. It is not so easy to make sure that the group is used correctly over time. You can facilitate the correct management and use of a group by documenting its purpose to help administrators understand how and when to use the group. The following best practices which, although unlikely to be addressed by the certification exam, will prove immensely useful to your enterprise group administration:

- **Establish and adhere to a strict naming convention** Lesson 1 addressed a suggested naming convention. In the context of ongoing group administration, establishing and following group naming standards increases administrative productivity. Using prefixes to indicate the purpose of a group, and using a consistent delimiter between the prefix and the descriptive part of the group names, can help locate the correct group for a particular purpose. For example, the prefix APP can be used to designate groups that are used to manage applications, and the prefix ACL can be used for groups that are assigned permissions on ACLs. With such prefixes, it becomes easier to locate and interpret the purpose of groups named APP\_Accounting versus ACL\_Accounting\_Read. The former is used to manage the deployment of the accounting software, and the latter provides read access to the accounting folder. Prefixes also help group the names of groups in the user interface. Figure 4-11 shows an example. When attempting to locate a group to use when assigning permissions to a folder, you can type the prefix ACL\_ in the Select dialog box and click OK. A Multiple Names Found dialog box appears, showing only the ACL\_ groups in the directory, thereby ensuring that permissions will be assigned to a group that is designed to manage resource access.



**FIGURE 4-11** Selecting a group by using a group prefix to filter the correct type of group

- Summarize a group's purpose with its description attribute** Use the *description* attribute of a group to summarize the group's purpose. Because the Description column is enabled by default in the details pane of the Active Directory Users And Computers snap-in, the group's purpose can be highly visible to administrators.
- Detail a group's purpose in its Notes** When you open a group's Properties dialog box, the Notes text box is visible at the bottom of the General tab. This text box can be used to document the group's purpose. For example, you can list the folders to which a group has been given permission, as shown in Figure 4-12.



**FIGURE 4-12** A group's Properties dialog box, showing the Notes box used to provide details of the group's purpose

## Protecting Groups from Accidental Deletion

Protect yourself from the potentially devastating results of deleting a group by protecting each group you create from deletion. Windows Server 2008 R2 makes it easy to protect any object from accidental deletion.

To protect an object, follow these steps:

1. In the Active Directory Users And Computers snap-in, click the View menu and make sure that Advanced Features is selected.
2. Open the Properties dialog box for a group.
3. On the Object tab, select the Protect Object From Accidental Deletion check box.
4. Click OK.

This is one of the few places in Windows in which you must click OK instead of Apply. Clicking Apply does not modify the ACL based on your selection.

The Protect Object From Accidental Deletion option applies an access control entry (ACE) to the ACL of the object that explicitly denies the Everyone group both the Delete permission and the Delete Subtree permission. If you really do want to delete the group, you can return to the Object tab of the Properties dialog box and clear the Protect Object From Accidental Deletion check box.

Deleting a group has a significant impact on administrators and, potentially, on security. Consider a group used to manage access to resources. If the group is deleted, access to that resource is changed. Either users who should have access to the resource are suddenly prevented access, creating a denial-of-service scenario, or inappropriate access to the resource becomes possible if you had used the group to deny access to a resource with a Deny permission.

Additionally, if you re-create the group, the new group object will have a new security identifier (SID), which will not match the SIDs on ACLs of resources. So you must instead perform object recovery to reanimate the deleted group before the tombstone interval is reached. When a group has been deleted for the tombstone interval—180 days by default—the group and its SID are permanently deleted from Active Directory.

When you reanimate a tombstoned object, you must re-create most of its attributes, including, importantly, the *member* attribute of group objects. This means you must rebuild the group membership after restoring the deleted object. Alternately, you can perform an authoritative restore or turn to your Active Directory snapshots to recover both the group and its membership.

Finally, Windows Server 2008 R2 introduces the Active Directory Recycle Bin, which lets you recover a deleted object in its entirety, reducing or eliminating the impact of accidentally deleting an object. Authoritative restore, snapshots, and the Active Directory Recycle Bin are discussed in Chapter 13, "Directory Business Continuity."

Recovering a deleted group is a skill you should hope to use only in worst-case scenarios, not in day-to-day operations of a production environment. Protect yourself from the potentially devastating results of group object deletion by protecting each group you create.

## Delegating the Management of Group Membership

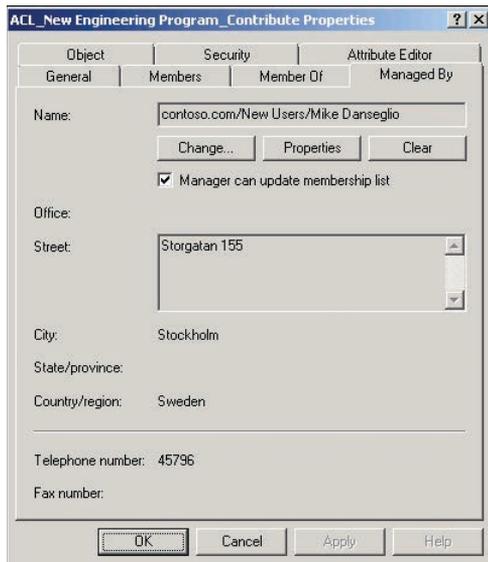
After creating a group, you might want to delegate the management of the group's membership to a team or an individual who has the business responsibility for the resource that the group manages.

For example, let's assume that your finance manager is responsible for creating next year's budget. You create a shared folder for the budget and assign Write permission to a group named ACL\_Budget\_Edit. If someone needs access to the budget folder, he or she contacts the help desk to enter a request, the help desk contacts the finance manager for business approval, and then the help desk adds the user to the ACL\_Budget\_Edit group. You can improve the responsiveness and accountability of the process by allowing the finance manager to change the group's membership. Then users needing access can request it directly from the finance manager, removing the intermediate step of contacting the help desk.

To delegate the management of a group's membership, you must assign to the finance manager the Allow Write Member permission for the group. The *member* attribute is the multivalued attribute that is the group's membership.

## Delegating Membership Management with the Managed By Tab

The easiest way to delegate membership management of a single group is to use the Managed By tab of a group object's Properties dialog box, shown in Figure 4-13.



**FIGURE 4-13** The Managed By tab of a group's Properties dialog box

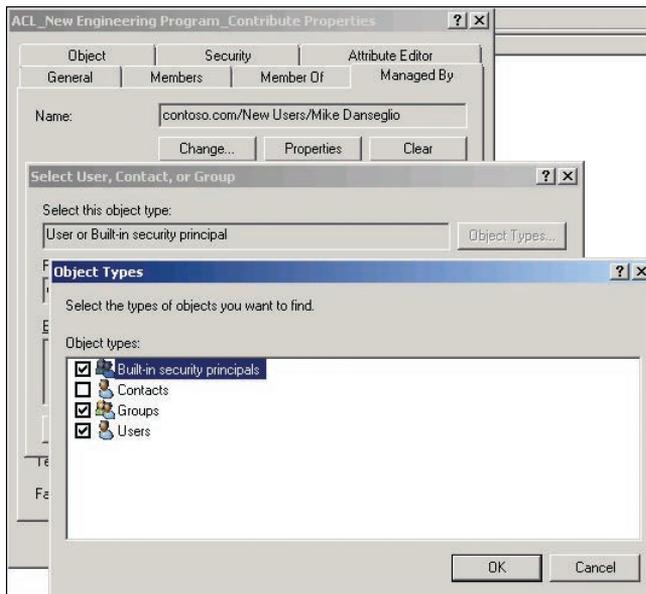
The Managed By tab serves two purposes. First, it provides contact information related to the manager of a group. You can use this information to contact the business owner of a group to obtain approval prior to adding a user to the group.

The second purpose served by the Managed By tab is to manage the delegation of the *member* attribute. Note the Manager Can Update Membership List check box shown in Figure 4-13. When this check box is selected, the user or group shown in the Name box is given the Allow Write Member permission. If you change or clear the manager, the appropriate change is made to the group's ACL.

**NOTE CLICK OK**

This is another of the strange and rare places in which you must actually click OK to implement the change. Clicking Apply does not change the ACL on the group.

It is not quite so easy to insert a group onto the Managed By tab of another group. When you click Change, the Select User, Contact, Or Group dialog box appears. If you enter the name of a group and click OK, an error occurs. That's because this dialog box is not configured to accept groups as valid object types, even though *Group* is in the name of the dialog box itself. To work around this odd limitation, click Object Types, and then select the check box next to Groups, as shown in Figure 4-14. Click OK to close both the Object Types and Select dialog boxes. Be sure to select the Manager Can Update Membership List check box if you want to assign the Write Member permission to the group. When a group is used on the Managed By tab, no contact information is visible because groups do not maintain contact-related attributes.



**FIGURE 4-14** Selecting a group for the Managed By tab

After you have delegated group membership management, users do not require Active Directory Users And Computers to modify the membership of the group. A user can simply use the Search Active Directory capability of Windows clients to find the group, and then change its membership.

To find a group:

1. Click Start, and then click Network.
2. Click the Search Active Directory button on the toolbar.
3. Type the name of the group and click Find Now.

## Delegating Membership Management Using Advanced Security Settings

You can use the Advanced Security Settings dialog box to assign the Allow Write Member permission directly. You can assign the permission for an individual group or for all the groups in an OU.

To delegate the management of membership for an individual group, perform the following steps:

1. In the Active Directory Users And Computers snap-in, click the View menu and make sure Advanced Features is selected.
2. Right-click the group's name and choose Properties.
3. On the Security tab, click Advanced.
4. In the Advanced Security Settings dialog box, click Add.

If the Add button is not visible, click Edit, and then click Add.

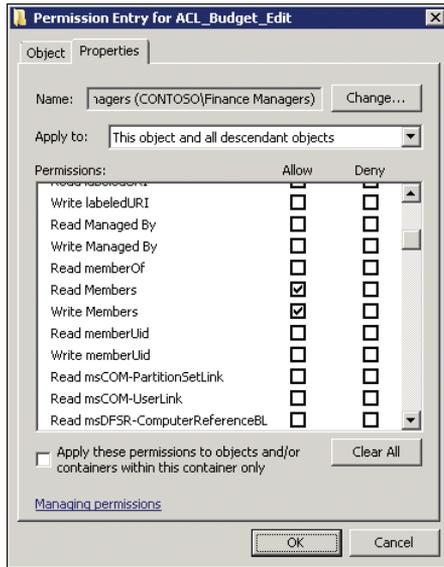
5. In the Select Users, Contacts, Service Account, Or Group dialog box, enter the name for the group to which you want to grant permission, or click Browse to search for the group. When you are finished, click OK.

The Permission Entry dialog box appears.

6. On the Properties tab, in the Apply To list, choose This Object And All Descendant Objects.
7. In the Permissions list, select the Allow check boxes for the Read Members and Write Members permissions.

By default, all users have the Read Members permission, so that permission is not required. However, role-based access control is best implemented by assigning all the permissions required to achieve the desired capability, rather than relying on permissions assigned indirectly.

Figure 4-15 shows the resulting Permission Entry dialog box.



**FIGURE 4-15** The Permission Entry dialog box showing the delegation of group membership management for a group

8. Click OK to close each of the security dialog boxes.

To delegate the ability to manage membership for all groups in an OU, perform the following steps:

1. In the Active Directory Users And Computers snap-in, click the View menu and make sure Advanced Features is selected.
2. Right-click the OU and then choose Properties.
3. On the Security tab, click Advanced.
4. In the Advanced Security Settings dialog box, click Add.

If the Add button is not visible, click Edit, and then click Add.

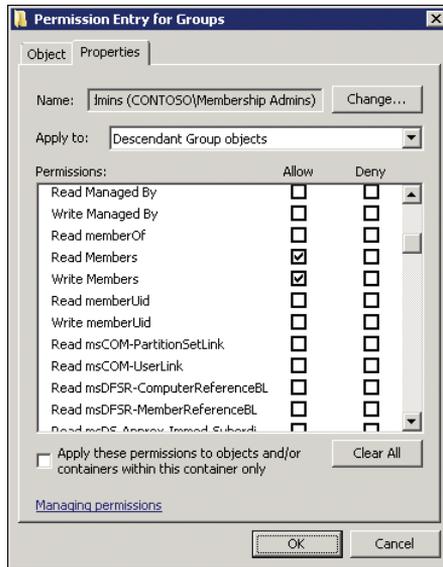
5. In the Select dialog box, enter the name for the group to which you want to grant permission, or click Browse to search for the group. When you are finished browsing, click OK.

The Permission Entry dialog box appears.

6. On the Properties tab, in the Apply To list, choose Descendant Group Objects.
7. In the Permissions list, select the Allow check boxes for the Read Members and Write Members permissions.

By default, all users have the Read Members permission, so that permission is not required. However, role-based access control is best implemented by assigning all the permissions required to achieve the desired capability, rather than relying on permissions assigned indirectly.

Figure 4-16 shows the resulting Permission Entry dialog box.



**FIGURE 4-16** The Permission Entry dialog box showing the delegation of group membership management for all groups in the Groups OU

8. Click OK to close each of the security dialog boxes.

## Understanding Shadow Groups

Most management of an enterprise is implemented with groups. Groups are assigned permission to resources. Groups can be used to filter the scope of Group Policy objects. Groups are assigned fine-grained password policies. Groups can be used as collections for configuration management tools such as Microsoft System Center Configuration Manager. The list goes on. OUs, however, are not used as frequently to manage the enterprise, and in some cases, they cannot be used. For instance, OUs cannot be assigned permissions to resources, nor can they be assigned fine-grained password policies (discussed in Chapter 8, “Improving the Security of Authentication in an AD DS Domain”). Instead, the primary purpose of an OU is to provide a scope of management for the delegation of administrative permissions for the objects in that OU. In other words, an OU of users enables you to delegate to your help desk the ability to reset passwords for all users in the OU. OUs are administrative containers.

The reason for this separation of purpose between OUs and groups is that OUs do not provide the same flexibility as groups. A user or computer (or other object) can exist only within the context of a single OU, whereas a security principal can belong to many groups. Therefore, groups are used for aligning identities with the capabilities required by those identities.

Sometimes, you might want to manage using an OU when it is not possible. For example, you might want to give all users in an OU access to a folder. Or you might want to assign a unique password policy to users in an OU. You cannot do so directly, but you can achieve your goal by creating what is called a *shadow group*. A shadow group is a group that contains the same users as an OU. More accurately, a shadow group contains users that meet a certain criterion.

The easiest way to create a shadow group is to create the group, and then, in the OU containing the users, press Ctrl+A to select all users. Right-click any selected user and choose Add To Group. Type the name of the group and click OK.



#### EXAM TIP

On the 70-640 exam, be prepared to see the term *shadow group* in use. Know that it means a group that contains, as members, the users in an OU.

Unfortunately, Windows does not yet provide a way to maintain the membership of a shadow group dynamically. When you add or remove a user in an OU, you must also add or remove the user in the shadow group.

#### MORE INFO MAINTAINING SHADOW GROUPS DYNAMICALLY

See *Windows Administration Resource Kit: Productivity Solutions for IT Professionals* for scripts that help maintain shadow groups dynamically.

## Default Groups

Several groups are created automatically on a server running Windows Server 2008 R2. These are called *default local groups*, and they include well-known groups such as Administrators, Backup Operators, and Remote Desktop Users. Additional groups are created in a domain, in both the Builtin and Users containers, including Domain Admins, Enterprise Admins, and Schema Admins. The following list provides a summary of capabilities of the subset of default groups that have significant permissions and user rights related to the management of Active Directory:

- **Enterprise Admins (Users container of the forest root domain)** This group is a member of the Administrators group in every domain in the forest, giving it complete access to the configuration of all domain controllers. It also owns the Configuration partition of the directory and has full control of the domain naming context in all forest domains.
- **Schema Admins (Users container of the forest root domain)** This group owns and has full control of the Active Directory schema.
- **Administrators (Builtin container of each domain)** This group has complete control over all domain controllers and data in the domain naming context. It can change the membership of all other administrative groups in the domain, and the Administrators

group in the forest root domain can change the membership of Enterprise Admins, Schema Admins, and Domain Admins. The Administrators group in the forest root domain is arguably the most powerful service administration group in the forest.

- **Domain Admins (Users container of each domain)** This group is added to the Administrators group of its domain. Therefore, it inherits all the capabilities of the Administrators group. It is also, by default, added to the local Administrators group of each domain member computer, giving Domain Admins ownership of all domain computers.
- **Server Operators (Builtin container of each domain)** This group can perform maintenance tasks on domain controllers. It has the right to log on locally, start and stop services, perform backup and restore operations, format disks, create or delete shares, and shut down domain controllers. By default, this group has no members.
- **Account Operators (Builtin container of each domain)** This group can create, modify, and delete accounts for users, groups, and computers located in any organizational unit in the domain (except the Domain Controllers OU), as well as in the Users and Computers containers. Account Operators cannot modify accounts that are members of the Administrators or Domain Admins groups, nor can they modify those groups. Account Operators can also log on locally to domain controllers. By default, this group has no members.
- **Backup Operators (Builtin container of each domain)** This group can perform backup and restore operations on domain controllers as well as log on locally and shut down domain controllers. By default, this group has no members.
- **Print Operators (Builtin container of each domain)** This group can maintain print queues on domain controllers. It can also log on locally and shut down domain controllers.

The default groups that provide administrative privileges should be managed carefully because they typically have broader privileges than are necessary for most delegated environments and because they often apply protection to their members.

The Account Operators group is a perfect example. If you examine its capabilities in the preceding list, you see that its rights are very broad, indeed. It can even log on locally to a domain controller. In very small enterprises, such rights are probably appropriate for one or two individuals who might be domain administrators anyway. In enterprises of any size, the rights and permissions granted to Account Operators are usually far too broad.

Additionally, the Account Operators group is, like the other administrative groups listed previously, a *protected group*. Protected groups are defined by the operating system and cannot be unprotected. Members of a protected group become protected. The result of protection is that the permissions (ACLs) of members are modified so that they no longer inherit permissions from their OU but, rather, receive a copy of an ACL that is quite restrictive. For example, if Jeff Ford is added to the Account Operators group, his account becomes protected and the help desk, which can reset all other user passwords in the User Accounts OU, cannot reset Jeff Ford's password.

#### **MORE INFO PROTECTED ACCOUNTS**

For more information about protected accounts, see Knowledge Base article 817433 at <http://support.microsoft.com/?kbid=817433> and Knowledge Base article 840001 at <http://support.microsoft.com/kb/840001>. If you want to search the Internet for resources, use the keyword *adminSDHolder*.

For these reasons—overdelegation and protection—strive to avoid adding users to the groups listed previously that do not have members by default: Account Operators, Backup Operators, Server Operators, and Print Operators. Instead, create custom groups to which you assign permissions and user rights that achieve your business and administrative requirements.

For example, if Scott Mitchell needs to perform backup operations on a domain controller, but he should not be able to perform restore operations that could lead to database rollback or corruption and he should not be able to shut down a domain controller, don't put Scott in the Backup Operators group. Instead, create a group, assign it only the Backup Files And Directories user right, and then add Scott as a member.

#### **MORE INFO DEFAULT GROUP CAPABILITIES INFORMATION**

There is an exhaustive reference to the default groups in a domain and the default local groups on Microsoft TechNet. If you are not familiar with the default groups and their capabilities, you should prepare for the examination by reading about them. The default local and domain groups reference is at <http://technet.microsoft.com/en-us/library/dd728026%28WS.10%29.aspx>.

## Special Identities

Windows and Active Directory also support *special identities*, groups for which membership is controlled by the operating system. You cannot view the groups in any list (in the Active Directory Users And Computers snap-in, for example), you cannot view or modify the membership of these special identities, and you cannot add them to other groups. You can, however, use these groups to assign rights and permissions. The most important special identities, often referred to as *groups* for convenience, are described in the following list:

- **Anonymous Logon** Represents connections to a computer and its resources that are made without supplying a user name and password. In versions of Windows earlier than Windows Server 2003, this group was a member of the Everyone group. In Windows Server 2003 and later versions, this group is no longer a default member of the Everyone group.

- **Authenticated Users** Represents identities that have been authenticated. This group does not include Guest, even if the Guest account has a password.
- **Everyone** Includes Authenticated Users and Guest. On computers running versions of Windows earlier than Windows Server 2003, this group includes Anonymous Logon.
- **Interactive** Represents users accessing a resource while logged on locally to the computer hosting the resource, as opposed to accessing the resource over the network. When a user accesses any given resource on a computer to which the user is logged on locally, the user is automatically added to the Interactive group for that resource. Interactive also includes users logged on through a remote desktop connection.
- **Network** Represents users accessing a resource over the network, as opposed to users who are logged on locally at the computer hosting the resource. When a user accesses any given resource over the network, the user is automatically added to the Network group for that resource.

The importance of these special identities is that they enable you to provide access to resources based on the type of authentication or connection rather than on the user account. For example, you could create a folder on a system that allows users to view its contents when logged on locally to the system but does not allow the same users to view the contents from a mapped drive over the network. This is achieved by assigning permissions to the Interactive special identity.

## **PRACTICE** Administering Groups in an Enterprise

---

In this practice, you perform best-practices group management tasks to improve the administration of groups in the contoso.com domain. To perform the exercises in this practice, you need to have the following objects in the contoso.com domain:

- A first-level OU named Groups.
- A global security group named Finance in the Groups OU.
- A first-level OU named User Accounts.
- A user account named Mike Danseglio in the User Accounts OU. Populate the user account with sample contact information: address, phone, and email. Reset the password of the account so that you know it. Make sure the account is enabled and that the user is *not* required to change the password at the next logon.

In this and other practices in this training kit, you will log on to the domain controller with user accounts that are not a member of Domain Administrators or the domain's Administrators group. Therefore, you must give all user accounts the right to log on locally to the domain controllers in your practice environment. Follow the steps in the article, "Grant a Member the Right to Logon Locally," at [http://technet.microsoft.com/en-us/library/ee957044\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee957044(WS.10).aspx) to grant the Allow Logon Locally right to the Administrators and Domain Users groups. If you will use Remote Desktop Services to connect to the domain controller—rather than logging on locally—grant the Allow Logon Through Remote Desktop Services right. This is for the practice environment only. In a production environment, you should not grant users the right to log on to domain controllers.

### EXERCISE 1 Create a Well-Documented Group

In this exercise, you create a group to manage access to the Budget folder, and you follow the best-practices guidelines presented in this lesson.

1. Log on to SERVER01 as Administrator and open the Active Directory Users And Computers snap-in.
2. Select the Groups OU in the console tree.
3. Right-click the Groups OU, point to New, and click Group.
4. In the Group Name box, type **ACL\_Budget\_Edit**.
5. Select Domain Local in the Group Scope section and Security in the Group Type section, and then click OK.
6. Click the View menu and ensure that Advanced Features is selected.
7. Right-click the ACL\_Budget\_Edit group and choose Properties.
8. On the Object tab, select the Protect Object From Accidental Deletion check box and click OK.
9. Open the group's Properties again.
10. In the Description box, type **BUDGET (EDIT)**.
11. In the Notes box, type the following paths to represent the folders that have permissions assigned to this group:  
\\server23\data\$\finance\budget  
\\server32\data\$\finance\revenue projections
12. Click OK.

### EXERCISE 2 Delegate Management of Group Membership

In this exercise, you give Mike Danseglio the ability to manage the membership of the ACL\_Budget\_Edit group.

1. Open the Properties dialog box of the ACL\_Budget\_Edit group.
2. On the Managed By tab, click Change.
3. Type the user name for Mike Danseglio, **mike.danseglio**, and then click OK.
4. Select the Manager Can Update Membership List check box. Click OK.

### EXERCISE 3 Validate the Delegation of Membership Management

In this exercise, you test the delegation you performed in Exercise 2, "Delegate Management of Group Membership," by modifying the membership of the group as Mike Danseglio.

1. Open Command Prompt and type the following command: **runas/user:mike.danseglio cmd.exe**.
2. When prompted, enter the password for Mike Danseglio.  
A new command prompt window appears, running as Mike Danseglio.

3. Type the following command on one line, and then press Enter:

```
dsmod group "CN=ACL_Budget_Edit,OU=Groups,DC=contoso,DC=com"
-addmbr "CN=Finance,OU=Groups,DC=contoso,DC=com"
```

4. Close both Command Prompt windows.
5. In the Active Directory Users And Computers snap-in, examine the membership of the ACL\_Budget\_Edit group and confirm that the Finance group was added successfully.

## Lesson Summary

- Use the Description and Notes text boxes in a group's Properties dialog box to document the purpose of the group.
- The Managed By tab lets you specify a user or group that is responsible for a group. You can also select the Manager Can Update Membership List check box to delegate membership management to the user or group indicated on the Managed By tab.
- To delegate the management of group membership, grant the Allow Write Members permission.
- Use the Protect Object From Accidental Deletion check box to prevent the potential security and management problems created when a group is accidentally deleted.
- Windows Server 2008 R2 and Active Directory contain default groups with significant permissions and user rights. You should not add users to the default domain groups that do not already have members (Account Operators, Backup Operators, Print Operators, and Server Operators), and you should seriously restrict membership in other service administration groups (Enterprise Admins, Domain Admins, Schema Admins, and Administrators).
- Special identities such as Authenticated Users, Everyone, Interactive, and Network can be used to assign rights and permissions. Their membership is determined dynamically by the operating system and cannot be viewed or modified.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 3, "Administering Groups in an Enterprise." The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE ANSWERS**

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

- 1.** Your company is conducting a meeting for a special project. The data is particularly confidential. The team is meeting in a conference room, and you have configured a folder on the conference room computer that grants permission to the team members. The folder is a subfolder of a shared folder to which all employees have access. You want to ensure that team members access the data only while logged on to the computer in the conference room, not from other computers in the enterprise. What must you do?
  - A.** Assign the Allow Read permission to the Interactive group.
  - B.** Assign the Allow Read permission to the team group.
  - C.** Assign the Deny Traverse Folders permission to the team group.
  - D.** Assign the Deny Full Control permission to the Network group.
  
- 2.** You want to allow a user named Mike Danseglio to add and remove users in a group called Special Project. Where can you configure this permission?
  - A.** The Members tab of the group
  - B.** The Security tab of Mike Danseglio's user object
  - C.** The Member Of tab of Mike Danseglio's user object
  - D.** The Managed By tab of the group
  
- 3.** Which of the following groups can shut down a domain controller? (Choose all that apply.)
  - A.** Account Operators
  - B.** Print Operators
  - C.** Backup Operators
  - D.** Server Operators
  - E.** Interactive

## Chapter Review

---

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

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenario. This scenario sets up a real-world situation involving the topics of this chapter and asks you to create a solution.
- Complete the suggested practices.
- Take a practice test.

## Chapter Summary

---

- Group scopes (global, universal, domain local, and local) define group characteristics related to membership, replication, and availability of the group.
- In an enterprise, role-based management suggests that groups should be viewed as either defining a role or defining a business rule. Role groups are generally implemented as global groups, and rules are defined by using domain local groups.
- A group's *member* attribute is a multivalued attribute containing the DNs of the group's members. Each member's *memberOf* attribute is automatically updated to reflect changes in membership. When you add a user to a group, you are always changing the group's *member* attribute. The *memberOf* attribute, which is read-only, is called a backlink.
- You can delegate the management of group membership by assigning the Allow Write Members permission, which grants write permission to the *member* attribute.
- You can use Directory Services tools such as DSQuery, DSGet, and DSMod to list, create, and modify groups and their membership.
- CSVDE and LDIFDE can import and export groups. Additionally, LDIFDE can modify the membership of existing groups.
- The DSAdd, DSMove, and DSRm commands can add, move, and delete groups, respectively.

## Key Terms

---

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

- backlink
- shadow group
- special identities

## Case Scenario

---

In the following case scenario, you apply what you've learned about administering groups in an enterprise. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario: Implementing a Group Strategy

You are an administrator at Trey Research. A new product development initiative called Sliced Bread is underway, and there is confidential information about the project in shared folders on three servers in three different sites. Users in Research, Marketing, and Finance need access to the project data. Additionally, the CEO and her assistant need access. Of these, only Marketing and Research require Write access. Several interns are currently working in the Marketing department, and you want to prevent them from gaining access. Finally, a team of auditors from Woodgrove Bank, an investor in Trey Research, need Read access as well. You have a trust relationship configured so that the Trey Research domain trusts the Woodgrove Bank domain.

1. What types and scopes of groups do you create to represent the user roles in Trey Research? What type and scope of group do you ask administrators at Woodgrove Bank to create to represent the auditors' role?
2. What types and scopes of groups do you create to manage Read and Write access to the Sliced Bread folders?
3. Describe the nesting of users and groups you implement to achieve the security required by this project.

## Suggested Practices

---

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

### Automate Group Membership and Shadow Groups

In this practice, you create a shadow group to reflect the user accounts in the User Accounts OU. You apply the DSQuery and DSMod commands to keep the membership up to date.

To perform this practice, you must have the following objects in the contoso.com domain:

- A first-level OU named Groups
- An OU named User Accounts
- Several sample user accounts in the User Accounts OU

Also, perform the following practices.

- **Practice 1** In the Groups OU, create a global security group named All Users. Then click the User Accounts OU in the tree pane of the Active Directory Users And

Computers snap-in. Click any user in the details pane and press Ctrl+A to select all. Right-click any selected user and choose Add To Group. Add the users to the All Users group. Examine the Members tab of the All Users group to confirm that all users were added successfully.

- **Practice 2** Open Command Prompt. Delete the All Users group you created in Practice 1. Type the following two commands to create the All Users shadow group:

```
dsadd group "CN=A11 Users,OU=Groups,DC=contoso,DC=com" -secgrp yes -scope g
dsquery user "OU=User Accounts,DC=contoso,DC=com" |
 dsmod group "CN=Users,OU=Groups,DC=contoso,DC=com" -addmbr
```

- **Practice 3** In a command prompt, type the following two commands to remove all members of the group and repopulate it with the current users in the User Accounts OU:

```
dsget group "CN=A11 Users,OU=Groups,DC=contoso,DC=com" -members |
 dsmod group "CN=A11 Users,OU=Groups,DC=contoso,DC=com" -rmmbr
dsquery user "OU=User Accounts,DC=contoso,DC=com" |
 dsmod group "CN=A11 Users,OU=Groups,DC=contoso,DC=com" -addmbr
```

## Take a Practice Test

---

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-640 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

### **MORE INFO** PRACTICE TESTS

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



# Improving the Security of Authentication in an AD DS Domain

When a user logs on to an Active Directory Domain Services (AD DS) domain, she enters her user name and password, and the client uses those credentials to *authenticate* the user—to validate the user’s identity against her Active Directory account. In Chapter 3, “Administering User Accounts,” you learned how to create and manage user accounts and their properties, including their passwords. In this chapter, you will explore the domain-side components of authentication, including the policies that specify password requirements and the auditing of authentication-related activities. You will also discover three new options to improve the security of accounts and authentication: managed service accounts’ password settings objects (PSOs, better known as fine-grained password policy); and read-only domain controllers (RODCs).

## Exam objectives in this chapter:

- Maintain Active Directory accounts.
- Configure account policies.
- Configure audit policy by using GPOs.
- Configure Active Directory replication.
- Configure the read-only domain controller (RODC).

## Lessons in this chapter:

- Lesson 1: Configuring Password and Lockout Policies **392**
- Lesson 2: Auditing Authentication **404**
- Lesson 3: Configuring Read-Only Domain Controllers **410**
- Lesson 4: Managing Service Accounts **425**

## Before You Begin

---

To complete the lessons in this chapter, you must have installed a domain controller named SERVER01 in the contoso.com domain.



### **REAL WORLD**

Dan Holme

As I work with clients to implement AD DS, I must constantly balance the need to maintain high levels of security with the need to continue conducting the client's business. With versions of Microsoft Windows prior to Windows Server 2008, I constantly encountered three scenarios in which this balance was particularly difficult to reach.

The first relates to the security of user accounts with high levels of privilege within the enterprise. Such accounts are especially attractive to hackers, so they should be locked down with particularly lengthy and complex passwords. In earlier versions of Windows, only one password policy could be applied to all accounts in the domain. Therefore, I either had to apply the highly restrictive password policy to all users in the domain, which was never a palatable solution, or ask administrators to follow the more restrictive policy but with no way to require compliance. Windows Server 2008 introduced fine-grained password policies that can be used to apply more or less restrictive password policies beyond the requirements for groups or users in a domain.

Branch offices were also problematic because I had to balance the need for quick and reliable user authentication at the branch office against the desire to centralize control over the physical security of domain controllers. Placing a domain controller in a branch office would clearly improve performance for users in the office but would also typically expose the domain controller to lower levels of security than those maintained at the data center. Coming to the rescue once again, Windows Server 2008 and Windows Server 2008 R2 can act as a read-only domain controller, authenticating users and the branch office without storing all domain user credentials, thus reducing the risk to the enterprise in the event of a stolen branch office domain controller.

Another significant challenge is the management of service accounts. Services such as backup, antivirus, Microsoft SQL Server, and IIS application pools run in the context of a user account. When you change the password of a service account, you must configure the service with the new password as well. Managing service accounts was so problematic that many organizations simply configured service accounts with non-expiring passwords, which is a very poor practice from a security perspective. Windows Server 2008 R2 addresses this scenario with a new feature: managed service accounts.

If you have worked with Active Directory for any period of time, you already appreciate the value of fine-grained password policies, read-only domain controllers, and managed service accounts. If you are new to Active Directory, you are lucky to be able to work with these much-anticipated features.

# Lesson 1: Configuring Password and Lockout Policies

---

By default in a Windows Server 2008 R2 domain, users are required to change their password every 42 days, and a password must be at least seven characters long and meet complexity requirements, including the use of three of four character types: uppercase, lowercase, numeric, and non-alphanumeric. Three password policies—maximum password age, password length, and password complexity—are among the first policies encountered by administrators and users alike in an Active Directory domain. Rarely do these default settings align precisely with the password security requirements of an organization. Your organization might require passwords to be changed more or less frequently or to be longer. In this lesson, you learn how to implement your enterprise's password and lockout policies by modifying the Default Domain Policy Group Policy object (GPO).

As you know, there are exceptions to every rule, and you likely have exceptions to your password policies. To enhance the security of your domain, you can enforce more restrictive password requirements for accounts assigned to administrators, for accounts used by services such as Microsoft SQL Server, or for a backup utility. In versions of Windows prior to Windows Server 2008, this was not possible; a single password policy applied to all accounts in the domain. In this lesson, you learn to configure fine-grained password policies, a feature of Windows Server 2008 and Windows Server 2008 R2 that lets you assign different password policies to users and groups in your domain.

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

- Implement your domain password and account lockout policy.
- Configure and assign fine-grained password policies.

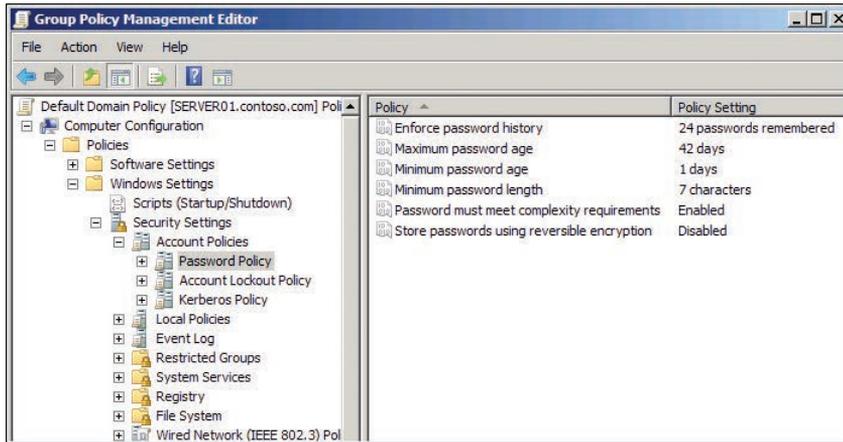
**Estimated lesson time: 45 minutes**

## Understanding Password Policies

Your domain's password policy is configured by a GPO scoped to the domain. Within the GPO, in the Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy node, you can configure the policy settings that determine password requirements. The Password Policy node is shown in Figure 8-1.

You can understand the effects of the policies by considering the life cycle of a user password. A user is required to change his or her password within the number of days specified by the Maximum Password Age policy setting. When the user enters a new password, the length of the new password is compared to the number of characters in the Minimum Password Length policy. If the Password Must Meet Complexity Requirements policy is enabled, the password must contain at least three of four character types:

- Uppercase—for example, A to Z
- Lowercase—for example, a to z



**FIGURE 8-1** The Password Policy node of a GPO

- Numeric—0 to 9
- Nonalphanumeric—symbols such as !, #, %, or &

If the new password meets the requirements, Active Directory puts the password through a mathematical algorithm that produces a representation of the password called the *hash code*. The hash code is unique; no two passwords can create the same hash code. The algorithm used to create the hash code is called a *one-way function*. You cannot put the hash code through a reverse function to derive the password. The fact that it is a hash code, and not the password itself, that is stored in Active Directory helps to increase the security of the user account.

Occasionally, applications require the ability to read a user's password. This is not possible because, by default, only the hash code is stored in Active Directory. To support such applications, you can enable the Store Passwords Using Reversible Encryption policy. This policy is not enabled by default, but if you enable the policy, user passwords are stored in an encrypted form that can be decrypted by the application. Reversible encryption significantly reduces the security of your domain, so it is disabled by default, and you should strive to eliminate applications that require direct access to passwords.

Additionally, Active Directory can check a cache of the user's previous hash codes to make sure that the new password is not the same as the user's previous passwords. The number of previous passwords against which a new password is evaluated is determined by the Enforce Password History policy. By default, Windows maintains the previous 24 hash codes.

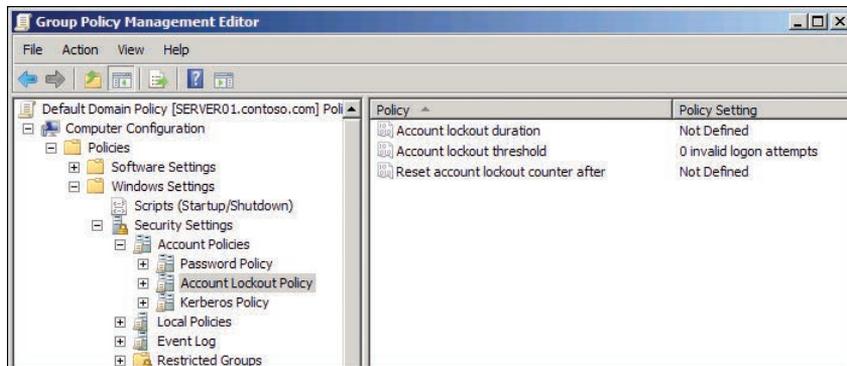
If a user is determined to reuse her password when the password expiration period occurs, she could simply change her password 25 times to work around the password history. To prevent that from happening, the Minimum Password Age policy specifies an amount of time that must pass between password changes. By default, it is one day. Therefore, the determined user would have to change her password once a day for 25 days to reuse a password. This type of deterrent is generally successful at discouraging such behavior.

These policy settings—history, minimum age, and maximum age—affect users changing their passwords. The settings do not affect administrators using the Reset Password command to change another user’s password.

## Understanding Account Lockout Policies

An intruder can gain access to the resources in your domain by determining a valid user name and password. User names are relatively easy to identify because most organizations create user names from an employee’s email address, initials, combinations of first and last names, or employee IDs. After a user name is known, the intruder might determine the correct password by guessing or by repeatedly logging on with combinations of characters or words until the logon is successful.

This type of attack, called *brute force*, can be thwarted by limiting the number of incorrect logons allowed. That is exactly what account lockout policies achieve. Account lockout policies are located in the node of the GPO directly below Password Policy. The Account Lockout Policy node is shown in Figure 8-2.



**FIGURE 8-2** The Account Lockout Policy node of a GPO

Three settings are related to account lockout. The first of these settings, Account Lockout Threshold, determines the number of invalid logon attempts permitted within a time specified by the second of these settings, Reset Account Lockout Counter After. If an attack results in more unsuccessful logons within that time frame, the user account is locked out. When an account is locked out, Active Directory denies logon to that account, even if the correct password is specified.

An administrator can unlock a locked user account by following the procedure you learned in Chapter 3. You can also configure Active Directory to automatically unlock the account after a delay specified by a third setting, the Account Lockout Duration policy setting.

# Configuring the Domain Password and Lockout Policy

Active Directory supports one set of password and lockout policies for a domain. These policies are configured in a GPO that is scoped to the domain. A new domain contains a GPO called Default Domain Policy that is linked to the domain and includes the default policy settings for password, account lockout, and Kerberos policies, shown in Figures 8-1 and 8-2. You can change the settings by editing the Default Domain Policy.

## **PRACTICE IT**

You can practice configuring a domain's password and lockout policies in Exercise 1, "Configure the Domain's Password and Lockout Policies," in the practice for this lesson.

## **BEST PRACTICE DO NOT OVERLOAD THE DEFAULT DOMAIN POLICY GPO**

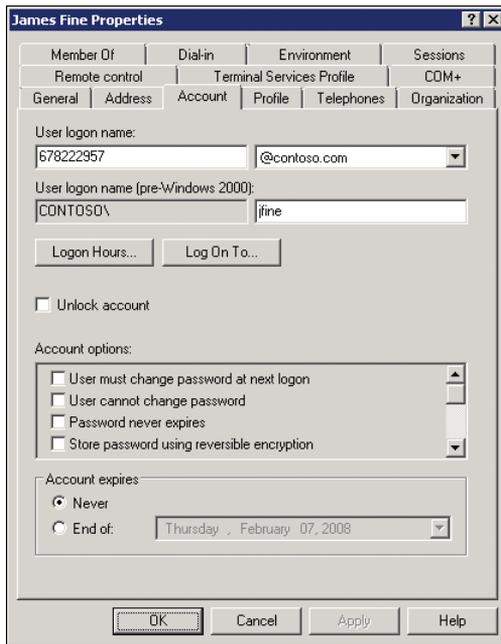
The best practice is to edit the Default Domain Policy GPO to specify the password policy settings for your organization. You should also use the Default Domain Policy GPO to specify account lockout policies and Kerberos policies. Do not use the Default Domain Policy GPO to deploy any other custom policy settings. In other words, use the Default Domain Policy GPO to define the password, account lockout, and Kerberos policies for the domain, and nothing else. Additionally, do not define password, account lockout, or Kerberos policies for the domain in any other GPO.

## **NOTE ACCOUNT SETTINGS OVERRIDE POLICIES**

The password settings configured in the Default Domain Policy affect all user accounts in the domain. The settings can be overridden, however, by the password-related properties of the individual user accounts. On the Account tab of a user's Properties dialog box, shown in Figure 8-3, you can specify settings such as Password Never Expires or Store Password Using Reversible Encryption. For example, if five users have an application that requires direct access to their passwords, you can configure the accounts for those users to store their passwords using reversible encryption.

## Fine-Grained Password and Lockout Policy

You can also override the domain password and lockout policy by using a feature introduced in Windows Server 2008 called *fine-grained password and lockout policy*, often shortened to simply *fine-grained password policy*. Fine-grained password policy enables you to configure a policy that applies to one or more groups or users in your domain.



**FIGURE 8-3** Password-related properties of a user account

Fine-grained password policy is a highly anticipated addition to Active Directory. There are several scenarios for which fine-grained password policy can be used to increase the security of your domain. Accounts used by administrators are delegated privileges to modify objects in Active Directory; therefore, if an intruder compromises an administrator's account, more damage can be done to the domain than could be done with the account of a standard user. For that reason, you should consider implementing stricter password requirements for administrative accounts. For example, you might require greater password length and more frequent password changes.

To use fine-grained password policy, your domain must be at the Windows Server 2008 domain functional level or higher, which means that all of your domain controllers in the domain are running Windows Server 2008 or later and the domain functional level has been raised to Windows Server 2008 or higher. Domain functional level is described in Chapter 12, "Managing Multiple Domains and Forests."

To confirm and modify the domain functional level:

1. Open Active Directory Domains And Trusts.
2. In the console tree, expand Active Directory Domains And Trusts, and then expand the tree until you can see the domain.
3. Right-click the domain and choose Raise Domain Functional Level.

Other account types that require special treatment in a domain are those used by services and Internet Information Services (IIS) application pools. A service performs its tasks with credentials that must be authenticated with a user name and password just like those of a human user. However, most services are not capable of changing their own password, so administrators configure service accounts with the Password Never Expires option enabled. When an account's password will not be changed, you should make sure the password is difficult to compromise. You can use fine-grained password policies to specify an extremely long minimum password length and no password expiration. Better yet, you can use a new feature of Windows Server 2008 R2—managed service accounts—for which passwords are automatically changed. Managed service accounts are discussed in Lesson 4 of this chapter.

## Understanding Password Settings Objects

The settings managed by fine-grained password policy are identical to those in the Password Policy and Accounts Policy nodes of a GPO. However, fine-grained password policies are not implemented as part of Group Policy, nor are they applied as part of a GPO. Instead, a separate class of object in Active Directory maintains the settings for fine-grained password policy: the *password settings object* (PSO).



---

### **EXAM TIP**

There can be one, and only one, authoritative set of password and lockout policy settings that applies to all users in a domain. Those settings are configured in the Default Domain Policy GPO. Fine-grained password policies, which apply to individual groups or users in the domain, are implemented using PSOs.

---

You can manage most Active Directory objects with user-friendly graphical user interface (GUI) tools such as the Active Directory Users And Computers snap-in. You manage PSOs, however, with low-level tools, including Active Directory Service Interface Editor (ADSI Edit).

### **MORE INFO PASSWORD POLICY BASIC**

Although it will not be addressed on the 70-640 exam, it is highly recommended that you use Password Policy Basic by Specops Software to manage fine-grained password policy. You can download the free GUI tool from <http://www.specopssoft.com>.

You can create one or more PSOs in your domain. Each PSO contains a complete set of password and lockout policy settings. A PSO is applied by linking the PSO to one or more global security groups or users. For example, to configure a strict password policy for administrative accounts, create a global security group, add the service user accounts as members, and link a PSO to the group. Applying fine-grained password policies to a group in this manner is more manageable than applying the policies to each individual user account. If you create a new service account, you simply add it to the group and the account becomes managed by the PSO.

## PSO Precedence and Resultant PSO

A PSO can be linked to more than one group or user, an individual group or user can have more than one PSO linked to it, and a user can belong to multiple groups. So which fine-grained password and lockout policy settings apply to a user? One and only one PSO determines the password and lockout settings for a user—this PSO is called the *resultant PSO*. Each PSO has an attribute that determines the precedence of the PSO. The precedence value is any number greater than 0, where the number 1 indicates the highest precedence. If multiple PSOs apply to a user, the PSO with the highest precedence (closest to 1) takes effect. Active Directory exposes the resultant PSO in a user object attribute, *msDS-ResultantPSO*, so you can readily identify the PSO that will affect a user. PSOs contain all password and lockout settings, so there is no inheritance or merging of settings. The resultant PSO is the authoritative PSO. The rules that determine precedence, and thus the resultant PSO, are as follows:

- If multiple PSOs apply to groups to which the user belongs, the PSO with the highest precedence wins.
- If one or more PSOs are linked directly to the user, PSOs linked to groups are ignored, regardless of their precedence. The user-linked PSO with highest precedence wins.
- If one or more PSOs have the same precedence value, Active Directory must make a choice. It picks the PSO with the lowest globally unique identifier (GUID). GUIDs are like serial numbers for Active Directory objects—no two objects have the same GUID. GUIDs have no particular meaning—they are just identifiers—so picking the PSO with the lowest GUID is, in effect, an arbitrary decision. You should configure PSOs with unique, specific precedence values so that you avoid this scenario.

To view the *msDS-ResultantPSO* attribute of a user:

1. Ensure that Advanced Features is enabled on the View menu.
2. Open the properties of the user account.
3. On the Attribute Editor tab, click Filter and ensure that Constructed is selected.  
The attribute you locate in the next step is a *constructed* attribute, meaning that the resultant PSO is not a hard-coded attribute of a user; rather, it is calculated by examining the PSOs linked to a user in real time.
4. Locate the *msDS-ResultantPSO* attribute.

### **PRACTICE IT**

**You will examine the *msDS-ResultantPSO* attribute in the practice at the end of this lesson.**

## PSOs and OUs

PSOs can be linked to global security groups or users. PSOs cannot be linked to organizational units (OUs). If you want to apply password and lockout policies to users in an OU, you must create a global security group that includes all of the users in the OU. This type of group is called a *shadow group*—its membership shadows, or mimics, the membership of an OU.

## ✓ Quick Check

- You want to require that administrators maintain a password of at least 15 characters and change the password every 45 days. The administrators' user accounts are in an OU called Admins. You do not want to apply the restrictive password policy to all domain users. What do you do?

### Quick Check Answer

- Create a global security group that contains all users in the Admins OU. Create a PSO that configures the password policies, and then link the PSO to the group.

Shadow groups are conceptual, not technical objects. You simply create a group and add the users that belong to the OU. If you change the membership of the OU, you must also change the membership of the group.

### **MORE INFO** SHADOW GROUPS

Additional information about PSOs and shadow groups is available at [http://technet.microsoft.com/en-us/library/cc770842\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc770842(WS.10).aspx).

### **MORE INFO** MAINTAINING SHADOW GROUP MEMBERSHIP WITH SCRIPTS

You can use scripts to maintain the membership of shadow groups dynamically so that they always reflect the users in OUs. You can find example scripts in *Windows Administration Resource Kit: Productivity Solutions for IT Professionals* by Dan Holme (Microsoft Press, 2008).

## **PRACTICE** Configuring Password and Lockout Policies

In this practice, you use Group Policy to configure the domain-wide password and lockout policies for contoso.com. You then secure administrative accounts by configuring more restrictive, fine-grained password and lockout policies.

### **EXERCISE 1** Configure the Domain's Password and Lockout Policies

In this exercise, you modify the Default Domain Policy GPO to implement a password and lockout policy for users in the contoso.com domain.

1. Log on to SERVER01 as Administrator.
2. Open Group Policy Management from the Administrative Tools program group.
3. Expand Forest, Domains, and contoso.com.
4. Right-click Default Domain Policy underneath the contoso.com domain and choose Edit.

5. You might be prompted with a reminder that you are changing the settings of a GPO. If so, click OK.  
The Group Policy Management Editor appears.
6. Expand Computer Configuration, Policies, Windows Settings, Security Settings, and Account Policies, and then click Password Policy.
7. Double-click the following policy settings in the console details pane and configure the settings indicated:
  - Maximum Password Age: 90 Days
  - Minimum Password Length: 10 characters
8. Select Account Lockout Policy in the console tree.
9. Double-click the Account Lockout Threshold policy setting and configure it for 5 Invalid Logon Attempts. Then click OK.
10. In the Suggested Value Changes dialog box, click OK.  
The values for Account Lockout Duration and Reset Account Lockout Counter After are automatically set to 30 minutes.
11. Close the Group Policy Management Editor window.

## **EXERCISE 2** Create a Password Settings Object

In this exercise, you create a PSO that applies a restrictive, fine-grained password policy to users in the Domain Admins group.

Before you proceed with this exercise, open Active Directory Users And Computers and confirm that the Domain Admins group is in the Users container. If it is not, move it to the Users container.

1. Open ADSI Edit from the Administrative Tools program group.
2. Right-click ADSI Edit and choose Connect To.
3. In the Name box, type **contoso.com**. Click OK.
4. Click and then expand contoso.com, and then click DC=contoso,DC=com.
5. Expand DC=contoso,DC=com and click CN=System.
6. Expand CN=System and click CN=Password Settings Container.  
All PSOs are created and stored in the Password Settings Container (PSC).
7. Right-click the PSC, point to New, and then choose Object.

The Create Object dialog box prompts you to select the type of object to create. There is only one choice: msDS-PasswordSettings—the technical name for the object class referred to as a PSO.

8. Click Next.

You are prompted for the value for each attribute of a PSO. The attributes are similar to those found in the GPO you examined in Exercise 1.

9. Configure each attribute as indicated in the following list. Click Next after each attribute.
- cn: **My Domain Admins PSO**. This is the friendly name of the PSO.
  - msDS-PasswordSettingsPrecedence: **1**. This PSO has the highest possible precedence because its value is the closest to 1.
  - msDS-PasswordReversibleEncryptionEnabled: **False**. The password is not stored using reversible encryption.
  - msDS-PasswordHistoryLength: **30**. The user cannot reuse any of the last 30 passwords.
  - msDS-PasswordComplexityEnabled: **True**. Password complexity rules are enforced.
  - msDS-MinimumPasswordLength: **15**. Passwords must be at least 15 characters long.
  - msDS-MinimumPasswordAge: **1:00:00:00**. A user cannot change his or her password within one day of a previous change. The format is d:hh:mm:ss (days, hours, minutes, seconds).
  - MaximumPasswordAge: **45:00:00:00**. The password must be changed every 45 days.
  - msDS-LockoutThreshold: **5**. Five invalid logons within the time frame specified by msDS-LockoutObservationWindow (the next attribute) will result in account lockout.
  - msDS-LockoutObservationWindow: **0:01:00:00**. A given number of invalid logons (specified by the previous attribute) within one hour will result in account lockout.
  - msDS-LockoutDuration: **1:00:00:00**. An account, if locked out, will remain locked for one day or until it is unlocked manually. A value of zero will result in the account remaining locked out until an administrator unlocks it.

The attributes listed are required. After clicking Next on the *msDS-LockoutDuration* attribute page, you can configure optional attributes.

10. Click More Attributes.
11. In the Select A Property To View list, select msDS-PSOAppliesTo.
12. In the Edit Attributes box, type the following:  
**CN=Domain Admins,CN=Users,DC=contoso,DC=com**
13. Click Add, click OK, and then click Finish.

### EXERCISE 3 Identify the Resultant PSO for a User

In this exercise, you identify the PSO that controls the password and lockout policies for an individual user.

1. Open the Active Directory Users And Computers snap-in.
2. Click the View menu and make sure that Advanced Features is selected.
3. Expand the contoso.com domain and click the Users container in the console tree.
4. Right-click the Administrator account and choose Properties.

5. On the Attribute Editor tab, click Filter and make sure that Constructed is selected.  
The attribute you will locate in the next step is a *constructed* attribute, meaning that the resultant PSO is not a hard-coded attribute of a user; rather, it is calculated by examining the PSOs linked to a user in real time.
6. In the Attributes list, locate *msDS-ResultantPSO*.
7. Identify the PSO that affects the user.

The My Domain Admins PSO that you created in Exercise 2, "Create a Password Settings Object," is the resultant PSO for the Administrator account.

#### **EXERCISE 4 Delete a PSO**

In this exercise, you delete the PSO you created in Exercise 2 so that its settings do not affect you in later exercises.

1. Repeat steps 1–6 of Exercise 2 to select the Password Settings Container in ADSI Edit.
2. In the console details pane, select CN=My Domain Admins PSO.
3. Press Delete.
4. Click Yes.

## **Lesson Summary**

- Password policy settings determine when a password can or must be changed and what the requirements of the new password are.
- Account lockout settings cause Active Directory to lock out a user account if a specified number of invalid logons occurs within a specified period of time. Lockout helps prevent intruders from repeatedly attempting to log on to a user account in an effort to guess the user's password.
- A domain can have only one set of password and lockout policies that affect all users in the domain. These policies are defined using Group Policy. You can modify the default settings in the Default Domain Policy GPO to configure the policies for your organization.
- Windows Server 2008 R2 gives you the option to specify different password and lockout policies for global security groups and users in your domain. Fine-grained password policies are deployed not with Group Policy but with password settings objects.
- If more than one PSO applies to a user or to groups to which a user belongs, a single PSO, called the resultant PSO, determines the effective password and lockout policies for the user. The PSO with the highest precedence (precedence value closest to 1) prevails. If one or more PSOs are linked directly to the user rather than indirectly to groups, group-linked PSOs are not evaluated to determine the resultant PSO, and the user-linked PSO with the highest precedence prevails.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, “Configuring Password and Lockout Policies.” The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE ANSWERS**

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

- 1.** You are an administrator at Tailspin Toys. Your Active Directory domain includes an OU called Service Accounts that contains all user accounts. Because you have configured service accounts with passwords that never expire, you want to apply a password policy that requires passwords of at least 40 characters. Which of the following steps should you perform? (Choose all that apply. Each correct answer is part of the solution.)
  - A.** Set the Minimum Password Length policy in the Default Domain Policy GPO.
  - B.** Link a PSO to the Service Accounts OU.
  - C.** Create a group called Service Accounts.
  - D.** Link a PSO to the Service Accounts group.
  - E.** Add all service accounts as members of the Service Accounts group.
  
- 2.** You want to configure account lockout policy so that a locked account will not be unlocked automatically. Rather, you want to require an administrator to unlock the account. Which configuration change should you make?
  - A.** Configure the Account Lockout Duration policy setting to 100.
  - B.** Configure the Account Lockout Duration policy setting to 1.
  - C.** Configure the Account Lockout Threshold to 0.
  - D.** Configure the Account Lockout Duration policy setting to 0.
  
- 3.** As you evaluate the password settings objects in your domain, you discover a PSO named PSO1 with a precedence value of 1 that is linked to a group named Help Desk. Another PSO, named PSO2, with a precedence value of 99, is linked to a group named Support. Mike Danseglio is a member of both the Help Desk and Support groups. You discover that two other PSOs are linked directly to Mike. PSO3 has a precedence value of 50, and PSO4 has a precedence value of 200. Which PSO is the resultant PSO for Mike?
  - A.** PSO1
  - B.** PSO2
  - C.** PSO3
  - D.** PSO4

## Lesson 2: Auditing Authentication

---

In Chapter 7, “Managing Enterprise Security and Configuration with Group Policy Settings,” you learned to configure auditing for several types of activities, including access to folders and changes to directory service objects. Windows Server 2008 R2 also allows you to audit the logon activity of users in a domain. By auditing successful logons, you can look for instances in which an account is being used at unusual times or in unexpected locations, which might indicate that an intruder is logging on to the account. Auditing failed logons can reveal attempts by intruders to compromise an account. In this lesson, you learn to configure auditing of logon authentication.

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

- Configure auditing of authentication-related activity.
- Distinguish between account logon and logon events.
- Identify authentication-related events in the Security log.

**Estimated lesson time: 30 minutes**

### Account Logon and Logon Events

This lesson examines two specific policy settings: Audit Account Logon Events and Audit Logon Events. It is important that you understand the difference between these two similarly named policy settings.

When a user logs on to any computer in the domain using a domain user account, a domain controller authenticates the attempt to log on to the domain account. This generates an account logon event on the domain controller.

The computer to which the user logs on—for example, the user’s laptop—generates a logon event. The computer did not authenticate the user against his or her account—it passed the account to a domain controller for validation. The computer did, however, allow the user to log on interactively to the computer. Therefore, the event is a logon event.

When the user connects to a folder on a server in the domain, that server authorizes the user for a type of logon called a *network logon*. Again, the server does not authenticate the user—it relies on the ticket given to the user by the domain controller. However, the connection by the user generates a logon event on the server.



#### **EXAM TIP**

Be certain that you can distinguish between *account logon events* and *logon events*. The simplest way to remember the difference is that an account logon event occurs where the account lives: on the domain controller that authenticates the user. A logon event occurs on the computer to which the user logs on interactively. It also occurs on the file server to which the user connects using a network logon.

---

# Configuring Authentication-Related Audit Policies

Account logon and logon events can be audited by Windows Server 2008 R2. The settings that manage auditing are located in a GPO in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy node. The Audit Policy node and the two settings detailed in the previous section are shown in Figure 8-4.

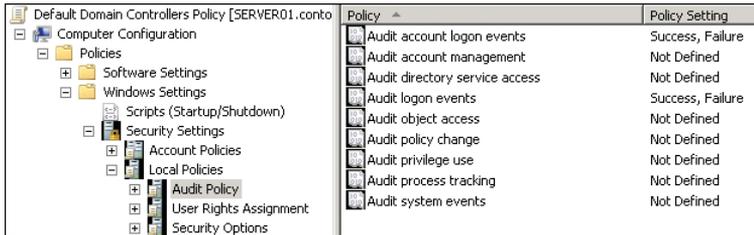


FIGURE 8-4 Authentication-related policy settings

To configure an audit policy, double-click the policy, and its properties dialog box appears. The Audit Account Logon Events Properties dialog box is shown in Figure 8-5.



FIGURE 8-5 The Audit Account Logon Events Properties dialog box

The policy setting can be configured to one of the following four states:

- **Not defined** If the Define These Policy Settings check box is cleared, the policy setting is not defined. In this case, the server audits events based on its default settings or on the settings specified in another GPO.

- **Defined for no auditing** If the Define These Policy Settings check box is selected, but the Success and Failure check boxes are cleared, the server will not audit these events.
- **Audit successful events** If the Define These Policy Settings check box is selected, and the Success check box is selected, the server will log successful events in its Security log.
- **Audit failed events** If the Define These Policy Settings check box is selected, and the Failure check box is selected, the server will log unsuccessful events in its Security log.

A server's audit behavior is determined by the settings that are applied as the resultant set of policy. In Windows Server 2008 R2, the default setting is to audit successful account logon events and successful logon events. So both types of events are, if successful, entered in the server's Security log. If you want to audit failures or turn off auditing, you must define the appropriate setting in the audit policy.

## Scoping Audit Policies

As with all policy settings, you should scope settings so that they affect the correct systems. For example, if you want to audit attempts by users to connect to remote desktop servers in your enterprise, you can configure logon event auditing in a GPO linked to the OU that contains your remote desktop servers. If, on the other hand, you want to audit logons by users to desktops in your human resources department, you can configure logon event auditing in a GPO linked to the OU containing human resources computer objects. Remember that domain users logging on to a client computer or connecting to a server will generate a logon event—not an account logon event—on that system.

Only domain controllers generate account logon events for domain users. Remember that an account logon event occurs on the domain controller that authenticates a domain user, regardless of where that user logs on. If you want to audit logons to domain accounts, you should scope account logon event auditing to affect only domain controllers. In fact, the Default Domain Controllers GPO that is created when you install your first domain controller is an ideal GPO in which to configure account logon audit policies.

### Quick Check

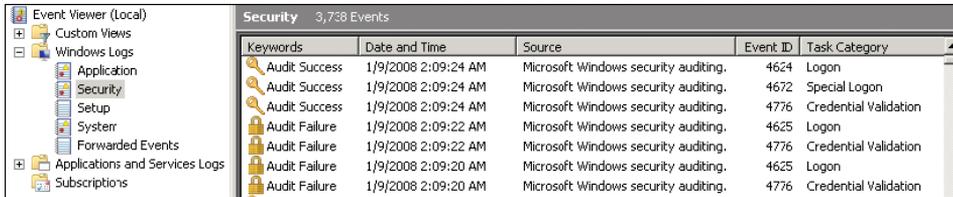
- You are concerned that an intruder is attempting to gain access to your network by guessing a user's password. You want to identify the times at which the intruder is trying to log on. What type of event should you audit? Should you configure the policy setting in the Default Domain Policy or in the Default Domain Controllers Policy?

### Quick Check Answer

- Enable auditing of failed account logon events (not logon events) in the Default Domain Controllers GPO. Only domain controllers generate account logon events related to the authentication of domain users. The Default Domain Controllers GPO is scoped correctly to apply only to domain controllers.

## Viewing Logon Events

Account logon and logon events, if audited, appear in the Security log of the system that generated the event. Figure 8-6 shows an example. So if you are auditing logons to computers in the human resources department, the events are entered in each computer's Security log. Similarly, if you are auditing unsuccessful account logons to identify potential intrusion attempts, the events are entered in each domain controller's Security log. This means, by default, that you will need to examine the Security logs of all domain controllers to get a complete picture of account logon events in your domain.



| Keywords       | Date and Time       | Source                               | Event ID | Task Category         |
|----------------|---------------------|--------------------------------------|----------|-----------------------|
| Audit: Success | 1/9/2008 2:09:24 AM | Microsoft Windows security auditing. | 4624     | Logon                 |
| Audit: Success | 1/9/2008 2:09:24 AM | Microsoft Windows security auditing. | 4672     | Special Logon         |
| Audit: Success | 1/9/2008 2:09:24 AM | Microsoft Windows security auditing. | 4776     | Credential Validation |
| Audit: Failure | 1/9/2008 2:09:22 AM | Microsoft Windows security auditing. | 4625     | Logon                 |
| Audit: Failure | 1/9/2008 2:09:22 AM | Microsoft Windows security auditing. | 4776     | Credential Validation |
| Audit: Failure | 1/9/2008 2:09:20 AM | Microsoft Windows security auditing. | 4625     | Logon                 |
| Audit: Failure | 1/9/2008 2:09:20 AM | Microsoft Windows security auditing. | 4776     | Credential Validation |

**FIGURE 8-6** Authentication events in the Security log

As you can imagine, in a complex environment with multiple domain controllers and many users, auditing account logons or logons can generate a tremendous number of events. If there are too many events, it can be difficult to identify problematic events worthy of closer investigation. You should balance the amount of logging you perform with the security requirements of your business and the resources you have available to analyze logged events.

### **PRACTICE** Auditing Authentication

In this practice, you use Group Policy to enable auditing of logon activity by users in the contoso.com domain. You then generate logon events and view the resulting entries in the event logs.

#### **EXERCISE 1** Configure Auditing of Account Logon Events

In this exercise, you modify the Default Domain Controllers Policy GPO to implement auditing of both successful and failed logons by users in the domain.

1. Open Group Policy Management from the Administrative Tools program group.
2. Expand Forest, Domains, Contoso.com, and Domain Controllers.
3. Right-click Default Domain Controllers Policy and choose Edit.  
Group Policy Management Editor appears.
4. Expand Computer Configuration, Policies, Windows Settings, Security Settings, and Local Policies, and then click Audit Policy.
5. Double-click Audit Account Logon Events.
6. Select the Define These Policy Settings check box.

7. Select both the Success and Failure check boxes. Click OK.
8. Double-click Audit Logon Events.
9. Select the Define These Policy Settings check box.
10. Select both the Success and Failure check boxes. Click OK.
11. Close Group Policy Management Editor.
12. Open Command Prompt and type **gpupdate.exe /force**.  
This command causes SERVER01 to update its policies, at which time the new auditing settings take effect.

### **EXERCISE 2** Generate Account Logon Events

In this exercise, you generate account logon events by logging on with both incorrect and correct passwords.

1. Log off of SERVER01.
2. Attempt to log on as Administrator with an incorrect password. Repeat this step once or twice.
3. Log on to SERVER01 with the correct password.

### **EXERCISE 3** Examine Account Logon Events

In this exercise, you view the events generated by the logon activities in Exercise 2.

1. Open Event Viewer from the Administrative Tools program group.
2. Expand Windows Logs, and then click Security.
3. Identify the failed and successful events.

## Lesson Summary

- Account logon events occur on a domain controller as it authenticates users logging on anywhere in the domain.
- Logon events occur on systems to which users log on—for example, to their individual desktops and laptops. Logon events are also generated in response to a network logon—for example, when a user connects to a file server.
- By default, Windows Server 2008 R2 systems audit successful account logon and logon events.
- To examine account logon events in your domain, you must look at the individual event logs from each domain controller.

## Lesson Review

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

## **NOTE ANSWERS**

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

- 1.** You want to obtain a log that will help you isolate the times of day that failed logons are causing a user’s account to be locked out. Which policy should you configure?
  - A.** Define the Audit Account Logon Events policy setting for Success events in the Default Domain Policy GPO.
  - B.** Define the Audit Account Logon Events policy setting for Failure events in the Default Domain Policy GPO.
  - C.** Define the Audit Logon Events policy setting for Success events in the Default Domain Policy GPO.
  - D.** Define the Audit Logon Events policy setting for Failure events in the Default Domain Policy GPO.
  
- 2.** You want to keep track of when users log on to computers in the human resources department of Adventure Works. Which of the following methods will allow you to obtain this information?
  - A.** Configure the policy setting to audit successful account logon events in the Default Domain Controllers GPO. Examine the event log of the first domain controller you installed in the domain.
  - B.** Configure the policy setting to audit successful logon events in a GPO linked to the OU containing user accounts for employees in the human resources department. Examine the event logs of each computer in the human resources department.
  - C.** Configure the policy setting to audit successful logon events in a GPO linked to the OU containing computer accounts in the human resources department. Examine the event logs of each computer in the human resources department.
  - D.** Configure the policy setting to audit successful account logon events in a GPO linked to the OU containing computer accounts in the human resources department. Examine the event logs of each domain controller.

## Lesson 3: Configuring Read-Only Domain Controllers

---

Branch offices present a unique challenge to an enterprise's IT staff: If a branch office is separated from the hub site by a wide area network (WAN) link, should you place a domain controller (DC) in the branch office? In previous versions of Windows, the answer to this question was not a simple one. Windows Server 2008, however, introduced a new type of domain controller—the read-only domain controller (RODC)—that made the question easier to answer. In this lesson, you explore the issues related to branch office authentication and domain controller placement, and you learn how to implement and support a branch-office RODC.

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

- Identify the business requirements for RODCs.
- Install an RODC.
- Configure password replication policy.
- Monitor the caching of credentials on an RODC.

**Estimated lesson time: 60 minutes**

## Authentication and Domain Controller Placement in a Branch Office

Consider a scenario in which an enterprise is characterized by a hub site and several branch offices. The branch offices connect to the hub site over WAN links that might be congested, expensive, slow, or unreliable. Users in the branch office must be authenticated by Active Directory to access resources in the domain. Should a DC be placed in the branch office?

In branch office scenarios, many of the services provided by IT are centralized in a hub site that is carefully maintained by the IT staff. In larger organizations, the hub site may include a robust datacenter. Branch offices, however, are often smaller sites at which no datacenter exists. In fact, many branch offices have no significant IT presence other than a small handful of servers. There may be no physically secure facility to house branch office servers. There may be few, if any, local IT staff to support the servers.

If a DC is not placed in the branch office, authentication and service ticket activities are directed to the hub site over the WAN link. Authentication occurs when a user first logs on to his computer in the morning. *Service tickets* are a component of the Kerberos authentication mechanism used by AD DS domains. You can think of a service ticket as a key issued by the domain controller to a user. The key allows the user to connect to a service such as the file and print services on a file server. When a user first tries to access a specific service, the user's client requests a service ticket from the domain controller. Because users typically connect to multiple services during a workday, service ticket activity happens regularly. Authentication and service ticket activity over the WAN link between a branch office and a hub site can result in slow or unreliable performance.

If a DC is placed in the branch office, authentication is much more efficient but there are several potentially significant risks. A DC maintains a copy of all attributes of all objects in its domain, including secrets such as information related to user passwords. If a DC is accessed or stolen, it becomes possible for a determined expert to identify valid user names and passwords, at which point the entire domain is compromised. At a minimum, you must reset the passwords of every user account in the domain. Because the security of servers at branch offices is often less than ideal, a branch office DC poses a considerable security risk.

A second concern is that changes to the Active Directory database on a branch office DC replicate to the hub site and to all other DCs in the environment. Therefore, corruption to the branch office DC poses a risk to the integrity of the enterprise directory service. For example, if a branch office administrator performs a restore of the DC from an outdated backup, there can be significant repercussions for the entire domain.

The third concern relates to administration. A branch office domain controller might require maintenance—for example, a new device driver. To perform maintenance on a standard domain controller, you must log on as a member of the Administrators group on the domain controller, which means you are effectively an administrator of the domain. It might not be appropriate to grant that level of capability to a support team at a branch office.

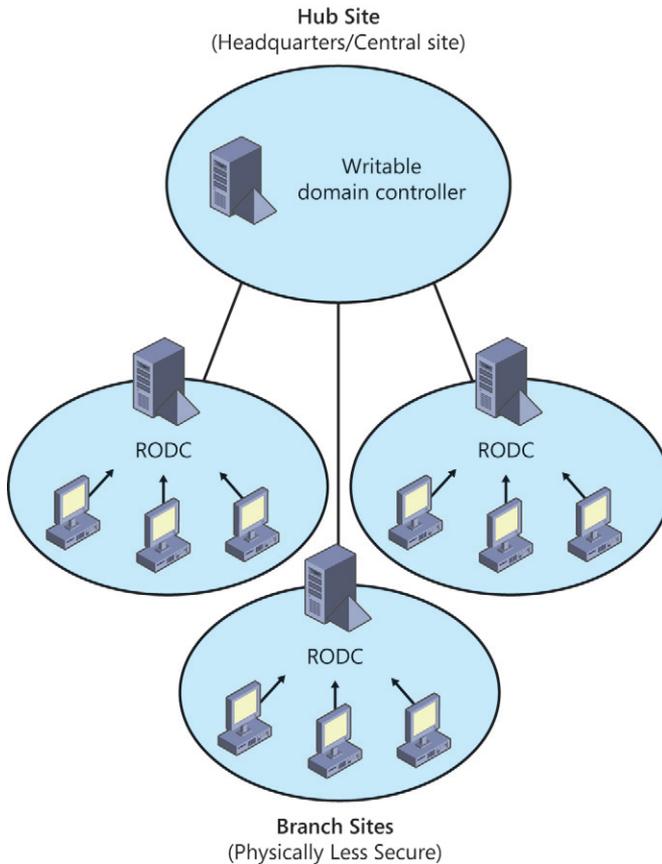
## Read-Only Domain Controllers

These concerns—security, directory service integrity, and administration—left many enterprises with a difficult choice to make, and there was no best practice answer. Windows Server 2008 introduced the RODC, which is designed specifically to address the branch office scenario. An RODC is a domain controller, typically placed in the branch office, that maintains a copy of all objects in the domain and all attributes except for secrets such as password-related properties. When a user in the branch office logs on, the RODC receives the request and forwards it to a domain controller in the hub site for authentication.

You can configure a password replication policy (PRP) for the RODC that specifies user accounts the RODC is allowed to cache. If the user logging on is included in the PRP, the RODC caches that user's credentials, so the next time authentication is requested the RODC can perform the task locally. As users who are included in the PRP log on, the RODC builds its cache of credentials so that it can perform authentication locally for those users. These concepts are illustrated in Figure 8-7.

Because the RODC maintains only a subset of user credentials, if the RODC is compromised or stolen, the effect of the security exposure is limited. Only the user accounts that had been cached on the RODC must have their passwords changed. Writable domain controllers maintain a list of all cached credentials on individual RODCs. When you delete the account of the stolen or compromised RODC from Active Directory, you have the option to reset the passwords of all user accounts that were cached on the RODC. The RODC replicates changes to Active Directory from DCs in the hub site. Replication is one way, from a writable domain controller to the RODC. No changes to the RODC are replicated to any other domain controller. This eliminates the exposure of the directory service to corruption resulting from

changes made to a compromised branch office DC. Finally, RODCs, unlike writable DCs, have some local groups, most notably a local Administrators group. You can give one or more local support personnel the ability to maintain an RODC fully, without granting them the equivalence of domain administrators.



**FIGURE 8-7** A branch office scenario supported by RODCs

## Deploying an RODC

The high-level steps to install an RODC are as follows:

- Ensure that the forest functional level is Windows Server 2003 or higher.
- If the forest has any DCs running Microsoft Windows Server 2003, run ADPrep /RODCPrep.
- Ensure that at least one writable DC is running Windows Server 2008 or Windows Server 2008 R2.
- Install the RODC.

Each of these steps is detailed in the following sections.

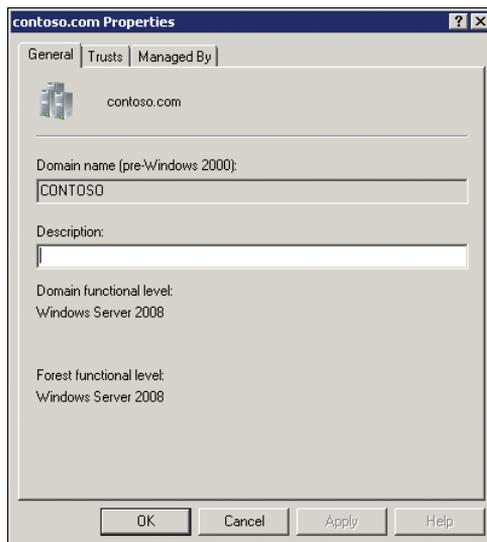
## Verifying and Configuring Forest Functional Level of Windows Server 2003 or Higher

Functional levels enable features unique to specific versions of Windows and are, therefore, dependent on the versions of Windows running on domain controllers. If all domain controllers are Windows Server 2003 or later, the domain functional level can be set to Windows Server 2003. If all domains are at Windows Server 2003 domain functional level, the forest functional level can be set to Windows Server 2003. Domain and forest functional levels are discussed in detail in Chapter 12.

RODCs require that the forest functional level is Windows Server 2003 or higher. That means that all domain controllers in the entire forest are running Windows Server 2003 or later.

To determine the functional level of your forest:

1. Open Active Directory Domains And Trusts.
2. In the console tree, right-click the root node, Active Directory Domains And Trusts [Server Name], and then click Properties..
3. Verify the forest functional level, as shown in Figure 8-8.



**FIGURE 8-8** The forest Properties dialog box

Any user can verify the forest functional level in this way. No special administrative credentials are required to view the forest functional level.

If the forest functional level is not at least Windows Server 2003, examine the properties of each domain to identify any domains for which the domain functional level is not at least Windows Server 2003. If you find such a domain, you must ensure that all domain controllers in the domain are running Windows Server 2003. Then, in Active Directory Domains And Trusts, right-click the domain and choose Raise Domain Functional Level. After

you have raised each domain functional level to at least Windows Server 2003, right-click the root node of the Active Directory Domains And Trusts snap-in and choose Raise Forest Functional Level. In the Select An Available Forest Functional Level drop-down list, choose Windows Server 2003 and click Raise. You must be an administrator of a domain to raise the domain's functional level. To raise the forest functional level, you must be either a member of the Domain Admins group in the forest root domain or a member of the Enterprise Admins group.

## Running ADPrep /RODCPrep

If you are upgrading an existing forest to include domain controllers running Windows Server 2008 or Windows Server 2008 R2, you must run ADPrep /RODCPrep. This command configures permissions so that RODCs can replicate DNS application directory partitions. DNS application directory partitions are discussed in Chapter 9, "Integrating Domain Name System with AD DS." If you are creating a new Active Directory forest that will have only domain controllers running Windows Server 2008 or Windows Server 2008 R2, you do not need to run ADPrep /RODCPrep.

The command is found in the \support\adprep folder of the Windows Server 2008 or Windows Server 2008 R2 installation DVD. Copy the folder to the domain controller acting as the schema master. The schema master role is discussed in Chapter 10, "Administering Domain Controllers." Log on to the schema master as a member of the Enterprise Admins group, open Command Prompt, change directories to the ADPrep folder, and type **adprep /rodcprep**.

Before running ADPrep /RODCPrep, you must run ADPrep /ForestPrep and ADPrep /DomainPrep. See Chapter 10 for more information about preparing a Windows Server 2003 domain and forest for the first Windows Server 2008 or Windows Server 2008 R2 domain controller.

## Placing a Writable Windows Server 2008 or Windows Server 2008 R2 Domain Controller

An RODC must replicate domain updates from a writable domain controller running Windows Server 2008 or Windows Server 2008 R2. It is critical that an RODC can establish a replication connection with a writable Windows Server 2008 or Windows Server 2008 R2 domain controller. Ideally, the writable domain controller should be in the closest site—the hub site. In Chapter 11, "Managing Sites and Active Directory Replication," you learn about Active Directory replication, sites, and site links. If you want the RODC to act as a DNS server, the writable Windows Server 2008 or Windows Server 2008 R2 domain controller must also host the DNS domain zone.

## ✓ Quick Check

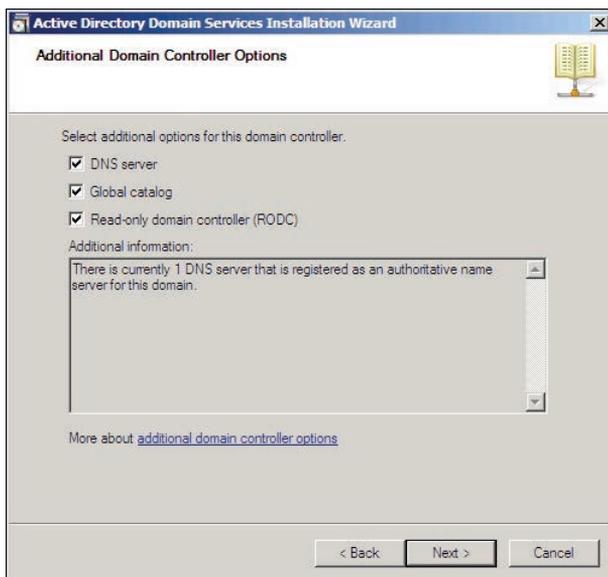
- Your domain consists of a central site and four branch offices. The central site has two domain controllers. Each branch office site has one domain controller. All domain controllers run Windows Server 2003. Your company decides to open a fifth branch office, and you want to configure it with a new Windows Server 2008 R2 RODC. What must you do before introducing the first RODC into your domain?

### Quick Check Answer

- You must first ensure that the forest functional level is Windows Server 2003. Then you must upgrade one of the existing domain controllers to Windows Server 2008 or Windows Server 2008 R2 so that there is one writable Windows Server 2008 domain controller. You must run ADPrep /DomainPrep and ADPrep /ForestPrep to prepare the domain and forest for the first Windows 2008 or Windows Server 2008 R2 domain controller, as you will learn in Chapter 10. You must also run ADPrep /RODCPrep from the Windows Server 2008 R2 installation DVD.

## Installing an RODC

After completing the preparatory steps, you can install an RODC. An RODC can be either a full or Server Core installation of Windows Server 2008 or Windows Server 2008 R2. With a full installation of Windows Server 2008 or Windows Server 2008 R2, you can use the Active Directory Domain Services Installation Wizard to create an RODC. Simply select Read-Only Domain Controller (RODC) on the Additional Domain Controller Options page of the wizard, as shown in Figure 8-9.



**FIGURE 8-9** Creating an RODC with the Active Directory Domain Services Installation Wizard

## **PRACTICE IT**

**Exercise 1, “Install an RODC,” in the practice at the end of this lesson walks you through the use of the Active Directory Domain Services Installation Wizard to create an RODC.**

Alternately, you can use the `dcpromo.exe` command with the `/unattend` switch to create the RODC. On a Server Core installation of Windows Server 2008 or Windows Server 2008 R2, you must use the `DCPromo /unattend` command.

It is also possible to delegate the installation of the RODC, which allows a user who is not a domain administrator to create the RODC by adding a new server in the branch office and running `Dcpromo.exe`. To delegate the installation of an RODC, pre-create the computer account for the RODC in the Domain Controllers OU and specify the credentials that will be used to add the RODC to the domain. That user can then promote a server running Windows Server 2008 or Windows Server 2008 R2 as an RODC, using the pre-staged RODC account. The server must be a member of a workgroup—not of the domain—when creating an RODC by using delegated installation.

## **MORE INFO OPTIONS FOR INSTALLING AN RODC**

For details regarding other options for installing an RODC, including delegated installation, see “Step-by-Step Guide for Read-only Domain Controllers” at <http://technet2.microsoft.com/windowsserver2008/en/library/ea8d253e-0646-490c-93d3-b78c5e1d9db71033.aspx?mfr=true>.

## **Password Replication Policy**

Password Replication Policy (PRP) determines which users’ credentials can be cached on a specific RODC. If PRP allows an RODC to cache a user’s credentials, authentication and service ticket activities of that user can be processed by the RODC. If a user’s credentials cannot be cached on an RODC, authentication and service ticket activities are referred by the RODC to a writable domain controller.

An RODC’s PRP is determined by two multivalued attributes of the RODC’s computer account. These attributes are commonly known as the *Allowed List* and the *Denied List*. If a user’s account is on the Allowed List, the user’s credentials are cached. You can include groups on the Allowed List, in which case all users who belong to the group can have their credentials cached on the RODC. If the user is on both the Allowed List and the Denied List, the user’s credentials will not be cached—the Denied List takes precedence.

## **Configuring Domain-Wide Password Replication Policy**

To facilitate the management of PRP, Windows Server 2008 R2 creates two domain local security groups in the Users container of Active Directory. The first group, Allowed RODC Password Replication Group, is added to the Allowed List of each new RODC. By default, the group has no members. Therefore, by default, a new RODC will not cache any user’s

credentials. If you have users whose credentials you want to be cached by all domain RODCs, add those users to the Allowed RODC Password Replication Group.

The second group is named Denied RODC Password Replication Group. It is added to the Denied List of each new RODC. If you have users whose credentials you want to ensure are never cached by domain RODCs, add those users to the Denied RODC Password Replication Group. By default, this group contains groups for security-sensitive accounts including Domain Admins, Enterprise Admins, and Group Policy Creator Owners.

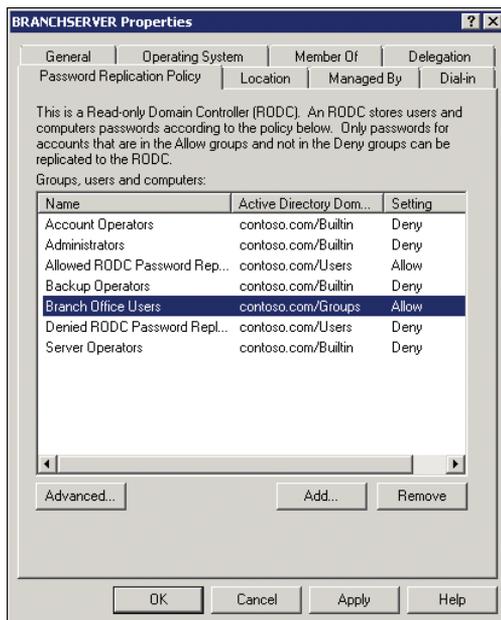
**NOTE COMPUTERS ARE PEOPLE, TOO**

**Remember that it is not only users that generate authentication and service ticket activity. Computers in a branch office also require such activity. To improve performance of systems in a branch office, allow the branch RODC to cache appropriate computer credentials as well.**

## Configuring RODC-Specific Password Replication Policy

The two groups described in the previous section provide a method to manage PRP on all RODCs. However, to best support a branch office scenario, you must allow the RODC in each branch office to cache credentials of users and computers in that specific location. Therefore, you must configure the Allowed List and the Denied List of each RODC.

To configure an RODC's PRP, open the properties of the RODC's computer account in the Domain Controllers OU. On the Password Replication Policy tab, shown in Figure 8-10, you can view the current PRP settings and add or remove users or groups from the PRP.



**FIGURE 8-10** The Password Replication Policy tab of an RODC

## Administering RODC Credentials Caching

When you click the Advanced button on the Password Replication Policy tab shown in Figure 8-10, an Advanced Password Replication Policy dialog box appears. An example is shown in Figure 8-11.

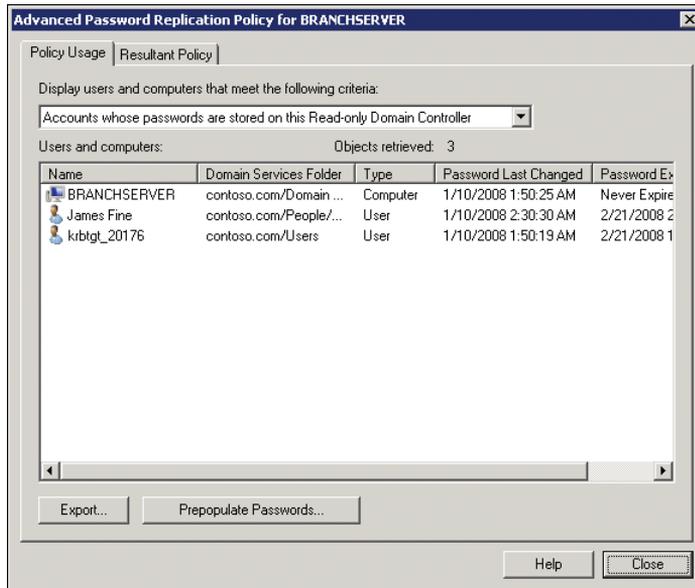


FIGURE 8-11 The Advanced Password Replication Policy dialog box

In the drop-down list at the top of the Policy Usage tab, you can select one of two reports for the RODC:

- **Accounts Whose Passwords Are Stored On This Read-Only Domain Controller** Displays the list of user and computer credentials that are currently cached on the RODC. Use this list to determine whether credentials are being cached that you do not want cached on the RODC. Then modify the PRP accordingly.
- **Accounts That Have Been Authenticated To This Read-Only Domain Controller** Displays the list of user and computer credentials that have been referred to a writable domain controller for authentication or service ticket processing. Use this list to identify users or computers that are attempting to authenticate with the RODC. If any of these accounts are not being cached, consider adding them to the PRP.

In the same dialog box, you can use the Resultant Policy tab to evaluate the effective caching policy for an individual user or computer. Click Add to select a user or computer account for evaluation.

Under normal circumstances, if a user or computer is on the Allowed List of an RODC, the account credentials can be cached on the RODC but will not be cached until the authentication or service ticket events cause the RODC to replicate the credentials from a writable domain controller. However, you can also use the Advanced Password Replication

Policy dialog box to prepopulate user and computer credentials in the RODC cache. This ensures that authentication and service ticket activity will be processed locally by the RODC even when the user or computer is authenticating for the first time. To prepopulate credentials, click Prepopulate Passwords and select the appropriate users and computers.

## Administrative Role Separation

RODCs in branch offices can require maintenance such as an updated device driver. Additionally, small branch offices might combine the RODC role with the file server role on a single system, in which case it is important to be able to back up the system. RODCs support local administration through a feature called *administrative role separation*. Each RODC maintains a local database of groups for specific administrative purposes. You can add domain user accounts to these local roles to enable support of a specific RODC.

You can configure administrative role separation by using the `Dsmgmt.exe` command. To add a user to the Administrators role on an RODC, follow these steps:

1. Open Command Prompt on the RODC.
2. Type **dsmgmt** and press Enter.
3. Type **local roles** and press Enter.

At the Local Roles prompt, you can type **?** and press Enter for a list of commands.

You can also type **list roles** and press Enter for a list of local roles.

4. Type **add *username* administrators**, where *username* is the pre–Windows 2000 logon name of a domain user, and press Enter.

You can repeat this process to add other users to the various local roles on an RODC.

### **MORE INFO** IMPROVING AUTHENTICATION AND SECURITY

RODCs are a valuable new feature for improving authentication and security in branch offices. Be sure to read the detailed documentation at <http://technet2.microsoft.com/windowsserver2008/en/library/ea8d253e-0646-490c-93d3-b78c5e1d9db71033.mspx>.

## **PRACTICE** Configuring Read-Only Domain Controllers

---

In this practice, you implement read-only domain controllers in a simulation of a branch office scenario. You install an RODC, configure password replication policy, monitor credential caching, and prepopulate credentials on the RODC. To perform this practice, you must complete the following preparatory tasks:

- Install a second server running a full installation of Windows Server 2008 R2. Name the server BRANCHSERVER. Do not join the computer to the domain. Set the server's IP configuration as follows:
  - IP Address: 10.0.0.12
  - Subnet Mask: 255.255.255.0

- Default Gateway: 10.0.0.1
- DNS Server: 10.0.0.11 (the address of SERVER01)
- Create the following Active Directory objects:
  - A global security group named Branch Office Users
  - A user named James Fine, who is a member of Branch Office Users
  - A user named Adam Carter, who is a member of Branch Office Users
  - A user named Mike Danseglio, who is *not* a member of Branch Office Users

In this and other practices in this training kit, you will log on to the domain controller with user accounts that are not a member of Domain Administrators or the domain's Administrators group. Therefore, you must give all user accounts the right to log on locally to the domain controllers in your practice environment. Follow the steps in the article, "Grant a Member the Right to Logon Locally," at [http://technet.microsoft.com/en-us/library/ee957044\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee957044(WS.10).aspx) to grant the Allow Logon Locally right to the Administrators and Domain Users groups. If you will use Remote Desktop Services to connect to the domain controller—rather than logging on locally—grant the Allow Logon Through Remote Desktop Services right. Reboot the server or otherwise refresh Group Policy. This is for the practice environment only. In a production environment, you should not grant users the right to log on to domain controllers.

### EXERCISE 1 Install an RODC

In this exercise, you configure the BRANCHSERVER server as an RODC in the contoso.com domain.

1. Log on to BRANCHSERVER as Administrator.
2. Click Start, and then click Run.
3. Type **dcpromo** and click OK.

A window appears, informing you that the Active Directory Domain Services binaries are being installed. When installation is complete, the Active Directory Domain Services Installation Wizard appears.

4. On the first page of the wizard, click Next.
5. On the Operating System Compatibility page, click Next.
6. On the Choose A Deployment Configuration page, click Existing Forest, and then click Add A Domain Controller To An Existing Domain. Click Next.
7. On the Network Credentials page, type **contoso.com**.
8. Click Set.
9. In the User Name box, type **CONTOSO\Administrator**.
10. In the Password box, type the password for the domain's Administrator account. Click OK, and then click Next.
11. On the Select A Domain page, select contoso.com and click Next.

12. On the Select A Site page, select Default-First-Site-Name and click Next.  
In a production environment, you would select the site for the branch office in which the RODC is being installed. Sites are discussed in Chapter 11.
13. On the Additional Domain Controller Options page, select Read-Only Domain Controller (RODC). Also ensure that DNS Server and Global Catalog are selected. Then click Next.
14. On the Delegation Of RODC Installation And Administration page, click Next.
15. On the Location For Database, Log Files, And SYSVOL page, click Next.
16. On the Directory Services Restore Mode Administrator Password page, type a password in the Password and Confirm Password boxes, and then click Next.
17. On the Summary page, click Next.
18. In the progress window, select the Reboot On Completion check box.

### **EXERCISE 2 Configure Password Replication Policy**

In this exercise, you configure PRP at the domain level and for an individual RODC. PRP determines whether the credentials of a user or computer are cached on an RODC.

1. Log on to SERVER01 as Administrator.
2. Open the Active Directory Users And Computers snap-in, expand the domain, and select the Users container.
3. Examine the default membership of the Allowed RODC Password Replication Group.
4. Open the properties of the Denied RODC Password Replication Group.
5. Add the DNSAdmins group as a member of the Denied RODC Password Replication Group. Click OK to close the group Properties dialog box.
6. Select the Domain Controllers OU.
7. Open the properties of BRANCHSERVER.
8. On the Password Replication Policy tab, identify the PRP settings for the two groups: Allowed RODC Password Replication Group and Denied RODC Password Replication Group.
9. Click Add.
10. Select Allow Passwords For The Account To Replicate To This RODC and click OK.
11. In the Select Users, Computers, Or Groups dialog box, type **Branch Office Users** and click OK, and then click OK again.

### **EXERCISE 3 Monitor Credential Caching**

In this exercise, you simulate the logon of several users to the branch office server and evaluate the credentials caching of the server.

1. Log on to BRANCHSERVER as James Fine, and then log off.
2. Log on to BRANCHSERVER as Mike Danseglio, and then log off.

3. Log on to SERVER01 as Administrator and open the Active Directory Users And Computers snap-in.
4. Open the properties of BRANCHSERVER in the Domain Controllers OU.
5. On the Password Replication Policy tab, click Advanced.
6. On the Policy Usage tab, in the Display Users And Computers That Meet The Following Criteria drop-down list, select Accounts Whose Passwords Are Stored On This Read-Only Domain Controller.
7. Locate the entry for James Fine.  
Because you had configured the PRP to allow caching of credentials for users in the Branch Office Users group, James Fine's credentials were cached when he logged on in step 1. Mike Danseglio's credentials are not cached.
8. In the drop-down list, select Accounts That Have Been Authenticated To This Read-Only Domain Controller.
9. Locate the entries for James Fine and Mike Danseglio.
10. Click Close, and then click OK.

#### **EXERCISE 4** Prepopulate Credentials Caching

In this exercise, you prepopulate the cache of the RODC with the credentials of a user.

1. Log on to SERVER01 as Administrator and open the Active Directory Users And Computers snap-in.
2. Open the properties of BRANCHSERVER in the Domain Controllers OU.
3. On the Password Replication Policy tab, click Advanced.
4. Click Prepopulate Passwords.
5. Type **Adam Carter** and click OK.
6. Click Yes to confirm that you want to send the credentials to the RODC. A dialog box informs you that the action was successful. Click OK.
7. On the Policy Usage tab, select Accounts Whose Passwords Are Stored On This Read-Only Domain Controller.
8. Locate the entry for Adam Carter.  
Adam's credentials are now cached on the RODC.
9. Click Close, and then click OK.

## Lesson Summary

- RODCs contain a read-only copy of the Active Directory database.
- An RODC replicates updates to the domain from a writable domain controller using inbound-only replication.

- Password replication policy defines whether the credentials of the user or computer are cached on an RODC. The Allowed RODC Password Replication Group and Denied RODC Password Replication Group are in the Allowed List and Denied List, respectively, in each new RODC. You can, therefore, use the two groups to manage a domain-wide password replication policy. You can further configure the individual PRP of each domain controller.
- An RODC can be supported by configuring administrator role separation to allow one or more users to perform administrative tasks without granting those users permissions to other domain controllers or to the domain. The DSMgmt command implements administrator role separation.
- An RODC requires a Windows Server 2008 or Windows Server 2008 R2 writable domain controller in the same domain. Additionally, the forest functional level must be at least Windows Server 2003, and the ADPrep /RODCPrep command must be run prior to installing the first RODC.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 3, “Configuring Read-Only Domain Controllers.” The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE ANSWERS**

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

1. Your domain consists of five domain controllers, one of which is running Windows Server 2008 R2. All other DCs are running Windows Server 2003. What must you do before installing a read-only domain controller?
  - A. Upgrade all domain controllers to Windows Server 2008.
  - B. Run ADPrep /RODCPrep.
  - C. Run DSMgmt.
  - D. Run DCPromo /unattend.
2. During a recent burglary at a branch office of Tailspin Toys, the branch office RODC was stolen. Where can you find out which users’ credentials were stored on the RODC?
  - A. The Policy Usage tab
  - B. The membership of the Allowed RODC Password Replication Group
  - C. The membership of the Denied RODC Password Replication Group
  - D. The Resultant Policy tab
3. Next week, five users are relocating to 1 of the 10 overseas branch offices of Litware, Inc. Each branch office contains an RODC. You want to ensure that when the users

log on for the first time in the branch office, they do not experience problems authenticating over the WAN link to the data center. Which steps should you perform? (Choose all that apply. Each correct answer is part of the solution.)

- A.** Add the five users to the Allowed RODC Password Replication Group.
- B.** Add the five users to the Password Replication Policy tab of the branch office RODC.
- C.** Add the five users to the Log On Locally security policy of the Default Domain Controllers Policy GPO.
- D.** Click Prepopulate Passwords.

## Lesson 4: Managing Service Accounts

---

Services, like users, must log on. A service is configured with a user name and password of an account with which it logs on. The rights, permissions, and privileges assigned to the account allow the service to access the resources it requires. Because service account credentials are registered in the Service Control Manager (SCM) of a machine on which a service runs, managing and securing service accounts often requires that you make changes not only to Active Directory, but to the SCM of one or more machines as well.

In Lesson 1, you learned to use fine-grained password policies to configure password requirements for service accounts. Windows Server 2008 R2 introduces a new feature, *managed service accounts*, which reduces the burden of password management for service accounts.

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

- Configure managed accounts.

**Estimated lesson time: 30 minutes**

### Understanding Managed Accounts

Services require access to resources, so they need rights, permissions, and privileges—at a minimum, the right to log on to a system. To be assigned access, a service must have an account—an identity with a user name and password—with which a system can authenticate the service when the service starts. The service is assigned the account in the SCM, which you manage by using the Services console in the Administrative Tools folder or one of several other tools, including the Sc.exe command and Windows PowerShell.

When a service runs on a single computer, an administrator can configure the service to run as Local Service, Network Service, or Local System. These three accounts are built in to Windows. They are simple to configure and use, but they are typically shared among multiple services and cannot be managed on a domain level.

You can centralize the management of service accounts by creating a domain account. After you create a domain account for a service, you can assign the account to the service on more than one system. For example, an enterprise backup service can be configured to run on multiple servers under a single domain account. You can create a unique account for each service to isolate the privileges for the services.

However, when you need to change the password of a domain service account, you must update the SCM on each computer on which the service is assigned the account. This management burden has led too many organizations to configure service accounts with non-expiring passwords, which is certainly not a security best practice. Other organizations have built or acquired custom scripts or tools to manage service account passwords in the enterprise.

Windows Server 2008 R2 reduces the management burden of service accounts with a new object class—the *managed service account*. The managed service account is a domain account that is associated with a service on a single computer, and one or more services on that computer can use the managed service account as a logon identity. The computer automatically changes the password of each managed service account on the computer, every 30 days by default.

Another burden associated with service accounts is the management of service principal names (SPNs). SPNs are a critical component of Kerberos authentication. Managed service accounts ensure that if the name of a computer is changed, SPNs associated with services running on the computer are changed in the domain. In addition, SPN management can be delegated to other administrators.

## Requirements for Managed Service Accounts

Managed service accounts require minimal changes to your domain. You must prepare your schema for managed service accounts. Run **adprep /forestprep** at the forest level, and then run **adprep /domainprep** in each domain where you want to use managed service accounts. For more information about ADPrep, see Chapter 10 and visit [http://technet.microsoft.com/en-us/library/cc731728\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731728(WS.10).aspx).

You use Windows PowerShell to administer managed service accounts. Therefore, at least one domain controller must support administration of Active Directory with Windows PowerShell by running one of the following:

- Windows Server 2008 R2
- Windows Server 2008 with the Active Directory Management Gateway Service
- Windows Server 2003 R2 with the Active Directory Management Gateway Service
- Windows Server 2003 with the Active Directory Management Gateway Service

Other domain controllers can be running Windows Server 2003 or later. If the domain functional level is Windows Server 2008 R2, you can take advantage of automatic password management of managed service accounts and simplified SPN management. If the domain functional level is lower than Windows Server 2008 R2, automatic password management of managed service accounts is available, but SPNs must be managed manually.

To create and configure managed accounts in Active Directory, you must use Windows PowerShell on a computer running Windows 7 or Windows Server 2008 R2. In other words, your administrative workstation must be running Windows 7 or Windows Server 2008 R2. You must ensure that the Active Directory Module For Windows PowerShell is installed on the computer. You can install the feature by using the Add Features link in Server Manager if the computer is running Windows Server 2008 R2, or the Turn Windows Features On Or Off link in Control Panel if the computer is running Windows 7. In Remote Server Administration Tools, Role Administration Tools, AD DS And AD LDS Tools group, you will find the Active Directory Module For Windows PowerShell feature.

Finally, each computer that uses a managed account—any computer on which services are associated with managed accounts—must be running Windows Server 2008 R2 or Windows 7 and must have the Active Directory Module For Windows PowerShell installed. Earlier versions of Windows cannot assign a managed account to a service.

## Creating and Configuring a Managed Service Account

To create and configure managed service accounts in the domain, you use Windows PowerShell cmdlets. There is no UI support for correctly creating and configuring managed service accounts. The *New-ADServiceAccount* cmdlet creates a managed service account.

The following example creates a managed service account:

```
New-ADServiceAccount SRV_APP01 -Enabled $true -Path "CN=Managed Service Accounts,
DC=contoso,DC=com"
```

The *-Path* parameter specifies the Managed Service Accounts container—a new container in Active Directory. You can specify a custom container or OU. You can also use the *-ServicePrincipalNames* parameter to specify SPNs for the account.

The *sAMAccountName* attribute of the managed service account is the name specified by the *New-ADServiceAccount* cmdlet, followed by a dollar sign (\$). For example, the *sAMAccountName* of the managed service account created in the preceding example is *SRV\_APP01\$*.

### **NOTE USE AN ACCOUNT NAME OF FEWER THAN 15 CHARACTERS**

**When you create a managed service account, specify a short account name of fewer than 15 characters. The dollar sign suffix will lengthen the name; the resulting *sAMAccountName* must be 15 characters or less. Although you can create a managed service account with a longer name in Active Directory, you will be unable to install or use the managed account on a computer.**

To configure properties of the account, you can use the *Set-ADServiceAccount* cmdlet or the Attribute Editor tab of the Active Directory Users And Computers snap-in. The *Get-ADServiceAccount* cmdlet returns an object reference to a managed service account. To delete a managed service account, use the *Remove-ADServiceAccount* cmdlet.

## Installing and Using a Managed Service Account

The *Install-ADServiceAccount* cmdlet installs the managed service account on a computer so that you can assign the account to one or more services on the computer. For example, the following command installs the managed service account named *SRV\_APP01* on the local computer:

```
Install-ADServiceAccount -Identity SRV_APP01
```

After you have installed the managed service account, you can configure a service to use the account as its logon identity. In the Services console, open the properties of a service and click the Log On tab. Select This Account, then click Browse. Type the name of the managed service account, and then click OK. On the Log On tab, confirm that the name appears with a dollar sign (\$). The account will be given the Log On As Service right (*SeServiceLogonRight*).

If you move a service to another computer and you want to use the same managed service account on the target system, you must first use the *Uninstall-ADServiceAccount* cmdlet to remove the managed service account from the current computer. Then repeat the same procedures described in the previous example on the target computer: Use the *Install-ADServiceAccount* cmdlet and then configure the service to use the managed service account.

You must be a local administrator on the computer to install a managed service account and configure the logon identity of a service. You must also have rights to modify the managed service account in Active Directory to install or uninstall a managed service account on a computer.

## Managing Delegation and Passwords

You can delegate permissions to configure a managed service account in Active Directory. There is no cmdlet in Windows PowerShell to do so. You must use the DSACLs command, which was introduced in Chapter 2, “Administering Active Directory Domain Services.” The following command delegates to the user named *ServiceAdmin* the permissions needed to manage a service account named *SRV\_APP01*.

```
dsacIs "CN=SRV_APP01,CN=Managed Service Accounts,DC=contoso,DC=com"
 /G "CONTOSO\ServiceAdmin:SDRCLCRPLOCA" "CONTOSO\ServiceAdmin:WP;Logon Information"
 "CONTOSO\ServiceAdmin:WP;Description" "CONTOSO\ServiceAdmin:WP;DisplayName"
 "CONTOSO\ServiceAdmin:WP;Account Restrictions"
 "CONTOSO\ServiceAdmin:WS;Validated write to DNS host name"
 "CONTOSO\ServiceAdmin:WS;Validated write to service principal name"
```

A managed service account is a unique object class, *msDS-ManagedServiceAccount*, that inherits from the *computer* object class. Managed service accounts, like computers, do not observe domain or fine-grained password policies. Instead, like computers, a managed service account establishes a complex, cryptographically random, 240-character password and changes that password when the computer changes its password—every 30 days by default. A managed service account cannot be locked out and cannot perform interactive logons.

Under normal circumstances, you will not need to worry about changing the password of a managed service account; however, there may be scenarios in which you want to force a reset of the password. You can use the *Reset-ADServiceAccountPassword* cmdlet to do so.

## **MORE INFO** MANAGED SERVICE ACCOUNTS

The following articles provide additional details regarding managed service accounts: “Managed Service Accounts Frequently Asked Questions (FAQ)” at [http://technet.microsoft.com/en-us/library/ff641729\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff641729(WS.10).aspx), and “Service Accounts Step-by-Step Guide” at [http://technet.microsoft.com/en-us/library/dd548356\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd548356(WS.10).aspx).

## Limitations of Managed Service Accounts

Managed service accounts are an important new feature of Windows Server 2008 R2, but here are some important restrictions and caveats related to their use:

- A component must support managed service accounts. Generally speaking, services that you add to a computer, and that are listed in the Services console, can be configured to use a managed service account, as can IIS application pools. You cannot use managed service accounts for identities of applications or non-Windows services. Furthermore, a component must support managed service accounts, and not all services do. For example, Microsoft SQL Server does not support managed service accounts, despite vague and contradictory information in some online resources including Microsoft TechNet. This notable exception is true for versions of SQL Server up to SQL Server 2008 R2. This limitation might be removed in future versions of SQL Server.
- Each managed service account can be used on only one computer. Services on multiple computers cannot use a single managed service account. Therefore, you cannot use managed service accounts for load balanced and clustered services. For example, you should not use managed service accounts as identities for Microsoft SharePoint Server, because a SharePoint farm can be more than one computer. Similarly, a managed service account cannot be used for a service in a cluster, because a cluster contains more than one computer.
- A computer can have more than one managed service account. For example, if you have five services running on a computer, those five services can share a single managed service account or can use five separate managed service accounts.

## **PRACTICE** Managing Service Accounts

---

In this practice, you create a managed service account for an IIS application pool.

### **EXERCISE 1** Add the Internet Information Services Role

In this exercise, you add the Internet Information Services (IIS) role and verify that the default website is created.

1. Log on to SERVER01 as Administrator.
2. Open Server Manager.

3. In the Roles Summary section, click Add Roles.  
You might need to scroll down to see the Roles Summary section.
4. In the Add Roles Wizard, on the Before You Begin page, click Next.
5. On the Select Server Roles page, select the Web Server (IIS) check box, and then click Next.
6. On the Web Server (IIS) page, click Next.
7. On the Select Role Services page, click Next.
8. On the Confirm Installation Selections page, click Install.  
The Web Server (IIS) role and its default services are installed.
9. On the Installation Results page, click Close.
10. Open Internet Explorer.  
If the Set Up Windows Internet Explorer 8 dialog box opens, click Next. On the Turn On Suggested Sites page, click No, Don't Turn On, and then click Next. On the Choose Your Settings page, click Use Express Settings, and then click Finish.
11. Browse to <http://server01.contoso.com>.  
The IIS7 page opens. This is the default page of the default web application that is created when you install IIS. Leave Internet Explorer running.

## EXERCISE 2 Create a Managed Service Account

In this exercise, you create a managed service account.

1. Open the Active Directory Users And Computers snap-in. Click the View menu and ensure that the Advanced Features option is selected.
2. Expand `contoso.com` and click the Managed Service Accounts OU. Note that the OU is currently empty.
3. Open Active Directory Module For Windows PowerShell from the Administrative Tools program group.
4. Type the following command:

```
New-ADServiceAccount SRV_APP01 -Enabled $true -Path "CN=Managed Service Accounts, DC=contoso,DC=com"
```

5. Type the following command:
6. Type the following command:

```
Get-ADServiceAccount -Identity SRV_APP01
```

```
Set-ADServiceAccount -Identity SRV_APP01 -Description "Application Pool 01 on SERVER01"
```

Question: What is the value of the `sAMAccountName` attribute for this account?

Answer: `SRV_APP01$`

7. Switch to Active Directory Users And Computers.
8. Click the Managed Service Accounts container and confirm that the SRV\_APP01 account exists.

You might have to refresh the view.

Question: What is displayed in the Type column for the account?

Answer: msDS-ManagedServiceAccount

9. Right-click SRV\_APP01 and choose Properties.
10. Observe the limited number of tabs in the Properties dialog box, and then close it.

### EXERCISE 3 Configure a Service to Use a Managed Service Account

In this exercise, you configure the default application pool of IIS to use the managed service account.

1. Switch to Active Directory Module For Windows PowerShell.
2. Type the following command:

```
Install-ADServiceAccount -Identity SRV_APP01
```

3. Switch to Server Manager.
4. In the console tree, expand Roles, expand Web Server (IIS), and then click Internet Information Services (IIS) Manager.
5. In the Connections panel, expand SERVER01, and then click Application Pools.
6. In the Application Pools panel, right-click DefaultAppPool and choose Advanced Settings.
7. In the Advanced Settings dialog box, in the Process Model section, click Identity, and then click the browse button.

The browse button is the button that appears next to the current identity. The button's label is an ellipsis (...).

8. In the Application Pool Identity dialog box, select Custom Account.
9. Click Set.
10. In the Set Credentials dialog box, type **CONTOSO\SRV\_APP01\$**.
11. Leave the Password and Confirm Password boxes blank.
12. Click OK to close each of the three open dialog boxes.
13. Right-click DefaultAppPool and choose Stop.
14. Switch to Internet Explorer and refresh the page, or browse back to *http://server01.contoso.com*.

The Service Unavailable page appears. IIS cannot serve the page to the browser, because the application pool that hosts the web server process for the site is stopped.

15. Switch to Server Manager.
16. Right-click DefaultAppPool and choose Start.

17. Switch to Internet Explorer and refresh the page.  
The default IIS 7 page appears.
18. Open Task Manager.
19. On the Processes tab, click the User Name column to sort by the identity used by each process.
20. Locate the process that is running with the SRV\_APP01\$ identity.  
W3WP.exe is the worker process thread that is supporting the IIS site.

## Lesson Summary

- You can create a managed service account in Active Directory, install the account on a computer, and then configure a service running on the computer to use the managed service account as the logon identity for the service.
- You use Windows PowerShell to create, install, and configure managed service accounts.
- A computer automatically changes the password of managed service accounts installed on the computer.
- If the domain functional level is Windows Server 2008 R2, SPNs associated with the managed service account are automatically changed if the name of the computer is changed.

## Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 4, "Managing Service Accounts." The questions are also available on the companion CD if you prefer to review them in electronic form.

### **NOTE ANSWERS**

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

1. You have been asked to create a new managed account and configure a service on SERVER02 to use the account. What tools must you use? (Choose all that apply. Each correct answer is part of the solution.)
  - A. Active Directory Users And Computers
  - B. Windows PowerShell
  - C. Regedit
  - D. Services.msc

2. You have been asked to create the first managed account in your domain and configure a service on SERVER02 to use the account. SERVER02 is a member server running Windows Server 2003. The domain has a mix of Windows Server 2003 and Windows Server 2008 domain controllers. Which of the following statements are true? (Choose all that apply.)
- A. You must upgrade SERVER02 to Windows Server 2008 R2.
  - B. You must raise the domain functional level to Windows Server 2008 R2.
  - C. You must upgrade the forest functional level to Windows Server 2008 R2.
  - D. You must run `adprep /forestprep`.
  - E. You must run `adprep /domainprep`.

## Chapter Review

---

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

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

## Chapter Summary

---

- Windows Server 2008 R2 allows you to specify password and account lockout settings for the entire domain by modifying the Default Domain Policy GPO. You can then use fine-grained password and lockout policies contained in password settings objects (PSOs) to configure specific policies for groups or individual users.
- When a domain user logs on to a computer in a domain, the computer generates a logon event, and the domain generates an account logon event. These events can be audited to monitor authentication activity. By default, Windows Server 2008 R2 audits successful account logon and logon events.
- Read-only domain controllers (RODCs) provide valuable support for branch office scenarios by authenticating users in the branch office. RODCs reduce the security risk associated with placing a domain controller in a less secure site. You can configure which credentials an RODC will cache. You can also delegate administration of the RODC without granting permissions to other domain controllers or to the domain.
- A managed service account can be used as the logon identity for a service running on a computer. The computer automatically changes the password of the managed service account.

## Key Terms

---

Use these key terms to understand better the concepts covered in this chapter.

- managed service account
- password replication policy (PRP)
- password settings object (PSO)
- read-only domain controller (RODC)
- resultant PSO

## Case Scenarios

---

In the following case scenarios, you apply what you've learned about fine-grained password policies and RODCs. You can find answers to these questions in the "Answers" section at the end of this book.

### Case Scenario 1: Increasing the Security of Administrative Accounts

You are an administrator at Contoso, Ltd., which recently won a contract to deliver an important and secret new product. The contract requires that you increase the security of your Active Directory domain. You must ensure that accounts used by domain administrators are at least 25 characters long and are changed every 30 days. You believe it would not be reasonable to enforce such strict requirements on all users, so you wish to limit the scope of the new password requirements to only domain administrators. Additionally, your contract requires that you monitor attempts by potential intruders to gain access to the network by using an administrative account.

1. Your domain currently contains four Windows Server 2003 domain controllers and eight Windows Server 2008 domain controllers. What must you do before you can implement fine-grained password policies that meet the requirements of the new contract?
2. Which tool do you use to configure fine-grained password and lockout policies?
3. You return from a vacation and discover that other administrators have created several new PSOs with precedence values ranging from 10 through 50. You want to ensure that the PSO you created for domain administrators has the highest precedence so that it always takes effect for those users. What value should you assign to the precedence of your PSO?
4. How should you configure the domain to monitor attempts by potential intruders to gain access to the network by using an administrative account? Which GPO should you modify? Which settings should you define?

### Case Scenario 2: Increasing the Security and Reliability of Branch Office Authentication

You are an administrator at Contoso, Ltd. You maintain the domain's directory service on four domain controllers at a data center in your main site. The domain controllers run Windows Server 2003. Contoso has decided to open a new office overseas. Initially, the office will have 10 salespeople. You are concerned about the speed, expense, and reliability of the connection from the branch office to the data center, so you decide to place a read-only domain controller in the branch office.

1. What must you do to your existing domain controllers and to functional levels before you can install an RODC?

2. Because of customs regulations, you decide to ask one of the employees in the branch office to purchase a server locally. Can you allow the employee to create an RODC without giving the user domain administrative credentials?
3. You want the same user to be able to log on to the RODC to perform regular maintenance. Which command should you use to configure administrator role separation?

## Suggested Practices

---

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

### Configure Multiple Password Settings Objects

In this practice, you experience the effects of PSO precedence by creating several PSOs that apply to a single user and evaluating the resultant PSO for that user.

To perform this practice, create the following objects in the contoso.com domain:

- A global security group named **Human Resources**
- A global security group named **Secure Users**
- A user account named **James Fine** that is a member of both the Human Resources and Secure Users groups
- **Practice 1** Create a PSO named **PSO1** that is linked to the Human Resources group. Give *PSO1* a precedence value of *10*. You can use any valid settings for the other attributes of the PSO. Create a second PSO named **PSO2** and give it a precedence value of *5*. You can use any valid settings for the other attributes of the PSO. Use the steps in Exercise 2, “Create a Password Settings Object,” of Lesson 1 as a reference if necessary.
- **Practice 2** Identify the PSO that affects James Fine. Use the steps in Exercise 3, “Identify the Resultant PSO for a User,” of Lesson 1 as a guide to evaluating resultant PSOs. Which PSO applies to James Fine?
- **Practice 3** Create a PSO named **PSO3** that is linked to James Fine’s user account. Give *PSO3* a precedence value of *20*. You can use any valid settings for the other attributes of the PSO. Use the steps in Exercise 2 of Lesson 1 as a reference if needed. Use the steps in Exercise 3 of Lesson 1 as a guide to evaluating resultant PSO. Identify the PSO that affects James Fine.

### Recover from a Stolen Read-Only Domain Controller

In this practice, you learn how to recover if an RODC is stolen or compromised, by simulating the loss of the server named BRANCHSERVER. To perform this practice, you must have completed the practice in Lesson 3, “Configuring Read-Only Domain Controllers.”

When an RODC is stolen or compromised, any user credentials that had been cached on the RODC should be considered suspect and should be reset. Therefore, you must identify the credentials that had been cached on the RODC and reset the passwords of each account.

- **Practice 1** Determine the user and computer accounts that had been cached on BRANCHSERVER by examining the Policy Usage tab of the BRANCHSERVER Advanced Password Replication Policy dialog box. Use the steps in Exercise 3, “Monitor Credential Caching,” of Lesson 3 if you require reminders for how to identify accounts whose passwords were stored on the RODC. Export the list to a file on your desktop.
- **Practice 2** Open the Active Directory Users And Computers snap-in and, in the Domain Controllers OU, select BRANCHSERVER. Press Delete and click Yes. Examine the options you have for automatically resetting user and computer passwords.

## Take a Practice Test

---

The practice tests on this book’s companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-640 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

### **MORE INFO PRACTICE TESTS**

**For details about all the practice test options available, see the “How to Use the Practice Tests” section in this book’s Introduction.**



# Index

## Symbols and Numbers

- \$error, PowerShell variables, 109
- \$false, PowerShell variables, 109
- \$true, PowerShell variables, 109
- %SystemRoot%, 219
- %WinDir%, 219
- .adm files, 268
- .adml files, 268–69
- .admx files, 268–69
- .csv files (comma-separated value text file)
  - exporting users, 92–93
  - importing computers with CSVDE, 225–26
  - importing groups, CSVDE, 176–77
  - importing user files, CSVDE, 93
  - importing users, PowerShell, 116–17
- .inf files, 333–34
- .ldf extension, 177
- .mcs files, 43
- .msi files, 353–54
- .msp (patch) files, 353–54
- .mst (transform) files, 353–54
- .NET objects, defined, 108
- .txt files, CSVDE importing user files, 93
- .zap files, 354
- \_tcp, Service Locator records, 566–68

## A

- access control. *See also* Active Directory Federation Services (AD FS); also authentication; also domain controllers; also groups
  - access control entries (ACEs), 72–73
  - Active Directory objects, 75–76
  - AD RMS, 865–68
  - AD RMS SCP, 852
  - file and folder access, auditing, 370–73
  - Group Policy Objects (GPOs), 259, 285–86
  - IDA infrastructure, 4–5
  - permissions, managing, 79

- Prevent Access To Registry Editing Tools, 251–52
- user access, resources, 640–44
- access control lists (ACLs)
  - default groups, 195–96
  - groups, accidental deletion, 188–89
  - migration and, 624–25
  - offline domain joins, 218
  - overview, 3
  - viewing, Active Directory Objects, 73–74
- Access database
  - exporting user files, CSVDE, 92–93
  - importing users from, CSVDE, 93–94
  - importing users, PowerShell, 116–17
- access-based enumeration (ABE), 610
- Account Expires, 135
- account federation server, defined, 889
- account flags, User Properties dialog box, 126
- Account Is Disabled, 135
- Account Is Trusted For Delegation, 135
- Account Lockout Duration, 394
- Account Lockout Threshold, 394
- account lockout, domain-based GPOs, 258
- account metadata, domain joins, 219
- Account Operators group, 194–96, 210
- account partner organization, defined, 889
- Account tab, User Properties dialog box, 126
- AccountPassword parameter, New-ADUser, 116
- AccountPassword parameter, Set-ADUser, 137
- ACLing, 625
- Account Policies, security templates, 333
- Action menu, MMC, 37–38
- Action pane, MMC, 37
- actions, Microsoft Management Console (MMC), 37–38
- Active Directory
  - administration tools, 39
  - auditing service changes, 374–75
  - infrastructure components, 9–11
  - master time source, 531–32
  - snap-ins
    - adding tools to Start menu, 40
    - creating custom MMC console, 40–41

## Active Directory Administrative Center (ADAC)

- Active Directory, *continued*
  - custom MMC, saving and distributing, 42–43
  - Microsoft Management Console, using, 37–39
  - overview, 37
  - tools with alternate credentials, 41–42
- Active Directory Administrative Center (ADAC), 102–03, 117–20
- Active Directory Application Mode (ADAM), 6.  
*See also* Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Certificate Services (AD CS)
  - backup, 681
  - best practices, deployment, 785–86
  - case scenario, managing certificate revocation, 829–30
  - common events, 815–16
  - configuring
    - Enterprise PKI, 815–17
    - issuing certificate authority, 804–10
    - management tools, AD CS, 814–16
    - online responder, 810–14
    - overview, 804
    - protecting the configuration, 818
    - revocation configuration, creating, 805–06
    - templates, 806–10
  - enrollment across forests, 789
  - hierarchy, creating, 782–85
  - IDA infrastructure, 6–7
  - installing, 791–93
  - new features, 788–90
  - overview, 771–77
  - planning requirements, 786–87
  - practice installing a CA hierarchy, 793–801
  - practice, configuring and using, 819–26
  - stand-alone vs. enterprise CAs, 780–82
  - understanding, 778–80
- Active Directory Diagnostic data collector, 714
- Active Directory Domain Service Installation Wizard
  - child domain, installing, 516
  - DNS namespace creation, 462–63
  - domain controller, installing, 509–11
  - installing, new forest, 512
  - new domain tree, installing, 517
- Active Directory Domain Services (AD DS). *See also* site management
  - administration
    - Active Directory tools, 39
    - categories, 660–62
    - Microsoft Management Console, using, 37–39
    - MMC custom console, creating, 40–41
    - MMC custom console, saving and distributing, 42–43
    - overview, 35–36
    - snap-ins, overview, 37
  - Start menu, adding tools, 40
  - tools with alternate credentials, 41–42
  - tools, overview, 664–67
- administrative task delegation, practice, 81–82
- authentication
  - account lockout policies, overview, 394
  - audit policies, configuring, 405–06
  - auditing account logons and events, 404
  - auditing, overview, 404
  - domain password, lockout policies, 395
  - fine-grained passwords, lockout policy, 395–97
  - logon events, viewing, 407
  - overview, 389–91
  - password policies, overview, 392–94
  - password settings object (PSO), 397
  - practice, auditing, 407–08
  - practice, password lockout policies, 399–402
  - PSO precedence and resultant PSO, 398
  - PSOs and organizational units, 398–99
  - scoping audit policies, 406
- case scenario
  - creating Active Directory forest, 33
  - organizational units, 84–85
- computer objects, 55–56
- custom MMC, practice, creating and managing, 44–47
- database, backup, 681
- delegation and security, Active Directory objects
  - ACLs, viewing, 73–74
  - administrative task delegation, 77–78
  - effective permissions, 79–80
  - organizational unit design for, 80–81
  - overview, 72
  - permissions and access rights, 75–76
  - permissions and inheritance, 76–77
  - permissions, removing or resetting, 78–79
  - permissions, reporting and viewing, 78
  - understanding delegation, 72–73
- DNS integration
  - DNS name resolution, 452–59
  - DNS structures, 448–49
  - new features, 459–61, 463–67
  - overview, 439–44, 461–63
  - Peer Name Resolution Protocol (PNRP), 446–47
  - split-brain syndrome, 449–51
- finding objects, overview, 57–62
- group objects, creating, 53–55
- IDA infrastructure, 6
- installing
  - Active Directory identity and access, 3–8
  - domain controller, creating, 13
  - forests, preparation for, 12
  - from media, 520–21

- overview, 1–3
- practice, creating forests, 14–21
- practice, installing DNS service, 468–77
- practice, Server Core domain controller installation, 27–30
- Server Core, adding AD DS, 27
- Server Core, configuration, 26–27
- Server Core, initial configuration tasks, 25–26
- Server Core, installation procedure, 24–25
- Server Core, overview, 23–24
- Server Core, removing domain controllers, 27
- using Windows interface, 12–13
- IPv6 and DNS, 445–46
- managed service accounts
  - creating and configuring, 427
  - delegations and passwords, 428–29
  - installing and using, 427–28
  - overview, 425–26
  - practice using, 429–32
  - requirements, 426–27
- names, understanding, 63
- objects
  - domain-based GPOs, 258
  - objects, practice creating and locating, 64–70
  - operation master roles, 528
  - organizational units, creating, 49–51
  - overview, 49
  - performance analysis, practice, 721–27
- read-only domains, configuring
  - administrative role separation, 419
  - deploying a RODC, 412–16
  - domain controller placement,
    - branch offices, 410–11
  - overview, 410
  - password replication policy (PRP),
    - configuring, 416–17
  - read-only domain controllers (RODC), 411–12
  - RODC credentials caching, 418–19
  - RODCs, practice configuring, 419–22
- resource management, 8
- user objects, creating, 51–53
- Active Directory Domain Services Installation Wizard
  - AD DS, installing from media, 520–21
  - domain controller, creating, 13
  - domain controllers, removing, 27, 521–22
  - forests, installing new, 20–21
  - global catalog server, configuring, 574
  - RODC account, attaching to server, 519–20
  - RODCs, installing, 415–16
  - zone delegations, DNS, 457
- Active Directory Domains And Trusts. *See also* trusts
  - create manual trust, 633–35
  - overview, 39, 664
  - userPrincipal Name, 132
  - validating trusts, 639–40
- Active Directory Federation Services (AD FS)
  - AD FS 2.0 vs. AD FS 1.1, 896
  - AD LDS scenarios, 739
  - AD RMS integration, 840, 843–44
  - architectural design types, 886–88
  - attribute store, 892
  - case scenarios, technology selection, 918
  - certificates, 895–96
  - claims and claim rules, 893–95
  - computer roles, 900
  - configuration database, 892–93
  - configuring, 904
  - firewalls, purpose of, 879–81
  - IDA infrastructure, 7
  - installing, 897–900
  - overview, 881–86
  - practice, finalizing configuration, 907–15
  - practice, preparing for deployment, 900–02
  - terminology, 888
  - using and managing, 905–07
- Active Directory Installation Wizard, 443
- Active Directory Integrated (ADI) zone, 453
- Active Directory Lightweight Directory Services (AD LDS)
  - Active Directory Schema snap-in, 758–59
  - Active Directory Sites and Services, 759–60
  - AD LDS Setup, location and use, 747
  - administration tools, overview, 664–67
  - ADSI Edit, 756–57
  - case scenario, instance prerequisites, 768
  - configuring
    - AD LDS tools, 747–49
    - creating instances, 749–55
    - overview, 747
  - IDA infrastructure, 6
  - installing, 741–42
  - LDP.exe, overview, 758
  - new features, 740–41
  - overview, 731–35
  - practice
    - installing, 743–45
    - working with, 761–65
  - scenarios, 738–40
  - understanding AD DS, 736–38
  - Windows PowerShell, working with, 760–61
- Active Directory Lightweight Directory Services Setup Wizard, 749–55
- Active Directory Management Gateway Service
  - download, 104–05
  - managed service accounts, 426–27
- Active Directory Migration Tool (ADMT), 623–24, 626–27

## Active Directory Module for Windows PowerShell

- Active Directory Module for Windows PowerShell, 741
- Active Directory Recycle Bin, 188, 740, 754–55
- Active Directory Rights Management Services (AD RMS)
  - case scenario, external AD RMS cluster, 876
  - certificates, understanding, 847–49
  - configuring
    - accounts and access rights, 867–68
    - certificates, preparing, 864–65
    - clients, 870–71
    - database management, 871–72
    - exclusion policies, 865–67
    - extranet URL, creating, 863
    - overview, 862
    - policy templates, 868–70
    - server licensor certificates, exporting, 864
    - trust policies, 863–64
  - features, 839–41
  - IDA infrastructure, 6–7
  - installation scenarios, 842–44
  - installing
    - moving to Windows Server 2008 R2, 853–55
    - overview, 844–45
    - practice, 855–60
    - prerequisites, 845–47
    - procedure for installing, 849–52
  - overview, 833–39
  - rights policy template, practice creating, 872–73
- Active Directory Schema
  - AD LDS instances, working with, 758–59
  - attributes, adding, 91
  - location and use, 747
  - overview, 39, 664
  - registering, 40, 534
- Active Directory Sites and Services
  - AD LDS instances, working with, 759–60
  - creating sites, 562–64
  - location, 39, 747
  - overview, 39, 664
  - Universal Group Member Caching, 574–75
- Active Directory Users And Computers
  - Attribute Editor, 115
  - computer accounts, deleting, 238–39
  - computer accounts, disabling and enabling, 238
  - computer properties, configuring, 232–33
  - computers, managing, 234
  - computers, moving, 233–34
  - groups, creating and naming, 157–59
  - groups, moving and renaming, 179–80
  - locating, 39
  - multiple user objects, managing, 128–29
  - Name column, details pane, 132
  - overview, 39, 664
  - protecting AD DS objects, 670–71
  - RODC, prestaged account, 518–19
  - secure channel, reset, 236
  - Specops Gpupdate, 662–63
  - user accounts, deleting, 138–39
  - user accounts, disabling and enabling, 138
  - user accounts, moving, 139–40
  - user attributes, managing, 125–29
  - user passwords, resetting, 136–37
  - view of objects, controlling, 59–60
- Active Directory Web Services (ADWS), 104–05, 741
- AD CS. *See* Active Directory Certificate Services (AD CS)
- AD DS. *See* Active Directory Domain Services (AD DS)
- AD DS Service Connection Point, 870
- AD FS Federation Server Configuration Wizard, 892
- AD LDS. *See* Active Directory Lightweight Directory Services (AD LDS)
- AD Recycle Bin, 672–75
- AD RMS. *See* Active Directory Rights Management Services (AD RMS)
- AD RMS Auditors, 840
- AD RMS Enterprise Administrators, 840
- AD RMS Service, 840
- AD RMS Template Administrators, 840
- ADAC (Active Directory Administrative Center), 102–03, 117–20
- ADAM. *See* Active Directory Lightweight Directory Services (AD LDS)
- AdamInstall.exe, 753–54
- ADAMInstall.exe, 748
- ADAMSync.exe, 748
- ADAMUninstall.exe, 748
- Add Features, Initial Configuration Tasks, 18
- Add Roles Wizard, 13, 19, 509–10
- Add Roles, Initial Configuration Tasks, 18
- Add To A Group, 167–68
- Add/Remove Columns, Active Directory Users and Computers, 59–60
- Add-ADGroupMember, 181
- Additional Domain Controller Options, 21
- addmbr parameter, DSMod, 179
- Address tab, User Properties dialog box, 126
- addresses. *See also* DNS (domain name system); IP addresses
  - configuring, 18
  - DNS and IPv6, 445–46
  - global address list (GAL), overview, 133
  - Peer Name Resolution Protocol (PNRP), 446–47
  - subnet objects, creating, 562–64
- ADFSAttributeStore, 906
- ADFSCertificate, 906
- ADFSCertSharingContainer, 906
- ADFSClaimDescription, 906
- ADFSClaimRuleSet, 906

- ADFSClaimsProviderTrust, 906
- ADFSContactPerson, 906
- ADFSEndpoint, 906
- ADFSOrganization, 906
- ADFSProperties, 906
- ADFSProxyProperties, 906
- ADFSRelyingPartyTrust, 906
- ADFSAMLEndpoint, 906
- ADFSyncProperties, 906
- Administrative Templates, Group Policy, 265–71
- Administrative Tools
  - Active Directory Administrative Center (ADAC), 117–20
  - ADSI Edit, overview, 756–57
    - custom consoles, saving, 43
    - WINS deployment, 491
- Administrators GPO, 257
- Administrators group
  - computer accounts, joining to domains, 213
  - create computer permission, 210
  - default groups, overview, 194–96
  - delegating computer support, 319
  - fine-grained passwords, lockout policy, 395–97
  - organizational unit design for, 80–81
  - passwords, 21, 25, 28
- ADMT (Active Directory Migration Tool), 623–24, 626–27
- ADPrep, 414, 513–14
- Adprep.exe, 513–14, 517
- ADSchemaAnalyzer.exe, 748
- ADSI Edit, 665, 748, 756–57
- Advanced Security Settings, object properties, 74, 191–93
- aging, DNS, 454
- alias (CNAME), DNS record types, 458, 488
- aliases
  - global name zones, 491–92
  - PowerShell cmdlets, 111–13
- All Settings Disabled, GPO status, 290
- Allow Apply Group Policy, 285–86
- Allow Read, GPO scope management, 285–86
- Allow rules, AppLocker, 361
- Allow Users To Continue To Use The Software, But Prevent New Installations, 360
- Allowed List, 416–17
- Allowed RODC Password Replication Group, 416–17
- alternate credentials, drives with, 137–38
- Always Wait For The Network At Computer Startup And Logon, 255
- Anonymous Logon, special identities, 196–97
- answer files, domain controller installations, 510–12
- application directory partitions
  - configuring, 576–77
  - DNS, 454, 494–96, 572–73
  - replication, 582
- application event logs, IDA infrastructure, 6
- Application log, Group Policy events, 307
- applications
  - authentication, 6–7
  - distributed, support for, 739
  - restriction policies, 265
  - software deployment options, GPSI, 354–56
- Applications tab, User Properties dialog box, 127
- AppLocker, 265, 361–62
- architecture
  - planning, additional resources, 623
  - Windows Server 2008 processors, 2
- Archive Subject's Encryption Private Key, 807
- Asynchronous Full Transfer (AXFR), 457
- Attribute Editor, 115, 127–28
- attribute store, AD FS, 892
- attribute store, defined, 889
- attributes, groups, best practices for, 186–87
- attributes, user accounts
  - adding, 91
  - list parameter, LDIFDE, 96
  - ListOfAttributes, CSVDE, 93
  - managing, Active Directory Users And Computers, 125–29
  - managing, DSMOD and DSGET, 129–31
  - managing, PowerShell, 131
  - objects, defined, 108
  - populating, PowerShell, 115–16
  - renaming accounts, 133
- Audit Logon Events, 368, 404
- Audit Object Access, 369, 372–73
- Audit Policy, 367–70
- Audit Policy Change, 368
- Audit Policy, Security Configuration Wizard, 343
- Audit Privilege Use, 369
- Audit Process Tracking, 369
- Audit System Events, 369
- auditing
  - Active Directory Domain Services (AD DS), 6
  - Active Directory service changes, 374–75
  - AD LDS, 749
  - AD RMS Auditors, 840
  - Audit Account Logon Events, 368, 404
  - Audit Directory Service Access, 368, 374–75
  - Audit Policy, enabling, 372–73
  - authentication
    - account logon and logon events, 404
    - logon events, viewing, 407
    - overview, 404
    - policies, configuring, 405–06
    - scoping policies, 406
  - directory changes, 671
  - disabling and enabling user accounts, 138

## Authenticated Users group

### auditing, *continued*

- domain-based GPOs, 258
  - file and folder access, 370–73
  - IDA infrastructure, 5
  - policies, configuring, 341
  - policies, implementing, 367–70
  - practice
    - audit policy, implementing, 375–79
    - auditing authentication, 407–08
  - Security log, viewing events, 375
  - system access control list (SACL), 72–73
- Authenticated Users group, 196–97, 216
- authentication. *See also* Active Directory Federation Services (AD FS); domain controllers
- Active Directory Certificate Services, 6–7
  - Active Directory data store, 4
  - Active Directory Domain Services (AD DS)
    - account lockout policies, overview, 394
    - domain password, lockout policies, 395
    - fine-grained passwords, lockout policy, 395–97
    - overview, 6, 389–91
    - password policies, overview, 392–94
    - password settings object (PSO), 397
    - practice, password lockout policies, 399–402
    - PSO precedence and resultant PSO, 398
    - PSOs and organizational units, 398–99
- AD LDS, 739
- auditing
- account logon and logon events, 404
  - logon events, viewing, 407
  - overview, 404
  - policies, configuring, 405–06
  - practice auditing, 407–08
  - scoping policies, 406
- case scenario, branch offices, 435–36
- computer accounts, renaming, 236–37
- computers, troubleshooting, 234–35
- managed service accounts
- creating and configuring, 427
  - delegations and passwords, 428–29
  - installing and using, 427–28
  - overview, 425–26
  - practice creating, 429–32
  - requirements, 426–27
- read-only domains, configuring
- administrative role separation, 419
  - deploying a RODC, 412–16
  - domain controller placement,
    - branch offices, 410–11
  - overview, 410
  - password replication policy (PRP),
    - configuring, 416–17
  - practice, configuring RODCs, 419–22

- read-only domain controllers (RODC), 411–12
  - RODC credentials caching, 418–19
  - selective authentication, 609, 642–44
  - workgroups, domains and trusts, understanding, 207
- author mode, MMC, 42
- authoritative restores, 692–94
- Authority Information Access (AIA), 810–14
- Authorization Manager, 609
- availability. *See also* directory business continuity
  - domain local groups, 161
  - global groups, 162
  - groups, 160
  - local groups, 161
  - round robin, DNS, 456
  - universal groups, 163

## B

- background refresh, Computer Configuration settings, 262
- background zone loading, 460
- backlink, group member attributes, 168
- Backlinks, Attribute Editor, 128
- backups
  - Active Directory, 520–21
  - Back Up command, GPMC, 260
  - Backup Once Wizard, 682
  - Backup Operators group, 194–96
  - certificate authorities, 818
  - computer accounts, troubleshooting, 235
  - restore, from complete backup, 694–97
  - Windows Server Backup
    - full system backups, 682–87
    - Installation From Media data, 681–82
    - overview, 678–80
    - system state only, 681
- base, Dsquery, 64
- baseline settings, configuration database, 341
- Bcredit.exe, 688–89
- best practices
  - Active Directory design, 731
  - AD CS deployment, 785–86
  - administrative tools, 43
  - comments, policy settings, 270
  - database, log files, and SYSVOL location, 21
  - Default Domain Policy GPO, 395
  - deleting user accounts, 139
  - domain controllers, security, 332
  - group management, 161–63, 169–71, 186–87
  - groups, naming, 158
  - namespaces, 450
  - operations master roles, placement, 532–33
  - password configuration, 135

- passwords, resetting, 136
  - permissions, managing, 79
  - program execution, 361
  - responsible person records, 484–85
  - securing computer creation and joins, 214–17
  - Windows domain zones, 12
  - Best Practices Analyzer, 665
  - Block Inheritance, 283
  - block lists
    - DNS, new features, 461
    - practice modifying, 501
  - boot files
    - backup, 681
    - DSRM, restarting in, 688–89
  - boot switches, Gpupdate.exe, 255, 302–03
  - branch offices
    - case scenario, authentication, 435–36
    - practice, configuring RODCs, 419–22
    - read-only domains, configuring
      - administrative role separation, 419
      - deploying a RODC, 412–16
      - domain controller placement, 410–11
      - overview, 410
      - password replication policy, configuring, 416–17
      - read-only domain controllers (RODC), 411–12
      - RODC credentials caching, 418–19
    - server placement, site planning, 562
  - bridgehead servers, 588–90, 593
  - browsers
    - browse lists, PDC Emulator, 532
    - Internet Explorer Maintenance, settings for, 263
    - spoofing protection, 461
  - brute force attacks, 394
  - business continuity
    - AD DS administration categories, 660–62
    - AD DS administration tools, overview, 664–67
    - case scenario, lost and found data, 729
    - overview, 655–57
    - performance management
      - baselines, AD DS and DNS, 717–18
      - Event Viewer, 710–12
      - overview, 707
      - Reliability Monitor, 712–13
      - system resources, overview, 707–08
      - Task Manager, 708–10
      - Windows Performance Monitor, 713–17
    - practice, AD DS performance analysis, 721–27
    - practice, working with AD DS database, 698–705
    - proactive maintenance, data store protection
      - AD Recycle Bin, 672–75
      - auditing directory changes, 671
      - built-in protection measures, overview, 669–70
      - offline maintenance, 669
      - online maintenance, 667
      - overview, 658–59
      - protecting AD DS objects, 670–71
      - protecting DCs as virtual machines, 697–98
      - Quest Object Restore For Active Directory, 676–78
      - restore deleted objects, LDP.exe, 675–76
      - restore, data set selection, 689–91
      - restore, DSRM, 688–89
      - restore, from complete backup, 694–97
      - restore, nonauthoritative or authoritative, 692–94
      - restore, overview, 687–88
      - Specops Gpupdate, 662–63
      - Windows Server Backup,
        - protection from, 678–87
      - Windows System Resource Manager (WSRM), 718–21
    - business-to-business partnerships, AD FS, 885
    - business-to-business partnerships, AD FS design types, 886–88
- ## C
- c FromDN, ToDN, LDIFDE, 95
  - c parameter, DSRM, 180
  - c switch, DSRM, 180
  - CA Web Enrollment, 779
  - caches
    - cache poisoning attacks, 464–66
    - Cache.dns, 456
    - CacheLockingPercent, 465
    - DNS cache locking, 465
    - RODC credentials caching, 418–19
    - Universal group membership caching, 574–75
  - canonical name (CNAME), 458
  - case scenario
    - AD FS, technology selection, 918
    - AD LDS instance prerequisites, 768
    - AD RMS external clusters, 876
    - administrative account security, 435
    - branch office authentication, 435–36
    - certificate revocation, managing, 829–30
    - computer accounts, creating and joining, 244
    - DNS names, blocking, 505
    - domains and forests, managing, 653
    - domains, upgrading, 554
    - Group Policy, implementing, 314
    - group strategies, 202
    - importing user accounts, 145–46
    - lost and found data, 729
    - sites and subnets, configuring, 602–03
    - software installation, Group Policy, 383

## Categories, software deployment GPOs

- Categories, software deployment GPOs, 358
- central store, creating, 269–70
- certificate authority
  - Active Directory Certificate Services, 6–7
  - hierarchy, creating, 782–85
  - issuing CA, configuring, 804–10
  - location and function, 814
  - overview, 772–77, 779
  - practice, installing a CA hierarchy, 793–801
  - stand-alone vs. enterprise, 780–82
- certificate management. *See* Active Directory Rights Management Services (AD RMS)
- Certificate Revocation List (CRL), configuring, 805–06
- certificate services. *See* Active Directory Certificate Services (AD CS)
- Certificate Templates tool, 814
- certificates
  - Active Directory authentication, 4
  - AD FS certificates, 895–96
  - AD RMS, configuring, 864–65
  - AD RMS, overview, 847–49
- Certification Authority Backup Wizard, 818
- Certification Revocation Lists (CRLs), 779
- ChangePasswordAtLogon, 116
- changeType parameter, LDIFDE, 95, 177
- Check Names, 57–58
- child domain, creating, 475–77
- claim rule templates, 894–95
- claim rules, AD FS, 893–95
- claim, AD FS, 889, 893–95
- claims aware application, defined, 889
- claims provider trust, defined, 889
- claims provider, defined, 889
- Clear This Database Before Importing, 335
- client licensor certificate (CLC), 848
- clients, configuring AD RMS, 870–71
- client-side extensions. *See also* Group Policy Software Installation (GPSI)
  - Group Policy Clients, 254–55
  - Group Policy object scope, 278
  - Group Policy, Scripts settings, 262–63
- clocks, synchronizing, 531–32
- cloud
  - Federation with Cloud Services, 886–88
  - Peer Name Resolution Protocol (PNRP), 447
- Cmd.exe, PowerShell aliases, 112
- cmdlets, overview, 102, 105–07. *See also* PowerShell
- CN (common name) objects, 51, 63, 132, 158
- CNAME, DNS record types, 458, 488
- collection of objects, defined, 110
- columns, Active Directory Users and Computers, 59–60
- COM+ Class Registration database, 681
- COM+ tab, User Properties dialog box, 127
- comma-delimited files
  - exporting user files, CSVDE, 92–93
  - importing computers, CSVDE, 225–26
  - importing groups, CSVDE, 176–77
  - importing user files, CSVDE, 93
  - importing users, PowerShell, 116–17
- Command Prompt (Cmd.exe)
  - computer accounts, joining to domains, 213
  - domain controller unattended installations, 510–11
  - PowerShell aliases, 112
- command-line utilities. *See also* Comma-Separated Value Exchange (CSVDE); *also* PowerShell
  - Adprep.exe, 513–14
  - Dsacls.exe, 78
  - Dsquery, 63–64
  - full server recovery, 696–97
  - Gpresult.exe, 305–06
  - PKIView, 815–17
  - Secedit.exe, 338–39
- Comma-Separated Value Exchange (CSVDE)
  - exporting users, 92–93
  - importing computers, 225–26
  - importing groups, 176–77
  - importing user files, 93
- comments, policy settings, 270
- common name (CN) objects, 51, 63, 132, 158
- components, displaying, 26
- computer accounts. *See also* groups
  - automating creation, computer objects
    - creating computers with DSAdd, 227
    - creating computers with NetDom, 227–28
    - creating computers with PowerShell, 228
    - importing computers with CSVDE, 225–26
    - importing computers with LDIFDE, 226–27
  - overview, 225
  - practice automating, 228–30
- case scenario, creating and joining accounts, 244
- creating computers
  - delegating permission to create, 210
  - joining to domain, 208, 211–13
  - offline domain join, 217–21
  - overview, 207
  - practice, joining domain, 221–23
  - prestaging computer account, 210–11
  - securing creation and joins, 214–17
- deleting accounts, 238–39
- disabling and enabling accounts, 238
- logon and secure channel, 234
- managing, Active Directory Users And Computers, 234
- moving computers, 233–34
- overview, 205–06
- properties, configuring, 232–33
- recycling computer accounts, 239

- renaming computers, 236–37
- resetting accounts, 235–36
- supporting objects and accounts, practice, 239–41
- troubleshooting, 234–35
- computer configuration settings, defined, 250–51
- Computer Configuration, Group Policy
  - Administrative Templates, 263
  - delegating administration, 322
  - enabling and disabling GPOs, 290
  - group membership, defining, 323–24
  - Preferences, 264
  - registry policy settings, 265
  - settings, 262
  - Windows Settings, 262–63
- Computer container, configuring, 214–15
- computer objects, creating, 55–56
- Computer Restrictions, Log On To, 134
- computer settings, defined, 250–51
- computer support
  - delegation of
    - Member Of settings, 322
    - Members Of This Group, 322–24
    - overview, 319
    - restricted Group Policies, 319–22
  - practice, delegating, 324–27
- ComputerDN, creating computers DSAdd, 227
- ComputerName, Djoin.exe, 219
- computers
  - practice, adding to groups, 69
  - practice, creating, 67–68
  - resource management, 39
- Computers container, 208–10
- conditional forwarders (CF), 462–63, 489–90
- configuration database, 341, 892–93
- configuration naming context, 572
- configuring. *See also* configuring, computer accounts
  - Active Directory Certificate Services (AD CS)
    - overview, 804
    - protecting the configuration, 818
    - revocation configuration, creating, 805–06
  - Active Directory Domain Services, post-installation
    - practice, 17–19
  - Active Directory Federation Service (AD FS),
    - finalizing configuration practice, 907–15
  - Active Directory Federation Services (AD FS), 904
  - Active Directory Rights Management Services (AD RMS)
    - accounts and access rights, 867–68
    - certificates, preparing, 864–65
    - clients, 870–71
    - database management, 871–72
    - exclusion policies, 865–67
    - extranet URL, creating, 863
  - overview, 862
  - policy templates, 868–70
  - server licenser certificates, exporting, 864
  - trust policies, 863–64
- AD DS administration categories, 660–62
- AD LDS, 747–49
- audit policy, practice, 376
- authentication audit policies, 405–06
- case scenario
  - configuring security, 383–84
  - sites and subnets, 602–03
- computer security, analyzing, 336–37
- DNS (domain name service), 26
  - administering DNS servers, 497–99
  - application directory partitions, 494–96
  - custom records, creating, 488
  - DHCP considerations, 492–94
  - DNS server settings, 481–85
  - DNS socket pools, 465–66
  - forwarders vs. root hints, 488–90
  - overview, 480
  - practice, DNS server configuration, 499–501
  - security considerations, 480–81
  - single-label name management, 490–92
- global catalog and application directory partitions
  - application directory partitions, overview, 576–77
  - global catalog server placement, 573
  - global catalog server, configuring, 574
  - overview, 572–73
  - Universal group membership caching, 574–75
- Group Policy scope, practice, 295–99, 307–11
- Local Security Policy, 331–32
- local security policy, practice, 346
- managed service accounts, 427
- managed service accounts, practice, 431–32
- password lockout policies
  - domain passwords, 395
  - fine-grained passwords, lockout
    - policy, 395–97
  - overview, 392–94
  - password settings objects (PSO), 397
  - practice configuring, 399–402
  - PSO precedence and resultant PSO, 398
  - PSOs and organizational units, 398–99
- policy settings, 251–52
- read-only domains
  - administrative role separation, 419
  - deploying a RODC, 412–16
  - domain controller placement,
    - branch offices, 410–11
  - overview, 410
  - password replication policy (PRP),
    - configuring, 416–17

## configuring, computer accounts

### configuring, *continued*

- practice configuring RODCs, 419–22
  - read-only domain controllers (RODC), 411–12
  - RODC credentials caching, 418–19
  - replication
    - bridgehead servers, 588–90
    - connection objects, 582–83
    - intersite replication, 590–94
    - intrasite replication, 584–85
    - Knowledge Consistency Checker, 583–84
    - monitoring replication, 594–96
    - overview, 581–82
    - practice configuring, 596–98
    - site links, 586–88
  - Secedit.exe, computer security, 338–39
  - Security Configuration And Analysis
    - snap-in, 335–36
  - Server Core installations, initial tasks, 25–26
  - sites and subnets
    - creating sites, 562–64
    - domain controller location, 566–69
    - domain controllers, managing, 565–66
    - overview, 557–60
    - planning sites, 560–62
    - practice configuring, 569–70
  - SYSVOL replication
    - domain functional levels, raising, 543–44
    - migration, 544–46
    - overview, 543
    - practice configuring, 546–51
  - configuring, computer accounts
    - automating creation, computer objects, 225
    - creating computers with DSAdd, 227
    - creating computers with NetDom, 227–28
    - creating computers with PowerShell, 228
    - importing computers with CSVDE, 225–26
    - importing computers with LDIFDE, 226–27
  - case scenario, creating and joining accounts, 244
  - creating computers
    - joining to domain, 208, 211–13
    - offline domain join, 217–21
    - overview, 207
    - prestaging computer account, 210–11
    - securing creation and joins, 214–17
  - default Computer container, 214–15
  - delegating permission to create accounts, 210
  - deleting accounts, 238–39
  - disabling and enabling accounts, 238
  - logon and secure channel, 234
  - managing, Active Directory Users And Computers, 234
  - moving computers, 233–34
  - overview, 205–06
  - practice
    - automating creation of computer objects, 228–30
    - creating computers, joining domains, 221–23
    - supporting objects and accounts, 239–41
  - properties, configuring, 232–33
  - recycling accounts, 239
  - renaming computers, 236–37
  - resetting accounts, 235–36
  - troubleshooting, 234–35
- connection objects, 582–83, 596
  - connections
    - Group Policy, slow links and disconnects, 256
    - speed, site planning and, 561
  - console tree, MMC, 37
  - constructed attribute, 128
  - containers
    - overview, 11
    - permission inheritance, 76–77
  - Context menu, MMC, 37
  - ConvertTo-SecureString, 116
  - Coordinated Universal Time (UTC), 531–32
  - Copy command, GPMC, 259
  - Copy Object User Wizard, 89
  - correspondingdnsname, 491
  - costs, adding domains, 621
  - costs, site link, 592
  - counters, System Monitor, 714, 716–17
  - Create A New Domain In An Existing Forest, 516
  - Create A Password Reset Disk, 17
  - Create Child-Allow permission, 218
  - create full Path, ifm prompt, 521
  - create rodc Path, ifm prompt, 521
  - create sysvol full, ifm prompt, 521
  - create sysvol rodc Path, ifm prompt, 521
  - CreateDCAccount, dcpromo, 511
  - creating
    - Active Directory objects
      - computer objects, 55–56
      - group objects, creating, 53–55
      - names, understanding, 63
      - organizational units, 49–51
      - overview, 49
      - user objects, 51–53
    - AD LDS instances, 749–55
    - AD RMS policy templates, 868–70
    - application directory partitions, 494–96
    - case scenario, Active Directory forests, 33
    - central store, 269–70
    - certificate authority hierarchy, 782–85
    - certificate authority, revocation, 805–06
    - computer accounts
      - delegating permission to create, 210
      - joining to domains, 208, 211–13

- offline domain join, 217–21
  - prestaging computer accounts, 210–11
  - securing creation and joins, 214–17
  - workgroups, domains, and trusts, 207
  - computer objects, automating creation
  - creating computers with DSAdd, 227
  - creating computers with NetDom, 227–28
  - importing computers with CSVDE, 225–26
  - importing computers with LDIFDE, 226–27
  - overview, 225
  - conditional forwarders, 489–90
  - connection object, 584
  - custom records, DNS, 488
  - domain controller, 13
  - full system backups, 682–87
  - global names, 490–92
  - GPOs, 258–59
  - GPOs, local, 257
  - Installation From Media data sets, 681–82
  - installation media, AD DS, 521
  - lookup zones and forwarders, 462–63
  - managed service accounts, 427
  - password reset disk, 17
  - performance baselines, AD DS and DNS, 717–18
  - practice
    - Active Directory objects, creating
      - and locating, 64–70
    - child domains, 475–77
    - computers, 67–68
    - connection object, 596
    - domain controllers, additional, 523–25
    - domain controllers, from backup file, 699–701
    - domain controllers, Server Core, 29–30
    - domain trees, 473–75
    - forests, 469–71
    - group policy objects, 271–72
    - Group Policy, central store, 271–72
    - groups, 68, 171–72, 182
    - installation media, 525
    - joining domains, 221–23
    - managed service accounts, 429–32
    - manual zone delegation, 471–73
    - MMC, creating custom, 44–47
    - organizational units, 64–65
    - password settings object (PSO), 400–01
    - rights policy template, 872–73
    - single-label names, 500–01
    - site links, 597
    - sites, 569–70
    - software deployment GPO, 362–63
    - user accounts, 97–100
      - Windows Server 2008 forest, 14–21
    - responsible person record, 484–85
    - reverse lookup zones (RLZ), 485–87
    - RODC, prestaged account, 518–19
    - security policy, 340–44
    - sites, creating and configuring, 562–64
    - software deployment GPO, 356–58
    - trusts, manual, 633–35
    - URLs, extranet, 863
    - user accounts
      - DSAdd User, 92
      - exporting with CSVDE, 92–93
      - importing with CSVDE, 93–94
      - importing with LDIFDE, 94–96
      - PowerShell cmdlets, 113–14
      - practice, using PowerShell, 120–23
      - templates and, 89–91
      - WMI filters, 288–90
  - credentials
    - administrative tools with alternate credentials, 41–42
    - alternate credentials, drives with, 137–38
    - computer accounts, joining to domain, 212–13
    - logon and secure channel, 234
    - password replication policy (PRP), configuring, 416–17
    - practice, credential caching, 421–22
    - RODC credentials caching, 418–19
  - CRLs (Certification Revocation Lists), 779
  - cryptographic signatures, 464
  - Cscript, 25–26
  - CSVDE.exe
    - computers, importing, 225–26
    - groups, importing, 176–77
    - location and use, 748
    - overview, 665
    - practice
      - creating computers, 229
      - groups, importing, 182
      - user account creation, 98–99
    - users, exporting, 92–93
    - users, importing, 93–94
  - custom records, DNS, 488
  - Custom Search, Active Directory Domain Services, 61
- ## D
- d RootDN parameter, CSVDE, 93
  - d RootDN parameter, LDIFDE, 96
  - DACL. *See* discretionary access control lists (DACLs)
  - Data Collector Set templates, 714
  - data store
    - AD DS administration categories, 660–62
    - AD DS administration tools, overview, 664–67
    - AD Recycle Bin, 672–75
    - auditing directory changes, 671

## database

### data store, *continued*

- built-in protection measures, overview, 669–70
- offline maintenance, 669
- online maintenance, 667
- overview, 9, 12, 658–59
- practice, working with AD DS database, 698–705
- protecting AD DS objects, 670–71
- protecting DCs as virtual machines, 697–98
- Quest Object Restore For Active Directory, 676–78
- restore
  - data set selection, 689–91
  - deleted objects, LDP.exe, 675–76
  - DSRM restarts, 688–89
  - from complete backup, 694–97
  - nonauthoritative or authoritative, 692–94
  - proactive, 687–88
- Specops Gpupdate, 662–63
- Windows Server Backup, protection from, 678–87

### database

- AD DS administration categories, 660–62
- AD RMS, database management, 871–72
- location, 21
- mounting tool, recovery, 689–91
- security settings, 336
- Dcdiag.exe, 594–96, 748
- DCDiag.exe, 534, 665
- dcname parameter, Djoin.exe, 219
- Dcpromo.exe
  - add and remove AD DS, 26
  - adding AD DS to Server Core installation, 27
  - child domain, installing, 516
  - domain controller, creating, 13
  - domain controllers, installing, 509–12
  - forests, creating, 20–21
  - overviews, 665
  - practice, create domain controllers, 29–30
  - promoting controllers, 26
  - removing domain controllers, 27, 521–22
  - RODC accounts, attaching servers, 519–20
  - RODCs, creating, 416
- Dcpromo/adv, 515
- DDNS, 454
- decryption, AD FS certificates, 895
- Default Computers container, 208–10, 214–15
- Default Domain Controllers Policy, 258
- Default Domain Policy, 258, 395
- default groups, managing, 194–96
- default passwords, Active Directory domains, 66
- Default-First-Site-Name, 565
- defragmentation, 669
- delegation
  - Account Is Trusted For Delegation, 135
  - Active Directory objects

- ACLs, viewing, 73–74
- administrative task delegation, 77–78
- effective permissions, 79–80
- organizational unit design for, 80–81
- overview, 72
- permissions and inheritance, 76–77
- permissions, removing or resetting, 78–79
- permissions, reporting and viewing, 78
- practice, administrative task delegation, 81–82
- case scenario, organizational units, 84–85
- computer accounts, authentication, 207
- computer support
  - Member Of settings, 322
  - Members Of This Group, 322–24
  - overview, 319
  - restricted Group Policies, 319–22
- domain functional levels, 609
- GPO creation permission, 258
- GPO editing permission, 259
- group management, 189–93
- managed service accounts, 428–29
- permission to create computers, 210
- practice
  - computer support delegation, 324–27
  - creating computer objects, 222–23
- RODC installation, 416
- understanding delegation, 72–73
- Delegation of Control Wizard, 77–78
- Delegation Of RODC Installation And Administration, 518–19
- deleting
  - AD Recycle Bin, 672–75
  - computer accounts, 238–39
  - Group Policy objects (GPOs), 260
  - Group Policy objects (GPOs), links, 280
  - groups, DSRM, 180–81
  - groups, protecting against, 188–89
  - organizational unit, 50
  - practice, password settings object (PSO), 402
  - Quest Object Restore For Active Directory, 676–78
  - restoring deleted objects, LDP.exe, 675–76
  - user accounts, 138–39
- Demotion, dcpromo, 511
- denial-of-service (DoS) attacks, 480–81
- Denied List, 416–17
- Denied RODC Password Replication Group, 417
- Deny permissions, GPO scope, 287–88
- deny permissions, options for, 671
- Deny rules, AppLocker, 361
- Deploy Software dialog box, 357–58
- deployment. *See also* installing
  - Active Directory Federation Services (AD FS), 897–900

- AD RMS installation scenarios, 842–44
- domain controllers
  - AD DS, installing from media, 520–21
  - additional domain controllers, installing, 513–15
  - new domain tree, installing, 517
  - removing domain controllers, 521–22
  - RODC installation, staging, 518–20
  - unattended installations, options and answer files, 510–11
  - Windows Server 2008 R2 forest, installing, 512
  - with Windows interface, 509–10
- practice
  - AD FS, preparing for deployment, 900–02
  - domain controllers, 522–25
  - read-only domain controllers (RODC), 412–16
- desc parameter, DSAdd, 176, 227
- desc parameter, DSMod, 179
- description attribute, groups, 179
- desktop appearance, 294
- desktop support, delegating
  - Member Of settings, 322
  - Members Of This Group, 322–24
  - overview, 319
  - practice, delegating, 324–27
  - restricted Group Policies, 319–22
- Detailed, Get-Help, 107
- Detailed, New-ADUser, 114
- details pane, MMC, 37
- DFR-R replication, SYSVOL, 609
- DFS Replicated Folders
  - All Counters, 715
- DFS Replication Connections
  - All Counters, 716
- DFS Replication logs, 710–12
- DFS Replication Service Volumes
  - All Counters, 716
- DFS, configuring, 26
  - SYSVOL replication
    - domain functional levels, raising, 543–44
    - migration, 544–46
    - overview, 543
    - practice, 546–51
- Dfscmd.exe, 26
- DFS-R, overview, 508
- DFSRadmin.exe, 665
- Dfsrmig.exe, 545–46
- DHCP, DNS configuration, 492–94
- Dial-in tab, User Properties dialog box, 127
- Digital Rights Management (DRM). *See* Active Directory Rights Management Services (AD RMS)
- digital signatures
  - Active Directory Certificate Services, 6–7
  - DNS Security (DNSSEC), 464
  - Peer Name Resolution Protocol (PNRP), 447
- directory business continuity
  - AD DS administration categories, 660–62
  - AD DS administration tools, overview, 664–67
  - case scenario, lost and found data, 729
  - overview, 655–57
  - performance management
    - baselines, AD DS and DNS, 717–18
    - Event Viewer, 710–12
    - overview, 707
    - Reliability Monitor, 712–13
    - system resources, overview, 707–08
    - Task Manager, 708–10
    - Windows Performance Monitor, 713–17
    - Windows System Resource Manager (WSRM), 718–21
  - practice, AD DS performance analysis, 721–27
  - practice, working with AD DS database, 698–705
  - proactive maintenance, data store protection
    - AD Recycle Bin, 672–75
    - auditing directory changes, 671
    - built-in protection measures, overview, 669–70
    - offline maintenance, 669
    - online maintenance, 667
    - overview, 658–59
    - protecting AD DS objects, 670–71
    - protecting DCs as virtual machines, 697–98
    - Quest Object Restore For Active Directory, 676–78
    - restore, data set selection, 689–91
    - restore, DSRM, 688–89
    - restore, from complete backup, 694–97
    - restore, nonauthoritative or authoritative, 692–94
    - restore, overview, 687–88
    - restoring deleted objects, LDP.exe, 675–76
    - Specops Gpupdate, 662–63
    - Windows Server Backup, protection from, 678–87
- Directory Replication Agent (DRA), 261–62, 585
- Directory Server Diagnosis (Dcdiag.exe), 594–96
- Directory Service logs, 710–12
- Directory Service Remote Procedure Call (DS-RPC), 588
- Directory Services Restore Mode (DSRM), 669, 672, 688–89
- Directory Services Restore Mode Administrator Password, 21
- disabled passwords, 135
- disabling computer accounts, 238
- disabling GPO links, 280
- disaster recovery. *See* business continuity
- disconnected systems, Group Policy, 256
- discretionary access control lists (DACLs)
  - delegation, overview, 72–73
  - IDA infrastructure, 4–5
  - migration, 624–25

## Diskidentifiers.txt

- Diskidentifiers.txt, 686
- Display Name, user objects, 133
- displayName, user objects, 133
- distinguished names (DN)
  - creating computers, DSAdd, 227
  - DS commands, 91–92
  - overview, 63
  - phantom objects, 530
  - UserDN, DSMod, 129
- Distributed File System Replication (DFS-R), 261–62, 531–32
- distribution groups, 53, 165
- division attribute, user objects, 128
- Djoin.exe, 217–21
- DN (distinguished names), 63
- DNS
  - All Counters, 716
  - DNS (domain name system)
    - Active Directory partitions, 8
    - AD DS administration categories, 660–62
    - AD DS integration, overview, 439–43, 461–63
    - administration, tools overview, 664–67
    - case scenario, blocking specific names, 505
    - configuring, 26
      - administering DNS servers, 497–99
      - application directory partitions, 494–96
      - DHCP considerations, 492–94
      - DNS server settings, 481–85
      - overview, 480
      - security considerations, 480–81
    - custom records, creating, 488
    - DNS name, offline domain join, 218
    - DNS structures, 448–49
    - forwarders vs. root hints, 488–90
    - installing Windows Server 2008 R2 forest, 512
    - installing, overview, 444
    - IPv6 and, 445–46
    - name resolution process, 452–59
    - names, selecting, 12
    - Peer Name Resolution Protocol (PNRP), 446–47
    - practice
      - DNS Server configuration, 499–501
      - installing DNS, 468–77
    - single-label name management, 490–92
    - split-brain syndrome, 449–51
    - userPrincipalName, 132
    - Windows Server 2008 R2 features, 459–61, 463–67
- DNS Manager, 497, 665
- DNS Notify, 454
- DNS Security Extensions (DNSSEC), 464–65
- DNS Server, 515
- DNS Server logs, 710–12
- DNS socket pool, 465–66
- Dnscmd.exe
  - AD DS integrated zones, 464
  - global name zone creation, 490–92
  - managing DNS servers, 497
  - overview, 665
  - Server Core configuration, 26
- Dnslint, 498
- dnsservername, 491
- dollar sign (\$), PowerShell variables, 108–09
- Domain Admins group
  - computer accounts, joining to domains, 213
  - computer permission, creating, 210
  - default groups, overview, 194–96
  - GPOs, creating, 258–59
  - offline domain joins, 218
  - RODC prestaged account, 518–19
- domain controllers. *See also* site management
  - AD LDS installations, 741
  - auditing account logon and events, 404
  - case scenario, branch office authentication, 435–36
  - case scenario, upgrading domains, 554
  - creating, 13
  - defined, 9
  - deploying
    - AD DS, installing from media, 520–21
    - installing additional domain controllers, 513–15
    - installing new child domain, 516
    - installing with Windows interface, 509–10
    - new domain tree, installing, 517
    - new Windows Server 2008 R2 forest, 512
    - overview, 509
    - practice deploying, 522–25
    - removing domain controllers, 521–22
    - RODC installation, staging, 518–20
    - unattended installation, options and answer files, 510–11
- domain-based GPOs, 258
- GPO links, 278–80
- Local Security Policy, 332
- location, sites and subnets, 566–69
- managing in sites, 565–66
- operations masters
  - domain-wide operation master roles, 529–32
  - failures, recognizing, 536
  - forest-wide operation master roles, 529
  - identifying, 533–35
  - overview, 527
  - placement, 532–33
  - practice transferring, 539–41
  - returning roles, 538–39
  - seizing roles, 536–37
  - single master operations, 527–28
  - transferring, 535–36

- overview, 507–08
- password lockout policies, 395
- practice
  - creating, Server Core, 29–30
  - installing Server Core domain controller, 27–30
  - read-only domain controllers (RODC), configuring, 419–22
- promoting, 26
- protecting DCs as virtual machines, 697–98
- read-only domains, configuring
  - administrative role separation, 419
  - deploying a RODC, 412–16
  - domain controller placement, branch offices, 410–11
  - overview, 410
  - password replication policy (PRP), configuring, 416–17
  - RODC credentials caching, 418–19
- Redircmp.exe, 215
- removing, 27
- service placement, site planning, 561–62
- SYSVOL replication, configuring
  - domain functional levels, raising, 543–44
  - migration, 544–46
  - overview, 543
  - practice, 546–51
- Windows System Resource Manager (WSRM), 719
- Domain Controllers OU, domain-based GPOs, 258
- Domain DNS zone, 454
- domain functional levels
  - confirm and modify, 396
  - installing, new forest, 512
  - overview, 10–11, 608–11
  - practice, raising, 614–16
  - SYSVOL replication, 543–44
  - understanding, 607
- domain GPOs, overview, 292
- domain hierarchy, ADAC, 118
- domain local groups, 54, 161–62, 164, 169
- domain name system. *See* DNS (domain name system)
- domain names, userPrincipalName, 132
- domain naming context, 572
- domain naming master role
  - failure, 537
  - identifying, 533
  - overview, 529
  - placement of operations master, 532–33
  - returning roles, 538
- domain quarantine, 641
- domain trees, creating, 473–75
- Domain Users group, 213
- domainControllerName, Djoin.exe, 219
- DomainDNSName, Djoin.exe, 218
- DomainDnsZones, 576–77
- domainName, SVR record, 567
- domains. *See also* DNS (domain name system)
  - administration of, 39
  - case scenario, managing, 653
  - computer accounts, joining, 208, 217–21
  - domain functional levels, overview, 608–11
  - forests and trees, overview, 9–10
  - functional levels, understanding, 607
  - GPO links, 278–80
  - GPOs, editing multi-site, 259
  - joining, 26, 211–13
  - overview, 9, 605–06
  - practice
    - creating computers and joining domains, 221–23
    - raising functional levels, 614–16
    - trust relationships, 645–49
  - trust relationships
    - administering trusts, 639–40
    - authentication protocols, 629–30
    - between domains, 627–28
    - dedicated forest root domain, 618
    - Kerberos, across domains in a forest, 630–32
    - Kerberos, within a domain, 630
    - manual trusts, 632–35
    - moving objects, domains and forests, 623–27
    - multiple forests, 622–23
    - multiple trees, 622
    - multiple-domain forest, 620–22
    - overview, 618, 629–30
    - shortcut trusts, 636–39
    - single-domain forest, 619–20
    - users, resource access, 640–44
    - within domains, 627
  - understanding, 207
- domain-wide operation master roles, 529–32
- dot notation ( . ), PowerShell cmdlets, 115
- down-level application packages, 354
- downlevel parameter, Djoin.exe, 219
- DS commands
  - finding objects, 63–64
  - overview, 91–92
- DSACLs
  - managed service accounts, delegation and passwords, 428–29
  - permissions, reporting and viewing, 78
- Dsacls.exe
  - permissions, reporting and viewing, 78
- DSACLs.exe
  - location and use, 748
  - overview, 665

## DSAdd

DSAdd  
  creating computers, 227  
  groups, creating, 175–76  
  overview, 91  
  practice  
    creating computers, 228–29  
    creating user accounts, 98  
    groups, creating, 182  
    user accounts, creating (DSAdd User), 92  
Dsadd.exe, 665  
Dsamain.exe, 665  
DSAMain.exe, 748  
DSDButil.exe, 665  
DSDBUtile.exe, 748  
DSGet  
  group membership, copying, 179  
  group membership, retrieving, 178  
  overview, 91  
  user attributes, managing, 129–31  
Dsget.exe, 665  
Dsmgmt.exe, 419, 665  
DSMgmt.exe, 748  
DSMod  
  computer attributes, configuring, 233  
  disabling or enabling accounts, 238  
  disabling and enabling user accounts, 138  
  group membership, changing, 179  
  group type and scope, changing, 166  
  overview, 91  
  practice, group membership, 183  
  resetting passwords, 137  
  user attributes, managing, 129–31  
Dsmod.exe, overview, 92, 665  
DSMove, 91, 139–40, 179–80, 233–34  
Dsmove.exe, 665  
dsnservname, 495  
DSQuery, 91, 129–30  
Dsquery, finding objects, 63–64  
Dsquery.exe, 92, 665  
DSRm  
  computer accounts, deleting, 238–39  
  deleting user accounts, 139  
  groups, deleting, 180–81  
  overview, 91  
Dsrms.exe, 666  
Dynamic DNS Servers (DDNS), 448–49  
Dynamic Host Configuration Protocol (DHCP), 444, 529  
dynamic link library (DLL), 45

## E

effective permissions, Active Directory objects, 79–80

EFS Recovery Agent template, 807  
email addresses, 132, 893–95. *See also* Active Directory Certificate Services (AD CS)  
email messages, 459  
employeeID, user object attribute, 128  
employeeNumber, user object attribute, 128  
employeeType, user object attribute, 128  
Enabled, GPO status, 290  
enabling computer accounts, 238  
Encrypting File System (EFS), 6–7, 807. *See also* Active Directory Certificate Services (AD CS)  
encryption. *See also* Active Directory Certificate Services (AD CS)  
  AD RMS, 841  
  DNS zone signatures, 464  
  Simple Authentication And Security Layer (SASL), 95  
  Store Password Using Reversible Encryption, 135  
Enforce Password History, 393  
enforced GPOs, 292  
Enter The Object Names, 57–58  
Enterprise Admins group  
  create computer permission, 210  
  default groups, overview, 194–96  
  RODC prestaged account, 518–19  
Enterprise PKI tool, 814–17  
Environment tab, User Properties dialog box, 126–27  
error messages, logon, 235  
Event Log Policies, security templates, 333  
event logs  
  account logon and logon events, auditing, 404  
  AD CS, common events, 815–16  
  AD LDS, 752  
  audit policies, 368  
  auditing directory changes, 671  
  failed events, auditing, 371  
  Group Policy, 293–94, 307  
  IDA infrastructure, 6  
  LDIFDE, location of, 95  
  location, 21  
  managing computers, 234  
  practice, viewing Group Policy logs, 309  
  Security log, viewing events, 375  
Event Viewer  
  location and use, 748  
  overview, 666, 710–12  
Event Viewer, DNS, 498  
Event Viewer, Group Policy, 307  
Everyone group, special identities, 196–97  
-Examples, Get-Help, 107  
Excel data  
  exporting user files, CSVDE, 92–93  
  importing users, CSVDE, 93–94  
  importing users, PowerShell, 116–17

Exchange Online, 887  
 Exchange Server 2007  
   Public Key Infrastructure (PKI), 774–75  
 -exclude parameter, DSRm, 180  
 Exclude User Account Wizard, 866  
 exclusion policies, AD RMS, 865–67  
 -expand parameter, DSGet, 178  
 exporting  
   AD RMS, server licenser certificates, 864  
   groups, CSVDE, 176–77  
   security templates, 338–39  
   users with CSVDE, 92–93  
 Extensions, Active Directory Schema, 46  
 external trusts, 632–35, 637

## F

-f filename, LDIFDE commands, 95  
 -f parameter, CSVDE, 93, 177, 225  
 -f parameter, LDIFDE, 177, 227  
 failover planning, operations master  
   placement, 533  
 fault tolerance  
   domain controllers, installing, 513–15  
   single-label names, 491  
 features, displaying, 26  
 federation. *See also* Active Directory Federation  
   Services (AD FS)  
   AD RMS, 840, 863–64  
   defined, 890  
   federated user, defined, 890  
   Federated Web SSO, 886–88  
   federation server, 890, 895  
   federation server proxy, 890  
   Federation Service, 885  
   Federation Service Proxy, 885, 895  
   Federation with Cloud Services, 886–88  
   metadata, defined, 890  
 file access, auditing, 370–73  
 file names, importing user files, CSVDE, 93  
 file permissions, migrating, 625  
 File Replication Service (FRS), 261–62, 531–32  
 File System Permissions, security templates, 333  
 Filename parameter, Djoin.exe, 219–20  
 Filter, Attribute Editor, 127  
 filtering  
   Administrative Template policy settings, 266  
   GPO scope management, 285–88  
   GPO scope management, WMI filters, 288–90  
   Group Policy object scope, 253  
   -r Filter parameter, CSVDE, 93  
   -r Filter parameter, LDIFDE, 96  
 Find Objects In Active Directory Domain Services, 60–61  
 fine-grained passwords, 395–97, 428–29  
 firewalls. *See also* Active Directory Federation Services  
   (AD FS)  
   AD LDS scenarios, 739  
   NetDom, remote use, 213  
   purpose of, 879–81  
   RSOP analysis, 304  
   Security Configuration Wizard, 342  
 Flexible Single Master Operations (FSMOs), 527–28, 660–62  
 folder access, auditing, 370–73  
 folder permissions, migration, 625  
 Folder Redirection, 263  
 force replication, 583  
 force switch, GPUUpdate, 302–03  
 forceremoval, dcpromo, 522  
 Forefront Identity Manager (FIM), 739  
 forests  
   case scenario, creating Active Directory forest, 33  
   case scenario, managing, 653  
   cross-forest enrollment, AD CS, 789  
   forest DNS zone, 454  
   forest functional levels  
     administration of, 39  
     overview, 10–11, 611–14  
     practice, raising, 614–16  
     RODC deployment, 413–14  
     understanding, 607  
     upgrades, 414  
   forest root domain, 9–10, 442–43  
   ForestDnsZones, 576–77  
   forest-wide operation master roles, 529  
   functional levels, understanding, 607  
   installing, 512  
   overview, 9–10, 605–06  
   practice  
     creating, 14–21, 469–71  
     installing, 19–21  
     raising functional levels, 614–16  
     trust relationships, 645–49  
   preparing, Windows Server 2008 R2, 513–14  
   trust relationships  
     administering trusts, 639–40  
     dedicated forest root domain, 618  
     Kerberos, across domains in a forest, 630–32  
     manual trusts, 632–35  
     moving objects, domains and forests, 623–27  
     multiple forests, 622–23  
     multiple trees, 622  
     multiple-domain forest, 620–22  
     shortcut trusts, 636–39  
     single-domain forest, 619–20  
     users, resource access, 640–44

## forward link attribute

- forward link attribute, 128
- forward lookup zones (FLZ)
  - configuring, 482–84
  - creating, 462–63
  - custom records, creating, 488
- forward lookup, DNS, 454
- forwarders, DNS, 455, 488–90
- FS configuration database, 889
- FSconfig.exe, 892
- Full Name, user objects, 51, 132
- Full, Get-Help, 107
- fully qualified domain name (FQDN)
  - application directory partitions, creating, 495
  - DNS devolution, 466–67
  - naming AD DS directories, 449–50
- functional level, overview, 10–11

## G

- GAL (global address list), 133
- General tab, User Properties dialog box, 126
- Generaterollback, security templates, 339
- Get-ADComputer, 228
- Get-ADFSSyncProperties, 892
- Get-ADGroup, 181
- Get-ADGroupMember, 107, 181
- Get-ADObject, 675
- Get-ADServiceAccount, 427
- Get-ADUser, 108, 131
- Get-Alias, 111–12
- Get-Command, 106
- getglobalstate, Dfsrmig.exe, 545–46
- Get-Help cmdlet, 107–08, 114
- getmigrationstate, Dfsrmig.exe, 545–46
- global address list (GAL), 133
- global catalog (GC)
  - Active Directory data store, 9
  - configuring partitions, 572–73
  - domain controllers, installing, 515
  - overview, 8
  - replication, 620
- global catalog (GC) server
  - configuring, 574
  - installing, new forest, 512
  - placement of, 573
  - removing domains, 463
- global cloud, PNRP, 447
- global groups, 54, 162–64, 169–71, 625–26
- global name zones (GNZ), 455, 490–92
- global query block lists, 461, 501
- Global Search, Active Directory Administrative Center (ADAC), 120
- global security groups, 398–99
- Global unicast addresses, 445–46
- globally unique identifier (GUID)
  - backup schedule, Wbadmin.exe, 686–87
  - overview, 398
  - phantom objects, 530
  - snapshots, creating, 689–91
- GPfixup.exe, 666
- GPME (Group Policy Management Editor), 250–51
- Gpotool.exe, 261–62
- Gpresult.exe, 303, 305–06, 308–09
- GPUUpdate, 302–03
- Gpupdate.exe, 255
- graphical full server recovery, 694–95
- Group Is A Member Of, Computer Configuration, 320–22
- Group Policy. *See also* Group Policy objects (GPOs); groups
  - Administrative Templates, settings, 263
  - audit policy
    - Active Directory service changes, 374–75
    - enabling audit policy, 372–73
    - file and folder access, 370–73
    - overview, 367–70
    - Security Log, viewing events, 375
  - case scenario
    - configuring security, 383–84
    - implementing Group Policy, 314
    - installing software, 383
  - certificate templates, configuring, 809
  - client-side extensions, 254–55, 260
  - Computer Configuration, policy settings, 262
  - computer support, delegation of
    - Member Of settings, 322
    - Members Of This Group, 322–24
    - overview, 319
    - restricted Group Policies, 319–22
  - configuration management, overview, 249
  - event logs, 307
  - GPOs, creating and managing overview, 252–53
  - Group Policy Modeling Wizard, 306–07
  - loopback processing, 294–95
  - object management, 6
  - offline domain joins, 218
  - overview, 247–49
  - policy setting, 250–52
  - practice
    - audit policy, implementing, 375–79
    - configuring scope, 295–99, 307–11
    - delegating support, computers, 324–27
    - implementing, 271–75
    - security settings, managing, 346–51
    - software management, 362–64
  - Preferences, 264
  - processing, overview, 292–94

- refresh, 255
- registry policies, Administrative Templates, 265–71
- Resultant Set Of Policy (RSOP), 255–56, 303–06
- security settings
  - applying database settings to computer, 336
  - computer configuration, analyzing, 336–37
  - correcting discrepancies, 337–38
  - Local Security Policy, 331–32
  - overview, 330–31
  - Secedit.exe, 338–39
  - Security Configuration And Analysis, 335–36
  - Security Configuration Wizard, 339–45
  - security templates, 333–34
  - Security Templates snap-in, 334–35
  - security templates, deploying, 335
  - templates, creating, 338
- settings, implementing, 301–03
- slow links and disconnected systems, 256
- Software Settings, 262
- software, managing
  - AppLocker, 361–62
    - Group Policy Software Installation, overview, 353–56
    - maintaining applications, 359–60
    - overview, 353
    - SDP, preparing, 355–56
    - slow links, GPSI and, 360–61
    - software deployment GPO, creating, 356–58
    - software deployment GPO, scope, 358
  - troubleshooting, 306
  - updates, PDC Emulators, 531
  - User Configuration, policy settings, 262
  - Windows Settings, 262–63
- Group Policy Client, 281
- Group Policy Container (GPC), 260
- Group Policy Creator Owners group, 258–59
- Group Policy Management Console (GPMC)
  - certificate templates, configuring, 809
  - creating and managing GPOs, 252–53
  - overview, 666
  - software deployment GPO, creating, 356–58
- Group Policy Management Editor (GPME)
  - binding GPOs, PDC Emulator, 531
  - computer administration, delegating, 322
  - editing GPOs, 252
  - Members Of This Group setting, 322–24
  - overview, 250–51
- Group Policy Modeling Wizard, 303, 306–07
- Group Policy Object Editor (GPO Editor), 252, 331–32
- Group Policy Objects (GPOs)
  - AD DS administration categories, 660–62
  - computer accounts, 209–10
  - configuring scope, 253
  - creating, linking and editing, 252–53, 258–59
  - Default Domain Policy, 395
  - deploying security policies, 345
  - domain-based GPOs, 258
  - local GPOs, 256–57
  - managing GPOs and settings, 252–53, 259–60
  - overview, 11, 247–49
  - policy settings, 251–52
  - replication, 261–62
  - restricted Group Policies, 319–22
  - scope management
    - enabling and disabling GPOs, 290
    - GPO links, 278–80
    - inheritance and precedence, 280–85
    - overview, 278
    - security filtering, 285–88
    - targeting preferences, 291
    - WMI filters, 288–90
  - software deployment GPO, creating, 356–58
  - software deployment GPO, scope, 358
  - starter GPOs, 270–71
  - storage of, 260
  - updates, PDC Emulators, 531
  - updates, Specops Gpupdate, 662–63
- Group Policy Operational Log, 307
- Group Policy Preferences, 253, 323–24
- Group Policy Results Wizard, 303–05, 308
- Group Policy Slow Link Detection, 360–61
- Group Policy Software Installation (GPSI)
  - overview, 353–56
  - slow links and disconnected systems, 256, 360–61
  - software deployment options, 354–56
- Group Policy Template (GPT), 260
- Group Policy Verification Tool, 261–62
- Group Scope, 54
- Group tab, User Properties dialog box, 126
- GroupDN parameter, DSAdd, 175–76
- GroupDN parameter, DSMod, 166
- groups. *See also* passwords
  - accidental deletion, protecting from, 188–89
  - AD DS administration categories, 660–62
  - AD FS claims, 893–95
  - automating creation and management
    - changing membership, DSMod, 179
    - copying membership, 179
    - creating groups with DSAdd, 175–76
    - deleting groups, DSRm, 180–81
    - importing with CSVDE, 176–77
    - importing with LDIFDE, 177–78
    - moving and renaming, DSMove, 179–80
    - PowerShell, 181
    - retrieving membership, DSGet, 178
  - case scenario, group strategy, 202

## -h parameter, LDIFDE

### groups, *continued*

- computer accounts, deleting, 238–39
- computer accounts, resetting, 235–36
- converting scope and type, 165–66
- default groups, 194–96
- domain local groups, 161–62
- fine-grained passwords, 395–97
- global groups, 162–63
- group attributes, 186–87
- group objects, creating, 53–55
- group scope, overview, 160
- group types, 159–60
- importance of groups, 151–57
- local groups, 160–61
- membership, managing, 166–68, 189–93
- membership, migration and, 625–26
- naming conventions, 157–59
- overview, 149–51
- practice
  - adding users and computers, 69
  - administering in an enterprise, 197–99
  - automating creation and management, 181–85
  - creating and managing, 68, 171–72
- role-based management, overview, 154–57
- shadow groups, 193–94
- special identities, 196–97
- strategy for, 169–71
- Super Users group, 867–68
- tokenGroups attribute, 128
- Universal Group, AD RMS, 867–68
- universal groups, 163–64, 574–75
- workgroups, understanding, 207

## H

- h parameter, LDIFDE, 95–96
  - Handling Unspecified Services, 342
  - hash code, defined, 393
  - help desk, delegating support
    - Member Of settings, 322
    - Members Of This Group, 322–24
    - overview, 319
    - practice, delegating support, 324–27
    - restricted Group Policies, 319–22
  - help, LDIFDE, 95
  - high-availability. *See* directory business continuity
  - high-availability, DNS, 456
  - HKEY\_CURRENT\_USER (HKCU), 265
  - HKEY\_LOCAL\_MACHINE (HKLM), 265
  - Holme, Dan, 36, 88, 150, 206, 248, 318, 390–91, 508, 558, 606
  - home folder, User Properties dialog box, 126
  - Host (A or AAAA) records, DNS, 459
  - host name, Service Locator records, 567
  - HTTP, AD FS, 7
  - HTTPS, AD FS, 7
  - Hypertext Transfer Protocol (HTTP), 788–89
  - Hyper-V virtual machines
    - DNS configuration, 493
    - mounting virtual disks, 220–21
- ## I
- i parameter, CSVDE, 93, 177, 225
  - i parameter, LDIFDE, 177, 227
  - i switch, LDIFDE commands, 95
  - identity management. *See also* user accounts
    - Active Directory Domain Services (AD DS), 6
    - group management, 169–71
    - identity and access (IDA) infrastructure, 3–8
    - Identity Integration Feature Pack (IIFP), 739
    - Identity Metasystem Interoperability Protocol (IMIP), 890
    - Identity parameter, Get-ADGroupMember, 107
    - identity parameter, PowerShell cmdlets, 109
  - identity store, 3–4, 207
  - identity, defined, 3
  - Identity, Set-ADUser, 115
  - special identities, 196–97
  - IGDAL, group management mnemonic, 169–71
  - Immediately Uninstall The Software From Users And Computers, 360
  - importing
    - case scenario, importing user accounts, 145–46
    - computer files, 225–27
    - GPO settings, 260
    - groups, CSVDE, 176–77
    - groups, LDIFDE, 177–78
    - Import Policy, security templates, 335
    - Import Settings, GPMC, 260
    - practice
      - groups, 182–83
      - importing computers, 229–30
    - security templates, 335–36, 339
    - user accounts, CSVDE, 93–94
    - user accounts, LDIFDE, 94–96
    - user accounts, PowerShell, 116–17
  - Incremental Zone Transfer (IXFR), 457
  - inetOrgPerson, 609
  - Information Card, 890
  - Information Card Group policies, 891
  - infrastructure master role, 530
  - failure, 536

- identifying, 533
  - operations roles, returning, 538–39
  - placement, 533
  - inheritance
    - Active Directory object permissions, 76–77
    - Group Policy objects, 280–85
  - Initial Configuration Tasks, 17–19
  - Initials, user objects, 51
  - Install Windows Wizard, 14
  - installing, Active Directory Domain Services (AD DS)
    - domain controller, creating, 13
    - forests, preparation for, 12
    - identity and access (IDA) infrastructure, 3–8
    - Install-ADServiceAccount, 427–28
    - Installation From Media (IFM), 515, 520–21, 681–82
    - installation media, creating, 525
    - overview, 1–3
    - practice, creating forest, 14–21
    - practice, Server Core domain controller, 27–30
    - Server Core
      - adding AD DS, 27
      - configuration, 26–27
      - initial configuration tasks, 25–26
      - installation, overview, 23–24
      - procedure, 24–25
      - removing domain controllers, 27
      - using Windows interface, 12–13
  - Interactive group, special identities, 196–97
  - inter-forest migrations, 623–27
  - Internet Explorer Enhanced Security Configuration (IE ESC), 304–05
  - Internet Explorer Maintenance, 263
  - Internet Protocol (IP), configuring, 12
  - Internet Protocol Security (IPSec). *See also* Active Directory Certificate Services (AD CS)
    - Active Directory Certificate Services, 6–7
    - DNS Security (DNSSEC), 464
    - Security Configuration Wizard, 343
  - Inter-Site Messaging-Simple Mail Transport Protocol (ISM-SMTP), 588
  - intersite replication, configuring, 590–94
  - Intersite Topology Generator (ISTG), 586–88
  - Initial Configuration Tasks, 18–19
  - intra-forest migrations, 623–27
  - Intra-site Automatic Tunnel Addressing Protocol (ISATAP), 461
  - IP addresses. *See also* DNS (domain name system)
    - practice, configuring, 18
    - Security Configuration Wizard, 340
    - sites, managing domain controllers, 565–66
    - subnet objects, creating, 562–64
  - IP subnets, defining, 564
  - Ipconfig, 498, 666
  - IPSec. *See* Internet Protocol Security (IPsec)
  - IPv4, 25, 486, 491
  - IPv6, 445–46, 486
  - Itanium 2 processors, 2
  - item-level targeting, GPO scoping, 291
- ## J
- j path parameter, LDIFDE, 95
- ## K
- k parameter, CSVDE, 93, 177, 225
  - k parameter, LDIFDE, 177
  - Kellington, Jason, 2
  - Kerberos authentication
    - across domains in a forest, 630–32
    - Active Directory domains, 4
    - domain-based GPOs, 258
    - master time source, 531–32
    - multiple-domain forests, 621
    - Service Locator records, 566–68
    - service principal names (SPNs), 426
    - WAN links, branch offices, 410–11
    - within a domain, 630
  - Kerberos Key Distribution Center (KDC)
    - authentication within a domain, 630
    - domain controllers, 9
    - SVR records, 568
  - Kerberos Password protocol (KPASSWD), 567
  - Knowledge Consistency Checker (KCC)
    - AD DS administration categories, 660–62
    - GPO replication, 261–62
    - replication, configuring, 583–84
  - Ksetup, 666
  - Ktpass.exe, 666
- ## L
- l list parameter, LDIFDE, 96
  - l ListOfAttributes parameter, CSVDE, 93
  - LAN Diagnostic data collector, 714
  - LAN Manager, 343
  - language, central store policies, 270
  - lastLogonTimestamp, 609
  - LDAP. *See* Lightweight Directory Access Protocol (LDAP)
  - Ldifde.exe. *See also* Lightweight Directory Access Protocol Data Interchange Format (LDIF)
    - importing computers, 226–27
    - importing groups, 177–78
    - importing user files, 94–96
    - parameters for, 95
    - practice

Ldifde.exe, *continued*

- groups, importing, 183
- user account creation, 99–100
- resetting passwords, 137
- LDIFDE.exe, 666. *See also* Lightweight Directory Access Protocol Data Interchange Format (LDIF)
  - location and use, 748
  - migrating LDAP to AD LDS instances, 754
- Ldp.exe, 666
- LDP.exe
  - AD LDS instances, 758
  - location and use, 748
  - restoring deleted objects, 675–76
- legacy directory applications,
  - migration of, 740
- legacy DNS, 455
- licensing management, 843–44. *See also* Active Directory Rights Management Services (AD RMS)
- Lightweight Directory Access Protocol (LDAP)
  - attribute names, importing computers, 225
  - IDA infrastructure, 6
  - importing computers with LDIFDE, 226–27
  - LDAP Data Interchange Format (LDIF), 94–96, 748
  - ldapDisplayName, New-ADUser, 113–14
  - name syntax, 115
  - registry settings, 343
  - Service Locator records, 566–68
- Lightweight Directory Access Protocol Data Interchange Format (LDIF). *See also* LDIFDE.exe
  - importing groups, 177–78
  - LDIF, AD LDS default files, 751
- limit switch, Dsquery, 63
- links
  - creating, 57
  - Group Policy objects (GPOs), 253, 278–80, 283–85
  - intersite replication, configuring, 590–94
  - Link-local addresses, 445–46
  - link-local cloud, PNRP, 447
  - password settings objects (PSOs), 398
  - site links, configuring replication, 586–88
  - sites and subnets, overview of, 559–60
- ListOfAttributes parameter, CSVDE, 93
- load balancing, bridgehead servers, 588–89
- loc parameter, DSAdd, 227
- Local Computer GPO, 257
- local computers, Resultant Set Of Policy (RSOP), 303–06
- local Group Policy objects (GPOs), 256–57, 292
- Local Group preferences, 323–24
- local groups, overview, 160–61, 164
- Local Policies, security templates, 333
- local profiles, migration and, 625

- Local Security Authority Subsystem (LSASS), 624
- Local Security Policy, 331–32, 338, 346
- Local Service, 425
- Local System, 425
- locals parameter, Djoin.exe, 219
- Location For Database, Log Files, And SYSVOL, 21
- locator records, 566–69
- log files
  - account logon, auditing, 404
  - AD CS, common events, 815
  - AD LDS, 752
  - audit policies, 368
  - auditing directory changes, 671
  - Event Viewer, overview, 710–12
  - failed events, auditing, 371
  - Group Policy, 293–94, 307
  - IDA infrastructure, 6
  - LDIFDE, location of, 95
  - location, 21
  - managing computers, 234
  - practice, Group Policy logs, 309
  - Security log, viewing events, 375
- Logically-deleted objects, 672–75
- logoff
  - Group Policy scripts, 262–63
  - Group Policy update, 255
- logoff switch, Gpupdate.exe, 255, 302–03
- logon. *See also* Active Directory Certificate Services (AD CS); also passwords; sAMAccountName
  - account lockout policies, overview, 394
  - Audit Account Logon Events, 368
  - auditing authentication
    - account logon and logon events, 404
    - logon events, viewing, 407
    - overview, 404
    - policies, configuring, 405–06
    - scoping policies, 406
  - computers, configuring, 234
  - DSAdd User, account creation, 92
  - error messages, 235
  - failed events, auditing, 369
  - group membership changes, 168
  - Group Policy scripts, 262–63
  - Group Policy, inheritance, 281
  - Group Policy, settings, 302
  - Log On As Service, 428
  - Log On To, user account properties, 134
  - Logon Hours, 134
  - logon script, User Properties dialog box, 126
  - managed service accounts, 428
  - practice, authentication auditing, 407–08
  - Smart Card Is Required For Interactive Logon, 135
  - unlocking accounts, 137–38

- User Logon Name, 51–52, 132
- User Properties dialog box, 126
- loopback processing, Group Policy, 294–95, 298–99
- Loopback, IPv6 addresses, 446
- loose coupling, 581
- LostandFound, 662
- LostandFoundConfig, 662

## M

- machine certificate, 848
- machineOU parameter, Djoin.exe, 219
- mail exchanger (MX), DNS record types, 459
- Main.xml, 341
- maintenance
  - AD DS administration categories, 660–62
  - AD DS administration tools, overview, 664–67
  - AD Recycle Bin, 672–75
  - auditing directory changes, 671
  - built-in protection measures, overview, 669–70
  - domain controllers, removing, 27
  - offline maintenance, 669
  - online maintenance, 667
  - overview, 658–59
  - practice, working with AD DS database, 698–705
  - protecting AD DS objects, 670–71
  - protecting DCs as virtual machines, 697–98
  - Quest Object Restore For Active Directory, 676–78
  - restore
    - data set selection, 689–91
    - deleted objects, LDP.exe, 675–76
    - DSRM, 688–89
    - from complete backup, 694–97
    - nonauthoritative or authoritative, 692–94
    - overview, 687–88
  - Specops Gpupdate, 662–63
  - Windows Server Backup, protection from, 678–87
- malware, 41–42. *See also* security
- Manage, Active Directory Users And Computers, 234
- Managed By
  - computer objects, 56
  - creating links, 57
  - group objects, 55, 189–91
  - organizational units, creating, 50
- managed policy settings, registry, 267–68
- managed service accounts
  - creating and configuring, 427
  - delegations and passwords, 428–29
  - installing and using, 427–28
  - overview, 426
  - practice creating, 429–32
  - requirements, 426–27
  - managedBy, 232–33
  - man-in-the-middle attacks, 464–65
  - master browser, PDC Emulator, 532
  - master time source, 531–32
  - Maximum Password Age, 392
  - Md, New-Item cmdlet, 113
  - membership
    - domain local groups, 161
    - global groups, 162
    - groups, overview, 160
    - local groups, 161
    - Member attribute, groups, 168
    - Member Of tab, Computer Properties, 233, 320–22
    - Member Of tab, Group Properties, 166–67
    - Member Of tab, User Properties, 126
    - memberOf attribute, DSGet, 178
    - memberof GroupDN, DSAdd, 176
    - memberof parameter, DSGet, 178
    - memberOf, group attribute, 128, 168, 530
    - members MemberDN, DSAdd, 176
    - Members Of This Group, Computer Configuration, 320–24
    - Members tab, Group Properties, 166–67
    - universal groups, 163
  - metadata, account domain joins, 219
  - metadata, federation, 890
  - Microsoft Exchange Server 2007, round robin, DNS, 456
  - Microsoft Exchange, global address list (GAL), 133
  - Microsoft Management Console (MMC)
    - Attribute Editor, 127–28
    - creating custom MMC console, 40–41
    - custom console, saving and distributing, 42–43
    - local GPOs, creating, 257
    - overview, 37–39
    - Security Templates snap-in, 334–35
  - Microsoft Office Access
    - exporting user files, CSVDE, 92–93
    - importing users, CSVDE, 93–94
    - importing users, PowerShell, 116–17
  - Microsoft SQL Server
    - AD FS configuration database, 893
    - managed service accounts, 429
  - Microsoft Windows NT 4.0
    - primary domain controllers (PDCs), 528
  - migration
    - AD RMS to Windows Server 2008 R2, 853–55
    - LDAP to AD LDS instances, 754
    - legacy directory applications, 740
    - objects, between domains and forests, 623–27
    - SYSVOL replication, 544–46
    - SYSVOL replication, practice, 547–51
- Minimum Password Age, 393
- Minimum Password Length, 392

MMC. See Microsoft Management Console (MMC)

mobile users

- AD RMS, configuring, 863
- domain controller location, 568

mounting disk drives, new computers, 220–21

mounting tool, database recovery, 689–91

Move Server, 566

Movetree.exe, 666

moving computers, 233–34

moving objects, between domains and forests, 623–27

msDS-DeletedObjectLifetime, 673

msDS-MachineAccountQuota, 215–17

msDS-ManagedServiceAccount, 428–29

msDS-ResultantPSO, 398

multimaster replication, 581. *See also* replication

Multiple Names Found, 58

mustchpwd parameter, DSAdd User, 92

MX record, creating, 488

## N

Name column, Active Directory Users And Computers, 132

-Name parameter, New-ADUser, 113–14

name recursion, DNS, 455

name resolution, process for, 452–59. *See also* DNS (domain name system)

names

- Active Directory partitions, 572
- AD LDS instances, 749–50
- aliases, PowerShell cmdlets, 111–12
- computer accounts, renaming, 236–37
- DNs, RDNs, and CNs, 63
- domain naming context, 572
- groups, conventions for, 157–59
- groups, moving and renaming, 179–80
- managed service accounts, 427
- multiple-domain forests, 621
- name switch, Dsquery, 63–64
- NetBIOS names, 12, 456, 460, 512
- practice, creating single-label names, 500–01
- renaming computers, DSMove, 233–34
- renaming GPOs, 260
- servers, AD CS deployment, 786
- service name, SVR record, 567–68
- service principal names (SPNs), 426
- single-label name management, 490–92
- user accounts, 89
- user objects, 51–52, 57–58, 131–33

namespaces

- PowerShell, 112
- WMI filters, GPO scope management, 288–90

navigation

- domains, Active Directory Administrative Center, 118
- partitions, PowerShell cmdlets, 113

nesting, groups, 169–71, 178

Net user administrator, 25

NetBIOS names, 12, 456, 460, 512

NetDom

- computer accounts, renaming, 237
- creating computers, 227–28
- operations masters, identifying, 535
- secure channel, reset, 236

Netdom.exe

- computer accounts, joining to domains, 213
- domain controller rename, 608
- domains, joining, 26
- overview, 666

NetLogon, 234

NETLOGON Event ID 3210

- Failed to Authenticate, 235

Netsh interface ipv4, 25

Network Access Protection (NAP), 789–90

network attached storage (NAS) device, 158

Network Device Enrollment Service (NDES), 780

Network group, special identities, 196–97

Network Interface

- Bytes Total/Sec, 714
- Packets Outbound Discarded, 714

network links, sites and subnets, 559–60

network logon, auditing, 404

Network Policy Server (NPS), 807

network prefix notation, subnet objects, 564

network proxy server settings, 461

Network Security, Security Configuration Wizard, 342

Network Service, 425

network topology, management of, 39

network traffic, Group Policy settings, 263

networked services, administration of, 660–62

New Object-Computer Wizard, 211

New Object-User Wizard, 125–29

New Zone Wizard, 472–73

New-ADComputer, 228

New-ADFSClaimRuleSet, 894–95

New-ADGroup, 181

New-ADServiceAccount, 427

New-ADUser, 113–14

-newname parameter, DSMove, 180, 233–34

-newparent parameter, DSMove, 180, 233–34

NewPassword, DSMod, 137

NLTest, secure channel reset, 236

Nltest.exe, 666

Non-Administrators GPO, 257

nonauthoritative restores, 692–94

- non-MSI application files (.zap), 354
- noprompt parameter, DSRm, 180
- notification, intrasite replication, 584–85
- Nslookup, 498, 666
- NTDS
  - DRA Inbound Bytes Total/Sec, 714
  - DRA Inbound Object Updates Remaining In Packet, 714
  - DRA Outbound Bytes Total/Sec, 715
  - DRA Pending Replication synchronizations, 715
  - DS Threads in Use, 715
  - LDAP Bind Time, 715
  - LDAP Client Sessions, 715
  - LDAP Searches/Sec, 715
  - LDAP Successful Binds/Sec, 715
  - LDAP Writes/Sec, 715
- Ntds.dit, 9, 12
- NTDS.dit, 453
- NTDSUtil, 534
- Ntdsutil.exe
  - Installation From Media data set creation, 681–82
  - installation media, creating, 521
  - location and use, 749
  - operation master roles, seizing, 537
  - overview, 666
  - practice, capturing system state data, 698–99
  - snapshots, creating, 689–91

## O

- o list parameter, LDIFDE, 96
- o switch, Dsquery, 64
- o upn switch, Dsquery, 64
- objects
  - case scenario, organizational units, 84–85
  - computer objects, creating, 55–56
  - creating
    - group objects, 53–55
    - organizational units, 49–51
    - overview, 49
    - user objects, 51–53
  - delegation and security
    - ACLs, viewing, 73–74
    - administrative task delegation, 77–78
    - effective permissions, 79–80
    - organizational unit design for, 80–81
    - overview, 72–73
    - permissions and access rights, 75–76
    - permissions and inheritance, 76–77
    - permissions, removing or resetting, 78–79
    - permissions, reporting and viewing, 78
  - finding objects, 57–62
  - managing
    - Active Directory Domain Services (AD DS), 6
    - user accounts, PowerShell commands, 108
  - migration workarounds, 626
  - names, understanding, 63
  - object type, DS commands, 91–92
  - ObjectDN parameter, DSMove, 180
  - ObjectDN parameter, DSRm, 180, 239
  - objectType, Dsquery, 64
  - practice
    - administrative task delegation, 81–82
    - creating and locating objects in Active Directory, 64–70
    - finding objects, 69–70
    - protecting AD DS objects, 670–71
    - Quest Object Restore For Active Directory, 676–78
    - restoring deleted objects, LDP.exe, 675–76
  - Ocllist.exe, 26
  - Ocsetup.exe, 26
  - OCSP Response Signing Certificate, 810–14
  - offline domain joins, 217–21
  - one-way function, defined, 393
  - Online Certificate Status Protocol (OCSP), 779–80
  - online responder
    - certificate validation, 779–80
    - configuring, 810–14
    - location and function, 814
    - Oobe.exe, 18–19
  - operating system, reinstalling, 234–35
  - operations masters
    - domain-wide operation master roles, 529–32
    - failures, recognizing, 536
    - forest-wide operation master roles, 529
    - identifying, 533–35
    - overview, 527
    - placement, 532–33
    - practice transferring, 539–41
    - returning roles, 538–39
    - seizing roles, 536–37
    - single master operations, 527–28
    - transferring, 535–36
  - Operations tokens, 527–28
  - Organizational tab, User Properties dialog box, 126
  - organizational units (OU)
    - case scenario, management and delegation, 84–85
    - computer accounts, 208–10
    - creating, 49–51
    - creating, practice, 64–65, 221–22
    - GPO links, 278–80
    - Group Policy processing, overview, 292
    - groups, creating and naming, 157–59
    - navigation, PowerShell cmdlets, 113
    - overview, 11

## **-p SearchScope parameter, CSVDE**

organizational units (OU), *continued*  
password setting objects (PSOs) and, 398–99  
permission inheritance, 76–77  
shadow groups, 193–94

## **P**

-p SearchScope parameter, CSVDE, 93  
-p SearchScope parameter, LDIFDE, 96  
partial attribute set (PAS), 8–9, 573, 582. *See also* global catalog (GC)

### partitions

Active Directory data store, 8  
AD LDS instances, 751  
application directory partitions, 494–96, 576–77  
data store, 582  
global catalog, configuring, 572–73  
navigating, PowerShell cmdlets, 113  
partitionfqdn, 495  
practice, replication and directory partitions, 577–79  
Server Core domain controller installation, 28

### passwords. *See also* authentication

Active Directory authentication, 4  
Active Directory domains, default password, 66  
administrators, 25, 28  
complexity requirements, 392  
computer accounts  
  joining to domains, 213  
  recycling, 239  
  resetting, 235–36  
  restore from backup, 235  
computer objects, 55  
Create A Password Reset Disk, 17  
Directory Services Restore Mode Administrator Password, 21  
disabling and enabling user accounts, 135, 138  
domain service accounts, 425  
domain-based GPOs, 258  
DSAdd User, account creation, 92  
importing users, LDIFDE, 96  
Kerberos Password protocol (KPASSWD), 567  
LM hash values, 343  
lockout policies  
  domain passwords, 395  
  fine-grained passwords, lockout policy, 395–97  
  overview, 392–94  
  password settings objects (PSO), 397  
  practice, configuring, 399–402  
  PSO precedence and resultant PSO, 398  
  PSOs and organizational units, 398–99  
managed service accounts, 428–29  
migration, 626

Password Must Meet Complexity Requirements, 392  
Password Never Expires, 135, 395, 397  
password replication policy (PRP)  
  configuring, 416–17  
  practice configuring, 421  
  read-only domain controllers (RODC), 411–12  
  RODC credentials caching, administering, 418–19  
resetting, 136–37  
security principals, 133  
Set-ADAccountPassword, 115–16  
Store Password Using Reversible Encryption, 135  
trusts, manual, 635  
unlocking user accounts, 137–38  
updates, PDC Emulator, 531  
User Cannot Change Password, 134  
User Must Change Password At Next Logon, 134  
user objects, creating, 52  
  User Properties dialog box, 126  
Paste command, GPMC, 259  
patch (.msp) files, 353–54  
-Path parameter, New-ADServiceAccount, 427  
-Path parameter, New-ADUser, 114  
PathToWindowsFolder, 220  
PDC Emulator  
  AD DS administration categories, 660–62  
  failure, 536  
  identifying, 533  
  multi-site domains, editing GPOs, 259  
  operations roles, returning, 538–39  
  role, overview, 531–32  
Peer Name Resolution Protocol (PNRP), 446–47  
performance. *See also* directory business continuity  
  baselines, AD DS and DNS, 717–18  
  Event Viewer, 710–12  
  overview, 707  
  practice, AD DS performance analysis, 721–27  
  Reliability Monitor, 712–13  
  site planning, 560–62  
  slow links, 360–61  
  system resources, overview, 707–08  
  Task Manager, 708–10  
  Windows Performance Monitor, 713–17  
  Windows System Resource Manager (WSRM), 718–21  
  WMI filters, 290  
Performance Log Users, 713–14  
permissions. *See also* groups  
  Active Directory objects  
    assigning permission, 75–76  
    effective permissions, 79–80  
    finding objects, 57  
    inheritance and, 76–77  
    removing or resetting, 78–79  
    reporting and viewing permissions, 78

- Create Child-Allow, 218
- create computers, permission delegation, 210
- create computers, permission restriction, 215–17
- creating GPOs, 258–59
- default groups, 195–96
- delegation, understanding, 72–73
- deny permissions, options for, 671
- DNS application directory partition replication, 414
- GPO scope management, 285–86
- group membership, management of, 191–93
- group objects, creating, 53–55
- groups, converting scope and type, 165
- joining computers to domains, 212–13
- migration, 624–25
- moving computers, 233–34
- special identities, 196–97
- phantoms of the directory, 530
- pipeline
  - group membership, copying, 179
  - GroupDN, DSAdd, 175–76
  - multiple DNs to DSMod, 129–30
  - overview, 109–11
  - pipe character ( | ), PowerShell, 109–11
- PKI. *See* public key infrastructure (PKI)
- PKIView, 815–17
- PNRP (Peer Name Resolution Protocol), 446–47
- pointer (PTR), DNS record types, 459
- policies. *See also* Group Policy
  - Active Directory administration, 8
  - AD RMS templates, 7, 868–70
  - authentication audit policies, configuring, 405–06
  - default password, Active Directory, 66
  - Information Card Group policies, 891
  - password lockout
    - configuring, practice, 399–402
    - fine-grain passwords, 395–97
    - overview, 392–94
    - password settings objects (PSO), 397
    - PSOs and organizational units, 398–99
  - Policy Events tab, Group Policy Results Wizard, 305
  - Policy-Based QoS, Group Policy settings, 262–63
  - rights policy template, practice creating, 872–73
- polling
  - intersite replication, 593
  - intrasite replication, 585
- ports
  - AD FS, 881
  - AD LDS instances, 750
  - DNS socket pool, 465–66
  - DNS, port 53, 440
  - HTTP, 7
  - HTTPS, 7
  - Service Locator records, 567–68
  - TCP/IP, 7
  - TCP/UDP port 53 traffic, 464
- PowerShell
  - AD CD support, 814
  - AD FS configuration database, 892
  - AD FS, managing, 905–07
  - AD LDS instances, working with, 760–61
  - AD RMS installing and administering, 854–55
  - additional resources, 117
  - cmdlets, overview, 105–07
  - computers
    - attributes, configuring, 233
    - creating, 228
    - moving, 234
    - practice creating, 230
  - DNS administration, 499
  - Get-Help, 107–08
  - groups, managing, 181
  - groups, practice managing, 181–82
  - location and function, 814
  - managed service accounts
    - creating and configuring, 427
    - installing, 427–28
    - requirements, 426–27
  - overview, 667
  - restore objects, 675
  - service accounts, managing, 425
  - user account administration
    - Active Directory Administrative Center, overview, 117–20
    - Active Directory PowerShell provider, 113
    - Active Directory, preparing, 103–05
    - aliases, 111–12
    - cmdlet parameters, 107
    - creating users, 113–14
    - importing users from database, 116–17
    - managing user attributes, 131
    - namespaces, providers, PSDrives, 112
    - objects, 108
    - overview, 102–03
    - pipeline, overview, 109–11
    - practice, creating users, 120–23
    - resetting passwords, 137
    - user attributes, populating, 115–16
    - variables, 108–09
- practice
  - Active Directory, creating and locating objects, 64–70
  - AD CS, configuring and using, 819–26
  - AD DS database, protecting and managing, 698–705
  - AD DS performance analysis, 721–27
  - AD FS, finalizing configuration, 907–15
  - AD FS, preparing for deployment, 900–02
  - AD LDS, installing, 743–45

## precedence, Group Policy objects

### practice, *continued*

- AD RMS, installing, 855–60
- audit policy, implementing, 375–79
- creating computers and joining domains, 221–23
- DNS server configuration, 499–501
- DNS service, installing, 468–77
- domain and forest functional levels, raising, 614–16
- domain controllers, deploying, 522–25
- Group Policy implementation, 271–75
- Group Policy, configuring, 295–99
- groups, administering in an enterprise, 197–99
- groups, creating and managing, 171–72
- replication and directory partitions, 577–79
- replication, configuring, 596–98
- security settings, managing, 346–51
- software management, Group Policy, 362–64
- SYSVOL replication, configuring, 546–51
- trust relationships, administering, 645–49
  - user objects and accounts, supporting, 140–43
- precedence, Group Policy objects, 280–85
- preferences, GPOs, 291, 323–24
- preferred bridgehead servers, 589–90
- prestaging, computer accounts, 210–11, 214
- Prevent Access To Registry Editing Tools, 251–52, 268–69
- primary DNS servers, 448
- primary domain controllers (PDCs), 528
- primary federation server, defined, 890
- primary zones, DNS, 455, 457
- Print Operators group, 194–96
- printers
  - permissions, migration, 625
  - resource management, 39
- processors, Windows Server 2008 R2 support, 2
- profile path, User Properties dialog box, 126
- Profile tab, User Properties dialog box, 126
- Promotion, dcpromo, 511
- properties
  - objects, defined, 108
  - security principal accounts, 133
  - user accounts, viewing, 90
- Properties parameter, Get-ADUser, 131
- Properties parameter, Get-NewADUser, 114
- property permissions, Active Directory objects, 75–76
- Protect Container From Accidental Deletion, 50
- Protected groups, overview, 195–96
- providers, PowerShell, 112–13
- provision parameter, Djoin.exe, 218
- PSDrives, PowerShell, 112
- PTR record, 485
- public key infrastructure (PKI)
  - Active Directory Certificate Services (AD CS),
    - overview, 6–7, 771–80
    - AD CS, installing, 791–93

- AD CS, new features, 788–90
- case scenario, managing certificate
  - revocation, 829–30
- configuring AD CS
  - Enterprise PKI, 815–17
  - issuing certificate authority, 804–10
  - management tools, AD CS, 814–16
  - online responder, 810–14
  - overview, 804
  - protecting the configuration, 818
  - revocation configuration, creating, 805–06
  - templates, 806–10
- deployment, additional resources, 786
- practice
  - AD CS, configuring and using, 819–26
  - installing a CA hierarchy, 793–801
- publishing applications, 355–56
- publishing license, 841, 849. *See also* Active Directory Rights Management Services (AD RMS)
- pull replication, 581–82
- pwd parameter, DSAdd User, 92

## Q

### queries

- Active Directory, 8
- Find Objects In Active Directory Domain Services, 60–61
- Resultant Set Of Policy (RSOP), 303–06
- saved queries, Active Directory Users and Computers, 61–62
- Quest Object Restore For Active Directory, 676–78
- quotation marks, CSVDE importing groups, 176

## R

- r Filter parameter, CSVDE, 93
- RAC (rights account certificates), 848
- RDN (relative distinguished name), 63, 132
- read-only DNS servers, 448, 460
- read-only domain controllers (RODC)
  - AD DS administration categories, 660–62
  - administrative role separation, 419
  - creating, 511
  - deploying a RODC, 412–16
  - domain controller placement, branch
    - offices, 410–11
  - domain controllers, installing, 515
  - installation, staging, 518–20
  - overview, 410–12
  - password replication policy (PRP), configuring, 416–17

- practice, configuring RODCs, 419–22
  - replicas and, 572
  - RODC credentials caching, 418–19
  - RODCPrep, 414, 514
  - read-write DNS servers, 448
  - realm trusts, 632–35, 638
  - reboot, Group Policy update, 255
  - recovery, disaster. *See* business continuity
  - Recycle Bin
    - enabling in AD LDS, 754–55
    - overview, 672–75
    - recovering deleted groups, 188
  - Recycled object, 672–75
  - recycling computer accounts, 239
  - Redeploy Application, 359–60
  - Redircmp.exe, 215
  - Redirusr.exe, 215
  - redundancy, DNS configuration, 493
  - refresh
    - computer and user settings for, 294
    - Computer Configuration settings, 262
    - GPOs, enabling and disabling, 290
    - Group Policy objects and, 260
    - Group Policy settings, implementing, 302–03
    - slow links and, 360–61
  - Regedit.exe
    - GPO inheritance and precedence, 282
    - policy settings, templates, 268–69
    - Prevent Access To Registry Editing Tools, 251–52
  - registry
    - backup, 681
    - DNS devolution, 467
    - GPO inheritance and precedence, 282
    - Group Policy settings, 265–71
    - permissions, migrating, 625
    - settings, security policy, 341
  - Registry Editor
    - Allow and Deny rules, 361
    - GPO inheritance and precedence, 282
    - policy settings, templates, 268–69
    - Prevent Access To Registry Editing Tools, 251–52
  - Registry Permissions, security templates, 333
  - Registry Settings, Security Configuration Wizard, 343
  - Registry Values, Security Templates, 334–35
  - registry-based Group Policy settings, 263
  - relational databases, vs. LDAP directories, 736
  - relative distinguished name (RDN), 63, 132
  - Reliability Monitor, 712–13
  - Relying party trust, defined, 891
  - Relying party, defined, 891
  - remote computers and users. *See also* branch offices
    - Group Policy refresh, 256
    - NetDom and firewalls, 213
  - Remote access, User Properties dialog box, 127
  - Remote Control tab, User Properties dialog box, 126–27
  - Remote Desktop, 26
  - Remote Desktop Services (Terminal Services), 294–95
  - Remote Desktop Users group, 194–96
  - Remote Installation Services (RIS), 263
  - Remote Installation Services, settings, 263
  - Remote Server Administration Tools (RAST)
    - download, 104
    - Group Policy preferences settings, 264
    - installing, 39
  - Resultant Set Of Policy (RSOP), 303–06
  - server placement, site planning, 562
  - site domain controllers, installing, 513–15
  - Specops Gpupdate, 662–63
  - virtual machines, loopback processing, 294–95
- removable devices, AD CS deployment, 785
  - Remove Software, 360
  - Remove-ADComputer, 228
  - Remove-ADGroup, 181
  - Remove-ADGroupMember, 181
  - Remove-ADServiceAccount, 427
  - Remove-ADUser, 139
  - Rename command, GPMC, 260
  - RepAdmin.exe, 594–96, 666, 749
  - replicas, naming contexts, 572
  - replication
    - Active Directory, 8
    - AD DS administration categories, 660–62
    - application directory partitions, DNS, 454
    - configuring
      - bridgehead servers, 588–90
      - connection objects, 582–83
      - intersite replication, 590–94
      - intrasite replication, 584–85
      - Knowledge Consistency Checker, 583–84
      - monitoring replication, 594–96
      - overview, 581–82
      - site links, 586–88
    - domain local groups, 161
    - forward lookup zones (FLZ), updates, 482–84
    - global catalog and application directory partitions
      - application directory partitions, overview, 576–77
      - global catalog server placement, 573
      - global catalog server, configuring, 574
      - overview, 572–73
      - Universal group membership caching, 574–75
    - global groups, 162
    - Group Policy objects (GPOs), 259, 261–62, 301–03
    - groups, 160–61
    - management of, 39
    - new domain controllers, adprep, 515
    - overview, 557–58

## reporting

### replication, *continued*

- password replication policy, RODC, 411–12
  - password updates, PDC Emulator, 531
  - practice
    - AD LDS instances, working with, 763–65
    - configuring replication, 596–98
    - replication and directory partitions, 577–79
  - Replication Diagnostics tool (Repadmin.exe), 594–96
  - ReplicationSourcePath, 521
  - restoring data, 670
  - signed zones and records, DNS, 464
  - single master operations, 527–28
  - sites and subnets, configuring
    - domain controller location, 566–69
    - domain controllers, managing, 565–66
    - overview, 559–60
    - planning sites, 560–62
    - practice configuring, 569–70
  - SYSVOL, configuring
    - domain functional levels, raising, 543–44
    - migration, 544–46
    - overview, 543
    - practice, 546–51
  - transport protocols, 588
  - universal groups, 163
- reporting
- AD DS administration categories, 662
  - Resultant Set Of Policy (RSOP), 303–06
- requestODJ, Djoin.exe, 219–20
- Reset Account Lockout Counter After, 394
- Reset parameter, SetADAccountPassword, 115–16
- resetting user passwords, 136–37
- resource management
- Active Directory, 8
  - Active Directory Users and Computers, overview, 39
  - AD DS administration categories, 660–62
  - Event Viewer, 710–12
  - group management strategy, 169
  - group objects, creating, 53–55
  - performance baselines, AD DS and DNS, 717–18
  - resource federation server, defined, 891
  - Resource Monitor, 708–10
  - resource partner organizations, defined, 891
  - resource records, DNS, 455
  - system resources, overview, 707–08
  - Task Manager, 708–10
  - user access, trusted domains, 640–44
  - Windows System Resource Manager (WSRM), 718–21
- responsible person record, creating, 484–85
- Responsible Person, DNS zone configuration, 483–84
- restore
- AD Recycle Bin, 672–75
  - computer accounts, troubleshooting, 235
  - data set selection, 689–91
  - from complete backup, 694–97
  - nonauthoritative or authoritative restores, 692–94
  - overview, 687–88
  - Quest Object Restore For Active Directory, 676–78
  - Windows Server Backup, protection from, 678–87
- Restore From Backup command, GPMC, 260
- Restore-ADObject, 675
- restricted Group Policies, 319–22
- Restricted Groups, security templates, 333
- Resultant Set Of Policy (RSOP)
- Group Policy Modeling Wizard, 306–07
  - local GPOs, 257
  - overview, 255–56, 303–06
- reuse parameter, Djoin.exe, 218
- reverse lookup zones (RLZ), creating, 462–63, 485–87
- reverse lookup, DNS, 455
- domain configuration, online responder, 812–14
- revocation policy, certificates, 787
- RID master
- failure, 536–37
  - identifying, 533
  - overview, 529
  - placement, 532
  - returning roles, 538
- rights account certificates (RAC), 841, 848.
- See also* Active Directory Rights Management Services (AD RMS)
- Rights Management Services. *See* Active Directory Rights Management Services (AD RMS)
- rights policy template, practice, creating, 872–73
- rmmber parameter, DSMod, 179
- RODC. *See* read-only domain controllers (RODC)
- RODCPrep, 414, 514
- role groups, defined, 157
- role groups, overview, 162–63
- role-base access control (RBAC), 80
- role-based management, overview, 154–57
- Role-Based Service Configuration, 341
- roles, displaying, 26
- roles, Security Configuration Wizard, 340
- root hints, DNS, 456, 488–90
- round robin, DNS, 456
- router discover, 461
- Ruest, Danielle, 442–43, 656–57, 734–35, 776–77, 836–37, 883–84
- Ruest, Nelson, 442–43, 656–57, 734–35, 776–77, 836–37, 883–84
- rule groups, defined, 157
- Run As Administrator, 41–42
- Run Only Specified Windows Applications, 265

## S

- s servername parameter, LDIFDE, 95
- SACL. *See* security access control lists (SACLs)
- sAMAccountName. *See also* logon
  - adding groups, DSAdd, 176
  - group membership changes DSMod, 179
  - groups, naming, 158
  - importing computers, CSVDE, 225
  - logon and secure channel, understanding, 234
  - managed service accounts, 427
  - overview, 131–32
  - renaming accounts, 133
- samid parameter, DSAdd, 176, 227
- samid parameter, DSGet, 131
- samid parameter, DSMod, 179
- samid, overview, 131–32
- SAML (Security Assertion Markup Language), defined, 891
- SAML security token, defined, 891
- Save Report, GPMC, 260
- saved queries, 61–62
- savefile parameter, Djoin.exe, 219
- Sc.exe, 425
- scalability, groups and, 153
- scavenging, configuring, 482
- schema
  - Active Directory, registering, 40
  - AD DS administration categories, 660–62
  - ADSchemaAnalyzer.exe, 748
  - failure, 537
  - forest-wide operations master roles, 529
  - identifying, 533
  - naming context, 572
  - overview, 8
  - placement of operations master, 532–33
  - returning roles, 538
  - Schema Admins group, 194–96
- sconfig.exe, 26–27
- scope. *See also* groups
  - authentication audit policies, 406
  - Group Policy objects (GPOs), 253
  - Group Policy, managing
    - enabling and disabling GPOs, 290
    - GPO links, 278–80
    - Group Policy processing, overview, 292–94
    - inheritance and precedence, 280–85
    - overview, 278
    - practice configuring, 295–99, 307–11
    - security filtering, 285–88
    - targeting preferences, 291
    - WMI filters, 288–90
  - software deployment GPO, 358
  - scope parameter, DSAdd, 176
  - scope parameter, DSMod, 166
  - scoped delegation, 72–73
  - Scripts, Group Policy settings, 262–63
  - SCWAudit.inf, 343
  - scwcmd.exe, 339, 345
  - SDP, preparing, 355–56
  - search
    - d RootDN parameter, LDIFDE, 96
    - Find Objects In Active Directory Domain Services, 60–61
    - Global Search, Active Directory Administrative Center (ADAC), 120
    - p SearchScope parameter, LDIFDE, 96
    - r Filter parameter, LDIFDE, 96
    - SearchScope, CSVDE, 93
    - SearchScope, LDIFDE, 96
  - Secedit.exe, 303, 338–39
  - secgrp parameter, DSAdd, 176
  - secgrp parameter, DSMod, 166
  - secondary DNS servers, 448
  - secondary zone, DNS, 456–57
  - Secure Hypertext Transfer Protocol (HTTPS), 773
  - Secure Multipurpose Internet Mail Extensions (S/MIME).
    - See* Active Directory Certificate Services (AD CS)
  - Secure Sockets Layer (SSL)
    - AD RMS installation scenarios, 843–44
    - DNS Security (DNSSEC), 464
    - IDA infrastructure, 6
    - server authentication certificate, AD FS, 895
  - Secure Sockets Tunneling Protocol (SSTP). *See* Active Directory Certificate Services (AD CS)
  - security. *See also* Active Directory Certificate Services (AD CS); authentication
    - Active Directory objects
      - ACLs, viewing, 73–74
      - administrative task delegation, 77–78
      - case scenario, organizational units, 84–85
      - delegation, understanding, 72–73
      - effective permissions, 79–80
      - organizational unit design for delegation, 80–81
      - overview, 72
      - permissions and access rights, 75–76
      - permissions and inheritance, 76–77
      - permissions, removing or resetting, 78–79
      - permissions, reporting and viewing, 78
      - practice, administrative task delegation, 81–82
    - AD DS administration categories, 660–62
    - administrative tools with alternate credentials, 41–42
    - case scenario
      - administrative account security, 435
      - configuring security, 383–84
    - computer account creation and joins, 214–17
    - DNS, configuring, 480–81
    - DNS, new features, 461, 463–67

## security access control lists (SACLs)

### security, *continued*

- domain and forest design, 621
- failed events, auditing, 371
- filtering, GPO scope, 285–88
- group objects, 53
- Group Policy settings
  - applying database settings to computer, 336
  - computer configuration, analyzing, 336–37
  - correcting discrepancies, 337–38
  - Local Security Policy, 331–32
  - overview, 330–31
  - Secedit.exe, 338–39
  - Security Configuration And Analysis, 335–36
  - security templates, 333–35
  - Security Templates snap-in, 334–35
  - templates, creating, 338
- groups, 165, 188–89
- Read-Only-Domain Controllers (RODC), 518–20
- Security Configuration Wizard
  - applying policies, 344
  - creating security policy, 340–44
  - deploying policies, 345
  - editing policies, 344
  - modifying settings, 345
  - overview, 339–40
  - rolling back policies, 344
  - security settings, practice managing, 346–51
  - Server Core installation, AD DS, 23
- security access control lists (SACLs), 5
- Security Accounts Manager (SAM)
  - local groups, 160–61
  - trusts within domains, 627
  - workgroups, domains, and trusts, 207
- Security Assertion Markup Language (SAML), defined, 891
- Security Configuration And Analysis snap-in, 335–37, 347–49
- Security Configuration Wizard
  - applying policies, 344
  - creating security policy, 340–44
  - deploying policies, 345
  - editing policies, 344
  - modifying settings, 345
  - overview, 339–40
  - practice using, 349–50
  - rolling back policies, 344
- security descriptor (SD), 624–25
- security groups, 53
- security identifier (SID)
  - computer accounts, deleting, 238–39
  - computer accounts, joining to domains, 213
  - computer accounts, resetting, 235–36
  - domain quarantine, 641
  - generation, RID master role, 529
  - groups, deleting, 180, 188–89
  - groups, understanding, 151–57
  - migration and, 624–25
  - overview, 3–4
  - phantom objects, 530
  - tokenGroup attribute, 128
- Security log, auditing, 373, 407
- Security Policy File Name, 343
- security principals
  - account properties, 133
  - delegation, understanding, 72–73
  - generation, RID master role, 529
  - migration, 624–25
- Security Settings, Group Policy, 262–63
- Security Settings, local GPOs, 256–57
- Security System-Wide Statistics
  - Kerberos Authentication, 715
  - NTLM Authentication, 715
- Security tab, object properties, 73–74
- security templates, 333–35, 346–47
- Security Templates snap-in, 334–35
- security translation, 625
- Select Additional Services, 342
- Select Users, Contacts, Computers Or Groups, 57–59
- selective authentication, 609, 642–44
- self-signed certificates, 851
- server authentication certificate, AD FS, 895
- Server Configuration tool, 26–27
- Server Core
  - Active Directory Domain Services installation
    - adding AD DS, 27
    - initial configuration tasks, 25–26
    - overview, 23
    - procedure for, 24–25
    - removing domain controllers, 27
    - server configuration, 26–27
  - overview of, 23–24
  - practice, installing Server Core domain controller, 27–30
- server licenser certificate (SLC), 840, 848, 864
- Server Manager
  - Add Roles, 13
  - Event Log, 710–12
  - global name zone creation, 490–92
  - location and use, 749
  - overview, 666
- server message block (SMB), 343
- server name, Server Core, 29
- Server Operators group, 194–96
- server scavenging, DNS, 456
- servers
  - bridgehead servers, 588–90, 593
  - placement, site planning, 562

- sites, managing domain controllers, 566
- service accounts, managed
  - AD LDS instances, 751
  - creating and configuring, 427
  - delegations and passwords, 428–29
  - installing and using, 427–28
  - migration, 626
  - overview, 425–26
  - practice creating, 429–32
  - requirements, 426–27
  - service placement, site planning, 560–62
- Service Communication Certificate, 895
- Service Configuration Manager (SCM)
  - managed service accounts
    - creating and configuring, 427
    - delegations and passwords, 428–29
    - installing and using, 427–28
    - requirements, 426–27
  - overview, 425–26
  - practice, creating managed service accounts, 429–32
- service localization, overview, 560
- service location, DNS record types, 459
- Service Locator (SRV), 566–69
- service packs, patch (.msp) files, 353–54
- service principal names (SPNs), 426
- service ticket, 4, 410–11
- ServicePrincipalName, 427
- services
  - password policies, 397
  - placement, site planning, 560–62
  - Security Configuration Wizard, 340–41
- SeServiceLogonRight, 428
- Session tab, User Properties dialog box, 126–27
- Set Forest Functional Level, 21
- Set-ADAccountPassword, 115–16
- Set-ADComputer, 228
- Set-ADFSSynchProperties, 892
- Set-ADGroup, 181
- Set-ADServiceAccount, 427
- Set-ADUser
  - managing user attributes, 131
  - resetting passwords, 137
  - user attributes, populating, 115–16
  - variables, 109
- setglobalstate, Dfsrmig.exe, 545–46
- Settings tab, Group Policy Results Wizards, 305
- setup command, GPSI, 354
- shadow groups, 193–94, 398–99
- shared access
  - Active Directory Federation Services, 7
  - permissions, migrating, 625
- shared folders, 39, 53–55
- SharePoint Online, 887
- shortcut trusts, 632–35
- shortcuts, Find Objects In Active Directory Domain Services, 61
- Show/Hide Action Pane, MMC, 37–38
- Show/Hide Console Tree, MMC, 37–38
- shutdown, Group Policy scripts, 262–63
- SID. *See* security identifier (SID)
- sidHistory, 624–25, 641
- signatures, digital. *See* Active Directory Certificate Services (AD CS)
- signing certificates, online responder, 810–14
- Simple Authentication And Security Layer (SASL), 95
- Simple Certificate Enrollment Protocol (SCEP), 780
- Simple Mail Transport Protocol (STMP), 588
- single master operations, 527–28
- Single master roles, 527–28
- single sign on (SSO), 7
- single-label names, DNS, 456, 460, 491–92, 500–01
- singlelabelname, 491
- site links, configuring replication, 586–88, 590–94
- site links, practice, creating, 597
- site management
  - case scenario, configuring sites and subnets, 602–03
  - global catalog and application directory partitions
    - application directory partitions,
      - overview, 576–77
    - global catalog server placement, 573
    - global catalog server, configuring, 574
    - overview of, 572–73
    - Universal group membership caching, 574–75
  - overview, 11, 557–58
  - practice
    - replication and directory partitions, 577–79
    - replication, configuring, 596–98
- replication, configuring
  - bridgehead servers, 588–90
  - connection objects, 582–83
  - intersite replication, 590–94
  - intrasite replication, 584–85
  - Knowledge Consistency Checker, 583–84
  - monitoring replication, 594–96
  - overview, 581–82
  - site links, 586–88
- sites and subnets, configuring
  - creating sites, 562–64
  - domain controller location, 566–69
  - domain controllers, managing, 565–66
  - overview, 559–60
  - planning sites, 560–62
  - practice configuring, 569–70
- site object, creating, 562–64
- site-link bridges, 591
- site-linked GPOs, 278–80, 292

## Site-local addresses

- Site-local addresses, 445–46
- siteName, SVR record, 568
- SLC (server licensor certificate), 840, 848, 864
- slow links, 256, 360–61
- smart card authentication. *See also* Active Directory Certificate Services (AD CS)
  - Active Directory Certificate Services, 6–7
  - certificate templates, configuring, 807
  - Smart Card Is Required For Interactive Logon, 135
- snap-ins, Active Directory
  - adding administrative tools to Start menu, 40
  - administration tools, 39
  - custom MMC console, creating, 40–41
  - custom MMC, saving and distributing, 42–43
  - Microsoft Management Console, using, 37–39
  - overview, 37
  - practice, creating and managing custom MMC, 44–47
  - tools with alternate credentials, 41–42
- snapshots, creating, 689–91
- socket pool, DNS, 465–66
- software distribution point (SDP), 354
- Software Installation, Group Policy settings, 262
- Software Restriction Policy (SRP), 361
- Software Settings, Group Policy settings, 262
- software, managing
  - AppLocker, 361–62
  - case scenario, software installation, 383
  - Group Policy Software Installation
    - overview, 353–56
    - software deployment options, 354–56
  - maintaining applications, Group Policy, 359–60
  - overview, 353
  - practice, management with Group Policy, 362–64
  - SDP, preparing, 355–56
  - slow links, GPSI and, 360–61
  - software deployment GPO, creating, 356–58
  - software deployment GPO, scope, 358
- Source Domain Controller, 516
- Source Domain Controller, adprep, 515
- Special Operations Software, Specops
  - Gpupdate, 662–63
- Specops Gpupdate, 662–63
- spoofing, protection against, 461, 464–65
- SQL Server
  - AD FS configuration database, 893
  - managed service accounts, 429
- SRV records, creating, 488
- SSL. *See* Secure Sockets Layer (SSL)
- Start menu
  - adding administrative tools, 40
  - custom MMC consoles, saving, 43
- Start Of Authority (SOA), 456, 483
- starter GPOs, 270–71
- startup
  - Always Wait For The Network At Computer Startup, 255
  - Group Policy processing, overview, 292–94
  - Group Policy settings, 302
  - Group Policy, inheritance, 281
  - scripts, Group Policy, 262–63
  - service startup policies, 342
- storage, Group Policy objects (GPOs), 260
- Store Password Using Reversible Encryption, 135, 393, 395
- store-and-forward replication, 582
- stub zone, DNS, 457–58
- subnet objects, creating, 562–64
- subtree parameter, DSRm, 180
- Summary tab, Group Policy Results Wizard, 304–05
- Super Users group, 867–68
- support, delegating
  - Member Of settings, 322
  - Members Of This Group, 322–24
  - overview, 319
  - practice, delegating, 324–27
  - restricted Group Policies, 319–22
- synchronizing
  - AD FS, 892, 897
  - data, AD DS to AD LDS, 748
  - timestamps, 531–32
- system access control list (SACL)
  - Active Directory service changes, auditing, 374–75
  - Audit Directory Services Access, 368
  - delegation, overview, 72–73
  - file and folder access, auditing, 370–73
  - migration, 624–25
- System and Application logs, Group Policy, 307
- System Diagnostic data collector, 714
- System log, Group Policy events, 307
- System Monitor, 499, 667
- System Performance data collector, 714
- system resources. *See* resource management
- System Services, security templates, 333
- system state data, backup, 681
- SYSVOL
  - AD DS, installing from media, 520–21
  - backup, 681
  - central store, 269–70
  - DFS-R, 508
  - GPO replication, 261–62
  - GPO storage, 260
  - location, installing, 12, 21
  - replication, configuring, 609
    - domain functional levels, raising, 543–44
    - migration, 544–46
    - overview, 543
    - practice, 546–51

## T

- tab completion, PowerShell cmdlets, 113
- tab expansion, PowerShell cmdlets, 113
- targeted preferences, Group Policy, 253, 302–03
- TargetOUDN, 139–40
- Task Manager, 708–10
- tattooing, 267–68
- TCP/IP. *See also* DNS (domain name system)
  - ports, Active Directory Federation Services, 7
  - practice, Server Core post-installation configuration, 29
  - service location, 459
- TCP/UDP port 53 traffic, 464
- Telephones tab, User Properties dialog box, 126
- templates
  - Active Directory Certificate Services (AD CS), configuring, 806–10
  - Active Directory Certificate Services (AD CS), online responder, 810–14
  - AD FS claim rule templates, 894–95
  - AD RMS Template Administrators, 840
  - AD RMS templates, configuring, 868–70
  - AD RMS usage policy, 7
  - Administrative Templates, overview, 268–69
  - Data Collector Set, 714
  - practice
    - rights policy template, creating, 872–73
    - security templates, creating, 346–47
  - Security Templates snap-in, 334–35
  - security templates, Group Policy, 333–35, 346–47
  - user account creation, 89–91
  - user account creation, practice, 97–98
- Terminal Services, 294–95
- Terminal Services Profile tab, User Properties dialog box, 126–27
- tick mark ( ` ), PowerShell, 110
- ticket granting ticket (TGT), 4, 630
- timeout value, Group Policy settings, 262–63
- timestamps, 531–32, 609
- Time-To-Live (TTL), DNS, 454, 457, 481–85
- tokenGroups attribute, 128, 530
- tokens
  - AD FS certificates, 895
  - migration and, 624–25
- tombstone containers, 676–78
- tombstone feature, Recycle Bin, 672–75
- tombstone interval, groups, 188
- tombstone lifetime, defined, 139
- tombstoneLifetime, 673
- topology, site links, 586–88
- traffic, managing, 263
- transform (.mst) files, 353–54
- Transmission Control Protocol/Internet Protocol (TCP/IP). *See* TCP/IP
- transport protocols, replication, 588
- tree, overview, 10
- troubleshooting
  - GPO replication, Gpoutil.exe, 261–62
  - Group Policy, 306–07
  - operations master failures, 536
  - Resultant Set Of Policy (RSOP), 303–06
- trust flow, 630–32
- trust path, 630–32
- trusts. *See also* Active Directory Federation Services (AD FS)
  - Account Is Trusted For Delegation, 135
  - AD RMS, configuring, 863–64
  - administration of, 39
  - DNS Security (DNSSEC), 464
  - domains, managing
    - administering trusts, 639–40
    - authentication protocols, 629–30
    - dedicated forest root domain, 618
    - Kerberos, across domains in a forest, 630–32
    - Kerberos, within a domain, 630
    - manual trusts, 632–35
    - moving objects, domains and forests, 623–27
    - multiple trees, 622
    - multiple-domain forest, 620–22
    - overview, 618
    - shortcut trusts, 636–39
    - single-domain forest, 619–20
    - trust relationships, overview, 629–30
    - trusts between domains, 627–28
    - trusts within domains, 627
    - users, resource access, 640–44
  - practice, administering relationships, 645–49
  - workgroups and, 207

## U

- UGDLA, 169
- Ultrasound.exe, 667
- unattended installations
  - AD LDS instance creation, 753–54
  - additional resources, 27
  - domain controllers, 510–11
- unicodePwd attribute, 96
- Uninstall This Application When It Falls Out Of The Scope Of Management, 360
- Uninstall-ADServiceAccount, 428
- UninstallBinaries, 522

## universal groups

### universal groups

- configuring, 867–68
  - management strategy, 169
  - membership caching, 574–75
  - objects, creating, 54
  - overview, 163–64
  - universal group membership caching (UGMC), 574–75, 578–79
- UNIX commands, PowerShell aliases, 112
- Unlock-ADAccount, 138
- unmanaged policy settings, registry, 267–68
- Unspecified addresses, IPv6, 446
- updates/upgrades
- AD RMS, 844
  - certificate authority, 806
  - DNS records, dynamic updates, 485
  - forests, 414
  - forward lookup zone (FLZ) replication, 482–84
  - Group Policy refresh, 255, 302–03
  - passwords, PDC Emulator, 531
  - patch (.msp) files, 353–54
  - software deployment GPOs, 358–60, 362–64
  - Specops Gpupdate, 662–63
  - Start of Authority (SOA) record, DNS, 456
- URLs, AD RMS, 863
- usage policy templates, 7
- Use Advanced Mode Installation, adprep, 515
- use license, overview, 849
- UseExistingAccount, dcpromo, 511, 519
- user accounts. *See also* groups
- account properties, 133
  - Active Directory Users and Computers, overview, 39
  - AD DS administration categories, 660–62
  - AD FS claims, 893–95
  - AD RMS exclusion policies, configuring, 865–67
  - AD RMS, configuring, 867–68
  - adding to groups, 57
  - administration, overview, 87–88
  - attributes, managing with DSMod and DSGet, 129–31
  - attributes, managing with PowerShell, 131
  - authentication, Active Directory Federation Services, 7
  - case scenario, importing user accounts, 145–46
  - creating
    - Active Directory command-line tools, overview, 91–92
    - automation, practice, 97–100
    - command line tools, 91–92
    - DSAdd, 92
    - exporting users with CSVDE, 92–93
    - importing with CSVDE, 93–94
    - importing with LDIFDE, 94–96
    - templates and, 89–91
  - deleting accounts, 138–39
  - disabling and enabling accounts, 138
  - moving accounts, 139–40
  - overview, 135–36
  - password settings, 395
  - passwords, resetting, 136–37
  - PowerShell, administering with
    - Active Directory Administrative Center, overview, 117–20
    - Active Directory PowerShell provider, 113
    - aliases, 111–12
    - cmdlet parameters, 107
    - cmdlets, overview, 105–07
    - creating users, 113–14
    - Get-Help, 107–08
    - importing users from database, 116–17
    - namespace providers, PSDrives, 112
    - objects, 108
    - overview, 102–03
    - pipeline, overview, 109–11
    - practice, creating users, 120–23
    - preparing Active Directory, 103–05
    - user attributes, populating, 115–16
    - variables, 108–09
  - practice
    - adding to groups, 69
    - creating in organizational units, 65–67
    - supporting user objects and accounts, 140–43
  - read-only domain controllers (RODC), 411–12
  - reassign vs. recreate, 669–70
  - renaming, 133
  - resource access, trusted domains, 640–44
  - rights
    - domain-based GPOs, 258
    - migration and, 625
    - site planning and, 561–62
  - unlocking accounts, 137–38
  - user attributes, managing, 125–29
  - user object names, 131–33
  - user settings, defined, 250–51
- User Cannot Change Password, 134
- user configuration settings, defined, 250–51
- User Configuration, Group Policy Administrative Templates, 263
- enabling and disabling GPOs, 290
  - group membership, defining, 323–24
  - policy settings, 262
  - Preferences, 264
  - registry policy settings, 265
  - Windows Settings, 262–63
- User Group Policy Loopback Processing Mode, 294–95

- User Logon Name, 51–52, 131–32
- user logs, Group Policy processing, 293–94
- User Mode-Full Access, 42–43
- User Mode-Limited Access, 42–43
- User Must Change Password At Next Logon, 52, 134
- user objects. *See* objects
- user principal name (UPN), 51–52, 64, 893–95
- userAccountControl, 225
- UserDN, DSMod, 129
  - disabling and enabling user accounts, 138
  - piping multiple DNs, 129–30
  - renaming accounts, 133
  - resetting passwords, 137
- userPassword, 609
- userPrincipalName, 132
- userWorkstations attribute, 134

## V

- v parameter, LDIFDE, 95
- validation
  - administering trusts, 639–40
  - online responder, 779–80
  - security templates, 339
- variables, PowerShell cmdlets, 108–09
- verbose mode, LDIFDE, 95
- View Security Policy, 344
- virtual desktop infrastructure (VDI), 294–95
- virtual hard disks, for backup, 685
- virtual machines
  - AD CS deployment, 785
  - loopback processing, Group Policy, 294–95
  - mounting virtual disks, 220–21
  - protecting DCs as virtual machines, 697–98
- virtual private networks (VPNs), AD CS, 6–7
- virtualization
  - AD LDS installation, 741–42
  - DNS configuration, 493

## W

- W32tm.exe, 667
- WAN links, 410–11
- Wbadmin.exe, backups, 684–87
- web browsers, spoofing protection, 461
- Web Enrollment, certificates, 779
- Web Proxy Automatic Discovery (WPAD), 461
- Web Server
  - backup, 681
  - certificate templates, configuring, 808
- Web Services, Active Directory (ADWS), 104–05

- Web Services, AD CS, 788–89
- Web services, defined, 891
- Web SSO, 886–88
- web-based authentication, AD CS, 6–7
- wildcards, Find Objects In Active Directory Domain Services, 61
- Win32Time service, 531–32
- Windows 2000
  - domain functional levels, raising, 543–44, 608
  - forest functional levels, 611
  - Gpresult.exe, 305–06
  - local GPOs, 256–57
- Windows 2000 Server
  - DNS, 456
  - domain controllers, installing, 513–15
- Windows 7
  - AppLocker and, 362
  - Peer Name Resolution Protocol (PNRP), 446–47
  - Start menu, adding tools to, 40
- Windows Azure, federation, 887
- Windows Boot Manager, DSRM restarts, 688–89
- Windows DNS Service, IP configuration, 12
- Windows Firewall
  - NetDom, remote use, 213
  - RSOP analysis, 304
- Windows Firewall With Advanced Security, 342–43
- Windows Installer, 353–54
- Windows Internet Name Service (WINS), 455
- Windows Live ID, 863–64
- Windows Management Instrumentation (WMI) filters, 253, 288–90
- Windows NT 4.0, 531–32
- Windows Performance Monitor, 713–17
- Windows PowerShell. *See* PowerShell
- Windows Reliability and Performance Monitor (WRPM), 713–17
- Windows Resource Protection files, 681
- Windows Server, 25
- Windows Server 2003
  - domain controllers, installing, 513–15
  - domain functional levels, raising, 543–44, 608–09
  - forest functional levels, 611–13
  - Group Policy refresh, 256
  - local GPOs, 256–57
  - managed service accounts, 426
  - zone delegations, DNS, 457
- Windows Server 2008
  - domain functional levels, raising, 543–44
  - Group Policy, 253
  - local GPOs, 257
  - placing on domain controllers, 414
- Windows Server 2008 R2
  - Active Directory Administrative Center (ADAC), 117–20

## Windows Server Backup

### Windows Server 2008 R2, *continued*

- Active Directory Certificate Services, new features, 788–90
  - AD LDS, new features, 740–41
  - AD RMS, moving to, 853–55
  - administrative templates, 268–69
  - AppLocker and, 362
  - child domain, installing, 516
  - DNS features, 459–61, 463–67
  - domain controllers, installing, 513–15
  - domain functional levels, 609–10
  - forest functional levels, 613
  - Global Name Zones (GNZ), 455
  - Group Policy event logs, 307
  - Group Policy preferences settings, 264, 291
  - Group Policy refresh, 256
  - legacy DNS, 455
  - managed service accounts, 426
  - Peer Name Resolution Protocol (PNRP), 446–47
  - placing on domain controllers, 414
  - practice
    - forests, installing, 19–21
    - installing, 14–17
  - processors, 2
  - read-only DNS servers, 448
  - Resultant Set Of Policy (RSOP), 303–06
  - root hints, DNS, 456
  - Security Configuration And Analysis snap-in, 335–36
  - Security Templates snap-in, 334–35
  - single-label names, DNS, 456
  - zone delegations, DNS, 457–59
- ### Windows Server Backup
- full system backup, 682–87
  - Installation From Media data, 681–82
  - location and use, 749
  - overview, 667, 678–80
  - system state only, 681
- ### Windows Server Network Access Protection (NAP), 789–90
- ### Windows Settings, Group Policy, 262–63
- ### Windows System Resource Manager (WSRM), 718–21
- ### Windows Vista
- administrative templates, 268–69
  - Group Policy event logs, 307
  - Group Policy preferences settings, 264, 291
  - Group Policy refresh, 256
  - local GPOs, 257
  - Software Restriction Policy, 361
  - Start menu, adding tools to, 40

### Windows XP

- Group Policy refresh, 256
  - local GPOs, 256–57
  - Software Restriction Policy, 361
- ### WINS service, removal of, 460
- ### WINS, DNS and, 491–92
- ### wireless networks
- Active Directory Certificate Services, 6–7
  - certificate templates, configuring, 807
- ### wizards. *See also* Active Directory Domain Services Installation Wizard
- Active Directory Lightweight Directory Services Setup Wizard, 749–55
  - Add Roles Wizard, 13, 509–10
  - Backup Once Wizard, 682
  - Certification Authority Backup Wizard, 818
  - Copy Object User Wizard, 89
  - Delegation of Control Wizard, 77–78
  - Exclude User Account Wizard, 866
  - Group Policy Modeling Wizard, 303, 306–07
  - Group Policy Results Wizard, 303–05, 308
  - Install Windows Wizard, 14
  - New Object-Computer Wizard, 211
  - New Object-User Wizard, 125–29
  - New Zone Wizard, 472–73
  - Security Configuration Wizard, 339–45, 349–50
- ### WMI (Windows Management Instrumentation)
- GPO scope management, 288–90
  - Group Policy objects, scope of, 253
- ### workgroups, understanding, 207
- ### WS Federation, defined, 891
- ### WS-Federation Passive Requestor Profile (WS-F PRP), 885

## X

- x64 processors, 2
- x86 processors, 2
- XML Notepad, 358, 362–64
- XML Web Services-based protocols, 104–05

## Z

- zone delegations, DNS, 457, 471–73
- zone loading, background, 460
- zone scavenging, DNS, 457, 482
- zone transfers, DNS, 457

# About the Authors



**DAN HOLME** is a graduate of Yale University and Thunderbird with more than 17 years of experience as a consultant and trainer to Fortune-caliber clientele implementing Windows and SharePoint technologies. Among the highlights of his career is his role as Microsoft Technologies Consultant for NBC Olympics during the Olympic Games in Vancouver, Beijing, and Torino. In addition to penning best-selling books for Microsoft Press, Dan is a contributing editor for *Windows IT Pro* and *SharePoint Pro* magazines as well as the community lead of SharePointProMag.com. Each year, Dan reaches hundreds of thousands of IT professionals and business decision makers. His efforts have earned him the prestigious title of Microsoft MVP (Windows Server Directory Services, 2007, and SharePoint Server, 2008–2011). He has also been recognized as one of the top 50 SharePoint influencers and one of the top 10 partner MVPs in the world. As the Chief SharePoint Evangelist for AvePoint, Dan works tirelessly to solve customers' IT business challenges, educate the global community, and develop solutions that will set the standard for the next generation of collaboration platforms. When the work and travel stop, Dan can be found on his home base, Maui, with Wyatt, Keith, Maddie, Jack, and the entire *ohana*, to whom this book is dedicated.



**DANIELLE RUEST** and **NELSON RUEST** are technology futurists focused on infrastructure design and optimization as well as continued service delivery. They have been working with complex infrastructures for more than 20 years. Their systems designs include core application deployments such as email and collaboration. They have also been working with virtualization for more than 10 years.

Their recent books include *MCITP Self-Paced Training Kit (Exam 70-238): Deploying Messaging Solutions with Microsoft Exchange Server 2007* (<http://www.microsoft.com/learning/en/us/book.aspx?ID=10938&locale=en-us>); *Virtualization: A Beginner's Guide* ([http://www.amazon.com/Virtualization-Beginners-Guide/dp/007161401X/ref=bxgy\\_cc\\_b\\_img\\_a](http://www.amazon.com/Virtualization-Beginners-Guide/dp/007161401X/ref=bxgy_cc_b_img_a)); a look at comprehensive virtualization infrastructure designs; and *MCTS Self-Paced Training Kit (Exam 70-652): Configuring Windows Server Virtualization* (<http://www.microsoft.com/learning/en/us/Book.aspx?ID=13695&locale=en-us#tab1>). They both work for Resolutions Enterprises Ltd. ([www.reso-net.com](http://www.reso-net.com)).



**JASON KELLINGTON, MCT, MCSE, MCITP, MCTS**, is a consultant, trainer, and author living in beautiful, cold northern Canada with his wife and two boys. Jason has spent time as an engineer, developer, administrator, and educator during his 15+ years in IT. His consulting and training practice specialize in enterprise infrastructure deployment as well as data management and business intelligence. He has assisted in the development of several projects with Microsoft Press and Microsoft Learning.