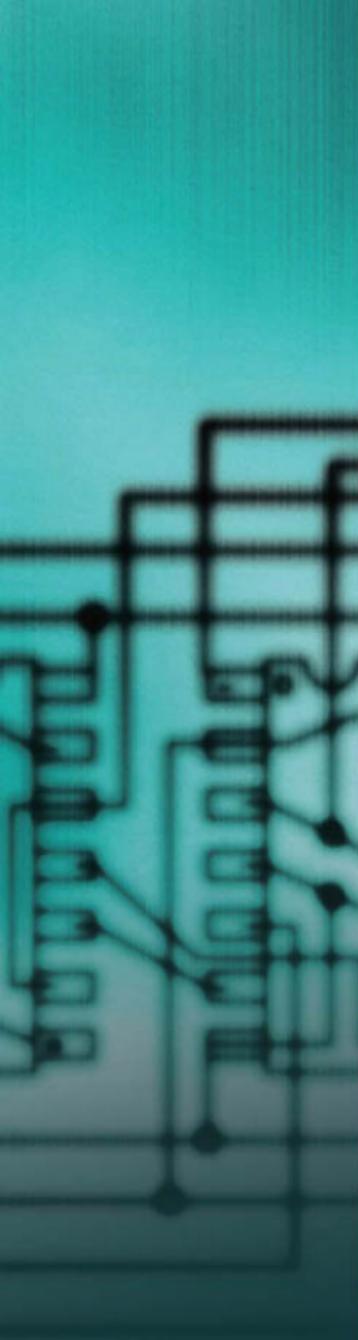


N E T W O R K I N G



MCTS Guide to Configuring Microsoft® Windows Server® 2008 Active Directory

Gregory Tomsho

MCTS
MCITP

Exam #70-640

Microsoft Certification Exam Objectives

Exam #70-640: Windows Server 2008

Active Directory, Configuring

Objective	Chapter
Configuring Domain Name System (DNS) for Active Directory	
Configure zones	9
Configure DNS server settings	9
Configure zone transfers and replication	9
Configuring the Active Directory Infrastructure	
Configure a forest or a domain	4, 10
Configure trusts	4, 10
Configure sites	4, 10
Configure Active Directory replication	4, 10
Configure the global catalog	4, 10
Configure operations masters	4, 10
Configuring Additional Active Directory Server Roles	
Configure Active Directory Lightweight Directory Services (AD LDS)	12
Configure Active Directory Rights Management Service (AD RMS)	12
Configure the read-only domain controller (RODC)	12
Configure Active Directory Federation Services (AD FS)	12
Creating and Maintaining Active Directory Objects	
Automate creation of Active Directory accounts	3, 5
Maintain Active Directory accounts	4, 5
Create and apply Group Policy objects (GPOs)	3, 7
Configure GPO templates	7
Configure software deployment GPOs	7
Configure account policies	3, 7
Configure audit policy by using GPOs	7
Maintaining the Active Directory Environment	
Configure backup and recovery	13
Perform offline maintenance	13
Monitor Active Directory	13
Configuring Active Directory Certificate Services	
Install Active Directory Certificate Services	11
Configure CA server settings	11
Manage certificate templates	11
Manage enrollments	11
Manage certificate revocations	11

This book is intended to be sold with a CD-ROM. If this book does not contain a CD-ROM, you are not getting the full value of your purchase.

This CD-ROM contains CertBlaster® software from DTI Publishing. The unlock code for the CertBlaster questions is: c_640 (case sensitive).

If the disks/CDs in this book are missing or if the package containing them has been opened, this book is not returnable. By opening and breaking the seal on this package, you are agreeing to be bound by the following agreement:

The software included with this product may be copyrighted, in which case all rights are reserved by the respective copyright holder. You are licensed to use software copyrighted by the Publisher and its licensor on a single computer. You may copy and/or modify the software as needed to facilitate your use of it on a single computer. Making copies of the software for any other purpose is a violation of the United States copyright laws.

This software is sold as is without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Neither the publisher nor its dealers or distributors assume any liability for any alleged or actual damages arising from the use of this program. (Some states do not allow for the excusing of implied warranties, so the exclusion may not apply to you.)



MCTS Guide to

Microsoft Windows Server 2008 Active Directory Configuration

This page intentionally left blank

MCTS Guide to **Microsoft Windows Server 2008 Active Directory Configuration**

Greg Tomsho



Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

MCTS Guide to Microsoft Windows Server 2008

Active Directory Configuration

Greg Tomsho

Vice President, Career and Professional Editorial:
Dave Garza

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Acquisitions Editor: Nick Lombardi

Senior Product Manager: Michelle Ruelos Cannistraci

Developmental Editor: Lisa M. Lord

Editorial Assistant: Sarah Pickering

Vice President, Career and Professional Marketing:
Jennifer McAvey

Marketing Director: Deborah S. Yarnell

Senior Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Jessica McNavich

Design Assistant: Hannah Wellman

Cover Designer: Robert Pehlke

Manufacturing Coordinator: Denise Powers

Copyeditor: Kathy Orrino

Proofreader: John Bosco

Composer: International Typesetting
and Composition

© 2010 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product,
submit all requests online at www.cengage.com/permissions

Further permissions questions can be emailed
to www.permissionrequest@cengage.com

Example: Microsoft® is a registered trademark of the Microsoft Corporation.

Library of Congress Control Number: 2008943783

ISBN-13: 978-1-423-90235-5

ISBN-10: 1-423-90235-1

Course Technology

20 Channel Center

Boston, MA 02210

USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: www.international.cengage.com/region

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit www.course.cengage.com

Visit our corporate website at www.cengage.com

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Microsoft and the Office logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Course Technology, a part of Cengage Learning, is an independent entity from the Microsoft Corporation, and not affiliated with Microsoft in any manner.

Any fictional data related to persons or companies or URLs used throughout this book is intended for instructional purposes only. At the time this book was printed, any such data was fictional and not belonging to any real persons or companies.

Course Technology and the Course Technology logo are registered trademarks used under license.

Course Technology, a part of Cengage Learning, reserves the right to revise this publication and make changes from time to time in its content without notice.

The programs in this book are for instructional purposes only. They have been tested with care, but are not guaranteed for any particular intent beyond educational purposes. The author and the publisher do not offer any warranties or representations, nor do they accept any liabilities with respect to the programs.

Brief Contents

INTRODUCTION	xv
CHAPTER 1	
Introducing Windows Server 2008	1
CHAPTER 2	
Installing Windows Server 2008	37
CHAPTER 3	
Introducing Active Directory	75
CHAPTER 4	
Active Directory Design and Security Concepts	111
CHAPTER 5	
Account Management	151
CHAPTER 6	
Windows File and Print Services	201
CHAPTER 7	
Configuring Group Policy	253
CHAPTER 8	
Introduction to Windows Networking	319
CHAPTER 9	
Configuring DNS for Active Directory	353
CHAPTER 10	
Configuring and Maintaining the Active Directory Infrastructure	397
CHAPTER 11	
Active Directory Certificate Services	449
CHAPTER 12	
Additional Active Directory Server Roles	485
CHAPTER 13	
Server Management and Monitoring	515
APPENDIX A	
MCTS 70-640 Exam Objectives	553
APPENDIX B	
Windows Server 2008 Active Directory Configuration Resources	557
APPENDIX C	
Virtual Machine Instructions for Selected Activities	561
APPENDIX D	
A Step-by-Step Guide to Using Server Virtualization Software	571
GLOSSARY	607
INDEX	613

This page intentionally left blank

Contents

INTRODUCTION	xv
CHAPTER 1	
Introducing Windows Server 2008	1
The Role of a Server Operating System	2
Server: Hardware or Software?	2
Server Operating System Versus Desktop Operating System	2
Windows Server 2008 Editions	3
Standard Edition	4
Enterprise Edition	4
Datacenter Edition	4
Windows Web Server 2008	5
Comparing Editions	5
Windows Server 2008 Core Technologies	6
NTFS	6
Active Directory	8
Microsoft Management Console	8
Disk Management	10
File and Printer Sharing	12
Windows Networking Concepts	13
Windows Networking Components	14
Internet Information Services	17
Windows Server 2008 Roles	19
Active Directory Certificate Services	19
Active Directory Domain Services	19
Other Active Directory Related Roles	20
Application Server	20
DHCP Server	20
DNS Server	20
Fax Server	20
File Services	20
Hyper-V	21
Network Policy and Access Services	21
Print Services	21
Terminal Services	22
UDDI Services	22
Web Server (IIS)	22
Windows Deployment Services	22
New Features in Windows Server 2008	22
Server Manager	23
Server Core	24
Hyper-V	25
Storage Management Enhancements	27
Networking Enhancements	28
Network Access Protection	28
Windows Deployment Services	29
New Active Directory Roles	29
Terminal Services Enhancements	29
Chapter Summary	31
Key Terms	31
Review Questions	32
Case Projects	36
CHAPTER 2	
Installing Windows Server 2008	37
Planning a Windows Server 2008 Installation	38
Installing the First Server in a New Network	38
Expanding Your Network	51
Upgrading to Windows Server 2008	53

Server Core: Windows That Doesn't Do Windows	53
Windows Server Installation and Postinstallation Tasks	54
When Not to Use Server Core	60
Virtualize Your Server with Hyper-V	60
Reviewing the Benefits of Virtualization	62
Creating Virtual Machines with Hyper-V	63
Basic Virtual Machine Management with Hyper-V Manager	66
Chapter Summary	69
Key Terms	70
Review Questions	70
Case Projects	74
 CHAPTER 3	
Introducing Active Directory	75
The Role of a Directory Service	76
Windows Active Directory	76
Overview of the Active Directory Structure	77
Installing Active Directory	80
What's Inside Active Directory?	82
The Active Directory Schema	83
Active Directory Container Objects	84
Active Directory Leaf Objects	86
Locating Active Directory Objects	91
Introducing Group Policies	96
The Computer Configuration Node	97
The User Configuration Node	98
How Group Policies Are Applied	101
Chapter Summary	104
Key Terms	105
Review Questions	106
Case Projects	108
 CHAPTER 4	
Active Directory Design and Security Concepts	111
Working with Organizational Units	112
OU Delegation of Control	115
Active Directory Object Permissions	117
Working with Forests, Trees, and Domains	126
Active Directory Terminology	126
The Role of Forests	130
Understanding Trusts	134
Understanding Domains and Trees	138
Understanding Sites	139
Site Components	141
Chapter Summary	143
Key Terms	144
Review Questions	145
Case Projects	148
 CHAPTER 5	
Account Management	151
Managing User Accounts	152
Creating and Modifying User Accounts	154
Understanding Account Properties	160
Using Contacts and Distribution Lists	165

Working with User Profiles	167
Roaming Profiles	168
Mandatory Profiles	169
Managing Profiles	175
The Cost of Roaming Profiles	175
Managing Group Accounts	175
Group Types	176
Group Scope	176
Nesting Groups	180
Converting Group Scope	181
Default Groups in a Windows Domain	182
Working with Computer Accounts	186
Creating Computer Accounts	186
Managing Computer Accounts	187
Automating Account Management	188
Command-Line Tools for Managing Active Directory Objects	188
Bulk Import and Export with CSVDE and LDIFDE	191
Chapter Summary	194
Key Terms	195
Review Questions	195
Case Projects	199

CHAPTER 6

Windows File and Print Services	201
Windows File Systems	202
The FAT File System	203
The NTFS File System	203
Securing Access to Files with Permissions	215
Share Permissions	216
NTFS Permissions	217
Windows File Sharing	223
Default and Administrative Shares	228
Managing Shares with the Shared Folders Snap-in	228
Accessing File Shares from Client Computers	231
Windows Storage Management	233
Share and Storage Management	234
Distributed File System	236
File Server Resource Manager	238
Windows Printing	240
Configuring a Print Server	240
Chapter Summary	246
Key Terms	246
Review Questions	247
Case Projects	250

CHAPTER 7

Configuring Group Policy	253
Group Policy Architecture	254
Group Policy Objects (GPOs)	254
Group Policy Replication	262
Creating and Linking GPOs	263
Group Policy Scope and Inheritance	269
Changing Default GPO Inheritance Behavior	271
Group Policy Settings	278
Policies in the Computer Configuration Node	278
Computer Configuration: Software Settings	279
Computer Configuration: Windows Settings	281

Computer Configuration: Administrative Templates	291
Policies in the User Configuration Node	292
User Configuration: Software Settings	292
User Configuration: Windows Settings	292
User Configuration: Administrative Templates	298
Using Security Templates	298
Security Templates Snap-in	298
Security Configuration and Analysis Snap-in	299
Scedit.exe	301
Group Policy Management and Monitoring	302
GPO Management with GPMC	302
GPO Backup and Migration	303
Group Policy Results and Modeling	306
The ADMX Central Store	307
Group Policy Preferences	308
Chapter Summary	311
Key Terms	312
Review Questions	313
Case Projects	317
 CHAPTER 8	
Introduction to Windows Networking	319
Understanding the Windows Networking Paradigm	320
Windows Networking Terminology	320
The Network and Sharing Center	321
TCP/IP Operation and Configuration	327
TCP/IP Communication	328
IPv4 Address Configuration	328
IP Configuration Command-Line Tools	334
Managing Protocols	338
Internet Protocol Version 6	343
IPv6 Overview	344
Chapter Summary	347
Key Terms	348
Review Questions	348
Case Projects	351
 CHAPTER 9	
Configuring DNS for Active Directory	353
Introduction to Domain Name System	354
The Structure of DNS	354
DNS Server Roles	357
DNS Zones	357
Using DNS in Windows Server 2008	361
Installing DNS	361
Creating DNS Zones	362
Configuring DNS Zones	368
Aging and Scavenging Resource Records	368
Start of Authority Records	371
Name Server Records	372
Zone Delegation	373
Zone Transfers	375
Using WINS with DNS	378
Advanced DNS Server Settings	380
DNS Forwarders	380
Root Hints	382

Round Robin	383
Recursive Queries	384
Event and Debug Logging	385
Monitoring and Troubleshooting DNS	387
DNS Troubleshooting	387
Monitoring DNS Performance	389
Chapter Summary	390
Key Terms	391
Review Questions	392
Case Projects	396
CHAPTER 10	
Configuring and Maintaining the Active Directory Infrastructure	397
Examining Active Directory Functional Levels	398
Forest Functional Levels	398
Domain Functional Levels	399
Raising Domain and Forest Functional Levels	402
Adding and Removing Domains	406
Preparing a Forest and Domain for Windows Server 2008 with Adprep	406
Preparing for a Read Only Domain Controller	407
Removing Domain Controllers and Domains	407
Migrating Domain Objects	409
Configuring Active Directory Trusts	410
Configuring Shortcut Trusts	410
Configuring Forest Trusts	414
Configuring External and Realm Trusts	418
Configuring Trust Properties	418
Configuring Intrasite Replication	421
Knowledge Consistency Checker (KCC)	422
Connection Objects	423
Global Catalog Replication	426
Special Replication Situations	427
RODC Replication	428
Understanding and Configuring Sites	428
Creating Sites	428
Configuring Site Links	432
The Global Catalog and Universal Group Membership Caching	436
Working with Operations Master Roles	436
Operations Master Best Practices	437
Managing Operations Master Roles	438
Chapter Summary	440
Key Terms	441
Review Questions	442
Case Projects	445
CHAPTER 11	
Active Directory Certificate Services	449
Introducing Active Directory Certificate Services	450
Public Key Infrastructure Overview	450
PKI Terminology	451
AD CS Terminology	453
Deploying the Active Directory Certificate Services Role	454
Standalone and Enterprise CAs	454
Online and Offline CAs	455
Creating a CA Hierarchy	455
Certificate Practice Statement	456
Installing the AD CS Role	456

Configuring a Certification Authority	461
Configuring Certificate Templates	461
Configuring Certificate Enrollment Options	464
Configuring the Online Responder	472
Creating a Revocation Configuration	474
Maintaining and Managing a PKI	476
CA Backup and Restore	476
Key and Certificate Archival and Recovery	477
Chapter Summary	480
Key Terms	481
Review Questions	481
Case Projects	484
 CHAPTER 12	
Additional Active Directory Server Roles	485
Active Directory Lightweight Directory Services	486
Active Directory LDS Overview	486
When to Use AD LDS	487
Installing and Configuring AD LDS	487
Active Directory Federation Services	494
AD FS Overview	494
AD FS Role Services	495
AD FS Design Concepts	496
Preparing to Deploy AD FS	498
Active Directory Rights Management Service	498
AD RMS Key Features	499
AD RMS Components	499
AD RMS Deployment	500
Read Only Domain Controllers	502
RODC Installation	503
RODC Replication	505
Credential Caching	505
Administrator Role Separation	508
Read-Only DNS	508
Chapter Summary	509
Key Terms	509
Review Questions	510
Case Projects	513
 CHAPTER 13	
Server Management and Monitoring	515
Active Directory Maintenance	516
Windows Server Backup and Restore	516
Active Directory Backup and Restoration	524
Active Directory Defragmentation	527
Active Directory Monitoring	528
Event Viewer	529
Task Manager	530
Reliability and Performance Monitor	531
Windows System Resource Manager	539
Analyzing Active Directory Performance	541
Monitoring Active Directory Replication	541
Managing Server Core	542
Common Server Core Configuration Tasks	542
Managing Server Core Remotely	544

Additional Server and Active Directory Tools	545
Chapter Summary	546
Key Terms	547
Review Questions	547
Case Projects	550
APPENDIX A	
MCTS 70-640 Exam Objectives	553
APPENDIX B	
Windows Server 2008 Active Directory Configuration Resources	557
APPENDIX C	
Virtual Machine Instructions for Selected Activities	561
APPENDIX D	
A Step-by-Step Guide to Using Server Virtualization Software	571
GLOSSARY	607
INDEX	613

This page intentionally left blank

Introduction

MCTS Guide to Microsoft® Windows Server® 2008 Active Directory

Configuration provides in-depth coverage of the 70-640 certification exam objectives and focuses on the skills needed to manage a Windows Server 2008 Active Directory environment. With more than 100 hands-on activities and dozens of skill-reinforcing case projects, you'll be well prepared for the certification exam and learn valuable skills to perform on the job.

After you finish this book, you'll have an in-depth knowledge of Windows Server 2008, Active Directory, and related services, such as Domain Name System, Certificate Services, Active Directory Lightweight Directory Services, Active Directory Rights Management Services, and Active Directory Federation Services. Several new features of Windows Server 2008 are also covered, such as Hyper-V, read only domain controllers, Server Manager, and Server Core.

Intended Audience

MCTS Guide to Microsoft Windows Server 2008 Active Directory Configuration is intended for people who want to learn how to configure and manage a Windows Server 2008 network and are considering becoming MCTS and MCITP certified. The focus on Active Directory configuration gives new and experienced users alike the opportunity to study in depth the core technologies in Windows Server 2008. This book serves as an excellent text for classroom teaching, but self-paced learners will also find that the clear explanations and challenging activities and case projects serve them equally well. Although this book doesn't assume previous experience with Windows servers, it does assume a familiarity with current Windows OSs, such as Windows XP or Vista. Networking knowledge equivalent to an introductory networking course is highly recommended.

This Book Includes

- A Windows Server 2008 Enterprise Edition evaluation DVD is bundled with the book. It can be installed on a computer or in a virtual machine, using Microsoft Hyper-V, Microsoft Virtual Server, VMware Workstation, VMware Player, or VMware Server.
- Step-by-step hands-on activities walk you through tasks ranging from a basic Windows Server 2008 installation to complex multiserver network configurations involving Active Directory, DNS, and many other services. All activities have been tested by a technical editor, reviewers, and validation experts.

- Extensive review and end-of-chapter materials reinforce your learning.
- Challenging case projects build on one another and require you to apply the concepts and technologies learned throughout the book.
- Coverage of features new to Windows Server 2008, including Server Core, Hyper-V, Server Manager, is included as well as new Active Directory features, such as group policy preferences, Active Directory Rights Management Services (AD RMS) and Active Directory Federation Services (AD FS).
- New appendixes cover using Windows Server 2008 with virtualization software, including VMware Workstation and Server, Microsoft Hyper-V, and Microsoft Virtual Server and Virtual PC.
- Abundant screen captures and diagrams visually reinforce the text and hands-on activities.
- A list of 70-640 exam objectives is cross-referenced with chapters and sections that cover each objective.

Chapter Descriptions

This book is organized to familiarize you with Windows Server 2008 features and technologies and then provide in-depth coverage of Active Directory and its related services. The book wraps up by discussing server management and monitoring. Chapter 6, “Windows File and Print Services,” and Chapter 8, “Introduction to Windows Networking,” cover material that isn’t strictly part of the 70-640 exam, but these chapters provide information on key Windows technologies to enhance your overall learning experience. The 70-640 exam objectives are covered throughout the book, and you can find a mapping of objectives and the chapters in which they’re covered on the inside front cover, with a more detailed mapping in Appendix A.

The following list describes this book’s chapters:

- **Chapter 1**, “Introducing Windows Server 2008,” begins by describing the role of a server operating system and compares the Windows Server 2008 editions. Next, you’re given an overview of Windows Server 2008 core technologies, such as NTFS, Active Directory, disk management, and networking. Finally, server roles and new features in Windows Server 2008 are described.
- **Chapter 2**, “Installing Windows Server 2008,” discusses the details of planning a Windows Server 2008 installation, including installing the first server on a new network, expanding an existing network, and upgrading to Windows Server 2008. Server Core, the newest installation option, is discussed, followed by the new Hyper-V virtualization role and how it can be used to reduce server sprawl and simplify training, testing, and development.
- **Chapter 3**, “Introducing Active Directory,” begins by discussing the role of a directory service in a network, followed by details on installing Active Directory. Next, Active Directory components, such as the schema and Active Directory objects, are explained. Finally, group policies are introduced.
- **Chapter 4**, “Active Directory Design and Security Concepts,” gives you an in-depth look at the core organizing object in Active Directory: organizational units. Active Directory object permissions and delegation of control are discussed in detail. Next, the roles of forests, trees, and domains are described, along with key Active Directory concepts, such as directory partitions, operations master roles, replication, and trust relationships. Finally, Active Directory sites are introduced.
- **Chapter 5**, “Account Management,” explains how to manage user accounts, work with user profiles, and manage group accounts. Key concepts include roaming, mandatory, and super mandatory profiles as well as group types and group scopes. In addition, you learn about the role of computer accounts in an Active Directory network. Finally, you see how to use command-line tools to automate account management.
- **Chapter 6**, “Windows File and Printer Services,” discusses the Windows file system, including NTFS, disk quotas, volume mount points, shadow copies, compression, and encryption. You learn how to secure access to files by using NTFS permissions and see

how permission inheritance works. Windows file sharing is explained along with details on default and administrative shares and how to manage shared folders. This chapter wraps up with brief discussions on Windows storage management and Windows printing.

- **Chapter 7**, “Configuring Group Policy” gives you a detailed look at the architecture of group policies. You learn how group policy replication works and how to create and link GPOs. New features, including Starter GPOs and group policy preferences, are discussed, and group policy scope and inheritance are explained in depth. Group policy nodes and their myriad settings are described, with particular attention to auditing, folder redirection, and software restrictions. This chapter also explains the use of security templates and group policy management and monitoring, including GPO delegation, backup, and migration.
- **Chapter 8**, “Introduction to Windows Networking,” focuses on Windows networking terminology with discussions about the network map and sharing and discovery. TCP/IP operation and configuration are explained, along with using key command-line tools. In addition, you learn about managing installed protocols, including binding and network providers. The chapter ends with a brief discussion of IPv6, including address structure, host IDs, and subnetting.
- **Chapter 9**, “Configuring DNS for Active Directory,” gives you an overview of the Domain Name System and explains how to install DNS and create DNS zones. You learn about configuring zones, including Active Directory–integrated zones, zone replication, forward and reverse lookup zones, dynamic updates, and zone transfers. Finally, you explore advanced DNS server settings, such as forwarders and root hints, and see how to monitor and troubleshoot DNS.
- **Chapter 10**, “Configuring and Maintaining the Active Directory Infrastructure,” gives you an in-depth look at Active Directory functional levels, adding and removing domains, Active Directory trust relationships (shortcut, forest, and realm), replication, site configuration, and operations master roles.
- **Chapter 11**, “Active Directory Certificate Services,” explains how to set up and run the Active Directory Certificate Services (AD CS) role. Public key infrastructure (PKI) elements are described as well as how to create a certification authority (CA) hierarchy with AD CS. You also learn how to configure CAs, including the use of certificate templates, enrollment options, online responders, and revocation lists. Finally, you learn how to maintain and manage an existing PKI.
- **Chapter 12**, “Configuring Additional Active Directory Server Roles,” introduces you to several Active Directory roles that can be installed on Windows Server 2008: Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS), Active Directory Rights Management Services (AD RMS), and read only domain controllers (RODCs). This chapter describes features and components of these services and discusses how to deploy them.
- **Chapter 13**, “Server Management,” guides you through several maintenance and monitoring tasks, including server backup and restore to protect your server from data loss and using Event Viewer, Task Manager, Performance Monitor, and Windows System Resource Manager to ensure that your server is running at peak performance. In addition, this chapter discusses managing a Server Core installation and a host of server and Active Directory tools.
- **Appendix A**, “MCTS 70-640 Exam Objectives,” maps each 70-640 exam objective to the chapter and section where you can find information on that objective.
- **Appendix B**, “Windows Server 2008 Active Directory Configuration Resources,” includes a list of Web resources and books for supplementary information and in-depth discussions on many of the topics in this book. Resources are organized by topic.
- **Appendix C**, “Virtual Machine Instructions for Selected Activities,” provides instructions for performing selected activities in VMware Workstation or Microsoft Virtual PC.
- **Appendix D**, “A Step-by-Step Guide to Using Server Virtualization Software,” is a general guide to using virtualization in your computing environment and covers Microsoft Virtual PC, Microsoft Virtual Server, VMware Server, and Hyper-V.

Features

This book includes the following learning features to help you master a Windows Server 2008 Active Directory environment and the 70-640 exam objectives:

- *Chapter objectives*—Each chapter begins with a detailed list of the concepts to be mastered. This list is a quick reference to the chapter's contents and a useful study aid.
- *Hands-on activities*—More than 100 hands-on activities are incorporated in the book, giving you practice in setting up, managing, and troubleshooting a Windows Server 2008 server, with emphasis on Active Directory configuration. The activities give you a strong foundation for carrying out server administration tasks in the real world.
- *Screen captures, illustrations, and tables*—Numerous screen captures and illustrations of concepts aid you in visualizing theories and concepts and seeing how to use tools and desktop features. In addition, tables are used often to provide details and comparisons of practical and theoretical information and can be used for a quick review.
- *Chapter summary*—Each chapter ends with a summary of the concepts introduced in the chapter. These summaries are a helpful way to recap and revisit the material covered in the chapter.
- *Key terms*—All terms in the chapter introduced with bold text are gathered together in the Key Terms list at the end of the chapter. This list gives you a method for checking your understanding of all terms introduced.
- *Review questions*—The end-of-chapter assessment begins with review questions that reinforce the concepts and techniques covered in each chapter. Answering these questions helps ensure that you have mastered important topics.
- *Case projects*—Each chapter closes with one or more case projects. Many of the case projects build on one another, as you take a small startup company to a flourishing enterprise.
- *On the DVD*—The DVD includes a free 120-day evaluation copy of Windows Server 2008, Enterprise Edition.

Text and Graphics Conventions

Additional information and exercises have been added to this book to help you better understand what's being discussed in the chapter. Icons throughout the text alert you to these additional materials:



Tips offer extra information on resources, how to solve problems, and time-saving shortcuts.



Notes present additional helpful material related to the subject being discussed.



The Caution icon identifies important information about potential mistakes or hazards.



Each Hands-on activity in this book is preceded by the Activity icon.



Case Project icons mark the end-of-chapter case projects, which are scenario-based assignments that ask you to apply what you have learned in the chapter.

Test Preparation Software CD

MCTS Guide to Microsoft Windows Server 2008 Active Directory Configuration includes the exam objectives coverage map from Appendix A as well as CertBlaster test preparation questions that mirror the look and feel of the MCTS exam 70-640. The unlock code for the CertBlaster questions is c_640. For more information about dti test prep products, visit the Web site at www.dtipublishing.com.

Instructor's Resources

The following supplemental materials are available when this book is used in a classroom setting. All the supplements available with this book are provided to instructors on a single CD, called the Instructor's Resource CD (ISBN 1-423-90269-6).

- *Electronic Instructor's Manual*—The Instructor's Manual that accompanies this book includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional activities.
- *Solutions*—The instructor's resources include solutions to all end-of-chapter material, including review questions, hands-on activities, and case projects.
- *ExamView*—This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this book, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers and also save the instructor time by grading each exam automatically.
- *PowerPoint presentations*—This book comes with Microsoft PowerPoint slides for each chapter. They are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel free to add your own slides for additional topics you introduce to the class.
- *Figure files*—All the figures and tables in the book are reproduced on the Instructor's Resource CD in bitmap format. Similar to the PowerPoint presentations, they are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

System Requirements

Hardware (Without Using Virtualization) Minimum two computers per student that meet the following requirements:

- 2 GHz or faster CPU
- 512 MB or more RAM (preferably more when using a Vista client for some activities)
- 15 GB or more disk space
- DVD-ROM drive
- Super VGA or higher resolution monitor
- Mouse or pointing device
- Keyboard
- Network interface card connected to the classroom, lab, or school network
- Printer (to practice setting up a network printer)

Hardware (Using Virtualization) One computer per student to act as the host machine that meets the following minimum requirements:

- 2.4 GHz CPU
- 2 GB or more RAM (more is always better with virtualization)
- 40 GB or more disk space
- DVD-ROM drive
- Super VGA or higher resolution monitor
- Mouse or pointing device
- Keyboard
- Network interface card connected to the classroom, lab, or school network
- Printer (to practice setting up a network printer)

Software:

- Windows Server 2008 Standard or Enterprise Edition (included with DVD in the book)
- Windows Vista: Any edition except Home Edition (an evaluation virtual machine can be downloaded from the Microsoft Web site)

Virtualization Windows Server 2008 and Windows Vista can be loaded into a virtual server environment, such VMware Workstation or Server, Microsoft Virtual PC, or Microsoft Hyper-V. The use of virtualization is highly recommended.

Acknowledgments

I would like to thank Course Technology/Cengage Learning Acquisitions Editor Nick Lombardi for his confidence in asking me to undertake this challenging book project. In addition, thanks go out to Michelle Ruelos Cannistraci, the Senior Product Manager, who assembled an outstanding team to support this project. A special word of gratitude goes to Lisa Lord, the Development Editor, who has a knack for taking an unrefined product and turning it into a polished manuscript. Lisa's good humor and understanding as well as her commendable skills as an editor made my life considerably easier during the 10 months it took to complete this book. The quality assurance staff at Green Pen Quality Assurance provided diligent testing of chapter activities to ensure that labs work as they were intended, and for that, I am grateful. Of course, this book was not written in a vacuum, and the group of peer reviewers provided thoughtful advice, constructive criticism, and much-needed encouragement: Ron Handlon, Remington College; Julie Hietschold, Orange County College; Jeff Palmer, Orange County College; Robert Sherman, Sinclair College; and Daniel Ziesmer, San Juan College.

Finally, my family: wife Julie, daughters Camille and Sophia, and son Michael deserve special thanks and praise for going husbandless and fatherless seven days a week, 14 hours a day, for the better part of a year. Without their patience and understanding, and happy greetings when I did make an appearance, I could not have accomplished this.

About the Author Greg Tomsho has more than 25 years of computer and networking experience and has earned the CCNA, MCTS, MCSA, A+, Security+, and Linux+ certifications. Greg is the director of the Computer Networking Technology Department and Cisco Academy at Yavapai College in Prescott, AZ. His other books include *Guide to Network Support and Troubleshooting*, *A+ CoursePrep ExamGuide*, and *Guide to Networking Essentials*.

Contact the Author I would like to hear from you. Please e-mail me with any problems, questions, suggestions, or corrections. I even accept compliments! Your comments and suggestions are invaluable for shaping the content of the next edition of this book. You can contact me at w2k8@tomsho.com.

Introducing Windows Server 2008

After reading this chapter and completing the exercises, you will be able to:

- Explain the function of a server operating system in a network
- Describe the editions of Windows Server 2008
- Discuss the core technologies of Windows Server 2008
- Explain the primary roles a Windows Server 2008 computer can fulfill
- Describe the new and enhanced features of Windows Server 2008

Windows Server 2008 is Microsoft's most ambitious server operating system

update since Windows 2000 Server. This new version of Windows Server is chock-full of new tools and features designed to help administrators increase the availability of network services while limiting security risks. This chapter discusses the editions of Windows Server 2008 and the requirements and uses for each. In addition, you learn about the roles a server operating system plays in a computer network and the many Windows Server 2008 features designed to fill those roles.

Most networks are set up so that the people using computers on them can communicate with one another easily. One of a server's functions is to facilitate communication between computers and, therefore, between people. The administrator of a computer network has the job of configuring servers and computers on the network to provide services that facilitate this communication. These services include, but aren't limited to, file sharing, device sharing (such as printers), security, messaging, remote access, Web services, and services that work in the background to ensure a user-friendly and secure experience. One such background service is a directory service. To server administrators, it's front and center in their daily activities, but to network users, the directory service is probably working best when they don't know it's there.

The primary focus of this book—and, indeed, Windows Server 2008—is the Microsoft directory service, Active Directory. Active Directory can be described as a control panel for a Windows network where user accounts are created, network use policies are defined, and security policies are configured, among a host of other functions. This chapter introduces you to Active Directory as well as other Windows Server 2008 technologies and services.

The Role of a Server Operating System

A server or collection of servers is usually at the center of most business networks. The functions a server provides depend on a number of factors, including the type of business using the server, size of the business, and extent to which the business has committed to using technology to aid operations. The latter factor is the crux of the matter. Technology is designed to help a person or an organization do things more efficiently or more effectively, and a server is used to provide services a business has deemed can help its operations. Before you explore these services in more detail, a few definitions are in order.

Server: Hardware or Software?

When most people hear the word “server,” they conjure up visions of a large tower computer with lots of hard drives and memory. This image is merely a computer hardware configuration that may or may not be used as a server, however. In short, a computer becomes a server when software is installed on it that provides a network service to client computers. In other words, you could install certain software on an inexpensive laptop computer and make it act as a server. By the same token, a huge tower computer with six hard drives and 16 GB of RAM could be used as a workstation for a single user. So although some computer hardware configurations are packaged to function as a server, and others are packaged as desktop computers, what makes a computer a server or desktop computer is the software installed on it.

Of course, with modern operating systems (OSs), the lines between desktop and server computer are blurred. OSs such as Windows Vista and its predecessors are designed to be installed on desktop computers or workstations; to run Web browser, word processing, spreadsheet, and other similar programs; and generally act as a personal computer. However, these OSs can perform server functions, such as file and printer sharing, and even act as a Web server. On the other hand, Windows Server 2008 and its predecessors are designed as **server operating systems**, but there's nothing to stop you from installing a word processor or Web browser and using Windows Server 2008 on your desktop computer. So what are the differences between a desktop OS, such as Windows Vista, and a server OS, such as Windows Server 2008? The following section explains.

Server Operating System Versus Desktop Operating System

Both Windows Server 2008 and Windows Vista can perform some server functions and some desktop functions, but important differences distinguish them. Vista is configured to emphasize



the user interface and is performance-tuned to run desktop applications. Windows Server 2008, on the other hand, deemphasizes many of Vista's user interface bells and whistles in favor of a less flashy and less resource-intensive user interface. In addition, Windows Server 2008 is performance-tuned to run background processes so that client computers can access network services faster. Speaking of network services, most Windows Server 2008 editions can run the following, among others:

- File and Printer Sharing
- Web Server
- Routing and Remote Access Services (RRAS)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- File Transfer Protocol (FTP) Server
- Active Directory
- Distributed File System (DFS)
- Fax Server

Of these services, Windows Vista supports only File and Printer Sharing, Web Server, and FTP Server and in a limited capacity. Windows Vista is restricted to only 10 network connections, whereas network connections to a Windows Server 2008 computer are limited only by the number of purchased licenses and available resources. In addition, because a server is such a critical device in a network, Windows Server 2008 includes a number of fault-tolerance features, such as redundant array of independent drives (RAID), load balancing, and clustering, none of which are standard features in Windows Vista or other Windows desktop OSs. Windows Server 2008 is also capable of supporting up to 32 processors compared with Vista, which supports a maximum of 2.

Microsoft has developed a number of Windows Server 2008 editions, discussed in the following section, so that businesses can choose the best solution for their size and the services they require.

Windows Server 2008 Editions

In the realm of server OSs, Microsoft has an edition for all types of businesses, large and small. From a simple Web server to a massive application server, Windows Server 2008 has it covered. The Windows Server 2008 editions remain the same as those in Windows Server 2003:

- Windows Server 2008 Standard Edition
- Windows Server 2008 Enterprise Edition
- Windows Server 2008 Datacenter Edition
- Windows Web Server 2008

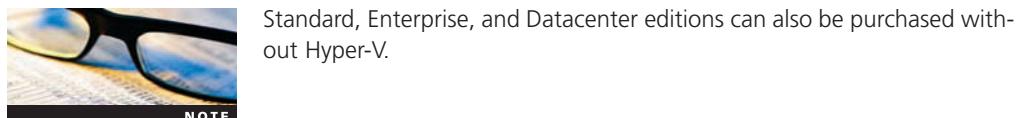


Two Windows server products targeted toward small and medium businesses are currently in development: Windows Small Business Server 2008 and Windows Essential Business Server.

NOTE

Why the need for several editions? One size doesn't fit all is the short answer. For example, a small organization with a few users up to a few hundred users who mainly need a centralized network logon along with file and printer sharing can probably use Standard Edition. A large company or one that needs a robust application server might opt for Enterprise Edition. A company that needs to host a gargantuan database requiring lots of processors, storage, and memory might need Datacenter Edition. As server virtualization has become an essential part of the Server 2008 family of products, there are important differences in editions for licensing the new

Hyper-V feature that comes with Standard, Enterprise, and Datacenter editions. (Hyper-V is covered in more detail in “New Features in Windows Server 2008” later in this chapter.) The following sections review the features and requirements of the four Windows Server 2008 editions.



Standard, Enterprise, and Datacenter editions can also be purchased without Hyper-V.

NOTE

Standard Edition

Standard Edition is suitable for most small to medium businesses that need a robust solution for file and printer sharing, centralized control over user accounts and network resources, and common services found in most networks, such as Web services, DNS, and DHCP. Standard Edition supports up to four processors. It bears mentioning, with multicore processors becoming commonplace, that for licensing purposes, Microsoft defines a processor as a physical chip or a socket on a motherboard. This means Standard Edition can support up to four single-core, dual-core, or even quad-core and higher processors. Standard Edition can be configured as a stand-alone server, a member of a domain, or a domain controller and can optionally be installed in **Server Core** mode, a new installation option that uses a limited version of the GUI to take up fewer resources.

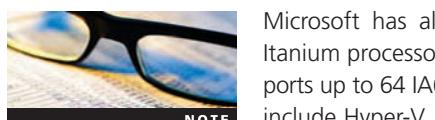
Standard Edition is available in 32-bit and 64-bit versions. The 32-bit version supports up to 4 GB RAM, and the 64-bit version supports up to 32 GB RAM. When you consider that this version supports up to four multicore processors, 64-bit processors, and a sizable amount of RAM, you might think Standard Edition is all you need. However, some advanced features, such as clustering and support for more processors, are reserved for higher-end editions. Users of the 64-bit Standard Edition can install one virtual instance of Server 2008 Standard Edition with Hyper-V.

Enterprise Edition

Enterprise Edition has all the features of Standard Edition but includes additional features that make this edition suitable for medium to large businesses that need high-availability network services. Enterprise Edition supports up to eight processors and 64 GB RAM in the 32-bit version and up to 2 TB of RAM in the 64-bit version. Server clustering is the most notable feature in Enterprise Edition that isn’t available in Standard Edition. With this feature, network administrators can tie two or more physical servers together logically to act as a single, high-performance, fault-tolerant machine. In addition, Enterprise Edition permits up to 16 cluster nodes. Another fault-tolerance feature in this edition is hot-add memory, which means you can add RAM to a server without shutting the system down, if the server hardware supports that feature. The 64-bit Enterprise Edition permits up to four virtual instances per purchased license with Hyper-V.

Datacenter Edition

For organizations managing huge amounts of data, using virtualization on a large scale, consolidating servers, or running high-volume, transaction-heavy applications, **Datacenter Edition** might be a good fit. Datacenter Edition includes all the features of Enterprise Edition with support for 32 processors in the 32-bit version and up to 64 processors in the 64-bit version. In addition, Datacenter Edition has these fault-tolerance features: hot-add memory, hot-replace memory, hot-add processors, and hot-replace processors. Datacenter Edition can’t be purchased as individual licenses; it must be purchased through volume licensing agreements or from OEMs, preinstalled on server hardware. The number of virtual instances allowed with the 64-bit Datacenter Edition is unlimited.



Microsoft has also released Itanium Edition, designed to run on Intel Itanium processors. This edition is comparable to Datacenter Edition, supports up to 64 IA64 processors, allows only eight cluster nodes, and doesn’t include Hyper-V.

NOTE



Windows Web Server 2008

Windows Web Server 2008 is designed to operate as a single-purpose Web server running Internet Information Services (IIS) 7.0. This edition provides hardware support similar to Standard Edition but has no virtualization support and can't be installed as a domain controller. It lacks many features of other editions, such as remote access and Terminal Services. Windows Web Server 2008 is a cost-effective solution, however, when you need a full-featured Web server but don't require the advanced features of other editions. Typical examples of this edition's intended audience are small businesses that don't require Active Directory or departments in large organizations that want to deploy their own Web applications.

Comparing Editions

Tables 1-1 and 1-2 summarize system requirements and compare features of the different Windows Server 2008 editions.



For an extensive comparison of Windows Server 2008 editions, go to www.microsoft.com/windowsserver2008/editions/overview.mspx.

Table 1-1 Windows Server 2008 system requirements (all editions)

Component	Requirement
Processor	Minimum: 1 GHz for x86 CPU or 1.4 GHz for X64 CPU Recommended: 2 GHz or faster
Memory	Minimum: 512 MB RAM Recommended: 2 GB RAM or more
Available disk space	Minimum: 10 GB Recommended: 40 GB or more
Additional drives	DVD-ROM
Display and peripherals	Super VGA or higher Keyboard and mouse

Table 1-2 Comparing features in Windows Server 2008 editions

Feature	Windows Web Server 2008	Standard Edition	Enterprise Edition	Datacenter Edition
Maximum RAM	32-bit: 4 GB 64-bit: 32 GB	32-bit: 4 GB 64-bit: 32 GB	32-bit: 64 GB 64-bit: 2 TB	32-bit: 64 GB 64-bit: 2 TB
Failover clustering	N/A	N/A	16 nodes	16 nodes
Supported processor sockets	X86 sockets: 4 X64 sockets: 4	X86 sockets: 4 X64 sockets: 4	X86 sockets: 8 X64 sockets: 8	X86 sockets: 32 X64 sockets: 64
Hot-add memory	N/A	N/A	Yes	Yes
Hot-replace memory	N/A	N/A	N/A	Yes
Hot-add processor	N/A	N/A	N/A	Yes
Hot-replace processor	N/A	N/A	N/A	Yes
Virtual licenses	Hyper-V not included	1 (64-bit only)	4 (64-bit only)	Unlimited (64-bit only)



Activity 1-1: Reviewing System Properties

Time Required: 10 minutes

Objective: View system properties of Windows Server 2008.

Description: You need to find some basic information about a Windows Server 2008 installation, such as the server edition, processors, amount of RAM, and so forth.

1. Log on to your server as Administrator. Click **Start**, and then right-click **Computer** and click **Properties**.
2. There are four sections in the System Properties dialog box: Windows edition, System, Computer name, and Windows activation. Review the information in each section. Make a note of the Windows edition that's running.
3. In the System section, make a note of the processor that's running and the system type, which tells you whether you're running a 32-bit or 64-bit version. This information will be useful later to determine what other features you can install.
4. On the left is a list of tasks. Click each task to familiarize yourself with these control panels. Note that the Remote settings and Advanced system settings tasks bring you to different tabs of the same dialog box.
5. Close all open windows.

Windows Server 2008 Core Technologies

The new features and enhancements Microsoft has added to Windows Server 2008 are getting all the attention. Before you can understand and use these new features, however, you need a firm grasp of the technologies that form the foundation of a Windows Server OS. The following is a list of many of the technologies on which Windows Server 2008 is built:

- New Technology File System
- Active Directory
- Microsoft Management Console
- Disk Management
- File and printer sharing
- Windows networking
- Internet Information Services

The following sections describe these technologies briefly, but most are covered in detail in later chapters.

NTFS

One of a server's main jobs is to store a variety of file types and make them available to network users. To do this effectively, a server OS needs a robust and efficient file system. **New Technology File System (NTFS)** was introduced in Windows NT. Although it has been updated throughout the years, NTFS has remained a reliable, flexible, and scalable file system. Its predecessor was FAT/FAT32, which had severe limitations for a server OS. It lacked features such as native support for long filenames, file and folder permissions, support for large files and volumes, reliability, compression, and encryption. NTFS supports all these features and more.

Perhaps the most important feature of NTFS is the capability to set user and group permissions on both folders and files. With this feature, administrators can specify which users can access a file and what users can do with a file if they're granted access. These permissions increase a server environment's security compared to FAT/FAT32, which has no user access controls. NTFS and other supported file systems are covered in Chapter 6.



Activity 1-2: Examining NTFS Permissions and Attributes

Time Required: 10 minutes

Objective: View NTFS file permissions and attributes.

Description: This is your first time using a Windows system with an NTFS-formatted disk, so you want to familiarize yourself with some capabilities of this file system.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, and then right-click **Computer** and click **Explore**.
3. Right-click the **(C:)** drive in the right pane and click **Properties**.
4. Click the **General** tab, if necessary. Verify that NTFS is listed for the file system. If the drive isn't formatted as NTFS, ask your instructor which drive is formatted as NTFS on your system and repeat from Step 3.
5. Click the **Security** tab (see Figure 1-1).

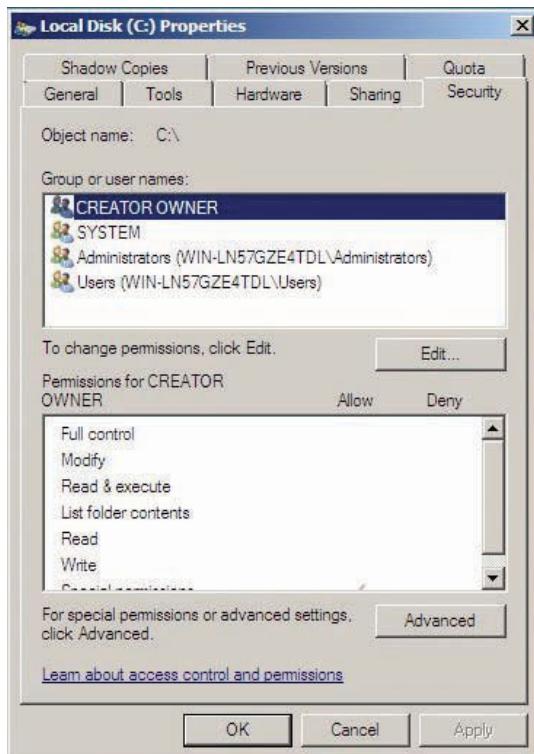


Figure 1-1 The Security tab showing NTFS permissions

6. Click each item in the Group or user names list box, and view the permission settings for each at the bottom.
7. Next, click the **Quota** tab. Quotas, a feature available only on NTFS-formatted disks, are discussed more in Chapter 6.
8. Now click the **Shadow Copies** tab. This feature is yet another one that requires NTFS.
9. Last, click the **General** tab again. Note the two check boxes at the bottom for enabling indexing and compression. NTFS volumes allow these features, which aren't available with FAT volumes.
10. Close the Properties dialog box.
11. Click the **Documents** icon under Favorite Links. Right-click the right pane, point to **New**, and click **Text Document**. Press **Enter** to accept the default filename New Text Document.
12. Right-click **New Text Document** and click **Properties**. Notice the two check boxes at the bottom next to Attributes. They are common file attributes in both the FAT and NTFS file systems. Click the **Advanced** button.
13. In the Advanced Attributes dialog box, notice four more check boxes for attributes. Only the archiving attribute is available with FAT volumes. The other three, for file indexing, file compression, and encryption, are available only with NTFS volumes.
14. Close all open windows.

As you can see, NTFS has numerous advantages over the older FAT file systems. You explore many of these features in detail in Chapter 6.

Active Directory

Active Directory is the foundation of a Windows network environment. This directory service enables administrators to create and manage users and groups, set network-wide user and computer policies, manage security, and organize network resources.

With Active Directory, you transform a limited, nonscalable workgroup network into a Windows domain with nearly unlimited scalability. (The differences between workgroup and domain models are explained in “Windows Networking Concepts” later in this chapter.) Active Directory and all its features and functions are the primary focus of this book, and you learn more about using and configuring Active Directory in subsequent chapters. To summarize, the following are Active Directory’s main purposes and features:

- Provides a single point of administration of network resources, such as users, groups, shared printers, shared files, servers, and workstations
- Provides centralized authentication and authorization of users to network resources
- Along with DNS, provides domain-naming services and management for a Windows domain
- Enables administrators to assign system policies, deploy software to client computers, and assign permissions and rights to users of network resources

You delve into all these functions and more in later chapters. In Chapter 3, you install Active Directory and learn about its basic functions. Subsequent chapters go into more detail.

Microsoft Management Console

A server OS requires a myriad of tools that administrators must use to manage, support, and troubleshoot a server system. One challenge that comes with so many tools is the numerous user interfaces an administrator has to learn. Microsoft has lessened that challenge by providing a common framework for running most administrative tools called the Microsoft Management Console (MMC). The MMC alone isn’t very useful, as you can see in Figure 1-2. What makes it useful is the bevy of snap-ins you can install. Each snap-in is designed to perform a specific administrative task, such as the Disk Management snap-in shown in Figure 1-3.

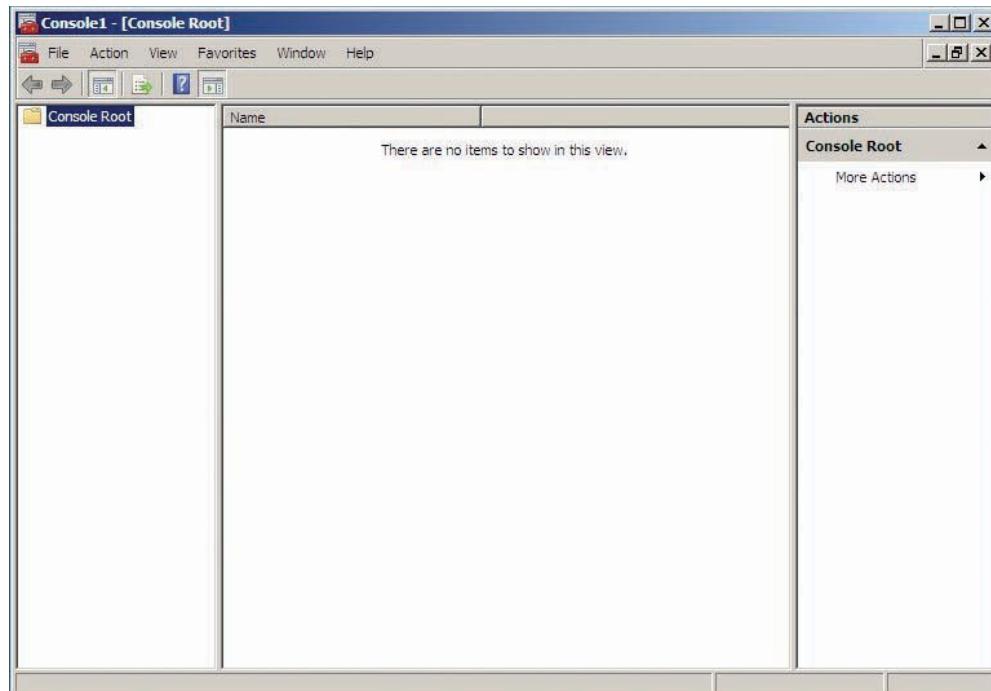


Figure 1-2 The Microsoft Management Console

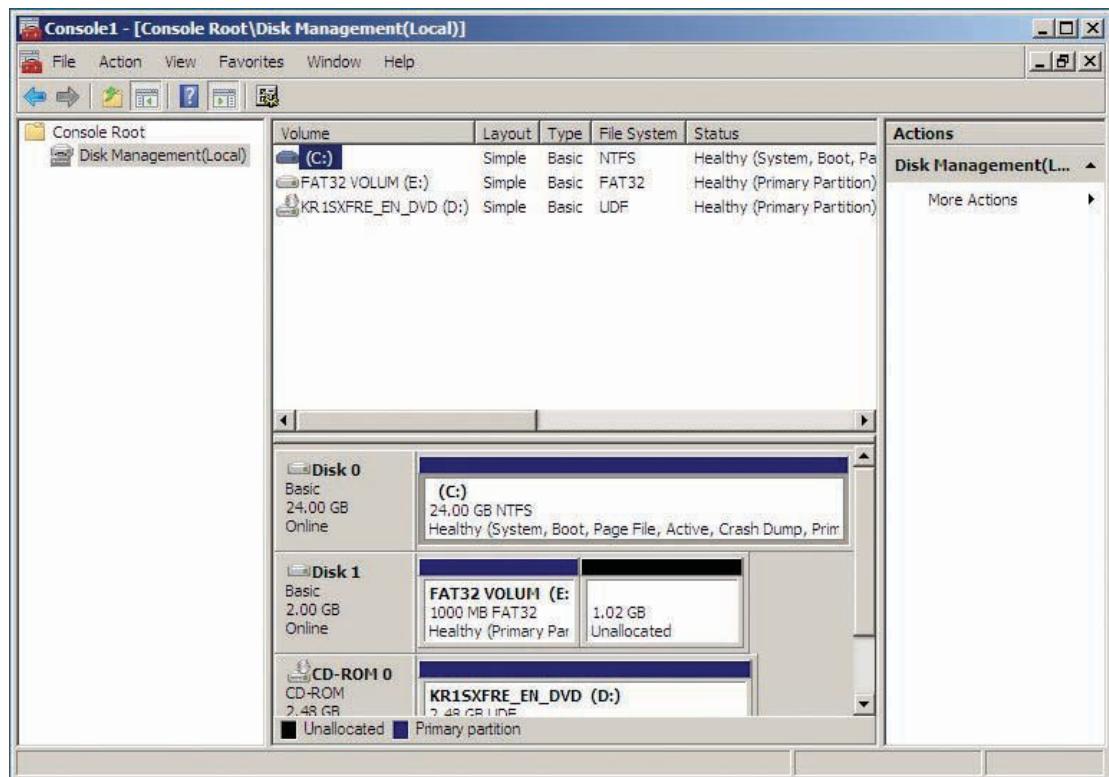


Figure 1-3 An MMC with the Disk Management snap-in

A number of MMCs are loaded in the Administrative Tools folder, depending on what roles and features are installed on the server. For example, after you install Active Directory, several new MMCs for managing it are created and stored in the Administrative Tools folder. Not all administrative functions can be accessed from these prebuilt MMCs, however; you might have to create a customized MMC to access some functions or to keep an MMC handy on your desktop with the administrative snap-ins you use most often.



Activity 1-3: Using a Prebuilt MMC

Time Required: 15 minutes

Objective: Explore the Administrative Tools folder and become familiar with prebuilt MMCs.

Description: You're a junior administrator for a Windows server and have been told to familiarize yourself with the management tools on your server and check the status of the Print Spooler service.

1. Log on to your server as Administrator, if necessary.
2. Click **Start** and point to **Administrative Tools**. Make a note of the tools you see.
3. Click the **Computer Management** tool. Notice that several tools in Computer Management are also available as separate MMCs in the Administrative Tools folder.
4. Explore some tools in Computer Management by clicking the tool name in the left pane. Some tools have a plus sign next to them, indicating additional components for that tool. Each tool is called a snap-in.
5. Click the plus (+) sign next to **Services and Applications** to expand it, and then click the **Services** snap-in.
6. Find the service called Print Spooler. Make a note of its status shown in the Status column.

7. Click **Shared Folders**. Next, click the **Help** toolbar icon (a question mark in a blue box), which opens a window with details about that snap-in. Do the same with several other tools, and read the descriptions for those snap-ins.
8. Close all open windows.



Activity 1-4: Creating a Custom MMC

Time Required: 10 minutes

Objective: Create your own custom MMC by selecting snap-ins.

Description: You're a junior administrator for a Windows server, and three of your most common tasks are monitoring installed devices, managing and monitoring the server's disks, and checking on scheduled tasks. You have decided that putting tools for these tasks in their own MMC on your desktop would make you more efficient.

1. Log on to your server as Administrator, if necessary.
2. Click **Start, Run**. Type **mmc** in the Open text box, and then click **OK**.
3. Click **File, Add/Remove Snap-in** from the MMC menu.
4. In the Available snap-ins list box, click **Device Manager** (for monitoring installed devices), and then click the **Add** button.
5. Note your choices in the next dialog box. You can decide whether to use the selected snap-in on the local computer or another computer. If you select the Another computer option, you can manage that computer remotely with your MMC. Leave the **Local computer** option selected, and then click **Finish**.
6. Repeat Steps 4 and 5, substituting the **Disk Management** and **Task Scheduler** snap-ins for Device Manager. (When you add Disk Management, click **This computer** instead of Local computer.) Click **Finish** for each snap-in, and when you're finished adding snap-ins, click **OK**.
7. To name your MMC, click **File, Save As** from the menu.
8. In the Save As dialog box, click the **Desktop** icon, type **DevDiskTask** for the filename, and then click **Save**. You now have a customized MMC on your desktop.
9. Close all open windows.

Disk Management

To manage the disks and volumes on a Windows Server 2008 computer, you mainly use the Disk Management snap-in. With this tool, you can monitor the status of disks and volumes, initialize new disks, create and format new volumes, and troubleshoot disk problems. The Disk Management tool also enables you to configure redundant disk configurations, such as RAID 1 and RAID 5 volumes. This important tool is covered in Chapter 6, but you can get a feel for it in the following activity.



Activity 1-5: Introducing the Disk Management Snap-in

Time Required: 15 minutes

Objective: Explore the features of the Disk Management snap-in.

Description: You have just arrived at a customer site that's having problems with disk storage on its Windows Server 2008 system. You don't know the configuration of the installed disks, so you need to view the disk configuration.

1. Log on to your server as Administrator, if necessary.
2. Open the MMC you created in Activity 1-4, or click **Start**, point to **Administrative Tools**, and click **Computer Management**.
3. Click the **Disk Management** snap-in in the left pane. There are two panes in Disk Management: The upper pane shows a summary of installed volumes, along with basic information about each volume. The lower pane shows installed disks and how each disk is being used.

4. Right-click the **(C:)** volume in the upper pane and note some of the options you have. A new option in Windows Vista is the capability to shrink a volume (assuming the volume isn't completely full). This feature is not available in Windows Server 2003.
5. In the lower pane, right-click **Disk 0**. Depending on your system's disk configuration, you should have more choices available and probably several choices that are disabled (grayed out). If Disk 0 is configured as a basic disk, you should see the option to convert it to a dynamic disk.
6. Right-click the unallocated space of Disk 0, and notice the options for making the unallocated space into a new volume. (Use Disk 1 if Disk 0 has no unallocated space.) In Windows XP and Windows Server 2003, basic disks use the term "partition" instead of volume. In Vista and Server 2008, the term "volume" is often used instead when preparing disks for use.
7. Right-click the unallocated space of Disk 0 again and click **New Simple Volume** to start the New Simple Volume Wizard. In the welcome window, click **Next**.
8. In the Specify Volume Size window, type **500**, and then click **Next**.
9. In the Assign Drive Letter or Path window, you have the option to assign a drive letter or mount the new volume into a folder on another volume. Click drive letter **S**, and then click **Next**. (If S isn't available, ask your instructor which drive letter to select.)
10. In the Format Partition window, click the **File System** list arrow, and note the available options. Click **FAT32** to select it as the file system. Notice that the Enable file and folder compression check box becomes disabled because FAT32 doesn't support compression. In the Volume label text box, type **FAT32Vol**, and then click **Next**.
11. Review the settings summary, and then click **Finish**. Watch the space where the new volume has been created. After a short pause, the volume should begin to format.
12. Close all open windows. If you're prompted to save changes to the MMC, click **No**.



Activity 1-6: Comparing NTFS and FAT32 Volumes



Time Required: 15 minutes

Objective: Compare the features of FAT32 and NTFS volumes.

Description: You can't remember which features are supported on NTFS and FAT32 volumes. Because the server you're working on has at least one volume in each file system, you decide to explore the properties of both file systems and compare them.

1. Log on to your server as Administrator, if necessary.
2. Open the Disk Management snap-in by using the method described in Activity 1-5.
3. In the upper pane, right-click the **(C:)** volume and click **Properties**.
4. Arrange the Properties dialog box so that you can see the list of disk drives in Disk Management. Right-click the **S** volume you created in Activity 1-5 and click **Properties**. Arrange the S volume's Properties dialog box next to the C volume's Properties dialog box.
5. Click the **General** tab, if necessary, in each volume's Properties dialog box. The first difference you should see is that the NTFS-formatted C volume has options to compress and index the drive, but the FAT32-formatted S volume does not.
6. The next three tabs, Tools, Hardware, and Sharing, are the same for both file system types. Click the **Security** tab of the C volume. Notice that the S volume doesn't have this tab.
7. Next, click the **Shadow Copies** tab of the C volume, where you can enable or disable shadow copies for a volume. Notice that the S volume doesn't have a Shadow Copies tab, and the S volume isn't listed in the Shadow Copies tab for the C volume.



The Shadow Copies service enables users to restore a deleted file or a previous version of a file in a shared folder.

NOTE

8. Next, click the **Quota** tab of the C volume. This is where you can assign disk quotas, which specify the maximum amount of space a user's files can occupy on a volume. Again, this tab isn't available for the FAT32 S volume.
9. Close all open windows. If you're prompted to save changes to the MMC, click **No**.

As you can see, an NTFS volume has a number of advantages over a FAT volume. So what good is a FAT or FAT32 volume? The main reason to use FAT or FAT32 on a Windows computer today is if the volume will be used by an older Windows version, such as Windows 98, or by another OS that might not support NTFS.

File and Printer Sharing

Probably the most common reason for building a network and installing a server is to share files, printers, and other resources among several users. Windows Server 2008 provides a robust system for file and printer sharing, offering advanced features such as shadow copies, disk quotas, and the Distributed File System (DFS). At its simplest, sharing files or a printer is just a few clicks away. More complex configurations that offer redundancy, version control, and user storage restrictions are also readily available. The following activity introduces you to sharing files in a folder, but file and printer sharing is discussed in more detail in Chapter 6.



Activity 1-7: Sharing a Folder in Windows Server 2008

Time Required: 15 minutes

Objective: Share the Public folder in Windows Server 2008.

Description: You have created a document that you need to make available to several colleagues. You decide to share the Public folder where the document is stored so that your colleagues can open or copy the document.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, **Control Panel**. Double-click the **Network and Sharing Center** applet to open the window shown in Figure 1-4.

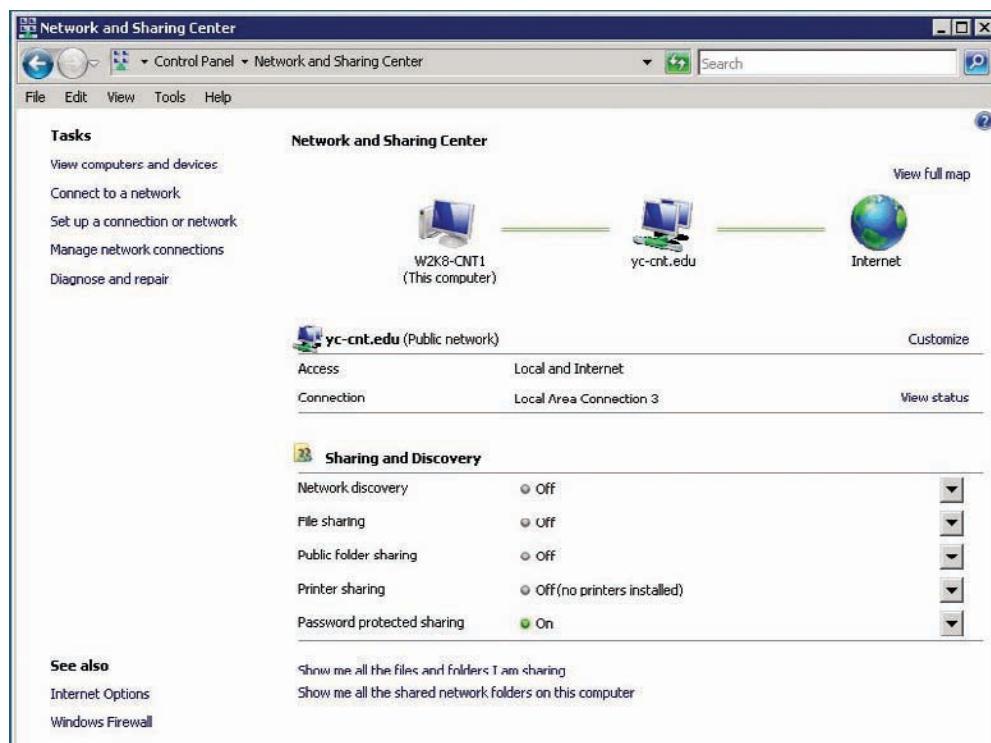


Figure 1-4 The Network and Sharing Center

3. In the Sharing and Discovery section, click the **Public folder sharing** list arrow.
4. Click the **Turn on sharing** option button so that anyone with network access can open files, and then click **Apply**. (If the “Network discovery and file sharing” warning message appears on the taskbar and begins blinking, click it, and then click the option beginning with “No.”) The icons next to Network discovery, File sharing, and Public folder sharing in the Network and Sharing Center turn green.
5. Click the **Show me all the shared network folders on this computer** link at the bottom. A window opens that shows the Public and Printers folders. Close all open windows.
6. Click **Start, Computer**. Click **Public** in the left pane of the Explorer window under Folders. This is the folder that has just been shared. Right-click a blank area of the right pane, point to **New**, and click **Text Document**.
- 7 Under Folders in the left pane, click **Network**. A list of computers on the network is displayed in the right pane (see Figure 1-5).

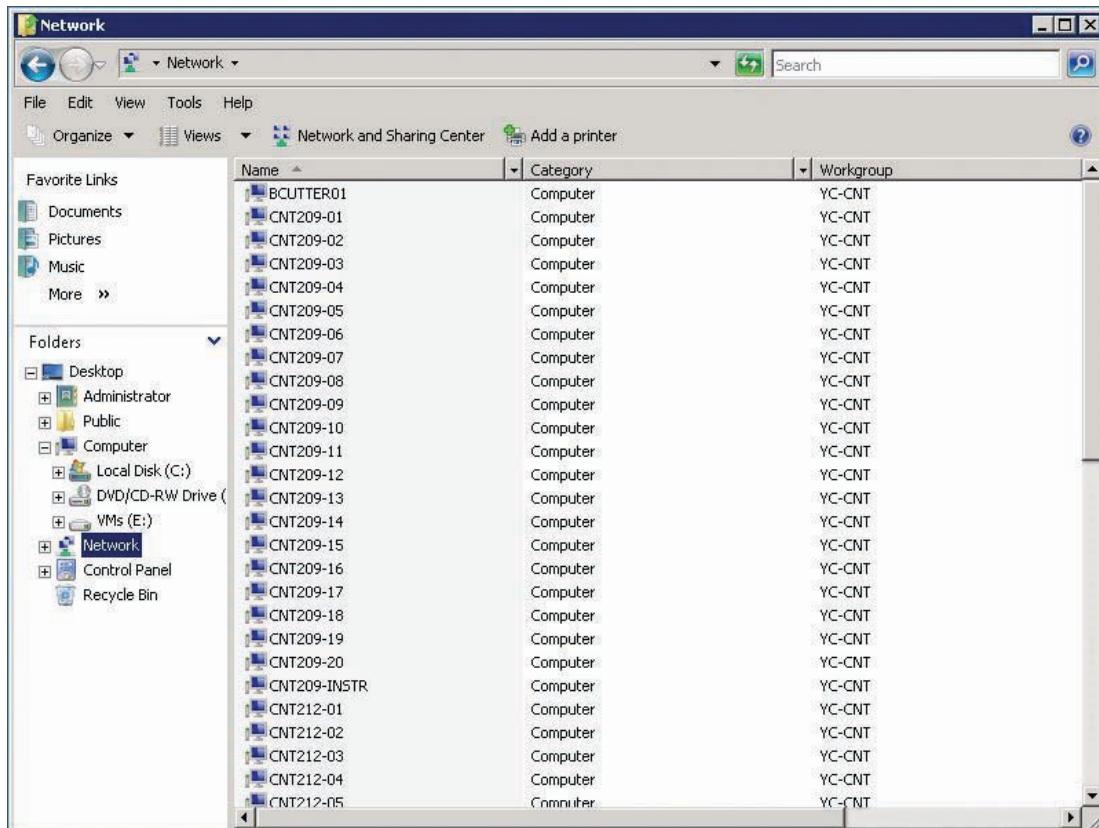


Figure 1-5 A list of computers on the network

8. In the right pane, find the computer of another student who has completed Step 6 and double-click it. You should see the Public folder that this student has shared.
9. Double-click the **Public** folder and verify that you can open the text document that was created.
10. Close all open windows.

Windows Networking Concepts

Administering a Windows server requires extensive knowledge of networking components and protocols as well as a solid understanding of the network security models used in Windows. In a Windows network environment, computers can be configured to participate in one of two network security models: workgroup or domain.

The Workgroup Model A **Windows workgroup** is a small collection of computers whose users typically have something in common, such as the need to share files or printers with each other. A workgroup is also called a peer-to-peer network sometimes because all participants are represented equally on the network, with no single computer having authority or control over another. Furthermore, logons, security, and resource sharing are decentralized, so each user has control over his or her computer's resources. This model is easy to configure, requires little expertise to manage, and works well for small groups of users (fewer than 10) who need to share files, printers, an Internet connection, or other resources. A Windows Server 2008 server that participates in a workgroup is referred to as a **stand-alone server**.

The Domain Model A **Windows domain** is a group of computers that share common management and are subject to rules and policies defined by an administrator. The domain model is preferred for a computer network that has more than 10 computers or requires centralized security and resource management. Unlike the workgroup model, a domain requires at least one computer configured as a domain controller running a Windows Server OS. In the domain model, a computer running a Windows Server OS can occupy one of two primary roles: a domain controller or a member server.

A **domain controller** is a Windows server that has Active Directory installed and is responsible for allowing client computers access to domain resources. The core component of a Windows domain is Active Directory. A **member server** is a Windows server that's in the management scope of a Windows domain but doesn't have Active Directory installed.

Windows Networking Components

Every OS requires these hardware and software components to participate on a network: a network interface, a network protocol, and network client or network server software. In most cases, today's OSs have both client and server software installed.

Network Interface A network interface is composed of two parts: the network interface card (NIC) hardware and the device driver software containing specifics of how to communicate with the NIC. In Windows Server 2008, you configure the network interface in the Network Connections window (see Figure 1-6). To open it, click Start, Network, and then click Network and Sharing Center. Under Tasks, click Manage network connections.

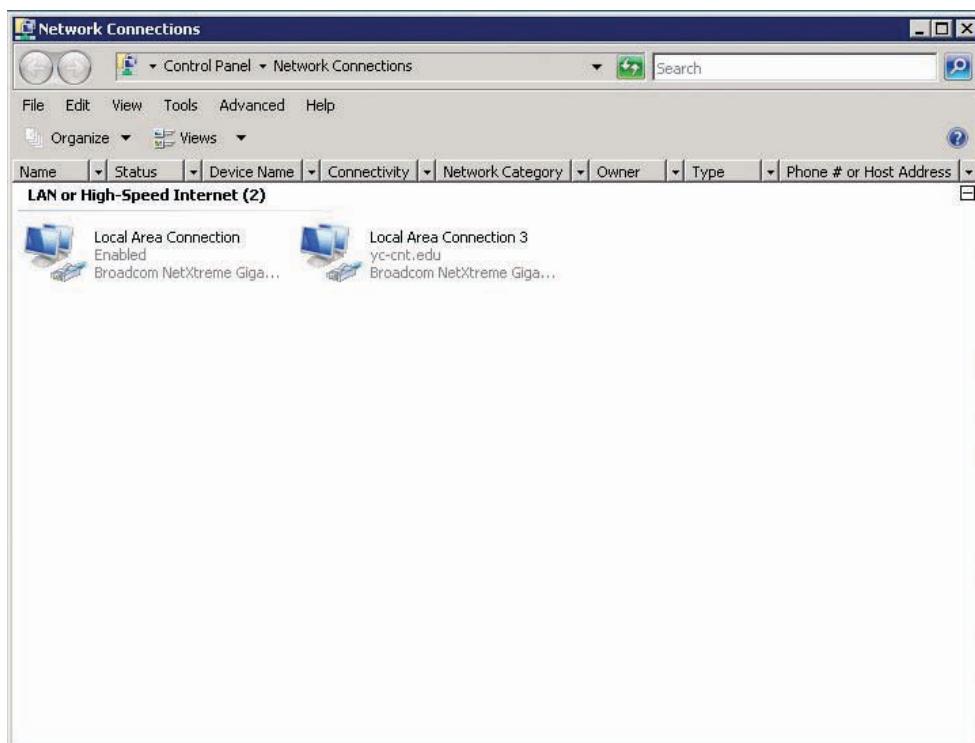


Figure 1-6 The Network Connections window

If you right-click a network connection and click Properties, a Properties dialog box similar to Figure 1-7 opens. The network interface used in this connection is specified in the Connect using text box. You can view details about the interface, including the device driver and configurable settings, by clicking the Configure button.

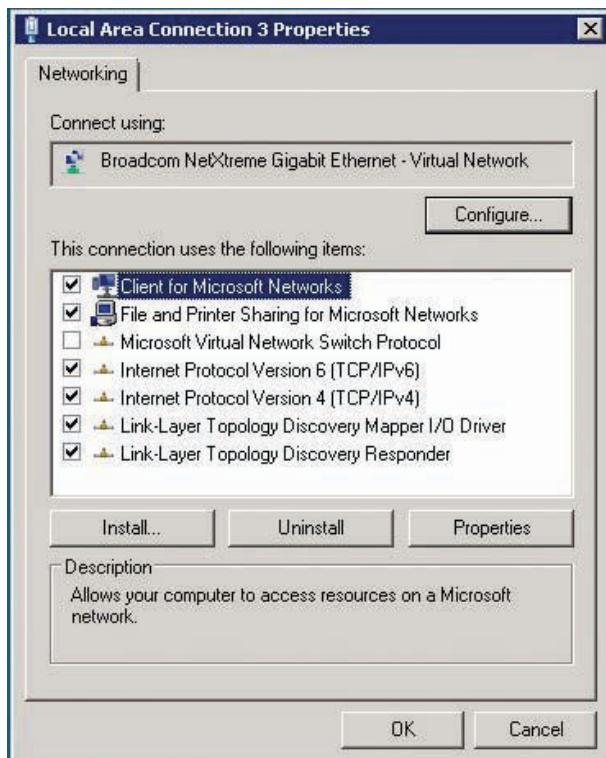


Figure 1-7 Properties of a network connection

Network Protocol A **network protocol** specifies the rules and format of communication between network devices. Several years ago, network administrators usually had to understand and support two or more protocols on their networks. Today, most administrators need to work with only TCP/IP or, more specifically, TCP/IPv4. However, TCP/IPv4's successor, TCP/IPv6, is now being installed by default on Windows Vista, Windows Server 2008, and some Linux systems. You can see in Figure 1-7 that both versions of TCP/IP are installed on this server. To configure a network protocol, select it and click the Properties button.

Network Client and Server Software Windows systems have both network client software and network server software installed. A **network client** is the part of the OS that sends requests to a server to access network resources. So if you want to access a file shared on a Windows computer, you need network client software that can make a request for a Windows file share. In Windows, this software is called Client for Microsoft Networks. **Network server software** is the part of the OS that receives requests for shared network resources and makes those resources available to a network client. So if you want to share files that other Windows computers can access, you need network server software installed that can share files in a format Client for Microsoft Networks can read. In Windows, this server software is File and Printer Sharing for Microsoft Networks.

Windows networking is quite robust, with a number of client and server components and a variety of configuration options. In fact, the topic deserves its own chapter, so Chapter 8 covers Windows networking in more detail. In the following activity, you explore some features of Windows networking.



Activity 1-8: Exploring Windows Networking Components

Time Required: 15 minutes

Objective: Explore features of Windows networking components.

Description: You are new to Windows Server 2008 and need to know how to manage the network connections on your server.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, **Control Panel**, and then double-click the **Network and Sharing Center** applet (shown previously in Figure 1-4).
3. At the top is a logical representation of the network. If you’re connected to the Internet, you also see an icon representing the Internet. Click the icon labeled with the name of your computer and “This computer” underneath to open an Explorer window showing your disk drives. Close this window.
4. Now click the icon representing the network that your computer is part of (yc-cnt.edu in Figure 1-4) to open an Explorer window listing all the computers found on your network. Close this window.
5. Next, click the **Internet** icon, if it’s available, to open an Internet Explorer window (or your default Web browser). Close this window.
6. Next, click the **View full map** link (usually above the Internet icon). Figure 1-8 shows an example of this map. By default, you should see Vista and Windows Server 2008 computers and any connection devices, such as switches and routers. You might see other computers as well. Close this window.

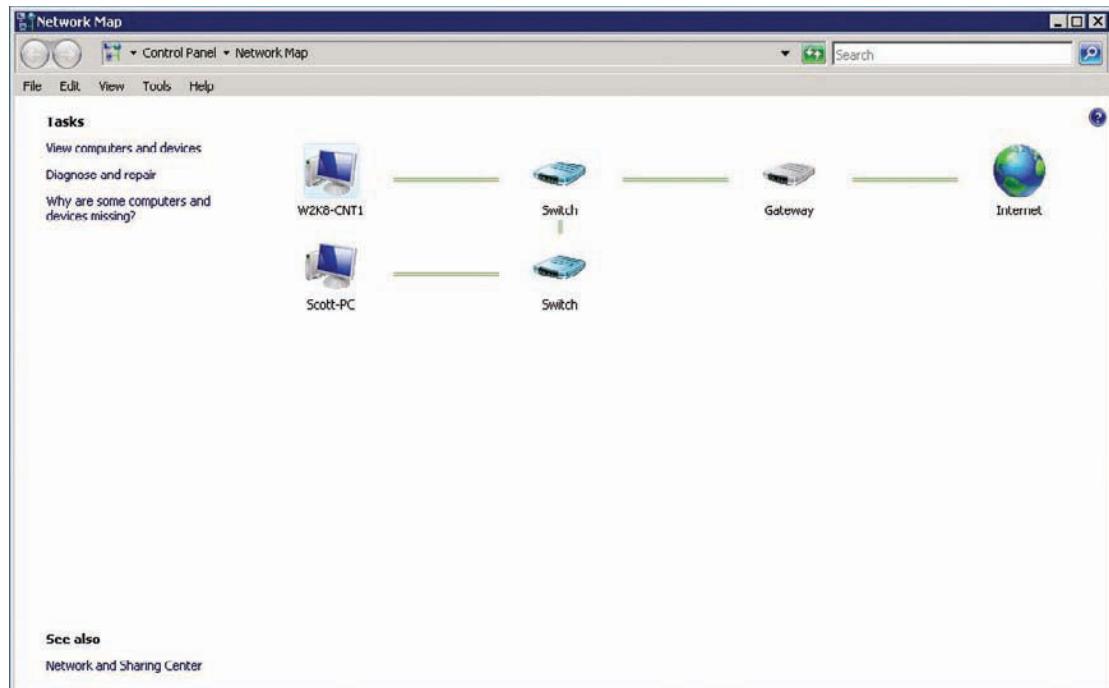


Figure 1-8 A network map

7. Click the **View status** link on the right in the Network and Sharing Center to display information about your network connection and the number of packets being sent and received (see Figure 1-9).



Figure 1-9 Viewing the status of a network connection

8. Click the **Details** button to view detailed address information about TCP/IP and physical address information about your NIC, and then click **Close**.
9. Click the **Properties** button to see details about the installed protocols, clients, and services. Each protocol and service has a check box for enabling or disabling it on the connection. Chapter 8 explores many of these items in more depth.
10. Click **Internet Protocol Version 4 (TCP/IPv4)**. (Don't clear the check box, or you'll disable the protocol.) Then click **Properties** to open a dialog box where you can change your server's IP address settings. For now, leave the settings as they are. Click **Cancel**, and then click **Cancel** again.
11. Close all open windows.

Internet Information Services

Most businesses today want a presence on the World Wide Web and often use Web technologies on their internal networks as well. Windows Server 2008 provides IIS 7.0 for building both public Web servers and private intranet servers. Like most services in Windows Server 2008, IIS isn't installed by default. To install it, you add the Web Server role in Server Manager. When you install this role, a new MMC called Internet Information Services (IIS) Manager is available in the Administrative Tools folder (see Figure 1-10).

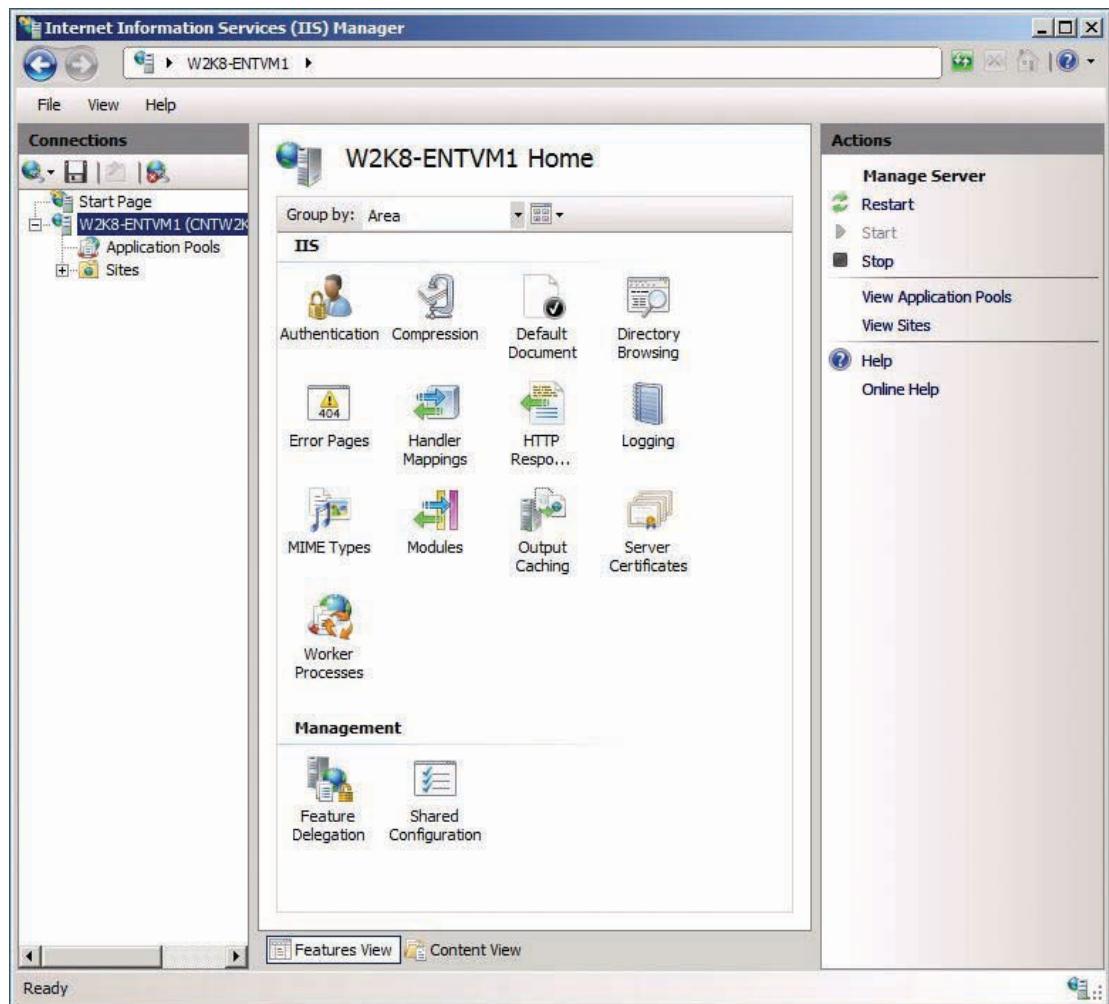
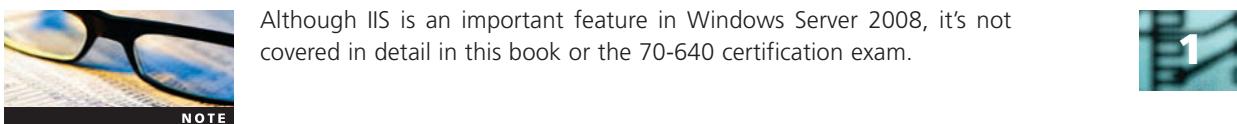


Figure 1-10 The Internet Information Services (IIS) Manager window

Microsoft has made a number of improvements to IIS 7.0:

- **Modular design**—All Web server features are designed as stand-alone components that can be installed, replaced, or uninstalled with little effort. This componentization provides a more secure environment because unused features aren't available for attackers to exploit. In addition, installing only necessary resources decreases CPU and memory use.
- **Extensibility**—Because of IIS's modular design, application developers can add functionality easily by building new server components to add to or replace existing components.
- **Manageability**—The new management interface for IIS 7.0 is a more efficient tool for managing Web servers. A key improvement over previous versions is delegated administration, so Web administrators can assign control over some aspects of the Web site to developers and content owners. In addition, a powerful command-line tool, Appcmd.exe, enables administrators to manage IIS by using scripts and batch files when necessary.



Although IIS is an important feature in Windows Server 2008, it's not covered in detail in this book or the 70-640 certification exam.

Windows Server 2008 Roles

In Windows, a **server role** is a major function or service that a server performs. Probably the best known and most common role is File Server, which allows the server to share files on a network. Along with roles are **role services**, which add functions to the main role. For example, with the File Server role, you can install a number of role services, such as Distributed File System, Windows Search Service, and File Server Resource Manager. Windows server roles and role services are installed in Server Manager.

In addition, you can add **server features**, which provide functions that enhance or support an installed role or add a stand-alone feature. For example, with the File Server role installed, you can add the Failover Clustering feature to provide fault tolerance to the file server. An example of a stand-alone feature is Desktop Experience, which adds some Vista features, such as Media Player and desktop themes. A server can be configured with a single role or several roles, depending on the organization's needs and the load a role puts on the server hardware. The following sections briefly describe the roles that can be installed on Windows Server 2008. Several of these roles, particularly those covered in Exam 70-640, are explained in detail in later chapters.

Active Directory Certificate Services

A driver's license provides information about the license holder, such as a photo, name, address, and so forth, and the state issuing the license. Similarly, a certificate, or digital certificate, is an electronic document containing information about the certificate holder and the entity that issued the certificate. This document is used to verify the identity of one or both parties who want to engage in a transaction.

The Active Directory Certificate Services (AD CS) role provides services for creating, issuing, and managing digital certificates that users and computers can use to provide verification of their identities when engaging in secure transactions over a network. When this role is installed, a number of role services can also be deployed for managing certificates. Chapter 11 covers the Active Directory Certificate Services role in more detail.

Active Directory Domain Services

The Active Directory Domain Services (AD DS) role installs Active Directory and turns a Windows Server 2008 computer into a domain controller. The main purpose of AD DS is to provide authentication and authorization to users and computers in a Windows domain environment. Active Directory stores information in a centralized database, giving administrators a tool that enables them to apply user and computer policies, install software, and apply patches and updates to client computers in the domain.

A key new feature of AD DS in Windows Server 2008 is the **read only domain controller (RODC)**, which provides the same authentication and authorization services as a standard domain controller, but administrators can't make changes on an RODC directly. RODCs are updated periodically by replication from standard domain controllers. Active Directory Domain Services, a main topic in this book, is covered in more depth in several chapters.

Other Active Directory Related Roles

In addition to Active Directory Domain Services, several other server roles related to Active Directory can be installed. Because most of these roles are new or have been updated quite a bit, they are discussed in “New Active Directory Roles” later in this chapter:

- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS)

Application Server

The Application Server role provides a high-performance integrated environment for managing, deploying, and running custom client/server business applications. Applications that depend on this role are usually built with one or more of these technologies: IIS, ASP.NET, the Microsoft .NET Framework, COM+, and Message Queuing. This book doesn’t cover the Application Server role, so for more information, see *MCTS Guide to Configuring Microsoft Windows Server 2008 Application Infrastructure* (Course Technology, 2008).

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) Server role provides automatic IP address assignment and configuration for client computers. A DHCP server responds to requests from network computers for their IP address configurations, which include an IP address and subnet mask. Optionally, a DHCP server can provide a default gateway address, DNS server addresses, WINS server addresses, and other options. A major enhancement to the DHCP Server role in Windows Server 2008 is its support for IPv6, the next generation of the IP protocol. This role isn’t covered in detail in this book. For more information, see *MCTS Guide to Configuring Microsoft Windows Server 2008 Network Infrastructure* (Course Technology, 2008, 1-4239-0236-X).

DNS Server

DNS is a critical component in the operation of the Internet and Windows domains. A DNS server resolves the names of Internet computers and computers that are members of a Windows domain to their assigned IP addresses. The DNS Server role can be tightly integrated with Active Directory, and your understanding of how to manage the DNS service in Windows Server 2008 is critical to proper Active Directory operation. When Active Directory is first installed in a Windows network, you’re prompted to specify an existing DNS server or install DNS on the same server as Active Directory. Chapter 9 covers the DNS Server role in depth.

Fax Server

The Fax Server role provides tools to manage shared fax resources and allow users to send and receive faxes through a network fax server. After the Fax Server role is installed, you can manage users who have access to fax resources, configure fax devices, create rules for routing incoming and outgoing faxes, and monitor and log use of fax resources.

File Services

The File Services role, along with a number of role services that can be optionally installed, enables administrators to provide high-availability, reliable, shared storage to Windows and other client OSs. After this role is installed, the File Server role service is installed automatically. Figure 1-11 shows Server Manager and a detailed look at the role services available when you install the File Services role. “Storage Management Enhancements” later in this chapter describes some new capabilities of this role, and Chapter 6 covers the File Services role with emphasis on the File Server role service.

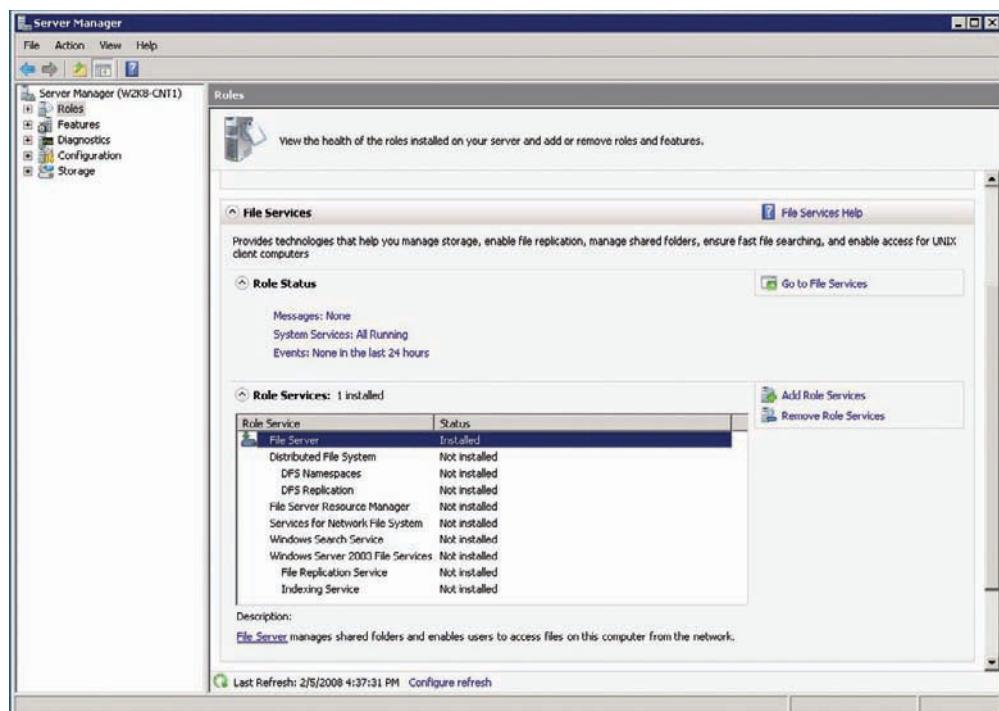


Figure 1-11 Role services for the File Services role

Hyper-V

Hyper-V provides the services needed to create and manage virtual machines running on a Windows Server 2008 computer. A **virtual machine** is a software environment that simulates the computer hardware an OS requires for installation. In essence, a virtual machine creates in software all the hardware you find on a computer, including BIOS, disk controllers, hard drives, CD/DVD drives, serial ports, USB ports, RAM, network interfaces, video cards, and even processors. An OS can be installed on a virtual machine by using the same methods for installing one on a physical machine. Of course, the most common method is to insert a CD or DVD containing the OS you want to install. With a virtual machine, however, because the CD/DVD drive is virtual, you can simply point it to an image of the OS installation disk, thus making the physical media unnecessary.

Network Policy and Access Services

This server role provides a familiar service: Routing and Remote Access Services (RRAS), which gives remote users access to a private network through traditional dial-up or, more commonly today, through a virtual private network (VPN). In addition to RRAS, other role services can be installed, including Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP). The primary goal of these services is to give users secure access to network resources by using a variety of authentication and authorization protocols that are consistent with the company's network policies. With this role installed, network administrators can use Network Access Protection (NAP). Some of these role services are described in Chapter 12, but for more detailed coverage, refer to *MCTS Guide to Configuring Microsoft Windows Server 2008 Network Infrastructure* (Course Technology, 2008, 1-4239-0236-X).

Print Services

The Print Services role enables administrators to manage access to network printers. Available role services include Print Server, which is installed by default when you install the Print Services role. The Internet Printing role service enables Web-based management of network printers and the capability to print to network printers by using HTTP. In addition, the Line Printer Daemon (LPD) role service provides print compatibility with Linux/UNIX clients. Chapter 6 covers Print Services in more detail.

Terminal Services

Terminal Services (TS) enables users and administrators to control a Windows desktop remotely or run applications hosted on a Windows server remotely. By default, the Terminal Server role service is enabled when this role is installed and permits up to two simultaneous remote desktop sessions. For additional remote desktop sessions or to run applications remotely without accessing the full desktop, the TS Licensing role service must be installed and client licenses must be purchased. Additional role services include TS Sessions Broker, which facilitates terminal server load balancing; TS Gateway, which allows connections from an external network over HTTP; and TS Web Access (discussed more in “Terminal Services Enhancements” later in this chapter), which allows access to terminal servers via a Web browser.

UDDI Services

Universal Description, Discovery, and Integration (UDDI) Services enables administrators to manage, catalog, and share Web services with an organization’s intranet users, corporate extranet partners, and Internet users. Installing this role allows users to search for Web services available for their use and provides developers with a catalog of existing applications and development work, thereby preventing the proverbial reinvention of the wheel. UDDI Services isn’t covered in this book, but for more information, see *MCTS Guide to Configuring Microsoft Windows Server 2008 Application Infrastructure* (Course Technology, 2008).

Web Server (IIS)

The Web Server role consists of the role services Web Server, Management Tools, and FTP Publishing. Each of these primary role services has a number of secondary role services that can be installed for additional functions. Covering the Web Server role alone is a chapter all on its own, but the focus of this book is on Active Directory and supporting services. “New Features in Windows Server 2008” later in this chapter discusses some new or improved features in IIS, but for a detailed discussion of the role and its supporting role services, refer to *MCTS Guide to Configuring Microsoft Windows Server 2008 Application Infrastructure* (Course Technology, 2008).

Windows Deployment Services

Windows Deployment Services (WDS) makes installing multiple Windows systems across the network fast and simple. Administrators can not only install, but also remotely configure Windows Vista and Server 2008 systems. WDS is a much improved version of Remote Installation Services (RIS), found in Windows Server 2003 and Windows 2000 Server. Some new and improved WDS features are discussed later in “New Features in Windows Server 2008,” and you can find an in-depth discussion in *MCTS Guide to Configuring Microsoft Windows Server 2008 Application Infrastructure* (Course Technology, 2008).

New Features in Windows Server 2008

Microsoft has added several new features and improved a host of existing features to make Windows Server 2008 a secure, highly available, enterprise-class server OS. Some of these features, discussed briefly in the following sections and in more detail in later chapters, are as follows:

- Server Manager
- Server Core
- Hyper-V virtualization
- Storage management enhancements
- Networking enhancements
- Network Access Protection
- Windows Deployment Services
- New Active Directory roles
- Terminal Services enhancements



Server Manager

The new Server Manager, shown in Figure 1-12, provides a single interface for installing, configuring, and removing a variety of server roles and features on your Windows server. It also summarizes your server's status and configuration and includes tools to diagnose problems, manage storage, and perform general configuration tasks. Server Manager consolidates several tools from Windows Server 2003, such as Manage Your Server, Add or Remove Windows Components, and Configure Your Server.

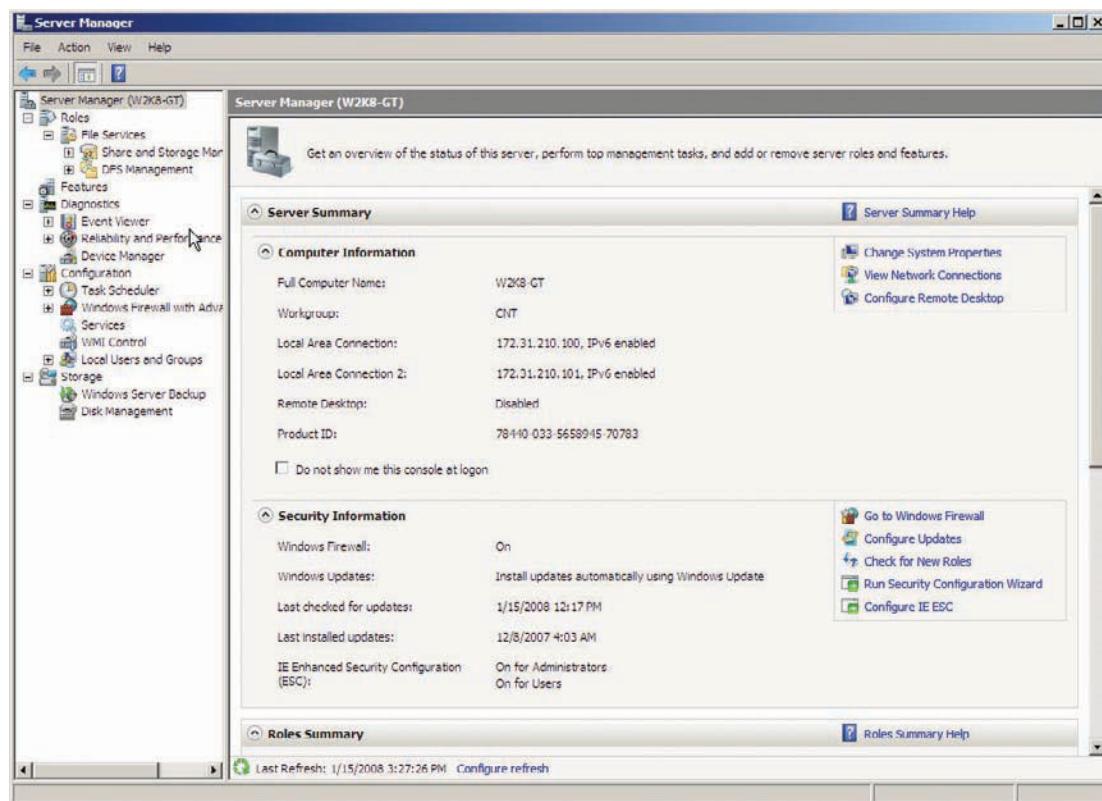


Figure 1-12 The Server Manager window



Activity 1-9: Exploring Server Manager

Time Required: 10 minutes

Objective: Review the features of Server Manager.

Description: You have just installed Windows Server 2008 and need to install some roles and features on the server. You open Server Manager to explore what's available in Windows Server 2008.

1. Log on to your server as Administrator, if necessary. Server Manager should start. If it doesn't, click the **Server Manager** icon on the Quick Launch toolbar.
2. Click **Server Manager** in the left pane, if necessary. In the right pane are several information sections: Server Summary, Security Information, Roles Summary, Features Summary, and Resources and Support.
3. In the left pane, click the **Roles** node. The right pane shows a summary of the installed roles followed by sections about each installed role. If you don't have any roles installed, you might see only limited information. You begin working with roles in Chapter 2.
4. Click the **Diagnostics** node in the left pane to display three tools for monitoring and solving problems on a server: Event Viewer, Reliability and Performance, and Device Manager.

5. Click the **Configuration** node to see five tools for performing configuration and maintenance tasks.
6. Click the **Storage** node. Here you find the Windows Server Backup program and the Disk Management tool that's part of the Computer Management MMC.
7. Close Server Manager.

Server Core

As mentioned previously, Microsoft recognized the need for a light version of Server 2008: Server Core. You can install it with the main editions discussed earlier, but it's not available in Itanium Edition. Server Core provides a minimal environment for running specific server roles. It doesn't include a full GUI and doesn't run the MMC. Server Core is intended to be managed from a command line or remotely by using an MMC, PowerShell, or Windows remote shell from another server running a full Windows Server 2008 installation. Figure 1-13 shows the standard Server Core interface with a command prompt window open.

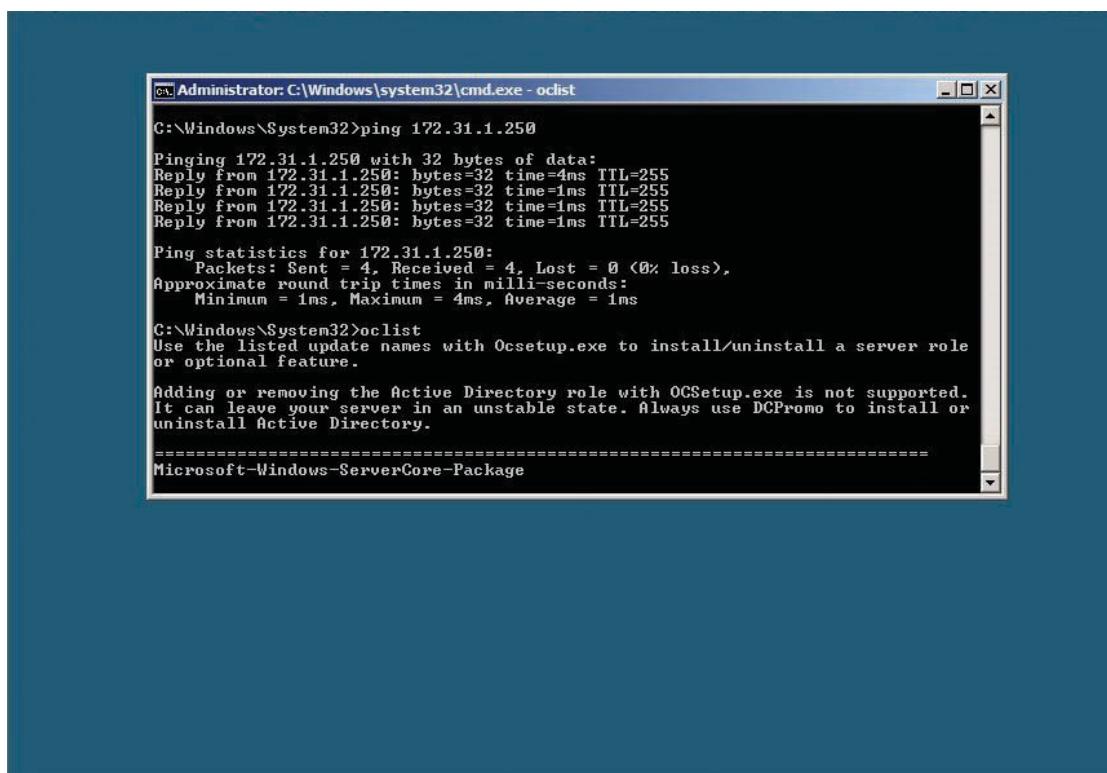


Figure 1-13 The Server Core interface

Not much to see, is there? Server Core has no Start menu or taskbar, just a command prompt window on a plain background. So what can you use this mode for? It might not be obvious, but Server Core has quite a bit under the hood. However, it lacks many of the user interface features that consume valuable hardware resources and slow critical processes down. Following is a list of server roles that can be installed on Server Core:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- Dynamic Host Configuration Protocol (DHCP) Server
- DNS Server
- File Services



- Print Server
- Streaming Media Services
- Web Server (IIS)
- Hyper-V

In addition to these roles (discussed later in “New Active Directory Roles”), Server Core supports a number of features to enhance server roles:

- Microsoft Failover Clustering
- Network Load Balancing
- Subsystem for UNIX-based Applications
- Windows Backup
- Multipath I/O
- Removable Storage Management
- Windows Bitlocker Drive Encryption
- Simple Network Management Protocol (SNMP)
- Windows Internet Naming Service (WINS)
- Telnet client
- Quality of Service (QoS)

As you can see, Server Core’s lightweight interface hides a powerful set of server capabilities that aren’t encumbered by a resource-intensive GUI. To get an idea of how streamlined Server Core is, a fresh installation takes up about 1.5 GB disk space compared with more than 5.5 GB for a fresh installation of the standard Windows Server 2008. Maintenance of Server Core is also reduced considerably because fewer patches are needed. Fewer installed components and a reduced need for patches and updates result in a more secure and reliable system. Keep in mind, however, that the following server roles can’t be installed in Server Core:

- Application Server
- Active Directory Rights Management Services
- Fax Server
- UDDI Services
- Windows Deployment Services
- Active Directory Certificate Services
- Network Policy and Access Services
- Terminal Services
- Active Directory Federation Services

In addition, the optional features that can be installed with these roles aren’t available in Server Core. Despite these drawbacks, Server Core includes the roles and features that most departmental and corporate servers need.

Hyper-V

Hyper-V is a new role that can be installed in the 64-bit versions of Windows Server 2008 Standard, Datacenter, and Enterprise editions, including Server Core. It provides tools for creating a virtual computing environment that enables you to run guest OSs on a Windows Server 2008 host server. With server virtualization, administrators can modularize network services and applications by installing a limited number of roles and features in several virtual machines and using fewer physical servers. Figure 1-14 shows Hyper-V Manager, and Figure 1-15 shows two virtual machines running on a single physical machine.

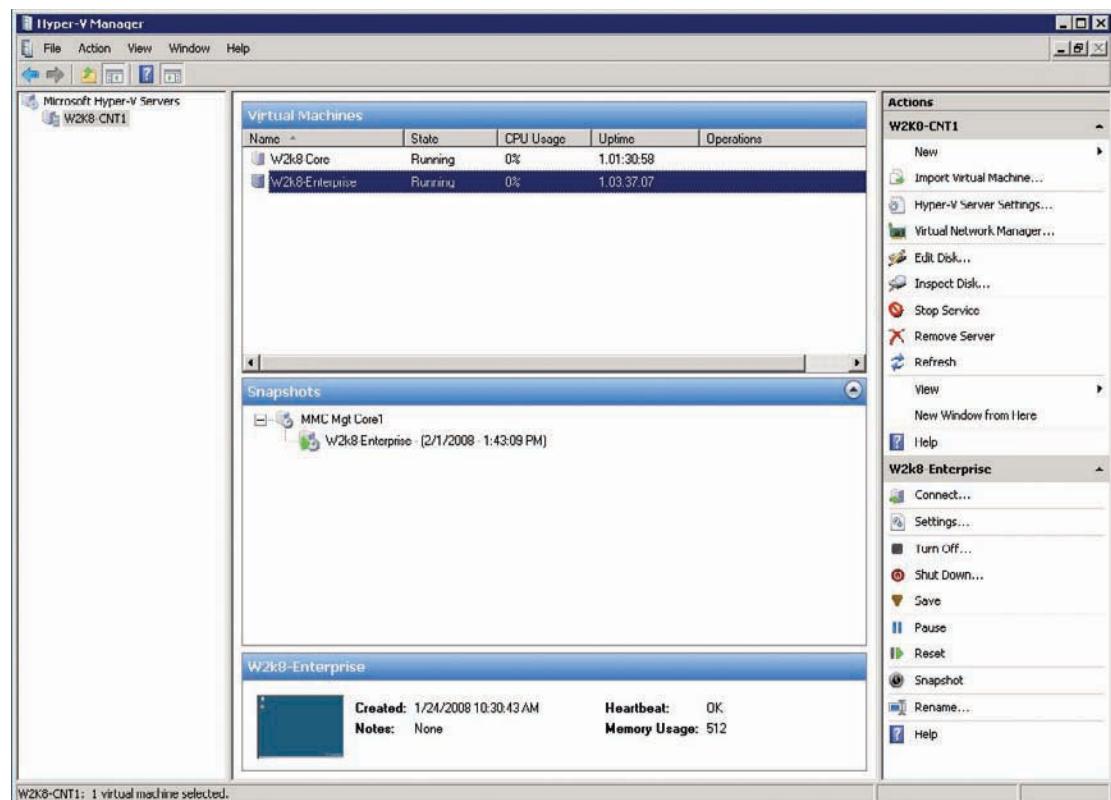


Figure 1-14 The Hyper-V Manager window

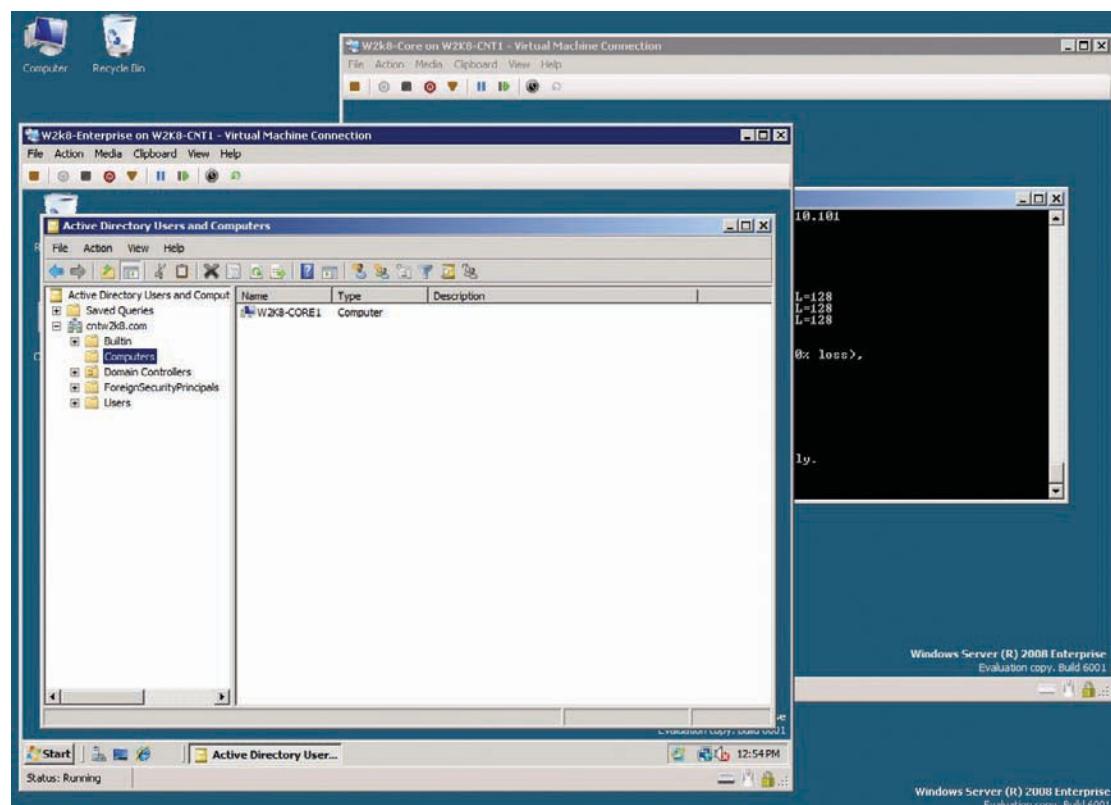


Figure 1-15 Two virtual machines running on Windows Server 2008



Using virtual machines has a number of advantages over running several applications and services on a single machine or using several physical machines to run multiple services and applications:

- Virtualization isolates critical applications so that testing, troubleshooting, and maintenance of a service or an application doesn't affect other services or applications running on the same machine.
- With virtualization, administrators can consolidate several physical servers into fewer physical servers, thereby using less power, space, and cooling. Running fewer physical computers also tends to increase reliability because there are fewer pieces of hardware that can fail.
- A virtual machine can be backed up simply by backing up the folder containing the files that make up the virtual machine. A virtual machine can also be redeployed to a new physical server by just copying those files to a new machine.
- Updates or changes to an OS or application can be tested thoroughly on a virtual machine that's a copy of a production system before actually deploying changes on the production system. This method of testing patches, updates, and changes is far easier and less expensive than trying to find an identical physical server to perform this testing.
- In an educational or training institution, students can have access to several OSs running in a virtual network environment instead of having to use multiple physical devices.

After you begin using virtualization, you'll likely find many uses and advantages for this versatile tool. Running the Hyper-V role and virtual machines has the following requirements:

- A 64-bit version of Windows Server 2008 Standard, Enterprise, or Datacenter Edition.
- A server running a 64-bit processor with virtualization support and hardware data execution protection. Typical processors include Intel Core 2 Duo processors and Intel Core 2 Extreme processors. AMD offers the Opteron 1000, 4000, and 8000 series processors and Phenom processors.
- Enough free memory and disk space to run virtual machines and store virtual hard drives. Virtual machines use the same amount of memory and disk space resources as a physical machine.

Storage Management Enhancements

Managing storage has become a full-time job for some administrators. The amount of data people need to store is always increasing, and the varying types of data they need to store are a challenge for server administrators. Windows Server 2008 includes tools to meet today's increasing storage requirements and make managing storage, well, a little more manageable. Many of these enhancements are included in the File Services role, described in more detail in the next section. The following list briefly describes some enhancements to storage management in Windows Server 2008:

- *Share and Storage Management MMC snap-in*—This management tool, shown in Figure 1-16, is new in Windows Server 2008 and provides a single interface for viewing status and monitoring and configuring shared folders and server volumes.
- *File Server Resource Manager (FSRM)*—This role service, introduced in Windows Server 2003 R2, can be added as a component after the File Services role has been installed. FSRM provides storage reports, allows configuration of disk quotas, and enables administrators to filter the types of files users can store on the server.
- *Windows Server Backup*—This tool replaces the NTBackup.exe tool in earlier versions of Windows Server. It doesn't have the same variety of options and backup configurations as NTBackup.exe; instead, it's intended as an easy-to-use wizard focused on small business users. Windows Server Backup is designed to back up entire volumes to another hard disk or DVD rather than tape and provides an improved complete system restore over the automatic system restore in previous server versions.
- *Other improvements*—They include Storage Explorer to better manage storage area networks (SANs); improvements to the file-sharing protocol Server Message Block (SMB)

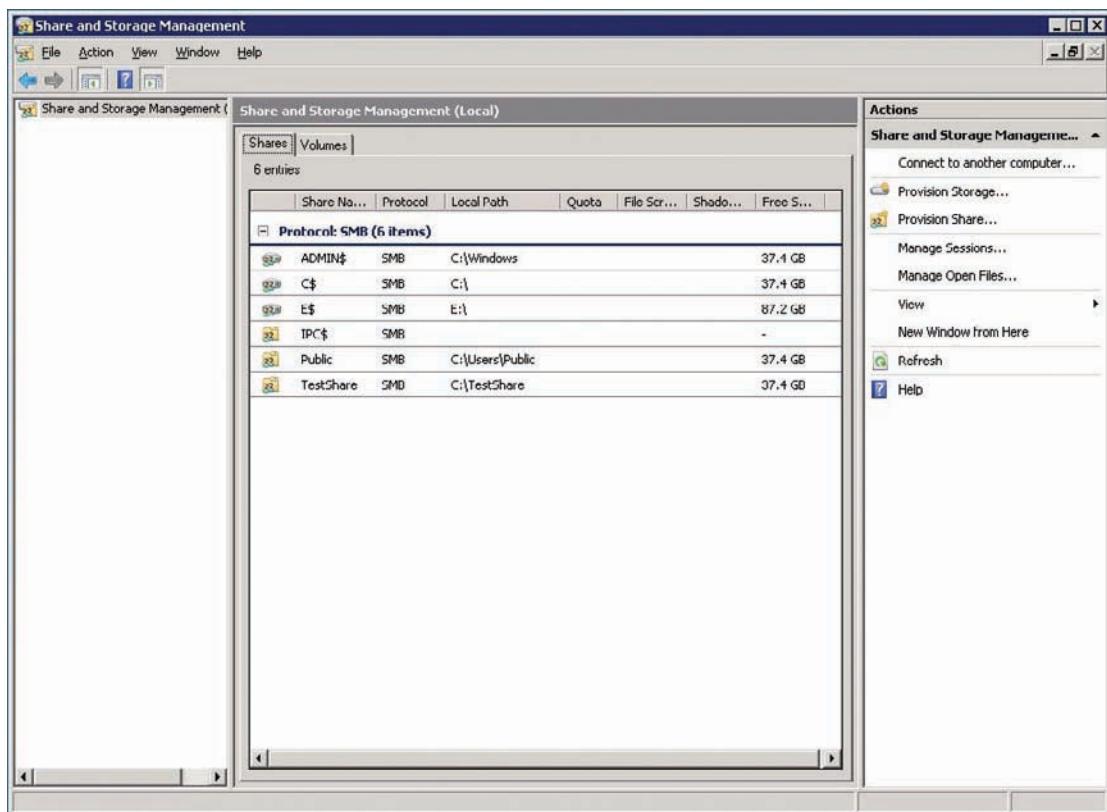


Figure 1-16 The Share and Storage Management MMC snap-in

with SMB 2.0; multipath I/O, which provides redundancy and load balancing for storage devices; and remote boot support over standard Ethernet connections.

The list could go on, but you can see that Microsoft is making an effort to ensure that storage management is easier and more effective in this version of Windows Server.

Networking Enhancements

Several networking enhancements in Windows Server 2008 were introduced in Windows Vista and some are new in Windows Server 2008. Many of the enhancements center on improved support for IPv6, such as the implementation of DHCPv6 and load-balancing support for IPv6. Other general networking enhancements include a redesigned TCP/IP stack, known as the Next Generation TCP/IP stack, that sports a host of performance, error-detection, and recovery improvements. For “road warriors” and telecommuters, Windows Server 2008 and Vista Service Pack (SP) 1 offer marked improvements in virtual private networking with a new protocol called Secure Socket Tunneling Protocol (SSTP). This new protocol vastly increases the number of situations in which a VPN connection works, whether the client or server computer is behind a Network Address Translation (NAT) router, firewall, or proxy.

Network Access Protection

Network Access Protection (NAP) gives network administrators a powerful tool to ensure that client computers on the network are equipped with required security features. For example, NAP policies can be defined that require all client computers to have the latest updates to antivirus software, the most recent OS updates, and compliant firewall settings. Computers can be monitored to make sure they meet security health requirements, and noncompliant machines can be restricted automatically from accessing certain network resources. In addition, NAP can remedy security-compliance problems by forcing computers to access servers that update them.



Windows Deployment Services

Windows Deployment Services (WDS) updates Remote Installation Services, available in earlier versions of Windows Server. WDS is designed to make unattended network installation of Windows OSs (in particular, Windows Server 2008 and Vista) easier and faster. A key feature in WDS is multicast deployment of disk images, which reduces the network bandwidth required when sending disk images to dozens or even hundreds of computers simultaneously. WDS also includes enhanced tools to create, monitor, and configure Windows OSs for network deployment.

New Active Directory Roles

Active Directory is the heart of any Windows network, and Microsoft has worked to improve on existing Active Directory functions and add new roles and features. Here's a partial list of new or upgraded roles in Active Directory (discussed in more detail in Chapter 12):

- *Active Directory Lightweight Directory Services (AD LDS)*—This role provides directory service functions to applications that store information in a directory instead of a database or flat file. Directory services, unlike databases, are optimized for data retrieval rather than read-write transaction processing. The types of applications that benefit from AD LDS are those requiring a lot of data retrieval, such as customer relationship management (CRM) and human resources applications. In essence, what AD LDS provides is an easy way to integrate applications that benefit from a directory service into a Windows network environment. Although AD LDS has much of the same functionality as Active Directory Domain Services, it doesn't require a domain controller or even a domain.
- *Active Directory Federation Services (AD FS)*—This role addresses the problem of users in partner organizations being required to provide new logon credentials to access Web applications in each other's extranets. For example, a supplier of hardware items has a Web site for its business customers to enter orders, check on inventory, and so forth. Currently, the supplier's customers are required to log on to the Web site to access the order processing/inventory application. With AD FS, two organizations can set up a trust relationship between their networks that allow one organization's credentials to be accepted by the other organization or vice versa. This arrangement enables the hardware supplier's customers to access the Web application seamlessly without providing new logon credentials. This process is called **single sign-on (SSO)**, which makes it possible for users to access resources in their own organization as well as partner organizations with just a single logon.
- *Active Directory Rights Management Services (AD RMS)*—This role is designed to be used with RMS-enabled applications, such as Microsoft Office 2007 and Internet Explorer 7.0. Active Directory RMS allows the creator of digital documents, such as e-mail, Web pages, and Office documents, to control how authorized users can use a document and prevent unauthorized users from accessing the document. For example, an e-mail message can be marked as Recipient Read Only, and the message can be prevented from being modified, forwarded, or even printed.

This list describes only a few of the new or improved Active Directory roles. Other roles, such as Active Directory Domain Services and Active Directory Certificate Services, also have major improvements over earlier versions, and these services are explained in detail in later chapters.

Terminal Services Enhancements

The Terminal Services role enables users to run Windows applications located on a remote server or control the desktop of another Windows computer remotely. One of the biggest enhancements to Terminal Services is the RemoteApp feature, which makes it possible for users to run a Windows application on a terminal server rather than their client computers. In previous versions of Terminal Services, when users connected to a terminal server, a Windows remote desktop opened in a window on their client computers, and they could then run applications on the terminal server from the remote desktop. With RemoteApp, the user runs the application on the terminal server and sees only the window the application is running in. So from the user's

perspective, running an application through Terminal Services looks no different from running the application locally.

Another new feature in Terminal Services is Terminal Services Web Access (TS Web Access), which enables users to connect to a remote desktop or remote application by using a Web browser. Windows Server 2003 and Windows XP had a similar feature called Remote Desktop Web Connection, but users had to download extra software, and RemoteApp wasn't an option. With TS Web Access, no additional software download is required if the client computer is running Vista. Furthermore, users can connect to a Web page listing available RemoteApp programs and select a program to run remotely. The program loads and looks like any other program running on the user's desktop. Figure 1-17 shows the Paint program accessed through TS Web Access and RemoteApp. The foreground window is the Paint application, and the background window is an Internet Explorer window connected to the TS Web Access server. Paint is listed as a program available via RemoteApp.

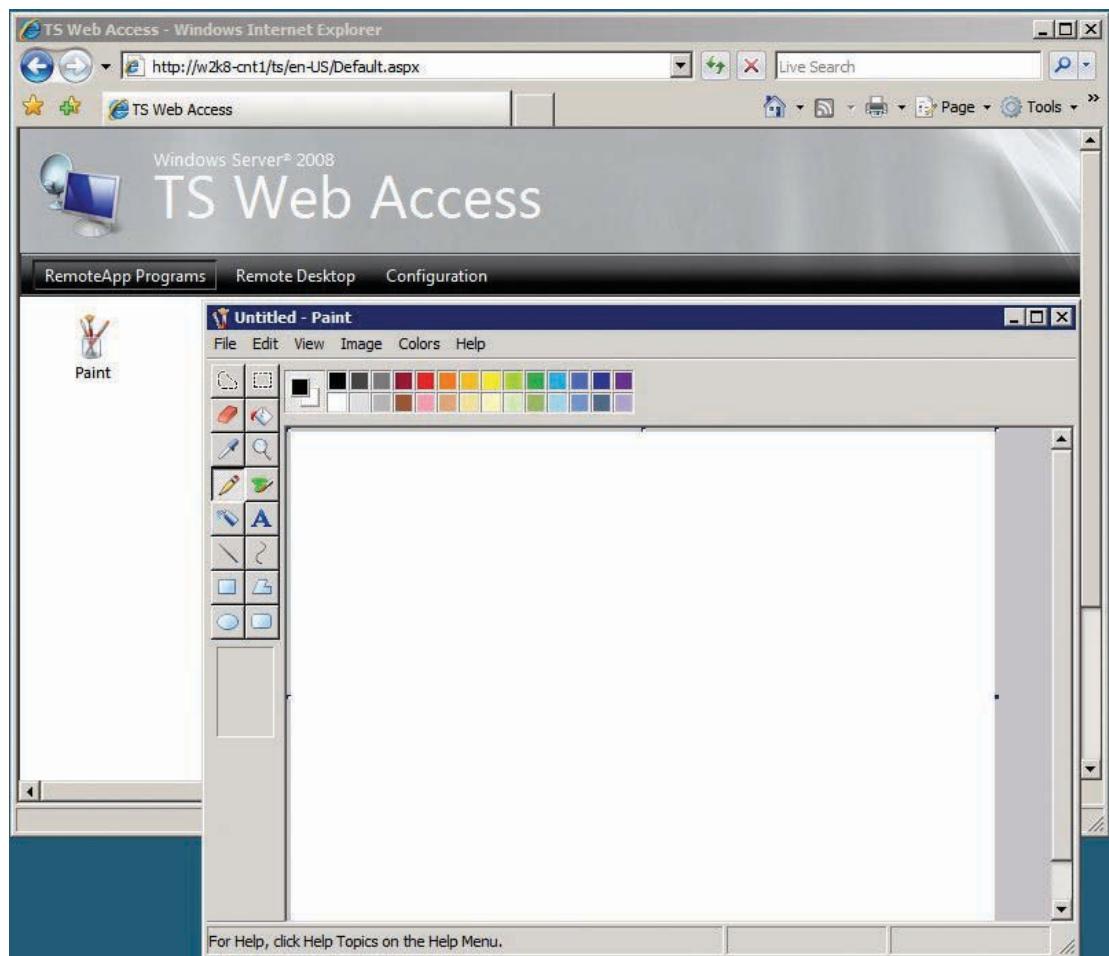


Figure 1-17 Running Paint through TS Web Access

Terminal Services Gateway (TS Gateway) adds to TS Web Access functionality by allowing a secure, encrypted connection using Secure HTTP (HTTPS) from a remote client to a TS Web Access server over the Internet. Without TS Gateway, remote users would have to access the Terminal Services server through a VPN, or the Terminal Services server would have to be directly accessible to the public Internet, which poses serious security risks.

The upgrades and enhancements covered in this section are by no means comprehensive, but they show that Windows Server 2008 is not just a simple update of Windows Server 2003. Some of these enhancements are discussed in more detail throughout this book.

Chapter Summary

- A server is largely defined by the software running on the computer hardware rather than the computer hardware on which the software is running. Although most client OSs now provide some server services, such as file and printer sharing, a true server OS is usually defined as providing these important network services: directory services, DNS, remote access, DHCP, and robust network application services. In addition, current server OSs include hardware support for multiple processors, disk fault tolerance, and clustering.
- Windows Server 2008 is available in four main editions: Standard, Enterprise, Datacenter, and Windows Web Server 2008. In addition, each edition except Windows Web Server 2008 can be purchased with or without the Hyper-V role. The differences between these editions revolve around hardware support and advanced fault-tolerance features. Windows Web Server 2008 and Standard Edition support up to 4 processors, Enterprise Edition supports up to 8, and Datacenter Edition supports up to 64. Other differences include support for clustering, hot-add or hot-replace hardware capabilities, and the number of virtual licenses included in 64-bit versions.
- The technologies that make up the core functionality of Windows Server 2008 include NTFS, Active Directory, the Microsoft Management Console, disk management, file and printer sharing, networking components, and IIS.
- Windows Server 2008 includes 17 primary server roles and a plethora of supporting role services, so administrators can configure a server as a narrowly focused device, providing just one or two specific services, or as a general, do-it-all system that's the center of a Windows network.
- Windows Server 2008 builds on the success of Windows Server 2003 by adding a host of new and improved services. They include an improved Server Manager, Server Core, Hyper-V, enhancements in storage management and networking (such as Network Access Protection features), improvements in Remote Installation Services and Terminal Services, and many new or improved Active Directory roles and role services.

Key Terms

Active Directory The Windows directory service that enables administrators to create and manage users and groups, set network-wide user and computer policies, manage security, and organize network resources.

Datacenter Edition A Windows Server 2008 edition with support for up to 64 processors, primarily intended for organizations managing huge amounts of data, using virtualization on a large scale, consolidating servers, or running high-volume, transaction-heavy applications.

domain controller A Windows server that has Active Directory installed and is responsible for allowing client computers access to domain resources.

Enterprise Edition A Windows Server 2008 edition suitable for medium to large businesses that need high-availability network services. Supports up to eight processors and up to 2 TB RAM. Its most notable feature that isn't available in Standard Edition is clustering.

member server A Windows server that's in the management scope of a Windows domain but doesn't have Active Directory installed.

network client The part of the OS that sends requests to a server to access network resources.

network protocol Software that specifies the rules and format of communication between devices on a network.

network server software The part of the OS that receives requests for shared network resources and makes those resources available to a network client.

New Technology File System (NTFS) A file system used on Windows OSs that supports compression, encryption, and fine-tuned permissions.

read only domain controller (RODC) A new feature of Active Directory Domain Services in Windows Server 2008, an RODC provides the same authentication and authorization services as a standard domain controller, but administrators can't make changes on an RODC directly.

role services Services that can be installed in Server Manager to add functions to the main server role. *See also* server role.

Server Core A new Windows Server 2008 installation option that uses a limited version of the GUI to take up fewer resources.

server features Components you can install that provide functions to enhance or support an installed role or add a stand-alone feature.

server operating systems OSs designed to emphasize network access performance and run background processes as opposed to desktop applications.

server role A major function or service that a server provides.

single sign-on (SSO) An authentication feature that makes it possible for users to access resources in their own organization as well as partner organizations with just a single logon.

stand-alone server A Windows server that isn't a domain controller or a member of a domain.

Standard Edition A Windows Server 2008 edition suitable for most small to medium businesses that need a robust solution for file and printer sharing, centralized control over user accounts and network resources, and common services found in most networks.

virtual machine A software environment that simulates the computer hardware an OS requires for installation. A virtual machine creates in software all the hardware you find on a computer, including BIOS, disk controllers, hard drives, CD/DVD drives, serial ports, USB ports, RAM, network interfaces, video cards, and even processors.

Windows domain A group of Windows computers that share common management and are subject to rules and policies that an administrator defines.

Windows Web Server 2008 A Windows Server 2008 edition designed to operate as a single-purpose Web server running IIS 7.0.

Windows workgroup Also called a peer-to-peer network, it's a small collection of Windows computers whose users typically have something in common, such as the need to share files or printers with each other. No computer has authority or control over another. Logons, security, and resource sharing are decentralized.

Review Questions

1. Which of the following best defines a computer used as a server?
 - a. Computer hardware that includes fast disk drives and a lot of memory
 - b. Operating system software that includes clients, such as a Web browser and Client for Microsoft Networks
 - c. Operating system software that includes directory services and domain name services
 - d. A computer with Linux installed
2. Which of the following best describes a Windows client OS?
 - a. Supports up to 64 processors
 - b. Includes disk fault-tolerance features, such as RAID
 - c. Supports network connections based on the number of purchased licenses
 - d. Supports only 10 network connections
3. Windows Server 2008 _____ Edition supports a maximum of eight processors.
4. Which of the following is true of Windows Web Server 2008?
 - a. Supports hot-add memory
 - b. Supports only four processors

- 
- c. Supports a single virtual license
 - d. Supports 2 TB of RAM in the 64-bit version
5. You have recently purchased a new computer that supports four processors, 64-bit processing, and up to 256 GB of RAM. You need to run several network applications that you expect will require at least 128 GB of RAM and possibly more. Which of the following Windows Server 2008 editions should you install on your server?
- a. Windows Web Server 2008
 - b. Standard Edition
 - c. Enterprise Edition
 - d. Datacenter Edition
6. Each core in a multicore processor counts toward the maximum number of processors that Windows Server 2008 supports. True or False?
7. You have purchased a new server that supports up to 8 GB RAM and two processor sockets. You're currently running three other servers that provide Active Directory services, file and printer sharing, and DNS. This new server will act as a departmental Web server for about 50 users. You want to keep costs to a minimum. Which of the following editions should you choose?
- a. Windows Web Server 2008
 - b. Standard Edition
 - c. Enterprise Edition
 - d. Datacenter Edition
8. You're considering purchasing a new server with Windows Server 2008 installed that has the capability to run four or more virtual machines and provides fault-tolerance features, such as adding and replacing memory and CPUs without shutting down the system. Which edition of Windows Server 2008 should you ask to be installed on the server?
- a. Windows Web Server 2008
 - b. Standard Edition
 - c. Enterprise Edition
 - d. Datacenter Edition
9. You need to support a large disk volume of 200 GB or more and limit the amount of space users' files can occupy on the volume. Which file format should you use?
- a. FAT
 - b. FAT32
 - c. NTFS
 - d. DFS
10. Which of the following disk formats supports encryption? (Choose all that apply.)
- a. FAT
 - b. FAT32
 - c. NTFS
 - d. DFS
11. What feature of the Windows Server 2008 file system should you enable if you want users to be able to restore deleted or previous versions of a file in a shared folder?
- a. Distributed File System
 - b. Disk quotas
 - c. Shadow copies
 - d. Bitlocker

12. You're a consultant for a small business with four computer users. The company's primary reason for networking is to share the Internet connection, two printers, and several documents. Keeping costs down is a major consideration, and users should be able to manage their own shared resources. Which networking model best meets the needs of this business?
 13. Which networking component includes a device driver?
 - a. Network server software
 - b. Network client software
 - c. Network protocol
 - d. Network interface
 14. If you want to share files with other Windows computers, you should have _____ installed and enabled on your computer.
 - a. Client for Microsoft Networks
 - b. File and Printer Sharing for Microsoft Networks
 - c. IPX/SPX protocol
 - d. Active Directory
 - e. Domain Name Services
 15. If you want to make a computer a domain controller, which of the following should you install?
 - a. Client for Microsoft Networks
 - b. File and Printer Sharing for Microsoft Networks
 - c. IPX/SPX protocol
 - d. Active Directory
 - e. Domain Name Services
 16. Which of the following server roles turns your computer into a Web server?
 - a. Active Directory Domain Services
 - b. DNS Server
 - c. IIS
 - d. Terminal Services
 - e. Hyper-V
 17. Which of the following is the common framework in which most Windows Server 2008 administrative tools run?
 - a. Windows Management Center
 - b. Microsoft Management Console
 - c. Server Configuration Manager
 - d. Windows Configuration Manager
 18. You have been asked to advise a business on how best to set up its Windows network. Eight workstations are running Windows Vista Business. The business recently acquired a new contract that requires running a network application on a server. A secure and reliable environment is critical to run this application, and security management should be centralized. There's enough budget for new hardware and software, if necessary. Which Windows networking model should you advise this business to use?
 - a. A Windows domain using Active Directory
 - b. A Windows workgroup using Active Directory
 - c. A peer-to-peer network using File and Printer Sharing
 - d. A peer-to-peer network using Active Directory

19. Which of the following is *not* a server role that can be installed in Windows Server 2008?
- Active Directory Domain Services
 - Failover Clustering
 - File Services
 - Hyper-V
20. Which of the following is required to install the Hyper-V role in Windows Server 2008? (Choose all that apply.)
- A CPU that has virtualization support
 - 16 GB RAM
 - A 64-bit version of Windows Server
 - A processor that supports hardware data execution protection
21. Your manager has asked you to audit 150 Vista client computers to make sure they are up to date with patches, virus software, and firewall settings. You realize that checking all these computers manually will take an inordinate amount of time. Which new feature can you configure in Windows Server 2008 to make this job much easier?
- Active Directory Rights Management Services
 - NTFS
 - Read only domain controller
 - Network Access Protection
 - UDDI Services
22. Your goal is to install Windows Server 2008 using as few hardware resources as possible. You plan to deploy only the DNS Server role on this new server. Your server supports a maximum of 8 GB RAM, and you might need to add failover clustering later. Which Windows Server 2008 edition should you install?
- Web Edition
 - Standard Edition 64-bit
 - Standard Edition 64-bit Server Core
 - Enterprise Edition 32-bit Server Core
 - Enterprise Edition 64-bit
23. The Terminal Services RemoteApp feature provides users with a desktop view of the remote computer. True or False?
24. If you want to provide users with secure network transactions that verify the identity of sender and receiver with a digital certificate, which role should you consider installing?
- Active Directory Federation Services
 - Active Directory Certificate Services
 - Active Directory Rights Management Services
 - Active Directory Lightweight Directory Services
25. You have just installed a human resources application that's directory service enabled on a Windows Server 2008 server. You're running mainly Linux in your organization and don't run a Windows domain, but you want to take advantage of the benefits a directory service would provide. Which Windows Server 2008 role should you install?
- Active Directory Federation Services
 - Active Directory Certificate Services
 - Active Directory Rights Management Services
 - Active Directory Lightweight Directory Services

Case Projects



CASE PROJECTS

Case Project 1-1: Selecting a Windows Server 2008 Edition

You're installing a new network for Cool Gadgets, a new manufacturing business. There will be 25 client computers running Vista, and Cool Gadgets plans to run a Web-based order processing/inventory program that for now will be used only by in-house employees while they are on site. Cool Gadgets wants to be able to manage client computer and user policies as well as share documents among employees. Growth is expected, but the budget is tight, so the company needs to purchase only what's necessary to get running and leave high-end server features, such as hot-add and hot-replace hardware, for future consideration. Which Windows Server 2008 edition do you recommend? Explain your answer.

Case Project 1-2: Choosing Server Roles

You have purchased a server and a 32-bit edition of Windows Server 2008 for your client, Cool Gadgets. Review Case Project 1-1 for its computing requirements. You have installed Windows Server 2008 and are now installing and configuring services that your client will need. Based on the needs described in Case Project 1-1, which server roles should you install at a minimum, and which networking model should you use? Explain your answer.

Case Project 1-3: Performing Additional Server Configuration Tasks

Cool Gadgets has been operating for six months, and business is good. You do a spot check on server resources and find that RAM use is at 50%, which is fine, but the data volume is approaching 90% full. There are two volumes on this server, one for OS and program files and one for data storage. You inspect the data volume and find that some users are storing large amounts of data on the server. You check with the owner and determine that each user should require only about 1 GB of storage on the server for necessary documents. Because some users are clearly exceeding this limit, you're asked to come up with a solution. What file system option can you use, and which file system format must be used with this option?

Case Project 1-4: Explaining Server Virtualization

The owner of Cool Gadgets is always thinking about how he can use technology to benefit the operation of his business. He read an article about Windows Server 2008 and the new Hyper-V feature. He has asked you to explain what Hyper-V is and whether he needs it now or in the future for the efficient operation of his network. Write a memo explaining what Hyper-V is and whether you recommend installing it now or waiting until later.

Installing Windows Server 2008

After reading this chapter and completing the exercises, you will be able to:

- Plan a Windows Server 2008 installation
- Work with Server Core systems
- Use Hyper-V for server virtualization

Once an arduous and sometimes intimidating task, installing a Windows server has become an easy, straightforward process with Windows Server 2008. The installation process in Windows Server 2008 is similar to the Vista process and requires little user interaction from start to finish.

The real work of a Windows Server 2008 installation takes place before you actually begin—in the planning phase. This chapter covers the actual installation process, but more important, discusses the planning that should go into installing a server in a production environment. Answers to questions about how the server will be used, whether the installation is an upgrade or new installation, and roles the server will play in the network factor into how you decide to install the operating system. After installing your server, you need to undertake some postinstallation tasks right away, many of which depend on decisions you made in the planning phase. This book doesn't cover in detail the tools for deploying Windows Server 2008 in large numbers; instead, it focuses on the planning process for both small and large installations and the postinstallation tasks.

Two new installation options in Windows Server 2008 also factor into your installation decisions. The lightweight server environment called Server Core offers a new option for installing a Windows server. Similarly, the Hyper-V role that can be installed on an existing server gives you the option of installing your server as a virtual machine rather than a physical server. This chapter explores all these options so that you can make wise choices when you deploy Windows Server 2008 on your network.

Planning a Windows Server 2008 Installation

The actual process of installing Windows Server 2008 has been simplified to the point that you might be inclined to get out the DVD and forge ahead without much forethought. However, that temptation could be a time-consuming and costly mistake if you don't have a well-thought-out plan for using the technologies in Windows Server 2008. Aside from selecting an edition, choosing an upgrade or a new install, and deciding whether to use a domain controller, among other decisions, your installation options have expanded. Today, you can do a full installation or just a Server Core installation, and you can install your server on physical hardware or as a virtual machine.

Admittedly, a single server installation for a small business with 25 users doesn't present a major challenge requiring weeks of careful consideration and planning. You can make a few decisions and get on with it. However, situations such as installing 400 servers or bringing a branch office online, which requires integrating its server with the existing network, involve more planning. This section doesn't attempt to cover every possible server installation you might encounter. Instead, it gives you the knowledge you need to understand some potential issues and arms you with questions you need to answer before proceeding.



This book doesn't cover Windows Deployment Services (WDS), a tool for deploying Windows OSs (particularly Vista and Server 2008) via a network installation, because it's not a topic of the 70-640 certification exam. WDS is described briefly in Chapter 1 and covered in *MCTS Guide to Configuring Microsoft Windows Server 2008 Application Infrastructure* (Course Technology, 2008).

The network environment in which you're deploying a server and the roles a server will play on the network are the key considerations in planning Windows Server 2008 installations. In the following sections, you examine these common installation situations and some of the issues and options involved:

- Installing the first server in a new Windows network
- Expanding your network by adding a second server or installing a server in a branch office
- Upgrading from earlier Windows versions

Installing the First Server in a New Network

Installing Windows Server 2008 in a new network that doesn't already have Windows servers operating is usually the most straightforward installation situation. The following descriptions assume you're installing the first server in a small network with fewer than 100 users.

One issue to consider for any server installation is hardware features. The following list describes a few of these features:



NOTE

The terms CPU and processor are often used interchangeably. A physical processor is a chip that's installed in a socket on a motherboard. However, today's physical processors might have multiple processor cores, and each core can perform the same work as a single-core physical processor.

2

- **CPU architecture**—Major CPU manufacturers typically have a workstation line and a server line of processors. The server line includes Intel Xeon and AMD Opteron. Depending on the expected server workload, you must also consider how many physical processors and how many CPU cores each processor should have. Server virtualization, which has special CPU requirements, is another factor. To sum up, here are some of the CPU architecture options:
 - **Workstation or server line of processors:** Typically, the workstation line supports only one or at most two physical CPUs; the server line supports four or more.
 - **Total number of physical processors:** You can buy a system with one processor now and add more later if the motherboard supports multiple physical processors. Be aware, however, that you must use identical processors in multiprocessor systems, and finding an identical match three or four years later can be difficult. Also, keep in mind the Windows Server 2008 edition you plan to install because the maximum number of processors varies.
 - **Number of cores in each processor:** With multicore CPUs becoming the norm today, buying a system that supports them makes sense. Multicore CPUs usually don't achieve the same performance as multiple physical processors, but they have become an inexpensive way to boost performance.



NOTE

Recall from Chapter 1 that Microsoft considers a physical processor, regardless of the number of cores, as a single processor when determining how many processors a particular edition supports. Also, it used to be necessary to install a new Hardware Abstraction Layer (HAL) that supports multiprocessing when a processor was added. Windows detects contemporary processors as multiple processors, so the correct HAL is already installed.

- **32-bit versus 64-bit processors:** Rumor has it that Windows Server 2008 is the last major server OS from Microsoft that will have 32-bit versions, so choosing a 64-bit processor is probably wise. In addition, Hyper-V requires using a 64-bit processor, and the only real drawback is less driver support than for 32-bit systems. On a server, driver support is less of an issue because you're unlikely to be running a wide variety of unusual devices.
- **Virtualization extensions:** With a 64-bit processor, chances are good that it supports virtualization extensions, but you must be certain if you want to run Hyper-V. On Intel processors, look for the Intel Virtualization Technology (Intel-VT) label, and on AMD processors, look for AMD-V. These extensions are a prerequisite to installing the Hyper-V role.
- **Disk subsystem**—Before the arrival of serial ATA (SATA) drives, the only real choice of hard drives for servers was SCSI. Both specifications are making performance improvements constantly, and now, to complicate matters, serial attached SCSI (SAS) is available. Current knowledge indicates that for entry-level or departmental servers, SATA is a good choice because it's inexpensive and offers excellent performance. For enterprise servers or servers accessed 24/7, SAS and the newest SCSI systems have a performance and reliability advantage. SCSI disks are generally designed for continuous use; SATA drives tend to be designed more for consumer use rather than around-the-clock use. Doing research on current technology and your network's needs before deciding is best.
- **Hot-add/hot-replace features**—Say you've noticed that memory use has increased to dangerously high levels after installing a new database application on your server. You need to

add memory to the server before it crashes; in the past, this process meant shutting down the server first. Not so with Windows Server 2008 Enterprise and Datacenter editions because both support **hot-add** memory. Unfortunately, the server hardware must also support this feature, and you find it only in high-end, enterprise-class servers. Some servers even support adding or replacing a processor without a system shutdown, but this feature is supported only in Datacenter Edition. The capability to hot-add disk drives is more common and can be found in almost all server classes. If you need more disk space or need to replace a failed disk in a RAID configuration, you can simply install the new disk without shutting down the server. All editions support disk **hot-replace** or hot-add if the hardware supports it.

This list covers just a few of the server hardware features you should consider before installing a new server. The best advice is to forge a good relationship with a knowledgeable vendor you can consult with when you need to make a purchase. This way, you can focus on managing your server, and your vendor can focus on keeping up with the latest hardware options.



To make sure hardware selections are compatible with Windows Server 2008, check the Windows Server Catalog at www.windowsservercatalog.com.

When installing the first server in a new network, you must make some decisions shortly after finishing the installation. Some are fairly straightforward, but others take some thought and consultation. Here's a list of some decisions you need to make:

- What should you name the server? This decision is more important than it sounds. Every computer needs a name so that it can be identified on the network. A server name must be unique on the network and should include some description, such as its location or primary function. Server names should also be simple and easy to remember because users often access servers by name.



Even if you expect the server to be the only one on the network, you shouldn't use just "Server" as the name. Situations often change and require adding a server, so at least give it a number, such as Server1. Subsequent server names can be a bit more descriptive, such as Mail1, Accounting1, or Room19.

- Which network protocols and addresses should you use? By default, Windows installs both TCP/IPv4 and TCP/IPv6 in Windows Server 2008 and Vista. You can't uninstall them, but you can disable them in a network connection's Properties dialog box. Disabling a protocol is recommended if you're not using it. TCP/IPv4 is still the predominant LAN protocol and probably will be for years. Previous Windows versions had the option of installing other protocols and services, such as IPX/SPX (NWLink) and client/server components for NetWare. Windows Server 2008 has no additional protocol or client options, so if they are important, you need to find a third-party solution or use Windows Server 2003 or earlier.
- How should I assign an IP address to the server? By default, Windows Server 2008 uses automatic IP addressing, but a server should have a static IP address. Some server roles actually require assigning a static address. If you haven't devised your addressing scheme, now is the time to do that. Generally, servers use one of the first or last addresses in the address range, such as 192.168.1.10 or 192.168.1.200. Whatever you decide, be consistent so that when more servers are added, you can assign addresses easily.
- Setting the correct time zone isn't a decision but a task you must complete because having the wrong time zone can cause all manner of problems, particularly in a domain environment. Certain functions in a domain network, such as user authentication, depend on client and server computers having their clocks well synchronized.
- Should I use the workgroup or domain model? As discussed in Chapter 1, the Windows domain model has advantages in usability, manageability, and security. If you've invested in

a Windows Server OS, it makes sense to get the most out of it by using the domain model and installing Active Directory. With a small network of fewer than 10 users, however, the workgroup model is a viable option, particularly if the main administrator isn't familiar with Active Directory. With either model, you need a workgroup or domain name, unless you're using the workgroup model and keep the default name "Workgroup." If you're using the domain model, you need to decide whether the domain name will be registered on the Internet. If so, making the Windows domain name the same as your Internet domain name makes sense. If the Internet name isn't already registered, make sure the name you have in mind is still available. If you aren't registering the domain name on the Internet, you can use any domain name you choose, but you should still follow the common naming convention of *SecondLevelName.TopLevelDomain*, such as mybusiness.com.

- What server roles should you install? This decision is one of the most important because it determines how this server will be used and what network services will be available to users. Chapter 1 summarized the available roles and many features you can install. For a first-server installation, however, there are some clear choices. With the domain model, you must install the Active Directory Domain Services (AD DS) role (discussed more in Chapter 3). AD DS requires DNS, so the DNS Server role is installed automatically. Other basic roles to consider on a first server include DHCP, for IP address configuration, and File Services and Print Services, which include tools for sharing and managing file storage and printer resources. Many other roles and features can be installed to meet your network and business needs; several are discussed in later chapters.

Now that you have a plan, it's time to move on to the actual installation of Windows Server 2008.

Ready, Set, Install For the first server installation on a new network, you usually use a DVD. Like any other OS installation, make sure the BIOS is set to boot from the CD/DVD drive first if you have an OS already installed. After installation begins, a message is displayed to let you know that Windows is loading files. Next, you see the window shown in Figure 2-1, where you choose the language, time, and keyboard configuration. Note that there's no longer a text mode portion of the installation; Windows Server 2008 is a GUI install from start to finish. After clicking Next, the window shown in Figure 2-2 is displayed with the options Install now, Repair your computer, and What to know before installing Windows (which takes you to help information).



Figure 2-1 The initial installation window for Windows Server 2008



Figure 2-2 The second installation window

Depending on your installation media, you might see a window asking which edition you want to install and whether you want a full or Server Core installation (see Figure 2-3). You might also be asked to enter the product code before choosing the edition. This section covers a full installation, and you perform a Server Core installation later in Activity 2-7. In subsequent windows, you accept the license terms and select an upgrade or a custom installation. The upgrade option is available only if you're starting the installation from an existing Windows version. A custom installation, described in this section, performs a clean install of Windows. After selecting the custom option, choose from a list of disks and/or partitions to specify where you want to install Windows. If you click the “Drive options (advanced)” link, you see more options for creating, deleting, extending, and formatting partitions or loading a new disk controller driver if Windows doesn't recognize all your drives (see Figure 2-4). If you just select a disk and click Next, Windows uses the entire disk and formats it as NTFS by default. Your computer then restarts twice.

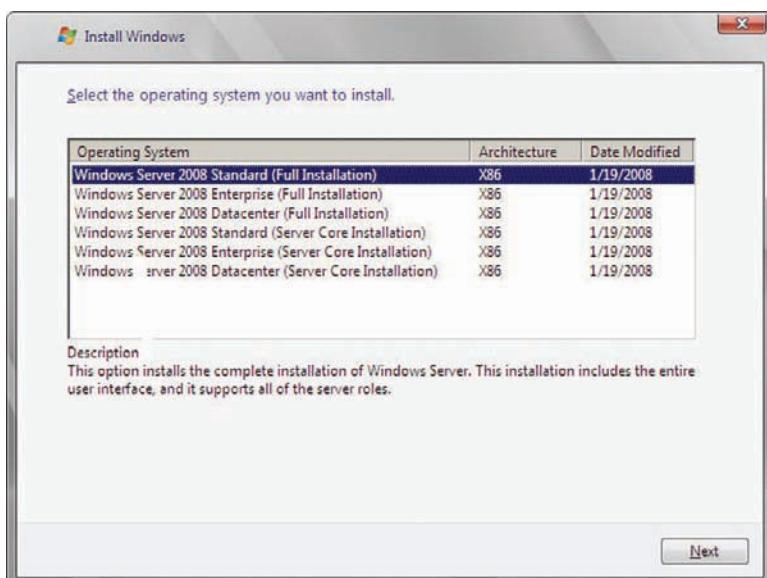
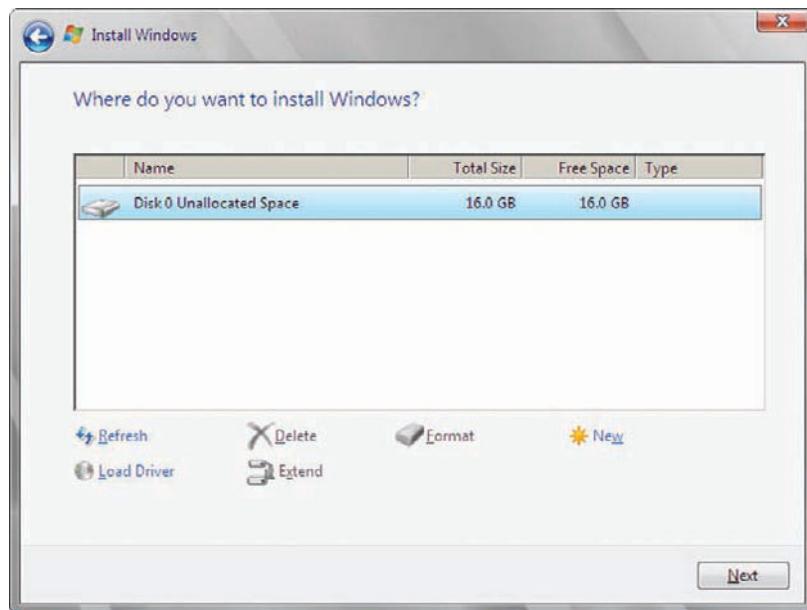


Figure 2-3 Choosing a full or Server Core installation



2

Figure 2-4 Additional options for partitions

After the installation is finished, you see a message stating that the user's password must be changed. The "user" referred to here is the initial Administrator account. Clicking Cancel doesn't do anything, so your only real choice is to click OK. Next, you see the window shown in Figure 2-5, where you must enter the Administrator password and then enter it again to confirm it. You can also click the "Create a password reset disk" option, if you want. Use the icon at the lower left to select Ease of Access options for hearing-, sight-, or mobility-impaired users. After you change the password, click the arrow icon. You're logged on, and the Initial Configuration Tasks applet is displayed (see Figure 2-6).



Figure 2-5 Change the Administrator password

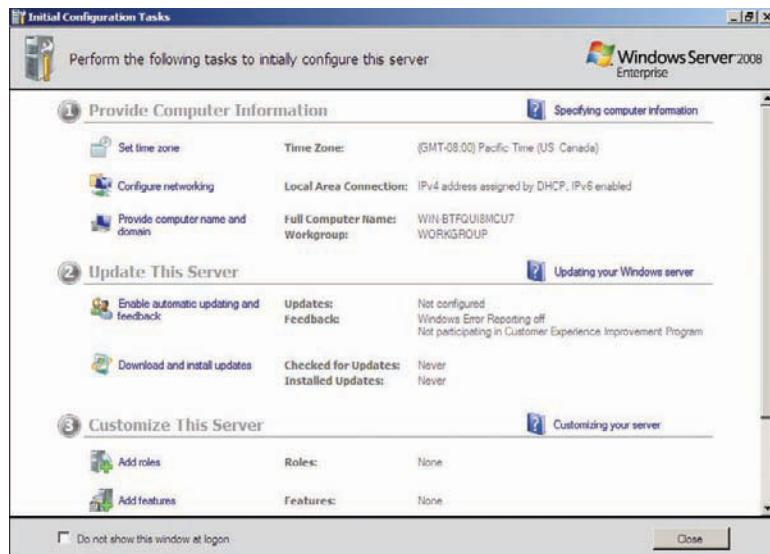


Figure 2-6 The Initial Configuration Tasks applet



Activity 2-1: Installing Windows Server 2008

 Instructions for performing this activity in a virtual machine are in Appendix C.

NOTE

Time Required: 30 minutes to more than an hour

Objective: Install Windows Server 2008.

Description: You're ready to install Windows Server 2008 on your client's new network. You have verified the hardware configuration and have the installation DVD in hand. The server has a single hard drive and all space is unallocated, so there's no need to change the BIOS boot order.

1. Power on the server and insert the Windows Server 2008 installation DVD.
2. In the first installation window (shown previously in Figure 2-1), verify the language, time, and keyboard choices for your environment. Make changes if necessary, and then click **Next**.
3. In the next window (shown previously in Figure 2-2), click the **What to know before installing Windows** link. Browse through the help document, and then close it. Click **Install now**.
4. In the next window, if necessary, enter your product key, and then click **Next**. The next window might differ slightly from Figure 2-3, but you should click **Windows Server 2008 Enterprise (Full Installation)** in the list box, and then click **Next**.
5. If necessary, click the option to accept the license agreement, and then click **Next**. In the Which type of installation do you want? window, click **Custom (advanced)**.
6. In the Where do you want to install Windows? window, click **Drive options (advanced)**. You see a window similar to Figure 2-4 (shown previously), where you can select options for drive partitions and load drivers for a disk controller. If you simply click Next with an unallocated disk selected, Windows uses the entire disk and formats it as NTFS. Click to select **Disk 0 Unallocated Space**, and then click **Next**. Now you can just sit back and let Windows do the rest. Your computer restarts at least twice, and then you see the window shown in Figure 2-7. Click **OK**.



Figure 2-7 The prompt to change the user password



In the Where do you want to install Windows? window, you can press Shift+F10 to open a command prompt window in the MINWINPC environment. From this command prompt, you can use a host of utilities, including Diskpart for performing advanced disk configuration tasks.

7. In the next window, enter **Password01** twice, and then click the arrow to log on. In the message box stating that your password has been changed, click **OK**.
8. After you're logged on, the Initial Configuration Tasks applet is displayed. If you're continuing to the next section right away, you can leave this window open, or you can log off.

Postinstallation Tasks Now that Windows Server 2008 is installed, it's time to attend to some postinstallation tasks. Some were discussed earlier, such as naming the server and configuring protocols and addresses. Here's a summary of the tasks you should perform immediately on the first server in a network:

- Activate Windows Server 2008.
- Set the correct date, time, and time zone.
- Assign a static IP address.
- Assign a computer name.
- Configure automatic updates.
- Download and install available updates.
- Add and configure roles and features.

Except for activating Windows Server 2008, all these tasks are in the Initial Configuration Tasks applet you see each time you log on as Administrator (unless you click the "Do not show this window at logon" check box at the lower left). Windows Server 2008 is activated automatically after several days. If it isn't activated for some reason, you must do so manually within 60 days after installation, or you can't log on. To activate it manually, open the System Properties dialog box. In the Windows activation section, click Activate Windows now. However, if you're using a Multiple Activation Key (MAK) license, you need to click "Change product key" first and then enter the product key.

In the following activities, you complete some of these postinstallation tasks.



Activity 2-2: Setting the Time, Date, and Time Zone

Time Required: 10 minutes

Objective: Perform the postinstallation task of setting the time, date, and time zone.

Description: You have completed the Windows installation and notice that the time zone is incorrect. You know that for all server functions to work correctly, the time, date, and time zone must be right on all clients and servers. In this activity, you use the Initial Configuration Tasks applet to change the time zone.

1. If necessary, log on to your server as Administrator, which starts the Initial Configuration Tasks applet. (If it doesn't open, click **Start**, **Run**, type **oobe** [which stands for "out-of-box experience"] in the Open text box, and then click **OK**.)



Another method for starting this applet uses a new Windows Server 2008/Vista feature. Click Start, type oobe in the Start Search text box, and then press Enter. Windows searches for this program and starts it for you.

2. Under Provide Computer Information, click **Set time zone** to open the Date and Time dialog box.
3. Click the **Change time zone** button, and select your time zone in the drop-down list. If your region observes daylight saving time, make sure the **Automatically adjust clock for Daylight Saving Time** check box is selected, and then click **OK**. If the time and date are incorrect, click the **Change date and time** button to modify them, and then click **OK**.
4. Click the **Additional Clocks** tab, where you can tell Windows to display the time in other time zones when you hover your mouse pointer over the taskbar clock.
5. Click the **Internet Time** tab, where you can select the option to synchronize with a time server on the Internet. By default, Windows Server 2008 is set to synchronize with <http://time.windows.com>, and synchronization occurs weekly. To use a different time server or disable Internet time synchronization, click the **Change settings** button. You can choose from a list of time servers or enter the name of another server. You can also tell Windows to synchronize now by clicking the **Update Now** button. If time synchronization isn't working, your company firewall might be blocking it.
6. Click **OK** twice to close the Date and Time dialog box.



Activity 2-3: Setting a Static IP Address

Time Required: 10 minutes

Objective: Perform the postinstallation task of setting a static IP address.

Description: After completing the Windows Server 2008 installation, you notice in the Initial Configuration Tasks applet that your IP address is assigned by DHCP. Your server will be performing some server roles that require static addressing. You have already decided that all your servers will occupy addresses starting with 200 in the last octet.



This activity and many others in this book use 192.168.100.xxx/24 for IP addressing. Please see your instructor for the actual addresses you should use.

NOTE

1. If necessary, log on to your server as Administrator. If the Initial Configuration Tasks applet doesn't start, open it as described in Activity 2-2.
2. Under Provide Computer Information, click **Configure networking** to open the Network Connections window.
3. Right-click **Local Area Connection** and click **Properties** to open the Local Area Connection Properties dialog box (see Figure 2-8).

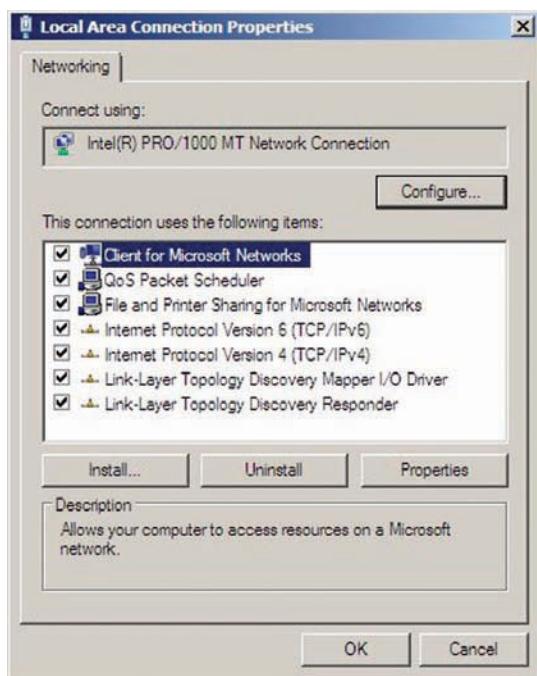


Figure 2-8 The Local Area Connection Properties dialog box

4. Notice that both TCP/IPv4 and TCP/IPv6 are installed and enabled, but you're going to configure only TCP/IPv4. Click **Internet Protocol Version 4 (TCP/IPv4)**, being careful not to clear the check box next to it. Click the **Properties** button.
5. In the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, click the **Use the following IP address** option button (see Figure 2-9).

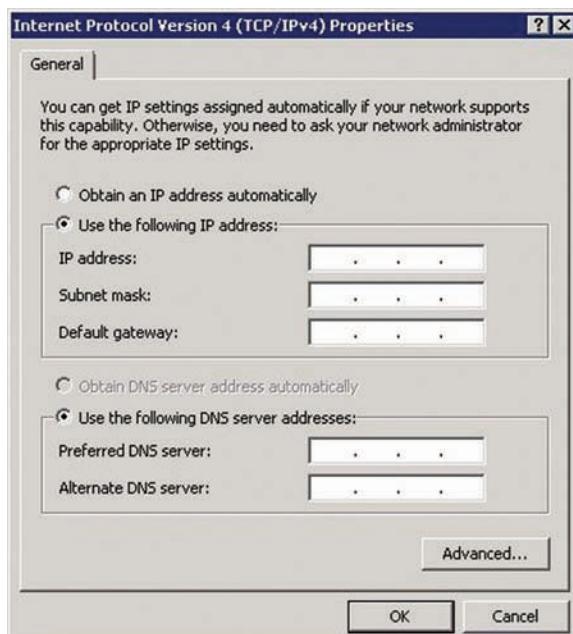


Figure 2-9 Configuring IP address settings

6. Fill in the following information:



If you're using a different IP addressing scheme, see your instructor for these values.

NOTE

IP address: **192.168.100.2XX** (replacing XX with your assigned two-digit student number, which your instructor will give you)

Subnet mask: **255.255.255.0**

Default gateway: **192.168.100.1** (or whatever your network requires)

Preferred DNS server: **192.168.100.200** (the classroom server's address, if you're using this addressing scheme)

Alternate DNS server: Leave blank or enter a value specified by your instructor.

7. Click **OK**, and then click **Close**.

8. To verify your settings, right-click **Local Area Connection** and click **Status**. Then click the **Details** button to open the Network Connection Details dialog box.

9. Verify all the information, and then click **Close**. Click **Close** again.

10. Close the Network Connections window.

After configuring networking on a server, most people test the configuration by using **Ping**, a network testing and troubleshooting tool that sends a series of **Echo Request** packets to a destination IP address to see whether there's a reply. If the Echo Request reaches the destination computer, an **Echo Reply** packet is sent back to the sender.



Activity 2-4: Testing Network Connectivity

Time Required: 10 minutes

Objective: Test network connectivity after configuring a static IP address.

Description: You have just finished setting a static IP address on your server and want to be sure all the information is correct and working.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, **Command Prompt**.
3. At the command prompt, type **ping 192.168.100.200** (which should be the instructor's server) and press **Enter**.



The instructor's server must be configured to allow incoming ping messages. This procedure is explained in Activity 2-11.

NOTE

4. Assuming you received four successful replies, ping the address of the default gateway you configured in Activity 2-3.



It's not uncommon to get one "Request timed out" or "Destination host unreachable" message followed by three successful replies, but if all four messages indicate an unsuccessful ping, recheck your address settings and the address settings of the computer you're trying to ping.

5. If you received replies from the default gateway, ping the DNS server address you specified in Activity 2-3.
6. If all went well, you have a working network connection. If any ping returned a "Request timed out" or "Destination host unreachable" message, verify your IP settings with your instructor.
7. Close the command prompt window by typing **exit** and pressing **Enter** or clicking the **X** at the upper right.



Activity 2-5: Changing the Computer Name and Workgroup

2

Time Required: 10 minutes

Objective: Change your computer name.

Description: After installing Windows, you examine the Initial Configuration Tasks applet and notice that the assigned computer name seems random and the workgroup name is the generic “Workgroup.” You want to personalize these settings according to your network plan.

1. Log on to your server as Administrator, if necessary. If the Initial Configuration Tasks applet doesn’t start, open it as described previously.
2. Under Provide Computer Information, click **Provide computer name and domain** to open the System Properties dialog box.
3. Click the **Computer Name** tab, if necessary, and then click the **Change** button.
4. In the Computer name text box, type **ServerXX** (replacing XX with your two-digit student number).
5. In the Workgroup text box, type **ADCONFIGCLASS** or another name assigned by your instructor, and then click **OK**. After a moment or two, you should see the message “Welcome to the ADCONFIGCLASS workgroup.” Click **OK**. When prompted to restart your computer, click **OK**. Click **Close**, and then click **Restart Now**.
6. When Windows restarts, log on as Administrator.
7. Verify your changes in the Initial Configuration Tasks applet. You can also click **Start**, right-click **Computer**, and click **Properties** to open the System Properties dialog box, which displays your computer name, workgroup or domain, and other system information.
8. Close all open windows.

Installing Updates One of the most important administrative tasks is installing updates. Almost immediately after an OS is released, bugs and security vulnerabilities are found and fixed. These fixes, normally released as **Patches**, can be installed through the Windows Update procedure. Windows Update also downloads and installs new drivers and service packs. A **Service Pack** is generally a collection of all bug fixes and security updates since the OS release. Service packs can also add features and performance enhancements or change the functionality of existing features, so you must understand the effects of a service pack on your server before installing it. Testing a service pack extensively on a test server is highly recommended before deploying it on production machines.



Interestingly, the initial release of Windows Server 2008 already has the suffix Service Pack 1 (SP1) because it shares a codebase with Vista, and Microsoft released Vista SP1 simultaneously with Windows Server 2008. Microsoft wants to keep the service pack versions of these two OSs in lockstep.

The Initial Configuration Tasks applet is a convenient option for configuring your server for automatic updates and downloading and installing updates for the first time. You can see these options under Update This Server in Figure 2-6, shown previously. Clicking the Enable automatic updating and feedback link displays two options: accepting the default settings or configuring the settings manually.

Good network administrators want to know exactly what their servers are doing and when, so checking the manual settings is a good idea. The default settings enroll you in the Customer Experience Improvement Program (which sends anonymous server use information to Microsoft periodically), download and install new updates automatically every day at 3:00 a.m., and send summary error reports to Microsoft when problems are detected and notify you if a solution has been found.



Activity 2-6: Enabling Automatic Updates

Time Required: 10 to 30 minutes, depending on number and size of updates

Objective: Configure automatic updates and download and install initial updates.

Description: After installing Windows, you notice that automatic updates haven't been enabled in the Initial Configuration Tasks applet. You want to be sure your server is up to date on bug fixes and security updates.



Before accessing the Internet with any computer, you should install antivirus software.

1. Log on to your server as Administrator, if necessary. The Initial Configuration Tasks applet should start.
2. Under Update This Server, click **Enable automatic updating and feedback** to open the Enable Windows Automatic Updating and Feedback dialog box.
3. Click the arrow next to **Manually configure settings**. If you click Enable Windows automatic updating and feedback (recommended), automatic updating and feedback are enabled with the default settings.
4. Under Windows automatic updating, click the **Change Setting** button to open the Change settings dialog box shown in Figure 2-10. No options are selected by default.

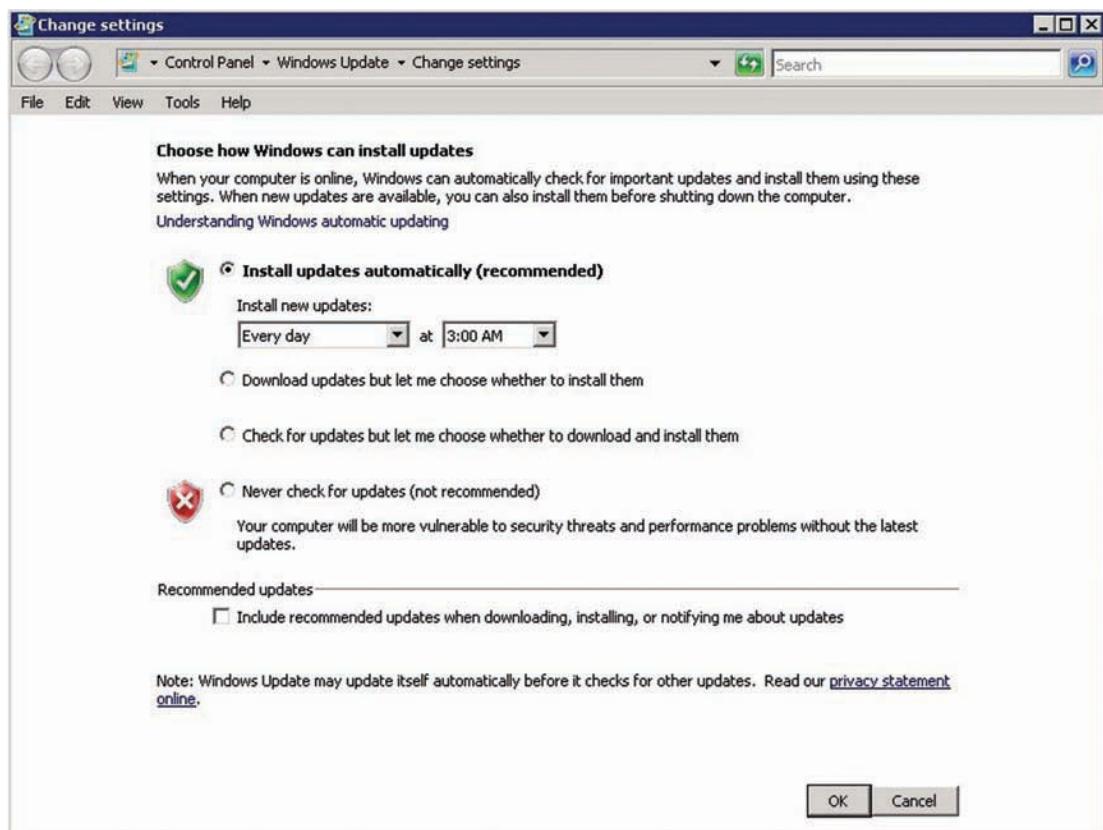


Figure 2-10 The Change settings dialog box

5. Click the **Download updates but let me choose whether to install them** option button. This setting is the best choice for an administrator who wants to decide whether to install an update. Critical updates are downloaded as soon as they're available on the Internet, and a notification icon is displayed on the taskbar when they're ready to install.

6. Click the **Include recommended updates when downloading, installing, or notifying me about updates** check box. This option includes new drivers or application updates in the downloaded updates. Click **OK**.
7. Under Windows Error Reporting, click the **Change Setting** button. Read the description of this feature. Error reporting is enabled by default with the option to notify you before sending the selected report. You can leave this option as is, but take note of the other choices. Click **OK**.
8. Under Customer Experience Improvement Program, click the **Change Setting** button. By default, you aren't enrolled in this program. Because this server is used only for lab purposes, click to select **No, I don't want to participate**, if necessary. Read the information about this program, and then click **OK**.
9. Click **Close**. Next, click **Download and install updates**. Windows checks for updates if you're connected to the Internet.
10. In the Windows Update window, notice that you receive updates for Windows only, but you can have Windows look for updates for other manufacturers' products. If updates are available, you can install them by clicking the **Install Updates** button. If you want to view information about updates before installing them, click the **View available updates** link.
11. Close all open windows.

To view a list of installed updates, open the Programs and Features applet in Control Panel and select the View installed updates task. In addition, you can check for updates manually by running the Windows Update applet in Control Panel. After your computer is configured and up to date, you can start installing server roles and additional features. If this server is the first and only one (at least for now), you'll probably install several roles on this server. As discussed previously, most networks in a domain environment usually run these services at a minimum: Active Directory Domain Services (AD DS), DNS, DHCP, and File Services. Other roles and features you install depend on how the network is used and what applications are running. In Chapter 3, you install AD DS and DNS. For now, you look at other server installation situations.

Expanding Your Network

Many businesses that start with a single server on the network eventually find a reason to install a second or third server and more. If your network requires two or more servers, you're almost certainly running in a domain environment, which is the perspective from which this topic is discussed.

When you're adding a server to an existing network, you must answer many of the same planning questions that you did for the first server. You need to decide on a static IP address, a server name, and what roles this new server will play on the network. However, you probably don't need to choose a domain name because this new server will likely be part of the existing domain or a stand-alone server. What you must decide is whether the new server will be one of the following:

- A domain controller (DC) in the existing domain
- A read only domain controller (RODC) in the existing domain
- A member server in the existing domain
- A stand-alone server

If you're installing the second server in the network, there are some good arguments for making it a domain controller. The second server can share the load of managing directory services and handling user logons and provide fault tolerance for Active Directory should the first server go offline. An RODC (discussed more later in this section) can provide some benefits of a standard domain controller but is better suited to handling domain services for branch offices than serving as a second DC.

A member server belongs to the domain and falls under domain management but doesn't run Active Directory or participate in managing directory services. Making a server a member server rather than a domain controller is best when you already have at least two DCs at a location or

when you plan to run resource-intense applications on it that shouldn't share server resources with other services.

A stand-alone server, as the name implies, doesn't fall under the domain's management umbrella; instead, it's configured as part of a workgroup. Configuring a stand-alone server makes sense when, for example, the server will be acting as a public Web server, providing services (such as DNS or DHCP) for a group of non-Windows clients, or serving as a departmental server when you want local management.

Some reasons you need to add servers to a network include the following:

- Company growth
- Excessive load on existing servers
- Need to isolate an application
- Need for fault tolerance
- Addition of branch offices

A company that's growing, particularly in the number of users, should plan ahead for the inevitable network slowdowns caused by increased activity. A server that has been humming along smoothly with 25 users might not perform as well when that number doubles. Ideally, if growth is foreseen, new resources are put in place before the server becomes taxed. Even without additional users on a network, existing users' use tends to increase over time as users and administrators find more functions for the server to handle. This gradual increase in network and server use can sneak up on you. A server that was running fine six months ago can gradually bog down, sapping user productivity as it takes longer to log on to the network or access shared files. Monitoring your server's performance regularly before this problem becomes a crisis is a good idea. Server monitoring is discussed more in Chapter 13.

Sometimes a network application works best when no other major services are competing for a server's CPU and memory resources. Even if your existing server isn't overused, introducing such an application into your network might prompt you to install it on its own server. Isolating applications in this way has the added benefit of not disturbing other network services when you perform maintenance on the server. The converse is also true: When you perform maintenance on other servers, you don't disturb the isolated application.

Access to network resources is so critical in today's business environment that loss of access to server services can reduce productivity and increase costs. Even in a smoothly running network where no server is loaded excessively, adding a server for fault tolerance might still be wise. Load balancing or fault tolerance are built into several Windows server roles, such as AD DS, DNS, and file sharing with Distributed File System (DFS). If you need a complete hot replacement for an existing server, Enterprise Edition provides **failover clustering**, in which a group of servers is connected by both cabling and software, so if one server fails, another takes over to provide those services.

When a business opens a branch office connected to the main office through a wide area network (WAN), installing a server at the branch office might be prudent. This setup can reduce WAN traffic created by authentication and authorization, DNS lookups, DHCP address assignment, access to shared files, and more. IT administrators are often concerned about security when installing a branch office server because a separate secure room is rarely available. The server might be placed in somebody's office or a common area, which leaves it vulnerable to theft or even attacks by employees. Having physical access to a server makes compromising the server's security much easier. To address this problem, administrators can use RODCs. As mentioned, RODCs have many of the benefits of a standard DC, but administrators can filter what information is replicated to the RODC, including passwords. Therefore, an administrator can configure the RODC to keep only local users' passwords, which limits what damage could be done if someone were able to compromise the server. In addition, you can create a local administrator for an RODC so that maintenance activities can be carried out without giving the local administrator domainwide administrative capabilities. Another option for a branch office server is using the Server Core installation mode to diminish the overall security risk.

Upgrading to Windows Server 2008

A Windows Server 2008 upgrade differs from upgrades in previous Windows versions, which were in-place upgrades that merged the previous OS version and the new version to keep existing settings and applications. With a Windows Server 2008 upgrade, a clean installation is performed after renaming the existing Windows directory as Windows.old. After the installation, settings, documents, and application information from the old OS are migrated to the new Windows Server 2008 installation directory. Here's an overview of upgrade considerations, followed by available upgrade paths in Table 2-1:

- The only previous Windows version supported for upgrade is Windows Server 2003.
- You can't upgrade to a Server Core installation.
- Cross-platform upgrades aren't supported, so you can upgrade only from a 32-bit version to a 32-bit version or a 64-bit version to a 64-bit version.
- There's no upgrade path to Windows Server 2008 Itanium Edition or Windows Web Server 2008.
- You can't upgrade to a different language.

Table 2-1 Windows Server 2008 upgrade paths

Current version	Server 2008 upgrade path
Windows Server 2003 Standard Edition SP1, SP2, or R2	Windows Server 2008 Standard or Enterprise Edition
Windows Server 2003 Enterprise Edition SP1, SP2, or R2	Windows Server 2008 Enterprise Edition
Windows Server 2003 Datacenter Edition SP1, SP2, or R2	Windows Server 2008 Datacenter Edition

Microsoft recommends a clean installation to a new disk or partition instead of an upgrade. If you're considering an upgrade, Microsoft recommends that any third-party software not specifically supported by the manufacturer for a Windows Server 2008 upgrade be removed before the upgrade. In addition, hardware requirements for Windows Server 2003 were considerably lower, so be sure your system meets the minimum CPU, RAM, and disk requirements for Windows Server 2008.

An upgrade is similar to a clean installation with a few exceptions. First, you must boot the existing OS and log on. Then you can start the Setup program from the DVD. Next, you're asked whether Windows should go online to get the latest updates for installation. This option is recommended. You aren't prompted for the language, time, and currency format or keyboard layout; they must match the settings for the Windows Server 2008 edition being installed. In addition, in an upgrade you aren't prompted for the location to install Windows. It's installed on the same disk partition as the OS you booted to.

After a successful upgrade on a domain controller, you might want to change Active Directory's functional level. This topic is covered in Chapters 4 and 10, but if you want to take full advantage of the new Active Directory features, all your domain controllers must be operating at the Windows Server 2008 functional level.

Now that you're familiar with some common standard installations, the next two sections focus on specialized server installations: Server Core and virtual server installations with Hyper-V.

Server Core: Windows That Doesn't Do Windows

As you learned in Chapter 1, the Server Core installation option provides a minimal server environment designed for running specific server roles. Server Core's reduced codebase minimizes OS vulnerabilities and lessens maintenance and management tasks. In addition, the overall disk and memory footprint is smaller, thereby requiring fewer hardware resources than a full installation.

The price you pay for these reductions and simplifications is a less user-friendly management interface.

Server Core isn't intended to be the only server in a single-server network but a server performing a specific role in a network where at least one full installation exists. Server Core is a good candidate for deployment in situations such as the following:

- As a secondary DC to provide redundancy for Active Directory running on a full installation
- As a branch office server when remote administration is likely and the reduced attack surface and maintenance are substantial benefits
- As an RODC for a department or branch office providing many of a standard DC's benefits but with reduced security risks
- As a virtual machine when reduced resource requirements are an important benefit
- As a specialized single-role server providing services such as DNS, DHCP, Web, or File Services
- As a departmental server for many of the same reasons as a branch office server

As businesses begin to work with Windows Server 2008 and the Server Core option, more deployment uses will become apparent. Server Core's benefits are well and good, but you might be wondering how you carry out server management tasks without a Start menu or Server Manager. That brings you to the next topic: performing tasks at the command line in Server Core.

Windows Server Installation and Postinstallation Tasks

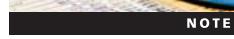
A Server Core installation is identical to a full installation, so there's no need to explain all the steps again. The only difference is that you choose the Server Core Installation option when prompted to select the OS you want to install. From there, the process is the same, including changing the administrator password and logging on the first time. The first difference you'll probably notice is the window you see after the initial logon, shown previously in Chapter 1.

The immediate postinstallation tasks for Server Core are the same as in a full installation. The big difference is how you accomplish these tasks. Windows has a full set of command-line tools for configuring most aspects of a Windows server. Although you can use them with a full installation, they are the only option for configuring many aspects of Server Core. The following activities walk you through the postinstallation tasks you carried out in the full installation, but this time, you use the command-line tools in Server Core. Ideally, you'll perform these activities in a Server Core installation, but you can also do them in a full installation by opening a command prompt window. In the next activity, you install Server Core.



Activity 2-7: Installing Server Core

Instructions for performing this activity in a virtual machine are in Appendix C.



Time Required: 30 minutes or longer, depending on the server's speed

Objective: Install Server Core.

Description: You're unfamiliar with the new Server Core installation option in Windows Server 2008. You have read about some benefits of using Server Core in your network, but you want to become familiar with it before deploying it in a production environment.

1. Power on the server and insert the Windows Server 2008 installation DVD.
2. In the first installation window, verify the language, time, and keyboard choices for your environment. Make changes if necessary, and then click **Next**.

3. In the next window, click **Install now**. If necessary, enter your product key, and then click **Next**.
4. Click **Windows Server 2008 Enterprise (Server Core Installation)** in the list box, and then click **Next**.
5. If necessary, click the option to accept the license agreement, and then click **Next**. In the Which type of installation do you want? window, click **Custom (advanced)**.
6. In the Where do you want to install Windows? window, click **Disk 0 Unallocated Space**, and then click **Next**.
7. When the installation is finished, press **Ctrl+Alt+Delete** as prompted to log on.
8. Click the **Other User** icon. In the User Name text box, type **Administrator**, and then click the arrow next to **Password prompt**. (Don't enter a password at this time; the initial password for Administrator is blank.)
9. In the next window, you're prompted to change the user's password. Click **OK**.
10. Type **Password01** in the New password text box and the Confirm password text box.
11. Click the arrow next to the Confirm password text box. When you see a message that the password has been changed, click **OK**. You're now logged on.

2



Activity 2-8: Restoring a Command Prompt Window in Server Core

Time Required: 5 minutes

Objective: Open the command prompt window after it has been closed.

Description: Out of habit, you closed the command prompt window in Server Core, and you need to restore it to finish some administrative tasks.

1. Log on to Server Core as Administrator, if necessary.
2. If the command prompt window is open, close it by typing **exit** and pressing **Enter** or by clicking the **X** at the upper right. You now have a blank desktop.
3. Press **Ctrl+Alt+Delete** to open the window shown in Figure 2-11. Click the arrow next to **Start Task Manager**.

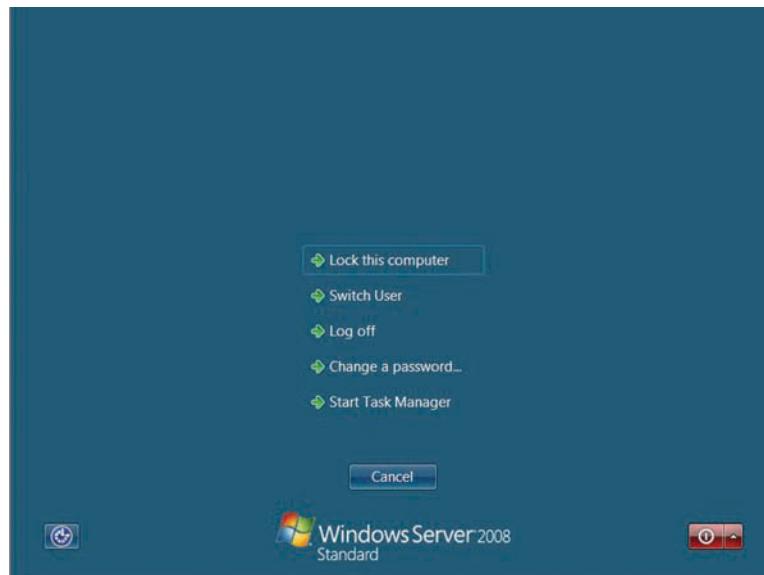


Figure 2-11 The Ctrl+Alt+Delete menu

4. In Windows Task Manager, click **File, New Task (Run)** from the menu.
5. In the Create New Task dialog box, type **cmd** and click **OK**. The command prompt window is restored.
6. Close Windows Task Manager, but leave the command prompt window open for the next activity.



If you ever close the command prompt window in a Server Core installation, simply follow these steps to restore it.



Activity 2-9: Setting the Time, Date, and Time Zone in Server Core

Time Required: 5 minutes

Objective: Perform the postinstallation task of setting the time, date, and time zone in Server Core.

Description: You have finished the Server Core installation and recall that setting the correct time, date, and time zone is essential for the server to operate properly.

1. Log on to Server Core as Administrator, if necessary.
2. Open a command prompt window, if necessary, and type **control timedate.cpl** and press **Enter**. This command opens the Date and Time control panel, one of two available in Server Core. (The other one is Regional and Language Options, which you can access by typing **control intl.cpl** and pressing Enter.)
3. Change the date, time, and time zone as needed, and then click **OK**.
4. Leave the command prompt window open for the next activity.



Any computer that becomes a member of a domain synchronizes its clock to a domain controller, so setting the time and date is unnecessary in these circumstances. You must still set the correct time zone, however.



Activity 2-10: Setting a Static IP Address in Server Core

Time Required: 10 minutes

Objective: Set a static IP address in Server Core.

Description: Because you're unfamiliar with Server Core, you want to know how networking is configured. You find that DHCP is used to assign the IP address by default, and you want to change this configuration to a static IP address assignment.



This activity and many others in this book use 192.168.100.xxx/24 for IP addressing. Please see your instructor for the actual addresses you should use.

1. Log on to Server Core as Administrator, if necessary.
2. At the command prompt, type **ipconfig /all | more** and press **Enter**. Make a note of the default gateway and preferred DNS server that have been assigned. If necessary, press the **spacebar** to see the rest of the output from the ipconfig command.
3. Before you can run commands to set IP address information, you need some information about your network interfaces. At the command prompt, type **netsh interface ipv4 show interfaces** and press **Enter**. You should get output similar to Figure 2-12.

```
C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>Windows\system32>netsh interface ipv4 show interfaces
Idx  Met  MTU  State           Name
-----  --  --  --  --
 2    10  1500  connected  Local Area Connection
 1    50  4294967295  connected  Loopback Pseudo-Interface 1
C:\>Windows\system32>
```

2

Figure 2-12 Output from the netsh interface command

4. Note the number in the **Idx** column of the Local Area Connection row. In Figure 2-12, this number is 2. You need this number for the next commands.
5. Next, type **netsh interface ipv4 set address name="2" source=static address=192.168.100.1xx mask=255.255.255.0 gateway=192.168.100.1** and press **Enter**. (Remember that the number after “name” is the number you noted in Step 4, and xx is your two-digit student number.)
6. To set the DNS server address, type **netsh interface ipv4 add dnsserver name="2" address=192.168.100.200 index=1** and press **Enter** (replacing the number after “name,” if needed). If you had a secondary DNS server to add, you would use the same command but use the secondary DNS server’s IP address and change the number after “index” to 2.
7. Verify the information by typing **ipconfig /all** and pressing **Enter**. Check that all addresses are correct.
8. Leave the command prompt window open for the next activity.

If you try to ping a computer running a freshly installed Windows Server 2008 (full or Server Core installation), there’s no reply. However, if you ping from a Windows Server 2008 computer to your default gateway or perhaps a Windows Vista computer, the ping probably works fine. The reason is that the Windows Server 2008 firewall blocks incoming Echo Request packets but allows Echo Reply packets. In the next activity, you configure the firewall to allow Echo Request packets so that your server can respond to ping packets.



Activity 2-11: Configuring the Server Core Firewall for Ping

To use two virtual machines instead of a partner computer for this activity, see the instructions in Appendix C.



Time Required: 10 minutes

Objective: Configure the Windows Server 2008 firewall to allow Echo Request packets.

Description: You have configured networking for your Windows Server 2008 Server Core network, and now you want to test the configuration by pinging known IP addresses and then ping-ing your server from another computer. In this activity, you work with a partner who’s also running Server Core.

1. Log on to Server Core as Administrator and open a command prompt window, if necessary.
2. To view your basic IP address settings, type **ipconfig** and press **Enter**.

3. Ping your default gateway by typing **ping 192.168.100.1** (or the address Ipconfig displayed as your default gateway) and pressing **Enter**.
4. If Step 3 was successful, type **ping ip_address** (replacing *ip_address* with the IP address of your partner’s Server Core computer) and press **Enter**. If the ping isn’t successful, you see the message “Request timed out.” Make sure your partner gets the same results before continuing.
5. To change the firewall settings so that Echo Request packets are permitted through the firewall, type **netsh firewall set icmpsetting 8** and press **Enter**.
6. After your partner has completed Step 5, try to ping your partner’s computer again by typing **ping ip_address** (replacing *ip_address* with the IP address of your partner’s Server Core computer) and pressing **Enter**. Both you and your partner should receive reply messages, as you did in Step 3 when you pinged the default gateway. If not, both you and your partner should verify that your IP address settings are correct and the command in Step 5 was entered correctly.



If you want to disable ping requests again, simply type **netsh firewall set icmpsetting 8 disable** and press Enter.

NOTE

7. Leave the command prompt window open for the next activity.

The Netsh command is not the only method for configuring the firewall in Server Core. Chapter 13 explains how to manage many aspects of Server Core remotely by using MMC snap-ins. However, the command line is the only way to manage most Server Core features locally. The next postinstallation steps to configure Server Core entail setting the computer name and workgroup name.



Activity 2-12: Configuring Computer and Workgroup Names in Server Core

Time Required: 10 minutes

Objective: Set computer and workgroup names in Server Core.

Description: You realize after installing Windows Server 2008 Server Core that you were never prompted to provide a computer name, as in other OS installations, nor were you prompted to specify a workgroup or domain to join. You need to access this server by name, and the randomized name that Windows sets by default (called the “hostname”) is too difficult to remember.

1. Log on to Server Core as Administrator and open a command prompt window, if necessary.
2. Type **hostname** and press **Enter**. Make a note of the hostname, which probably starts with WIN. You need to specify the entire hostname in the next step.
3. Type **netdom renamecomputer computename /newname:ServerCoreXX** (replacing *computename* with the hostname you noted in Step 2 and XX with your two-digit student number). When asked whether you want to proceed, type **y** and press **Enter**.
4. To complete the name change, you must restart the computer. Type **shutdown /r /t 0** and press **Enter**. The /r option specifies a computer restart, and the /t 0 option specifies restarting in 0 seconds (that is, immediately).
5. After your computer has restarted, log on to your server as Administrator.
6. Oddly enough, changing the workgroup name involves using a different type of command called Windows Management Instrumentation Command-line; each command is preceded with “wmic.” Type **wmic computersystem where name="ServerCoreXX" call joindomainorworkgroup name="ADCONFIGCLASS"** (replacing XX with your student number) and press **Enter**.

7. The Windows workgroup name isn't displayed by using the Ipconfig command. To display your NetBIOS name and workgroup name, type **nbtstat -n** and press **Enter**. The workgroup name is shown in the Name column in the row listing GROUP in the Type column.
8. Leave the command prompt window open for the next activity.

2

If your Server Core system is going to participate as a member of a Windows domain, you can use the Netdom command as follows:

```
netdom join ComputerName /domain:DomainName /userd:UserName  
/passwordd:password
```

ComputerName is the name of your computer, *DomainName* is the name of the domain you want to join, and *UserName* is the name of the domain user account with permission to join the domain. The *password* is the password for the user account specified by *UserName*. (The two Ds in the /passwordd option are indeed correct.)

One of the final postinstallation tasks is enabling automatic updates. The command for configuring automatic updates is actually a Visual Basic script that edits the Registry, as you see in Activity 2-13.



Activity 2-13: Enabling Automatic Updates in Server Core

Time Required: 10 minutes

Objective: Enable automatic updates to keep your Server Core system up to date with patches and bug fixes.

Description: You're working on a Server Core system that you're unfamiliar with, so you want to verify that automatic updates are enabled and, if not, enable them.

1. Log on to Server Core as Administrator and open a command prompt window, if necessary.
2. If necessary, type **cd \windows\system32** and press **Enter** to change to this directory. To view the current status of automatic updates, type **cscript scregedit.wsf /au /v** and press **Enter**. If they aren't configured, you should see the reply "Value not set."
3. To enable automatic updates, type **cscript scregedit.wsf /au 4** and press **Enter**. You should see the reply "Registry has been updated." The value 4 in this command specifies enabling automatic updates and having available updates downloaded and installed automatically at 3:00 a.m. every day.



You can disable automatic updates by typing **cscript scregedit.wsf /au 1** and pressing **Enter**.

NOTE

4. Next, restart the Automatic Updates service by typing **net stop wuauserv** and pressing **Enter**, followed by typing **net start wuauserv** and pressing **Enter**.
5. To check for updates immediately, type **wuauctl /detectnow** and press **Enter**. Finally, to check which updates are installed, type **wmic qfe list** and press **Enter**. If no updates are installed, you see the message "No Instance(s) Available."
6. Close the command prompt window.

If you want to configure automatic updates beyond using the default settings, you can edit the Registry. The Registry Editor is one of the few graphical utilities available in Server Core. For details on editing the Registry for automatic updates, consult a good book on the subject. The best method for configuring automatic updates in Server Core and applying this policy to all computers in the domain is to use Group Policy in Active Directory (discussed in Chapters 3 and 7).

Of course, you might want to perform more configuration tasks in Server Core, such as installing and configuring server roles and features. Chapter 13 covers managing Windows Server 2008 and the Server Core option in depth.

When Not to Use Server Core

As you might have noticed, a Server Core installation does have its drawbacks. You need to learn quite a few commands or keep them in a handy reference file. Server Core has its place in some networks, but it's not for all people or all situations. Server Core isn't suitable in situations such as the following:

- When it's the first server in a network
- When you need to install server roles and features that Server Core doesn't support
- When the server administrator isn't well versed in using command-line programs
- When you need to run applications that require the Microsoft .NET Framework, as it's not included in Server Core
- When you're upgrading from Windows Server 2003 (no upgrade path to Server Core)
- When you want to run Windows Web Server 2008 (no Server Core option in this edition)
- When you absolutely, positively can't live without the Windows GUI running on your server

Because of Server Core's lower resource demands and smaller attack surface, however, it's likely to be a staple in many Windows networks, particularly large networks that use virtualization or have branch offices—that is, after administrators get used to not having a GUI.

Virtualize Your Server with Hyper-V

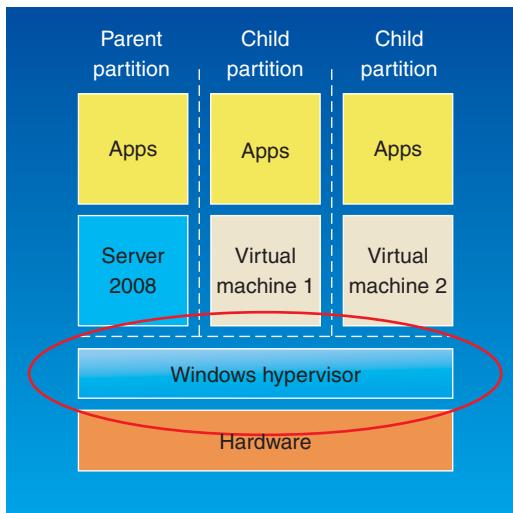
The Hyper-V server role was described in Chapter 1 as a virtual hardware environment in which you can install and run an OS. A virtualized OS functions identically to the same OS installed on physical hardware. Network administrators are turning to virtualization as a solution to consolidating server hardware, reducing space and power consumption, and easing server management. In addition, developers and testers use virtualization because virtual OSs are quick and easy to install, clone, and remove. Because there's no physical hardware environment, aside from the server Hyper-V is running on, you can work with and manage virtual machines easily.

A virtual machine (VM) is a collection of files, usually consisting of a configuration file and one or more files representing the virtual machine's attached hard disks. After an OS has been installed and is running, you can create additional files for saving a suspended virtual machine's state or taking a snapshot of a virtual machine. A **snapshot** is a set of files containing a virtual machine's state at a particular moment in time. For example, you can take a snapshot of a virtual machine right before you install a new application. If problems happen after you install the application, you can revert to the operating condition the virtual machine was in before you installed the application.

Several virtualization products are available, including Microsoft Virtual PC and Virtual Server, but Hyper-V is the first virtual environment that's an integral part of the Windows OS. Hyper-V gets its name from the technology used to create the virtual environment, called hypervisor. A **hypervisor** is a layer of software between the hardware and OSs that allows multiple OSs or multiple instances of the same OS to share physical hardware resources. The Windows Hyper-V hypervisor manages CPU, memory, timer, and interrupt hardware, and Windows Server 2008 manages the balance of hardware devices. The physical server on which Windows Server 2008 is installed is referred to as the **host computer**, and Windows Server 2008 running Hyper-V is considered the **host operating system**. The virtual machines running on the host are considered the **guest operating systems**. Figure 2-13 shows the basic architecture of Windows Server 2008 running Hyper-V and a couple of virtual machines.

Hyper-V is installed as a server role by using Server Manager. For a successful installation, review the following prerequisites:

- You must be running a 64-bit version of Windows Server 2008 Standard, Enterprise, or Datacenter Edition.
- The CPU must support virtualization extensions, such as AMD-V and Intel-VT.



2

Figure 2-13 The Windows Hyper-V architecture

- You must have free disk space at least equal to the minimum requirement for the OS you're going to install as a virtual machine.
- The amount of RAM must be at least equal to the minimum amount required for Windows Server 2008 plus the minimum amount required for the OS you're installing. The bare minimum should be 1 GB of RAM and preferably more.

After you have an adequately configured system running a 64-bit version of Windows Server 2008, you can install the Hyper-V role. Keep in mind that you can't install Hyper-V on Windows Server 2008 that's running as a virtual machine.



Activity 2-14: Installing the Hyper-V Role on a Windows Server 2008 Full Installation

Time Required: 15 minutes

Objective: Install the Hyper-V server role.

Description: You want to install a new application on your Windows Server 2008 system. You have read about the benefits of virtualization and believe that this new application is a good candidate to install in a virtual machine, but first you need to install the Hyper-V server role.

1. Log on to your full installation of Windows Server 2008 as Administrator, if necessary. If Server Manager doesn't start, click the **Server Manager** icon on the Quick Launch toolbar.
2. In the left pane of Server Manager, click **Roles**.
3. Click **Add Roles** in the Roles Summary pane on the right. In the Before You Begin window, review the information, and then click **Next**.
4. In the Select Server Roles window, click to select the **Hyper-V** check box, and then click **Next**. If you see a message stating that Hyper-V can't be installed, you don't have a compatible processor, or the virtualization technology isn't enabled in the BIOS.
5. The next window displays information about Hyper-V, including an overview, prerequisites, and information on configuring Hyper-V and virtual machines. Read this information, and then click **Next**.
6. In the Create Virtual Networks window, click to select the check box next to the name of your network adapter, and then click **Next**.
7. Now you're ready to install Hyper-V. Click the **Install** button. After a few minutes, if the installation is successful, you get a message stating that you must restart the server to complete the installation. Click the **Close** button, and then click **Yes** to restart your server.

8. When your machine has finished restarting, log on, and the Hyper-V installation finishes. Click **Close** in the Installation Results window.
9. In Server Manager's left pane, click **Roles**. Under Roles Summary on the right, Hyper-V should be listed, if all went well.
10. Close all open windows.

Reviewing the Benefits of Virtualization

Before jumping into creating a virtual machine, you should review some benefits of virtualization in the following sections.

Solving Server Sprawl Using virtualization for server consolidation has several advantages. As the number of physical servers increases, so do space, power, and cooling requirements. Consolidating servers by converting physical servers to virtual machines helps decrease these physical plant requirements. At the same time, network administrators have fewer physical servers to manage and maintain. Fewer physical components means higher overall reliability because not only are servers usually better maintained, but also fewer parts exist that could potentially fail. Backups are streamlined, too. A virtual machine can be backed up simply by copying a few files to backup media. In addition, you can back up all your virtual machines and their hosts with a single backup operation instead of running backup jobs on each physical server.

You might be wondering how organizations wind up with too many physical servers. Server sprawl can occur for several reasons. For example, when a new application is added to the network, installing it on existing servers might not be practical. The installation process might require several server shutdowns and restarts and modifying the server's configuration during testing; both procedures are usually unacceptable on a production server. In addition, some applications run best when they're isolated from other applications to avoid conflicts. The solution to these problems is to put the new application on its own server.

Server sprawl also happens when new servers are purchased to supplement existing servers because of network growth or increased use. Adding memory, disk space, and processing power to existing servers running at full capacity might not be practical or even possible. Adding a server to the network can improve overall performance, too. After a few years, you wind up with several servers, with some running obsolete hardware technology.

Virtualization can reduce server sprawl and the resulting problems. By using virtual machines, you can stop, start, and reconfigure a new server without affecting the VM's host machine. In addition, applications running on a VM are isolated from both the host and other virtual machines, thus preventing conflicts. If you have half a dozen old servers, it makes sense to implement them as VMs instead of buying new hardware. Today, a typical server can run several VMs at the same performance level for the same cost of a single server 10 years ago. In addition, with programs to convert a physical computer to a virtual machine, time-consuming reinstallations aren't necessary.

Simplifying Training, Testing, and Development Trainers, testers, and developers were among the first to use virtualization. With virtualization, you can run your favorite OS on your host machine and install a new version of the same OS or a different OS as a VM. In fact, you can run several different OSs simultaneously in VMs on the same host machine and network them together. Want to try out the latest beta of a new Windows version? Instead of having to wipe your existing computer's hard disk, install a new disk, or find another computer, you can just install it as a virtual machine. Need to teach a survey of operating systems class? You can install DOS, Windows 98, countless Linux distributions, all the Windows Server editions, and more as VMs, which gives students instant access to all these OSs.

As a network administrator, you'll find no end to the uses for virtualization. Servers are a critical component of today's business operations, and downtime of any service affects productivity and costs money. Unfortunately, certain maintenance tasks, such as installing patches and service packs, often require testing and server restarts. By using virtualization, administrators can copy an existing VM to a test environment, apply the patch or service pack, and test the updated server thoroughly. After testing is finished, the update can be applied to the production machine without having to disrupt it with a lengthy test cycle.

Extensive testing is also essential when you're installing new applications. Frequently, testing an application requires a network environment that includes several clients with different OSs and possibly other servers, and setting up this physical environment can require a lot of time, space, and equipment. With virtualization, you can maintain a library of prebuilt VMs with different OSs installed and simply run test components on a virtual network in a single host computer.

Software developers use virtualization to install and test new programs on different OSs from the comfort of their development computers. Before virtualization, they had to load the program in development on another computer with the right OS installed. This limitation often resulted in maintaining a room full of computers with different OSs or different configurations of the same OS.

Creating Virtual Machines with Hyper-V

With Hyper-V installed, a new MMC called Hyper-V Manager is added to your Administrative Tools folder. You use Hyper-V Manager to create and manage virtual machines. The first time you run Hyper-V Manager, the end user license agreement (EULA) is displayed. After you accept the EULA, the Hyper-V Manager console shown in Figure 2-14 is displayed. To begin using Hyper-V, click the name of your server in the left pane.

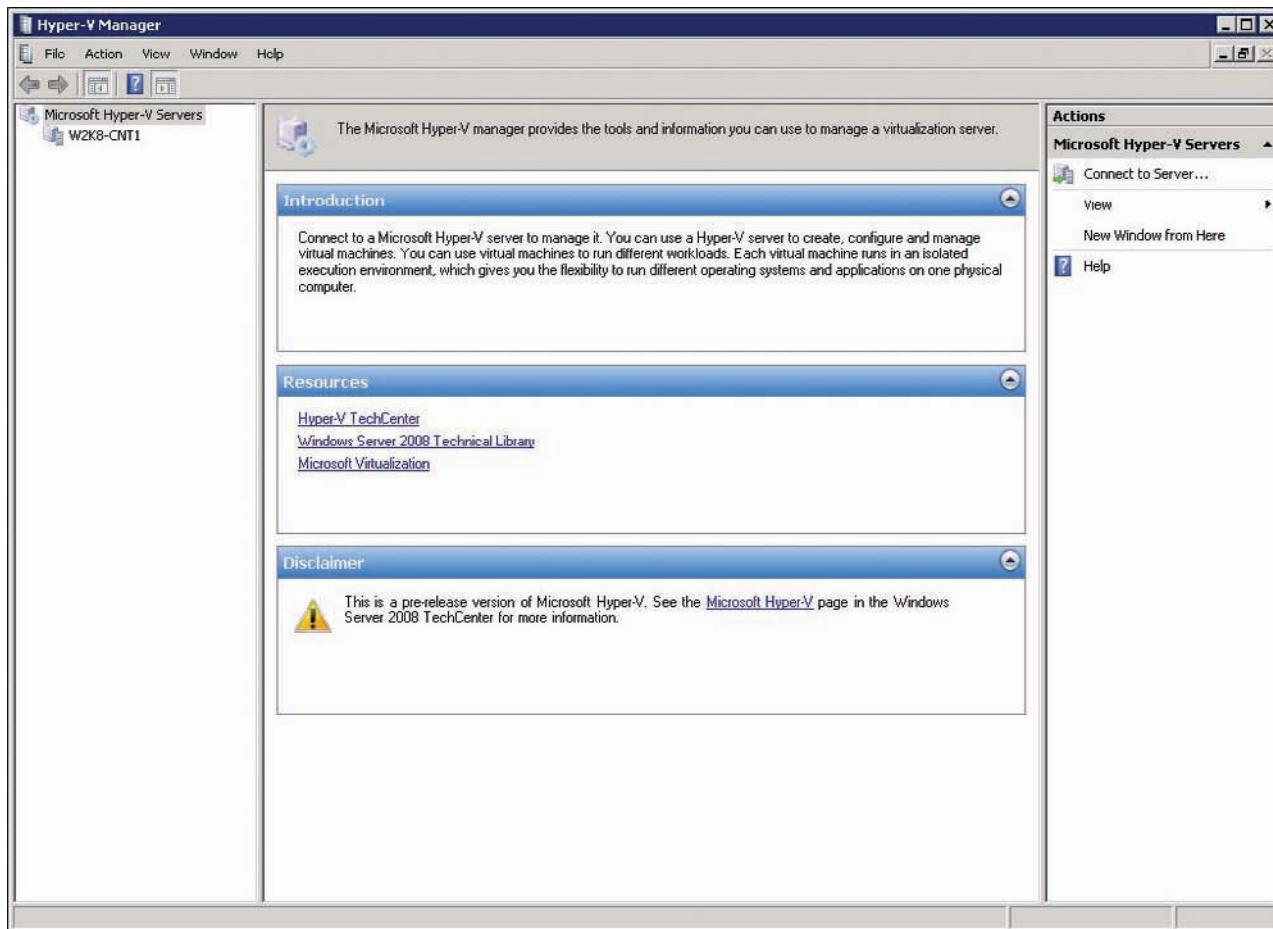


Figure 2-14 The Hyper-V Manager console

To use virtualization, you must first create a virtual machine. In Hyper-V Manager, all the tasks related to virtual machine creation and management are listed in the right pane under Actions. The process of creating a VM involves just a few steps:

1. Start the New Virtual Machine Wizard from Hyper-V Manager.
2. Give the new VM a descriptive name, such as "Read Only Domain Controller 1."

3. Choose a location for the VM. Storing virtual machines on a hard drive that's separate from your Windows Server 2008 installation is usually best.
4. Assign the amount of memory this VM requires. Memory requirements for virtual machines are the same as the requirements for installing the OS on a physical computer.
5. Configure networking. You have the choice of connecting through one of the host network adapters or leaving the VM disconnected from a network. This option can be changed later.
6. Create a virtual hard disk. You can give the virtual disk a name or accept the default, and you can choose the virtual disk's size and location. Again, putting virtual disks on a drive separate from your Windows Server 2008 installation files is best. You also have the option to use an existing virtual hard disk or attach a hard disk later.
7. Install an OS. In this step, you can choose to install an OS from media inserted in the physical CD/DVD drive, a CD/DVD image file (an .iso file), a boot floppy disk image, or the network using PXE boot. You can also choose to install an OS later.



Activity 2-15: Creating a Virtual Machine

Time Required: 10 minutes

Objective: Create a new virtual machine.

Description: You have installed the Hyper-V role on your server and are ready to create a virtual machine. You have the installation DVD for Windows Server 2008.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Hyper-V Manager**. If a license agreement window opens, click the option to accept the license.
3. If necessary, click your server name in the left pane of Hyper-V Manager (see Figure 2-15). Click **Action** from the menu, point to **New**, and click **Virtual Machine**.

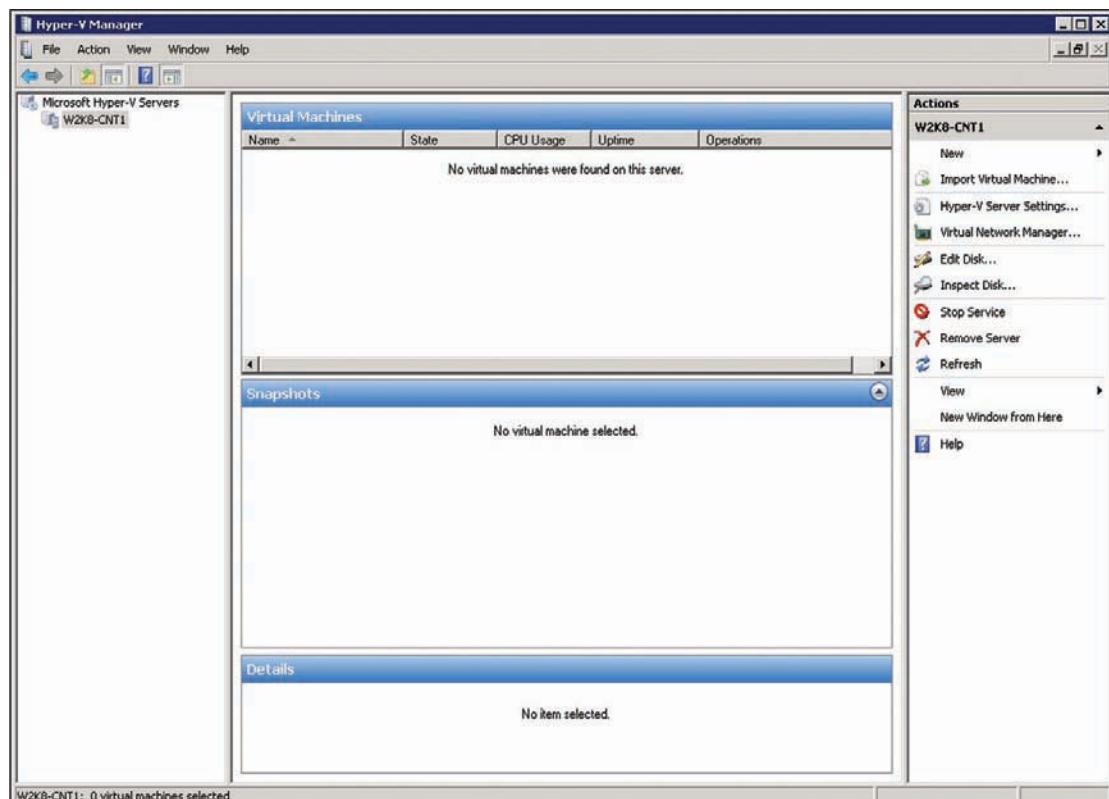


Figure 2-15 Hyper-V Manager with no virtual machines

4. Read the information in the Before You Begin window. Note that you can create a default virtual machine simply by clicking Finish in this window. For this activity, click **Next**.
5. In the Name text box, type **W2K8-VMTest** or another descriptive name. You can accept the default location or select a different location for your virtual machine. To use the default location of C:\ProgramData\Microsoft\Windows\Hyper-V, just click **Next**.
6. In the Assign Memory window, verify that the value in the Memory text box is **512 MB** (the minimum requirement for Windows Server 2008), and then click **Next**.
7. In the Configure Networking window, click the **Connection** list arrow, click your network connection in the drop-down list, and then click **Next**.
8. In the Connect Virtual Hard Disk window, you can enter the virtual hard disk's name, size, and location. You can also use an existing virtual disk or attach one later. Click **Next** to accept the default settings.
9. In the Installation Options window, click the **Install an operating system from a boot CD/DVD-ROM** option button, and then click **Next**.
10. The Completing the New Virtual Machine Wizard window displays a summary of your virtual machine configuration. Note that you can select to have the VM start after the wizard is finished. For now, click **Finish**. After the virtual machine is created, you're returned to Hyper-V Manager.
11. Close all open windows, or leave Hyper-V Manager open if you're going on to the next activity.



Activity 2-16: Installing Windows Server 2008 on a Virtual Machine

ACTIVITY

Time Required: 30 to 60 minutes, depending on your server's speed

Objective: Install Windows Server 2008 Enterprise Edition on your new virtual machine.

Description: You have created a new virtual machine and are ready to install Windows Server 2008. You have the installation DVD for Windows Server 2008.



This activity covers only the initial steps to get the installation started. The actual installation on a virtual machine is identical to installing Windows Server 2008 on a physical server.

NOTE

1. Log on to your server as Administrator, if necessary.
2. Insert your Windows Server 2008 installation DVD. (If Autorun is enabled on your DVD drive, the Windows Server 2008 Setup program starts. If it does, exit it.)
3. If necessary, click **Start**, point to **Administrative Tools**, and click **Hyper-V Manager**.
4. In the center pane, right-click the virtual machine you created in Activity 2-15 and click **Connect**. You see the window shown in Figure 2-16.
5. The virtual machine isn't started yet, so click **Action**, **Start** from the menu. (You can also start the VM by clicking the blue Start icon.)
6. From this point, the installation is identical to the Windows Server 2008 installation steps in Activities 2-1 and 2-7, until you need to press Ctrl+Alt+Delete to log on. For a virtual machine, press **Ctrl+Alt+End** instead. (You can also click Action, Ctrl+Alt+Delete from the menu, and Hyper-V sends the keystroke combination to the virtual machine.)
7. After you're logged on to the VM, shut it down by clicking **Start**, **Shutdown**.
8. Close all open windows.

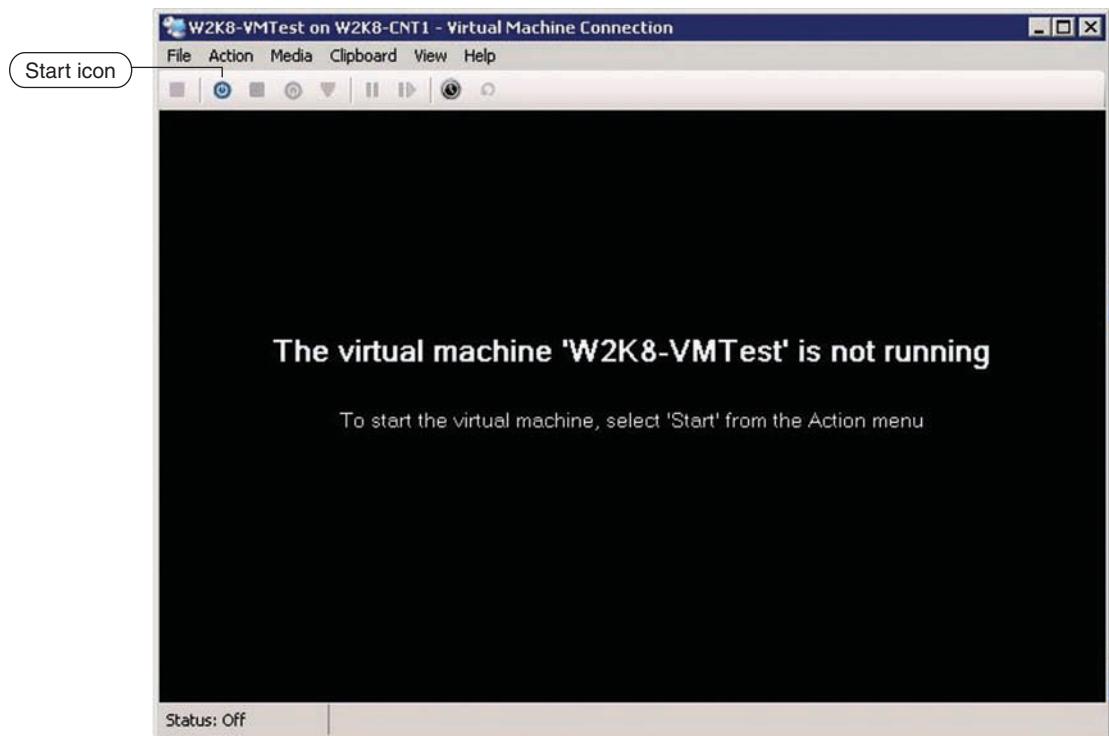


Figure 2-16 A virtual machine before it's started

Basic Virtual Machine Management with Hyper-V Manager

With Hyper-V, a virtual machine runs in the background until you connect to it with Hyper-V Manager. A running VM doesn't require using Hyper-V Manager, nor does it require anybody to be logged on to the server. Furthermore, you can configure a VM to start and shut down automatically when the host server starts and shuts down. In addition, like any OS, you can manage a VM remotely by using tools such as Remote Desktop and MMCs.

When you want to configure and manage a VM's properties or access it locally, you do need to run Hyper-V Manager. The middle pane of Hyper-V Manager shows all installed virtual machines at the top; in Figure 2-17, one VM is running and one VM is powered off. This pane also displays name, state, CPU usage, uptime, and current operations for each VM. Normally, the Operations column doesn't display anything unless you perform a task such as exporting a VM or creating a snapshot of it. When you select a VM, the Snapshots section shows a list of snapshots created for it. If you click the VM's name in the Snapshots section, you see a screen shot of the VM at the time the snapshot was taken along with the time and date it was taken. The bottom section shows a real-time screen shot of a running VM. When a running VM changes, the screen shot in Hyper-V Manager reflects the change almost immediately.

Connecting to a virtual machine opens a window that serves as the user interface to the VM and looks similar to a remote desktop connection. You can connect to a VM by using any of the following methods:

- Right-click the VM and click Connect.
- Double-click the VM.
- Select the VM and double-click its screen shot in the bottom section.
- Select the VM and click Connect in the Actions pane.

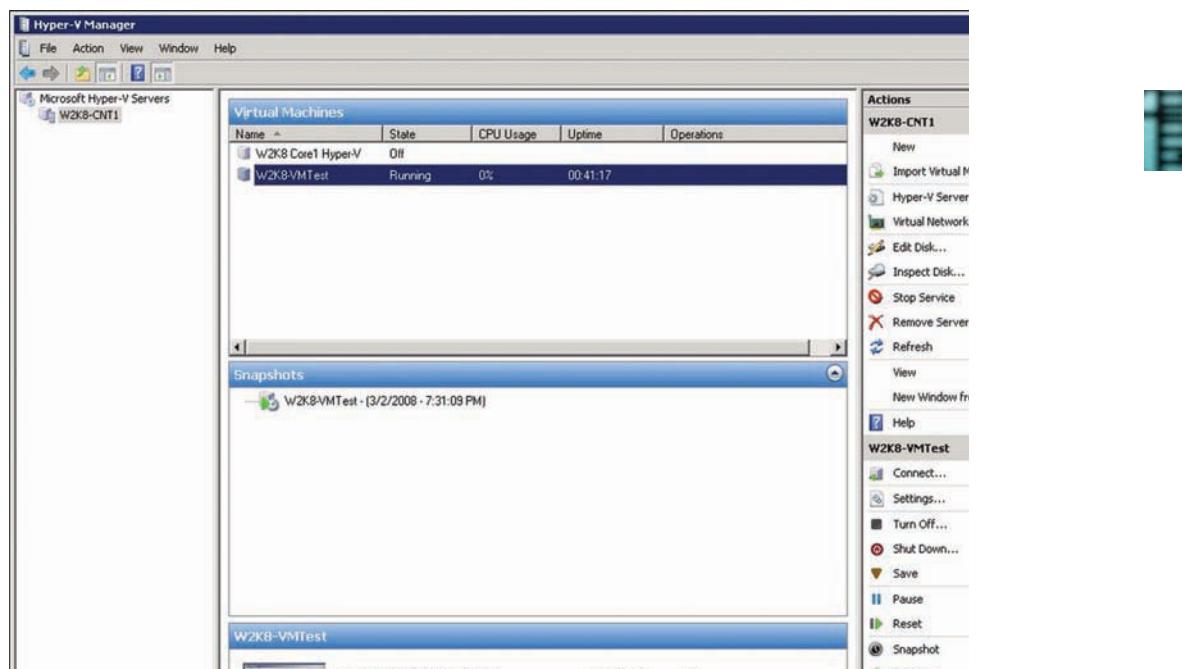


Figure 2-17 Hyper-V Manager showing two virtual machines

After you’re connected, you see the Virtual Machine Connection console shown in Figure 2-18. The toolbar icons from left to right are as follows:

- Ctrl+Alt+Delete (sends a Ctrl+Alt+Delete keystroke to the VM)
- Start (starts the VM)

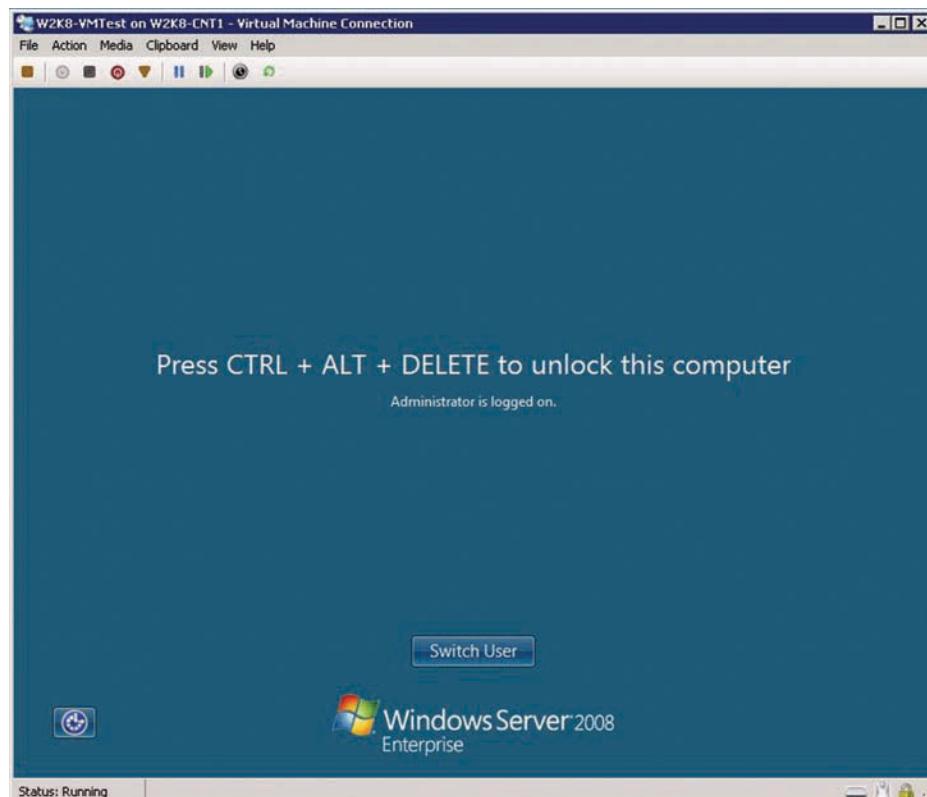


Figure 2-18 The Virtual Machine Connection console

- Turn Off (turns off the VM)
- Shut Down (sends a signal to the OS to perform a shutdown)
- Save (saves the VM's state, similar to Windows hibernation mode)
- Pause (pauses the VM, similar to Windows sleep mode)
- Reset (resets the VM)
- Snapshot (creates a snapshot of a VM)
- Revert (reverts to a snapshot of a VM)

You can access all these toolbar operations from the Action menu, too. The following list summarizes some tasks you can perform with other menus:

- *File*—Access the VM's settings and exit the VM.
- *Media*—Specify a CD/DVD drive the VM should connect to, specify an .iso file the VM mounts as a virtual CD/DVD drive, or specify a floppy disk image that can be mounted as a virtual floppy disk.
- *Clipboard*—Copy a screen shot of the VM to the Clipboard or paste Clipboard text into the VM. You can also copy and paste between the host computer and virtual machines or between virtual machines.

If you want to disconnect from a virtual machine, thereby closing the connection console but not shutting down the VM, simply click File, Exit from the menu or close the window.



Activity 2-17: Working with Virtual Machines in Hyper-V Manager

Time Required: 30 minutes

Objective: Explore Hyper-V Manager.

Description: You have installed a test VM that you can use to become familiar with managing virtual machines in Windows Server 2008.

1. Log on to your host server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Hyper-V Manager**.
3. Right-click the virtual machine you created in Activity 2-15 and click **Connect**.
4. If the VM was powered down, power it on by clicking the **Start** toolbar icon in the connection console or clicking **Action**, **Start** from the menu. Go immediately to the next step.
5. While Windows is booting, close the connection console by clicking the **X** at the upper right or clicking **File**, **Exit** from the menu. Notice that in Hyper-V Manager, the VM's CPU usage changes as Windows boots, and the VM's screen shot in the bottom pane changes periodically.
6. Double-click the VM's screen shot at the bottom of Hyper-V Manager to open the connection console to your VM.
7. After Windows finishes booting, click the **Ctrl+Alt+Delete** toolbar icon (the brown square icon at the far left) to send a Ctrl+Alt+Delete keystroke to the VM.



To see a description of any toolbar icon, hover your mouse pointer over it.

8. In the logon window, enter the password you created for the Administrator account and log on.
9. Close any open windows in the VM until only the desktop is displayed.

10. Click **Start**, type **notepad** in the Start Search text box, and press **Enter** to start Notepad.
11. Type your name in a new text document, and then click the **Save** toolbar icon or click **Action, Save** from the menu.
12. Close the virtual machine console. In Hyper-V Manager, note that the State column for the VM shows Saved. Open the VM by double-clicking it. Start the VM by clicking the **Start** toolbar icon, which takes you right where you left off in Notepad.
13. Save the Notepad file to your desktop by clicking **File, Save As** from the menu. In the Save As dialog box, click the **Browse Folders** button. Click **Desktop** under Favorite Links, type **File1.txt** in the File name text box, and then click **Save**. Exit Notepad.
14. Click the **Snapshot** toolbar icon or click **Action, Snapshot** from the menu. When you're prompted to enter a name, type **AfterFile1**, and then click **Yes**.
15. Minimize your VM, and note that the snapshot is listed in Hyper-V Manager in the Snapshots section. Maximize your VM, and delete the Notepad file you created.
16. Click the **Revert** toolbar icon or click **Action, Revert** from the menu.
17. Click **Revert** when prompted. The VM displays a message that it's restoring. When the desktop is displayed again, you should see the Notepad file back on the desktop. Close the virtual machine console.
18. In Hyper-V Manager, right-click the VM and click **Shutdown**. When prompted, click the **Shutdown** button. The Operations column displays "Shutting Down Virtual Machine."
19. Close Hyper-V Manager.

This section has introduced you to using Hyper-V to manage virtual machines. You delve into this topic in more detail in Chapter 13.



Chapter Summary

- The process of installing Windows Server 2008 is fairly straightforward. Most of the work takes place in the planning phase. Some issues to consider include the server's CPU architecture (32-bit or 64-bit), total number of processors or cores the server requires, number and types of disks, and advanced hardware features.
- Installing from a DVD is common for a single-server installation. Only a few choices must be made, such as selecting a full or Server Core installation and choosing the disk or partition where Windows Server 2008 should be installed.
- Postinstallation configuration tasks include giving the server a name, configuring network protocols, setting time zone information, selecting a network model (workgroup or domain), and installing and configuring Windows Updates. After completing these tasks, you can install server roles.
- When adding new servers to an existing network, you must decide whether the server will be a new domain controller in the existing domain, a read only domain controller, a member server, or a stand-alone server. Reasons for adding new servers include company growth, excessive server load, application isolation, fault tolerance, and branch office server installations.
- You can upgrade to Windows Server 2008 only if the existing OS is Windows Server 2003. A clean installation to a new disk or partition is recommended. If you do an upgrade, the old Windows directory is copied to Windows.old, and Windows Server 2008 is installed clean. Then the old OS settings are migrated to Windows Server 2008.
- Windows Server Core is a new installation option in Standard, Enterprise, and Datacenter editions. The traditional Windows GUI isn't available in Server Core. Initial configuration tasks, such as changing the server name and setting IP address information, must be done from the command line.

- The Hyper-V server role can be installed on 64-bit versions of Windows Server 2008. Your system's CPU must support AMD-V or Intel-VT virtualization extensions. Server virtualization offers benefits such as server consolidation and optimal training, development, and testing environments.
- Virtual machines are managed in Hyper-V Manager. They run in the background until you connect to them in Hyper-V Manager. Virtual machines can be configured to start and shut down when the host computer starts and shuts down. You can also use Hyper-V Manager to take snapshots of a VM, which makes it possible to revert to the VM's previous state.

Key Terms

- Echo Reply** An ICMP message that's the response when a computer receives an Echo Request, generated by the Ping program.
- Echo Request** An ICMP message generated by the Ping program used to test network connectivity and IP configuration. If a computer receives an Echo Request, it responds with an Echo Reply.
- failover clustering** A Windows Server 2008 feature in Enterprise and Datacenter editions in which a group of servers is connected by both cabling and software; if one server fails, another takes over to provide services.
- guest operating systems** OSs running in virtual machines on host computers.
- host computer** The physical computer on which Windows Server 2008 is installed.
- host operating system** An OS running virtualization software for the purposes of running virtual machines or guest operating systems.
- hot-add** A high-end feature that allows adding hardware (usually memory, processors, or disk drives) to a system while it's running.
- hot-replace** A high-end feature that allows replacing faulty hardware (usually memory, processors, or disk drives) in a system while it's running.
- hypervisor** A layer of software between hardware and OSs that allows multiple OSs or multiple instances of the same OS to share physical hardware resources.
- patches** Software updates normally intended to fix security vulnerabilities and software bugs.
- Ping** A utility used to test network connectivity and IP address configuration.
- service pack** A collection of bug fixes and security updates or patches that can be installed on an OS to bring it up to date.
- snapshot** A set of files containing a virtual machine's state at a particular time.

Review Questions

1. Which of the following is *not* a valid Windows Server 2008 installation option?
 - a. A full clean installation
 - b. A Server Core upgrade from Windows Server 2003
 - c. A full upgrade from Windows Server 2003
 - d. A Server Core installation in Hyper-V
2. What is required to install the Hyper-V server role? (Choose all that apply.)
 - a. A 64-bit processor
 - b. A 32-bit version of Windows Server 2008
 - c. AMD-V or Intel-VT extensions
 - d. At least 384 MB RAM
3. Which Windows Server 2008 edition does not support the Server Core installation?

4. Which of the following is true when purchasing a motherboard with multiple CPU sockets?
- Windows Server 2008 does not support multiple CPU sockets.
 - You must run a 64-bit version of Windows Server 2008.
 - All installed CPUs must be identical.
 - Virtualization is not supported on multiple CPUs.
5. You're trying to decide which disk technology to use on your new server. The server will be in heavy use around the clock every day, so high performance is a necessity. Which technology is the best choice?
- IDE
 - ATA-166
 - SATA
 - SCSI
6. You can use a 32-bit processor to install the Hyper-V role as long as it supports virtualization extensions. True or False?
7. Which networking protocol is installed by default in Windows Server 2008? (Choose all that apply.)
- TCP/IPv4
 - IPX/SPX
 - TCP/IPv5
 - TCP/IPv6
8. Which of the following is *not* a typical Windows Server 2008 postinstallation task?
- Installing the Server Core role
 - Setting the correct time zone
 - Setting IP configuration parameters
 - Changing the server name
9. Which of the following is a task you must do *during* Windows Server 2008 installation?
- Name the server.
 - Choose the disk where it will be installed.
 - Set the Administrator password.
 - Set the workgroup or domain.
10. What command should you use to test your IP configuration settings after a new Windows Server 2008 installation?
- Dir
 - Arp
 - Ping
 - Hostname
11. Which graphical utility runs in Server Core?
- Explorer
 - Date and Time control panel
 - Computer Management
 - Server Manager
12. You installed Windows Server 2008 recently, and it has been running well for the past several days. You read about a critical security patch that has been available for about a

week. You view the currently installed updates in Control Panel's Programs and Features and don't see any installed updates. You need to install this update immediately and make sure your server is kept up to date without your intervention in the future. What should you do?

13. Which of the following is a reason for installing a new server? (Choose all that apply.)
 - a. Excessive load on existing servers
 - b. Fault tolerance
 - c. Adding a new network protocol
 - d. To isolate a new application
14. Windows Server Core is a good installation option with all but which of the following?
 - a. A secondary domain controller
 - b. For running Windows Web Server 2008
 - c. As a branch office server
 - d. As a virtual machine
 - e. As a remotely managed departmental server
15. You approach one of your servers running Server Core and see a completely blank desktop except for the mouse pointer. You need to do some management tasks on the server. What should you do?
 - a. Right-click the mouse pointer and click Open a command prompt.
 - b. Click Start and type cmd in the Run dialog box.
 - c. Press Ctrl+Alt+Delete and click Start Task Manager.
 - d. Right-click the desktop, point to New, and click Task.
16. What command do you use to configure addresses for network interfaces?
 - a. netdom interface
 - b. ipconfig /interface
 - c. netsh interface
 - d. netstat interface
 - e. nbtstat /interface
17. You have just finished installing Windows Server 2008. You have assigned it a name and have finished configuring IP addresses. You have tested your configuration by using Ping to verify network connectivity with your default gateway and another server on the network, and everything worked fine. However, the next day, a colleague tells you that when he tried to ping the server, his request timed out. You try to ping your colleague's computer and receive a reply just fine. Why can't your colleague ping your server successfully?
 - a. Your server's default gateway is incorrect.
 - b. Windows Firewall is blocking the packets.
 - c. Your colleague's IP address configuration is incorrect.
 - d. You don't have DNS installed.
18. Which command do you use to restart Server Core?
 - a. shutdown /r /t 0
 - b. restart /t 0
 - c. net stop /r /t 0
 - d. net computer /reset /t 0

19. In Server Core, which command do you use to join your server to a Windows domain?
- net domain /join
 - cscript domain.wsf
 - netdom join
 - net join /domain
20. Which of the following is the default setting for Windows Update after a new Windows Server 2008 installation?
- Download and install updates at 3:00 a.m.
 - Download but do not install updates.
 - Inform when updates are available but do not download updates.
 - Not enabled.
21. You're about to install a new application on Windows Server 2008 running in Hyper-V. You're concerned that this application might cause conflicts with other applications and services on the virtual machine. You can take the server down for a short time if necessary, but you're concerned that if the application does cause problems, getting the server back in working order could take quite a long time. What is the best course of action?
- Install the new application on the host server.
 - Use the Save function in the VM console, install the application, and then restore the VM if necessary.
 - Suspend the virtual machine, install the application, and then unsuspend the VM if necessary.
 - Take a snapshot of the virtual machine, install the application, and then revert to the snapshot if necessary.
22. The layer of software sitting between the server hardware and OS that allows multiple OSs to share hardware resources is called which of the following?
- Guest operating system
 - Device driver
 - Hypervisor
 - Host operating system
 - Virtual machine
23. Virtual machines must be allocated a minimum of 1 GB RAM to run properly. True or False?
24. Which of the following is an advantage of using virtual machines? (Choose all that apply.)
- Fewer physical devices to manage
 - Lower overall power consumption
 - Easier backup of servers
 - Facilitates testing
25. You want to install a new server in Hyper-V. You create the virtual machine and insert the installation DVD, only to find that the DVD drive on your server has failed. You need to install this virtual machine today and don't have any spare DVD drives handy, nor do you want to shut down the server to install a DVD drive, if you can avoid it. What can you do?
- Copy all the files on the DVD and put them on a network share. Start the virtual machine and tell it to boot from the network share.
 - Create an .iso file from the DVD and copy it to the server. Use the VM console to mount the .iso file as a virtual DVD.

- c. Share the DVD on a system with a working drive. Insert a boot floppy disk into the server's floppy drive, and instruct the VM to boot to the floppy and then install from the shared DVD.
- d. Run the Windows Server 2008 Setup program from the host computer and choose the VM's virtual disk as the installation destination.

Case Projects



Case Project 2-1: Adding a Server to Your Network

Your client, Cool Gadgets, has been running Windows Server 2008 32-bit Standard Edition, which you installed about six months ago. Cool Gadgets is running the Active Directory Domain Services, DNS, IIS, and File Services roles. The number of computer clients has grown from 25 to 50 in the past six months, and additional growth is expected. Cool Gadgets just purchased an expensive material requirements planning (MRP) system to help manage production. This application has hefty memory (4 GB or more) and CPU requirements (recommended 2.0 GHz dual-core processor). All desktop computers will have the MRP client application installed. The owner doesn't want to install the MRP client application on mobile users' laptops, so a remote solution is needed for these systems. The owner also mentions that he's familiar with this application and will need to log on to the server periodically to do maintenance and monitoring.

The owner tells you that in the future, Cool Gadgets might need system fault tolerance to ensure that there's little or no downtime because this critical application will eventually be accessed at all times of the day and night. For now, he's just concerned about getting the system up and running. You check the existing server's capacity and determine that the new application's memory and disk requirements will likely exceed the existing server's 4 GB capabilities. The owner explains that there's enough budget for a new server, so you should plan for growth. As an aside, he mentions that because all his employees log on at about the same time, the time it takes to log on has been increasing. You need to come up with specifications for a new server. Describe some hardware features you will recommend for this new server, in particular the CPU architecture, number of processors, amount of RAM, and disk system. Explain your answers.

Case Project 2-2: Choosing the Right Edition

You have your new server for the Cool Gadgets upgrade project and are ready to install Windows Server 2008. Case Project 2-1 describes the current environment and requirements of Cool Gadgets. Which edition of Windows Server 2008 will you install? Include information on 32-bit or 64-bit versions and whether it should be a full or Server Core installation. Explain your answer.

Case Project 2-3: Server Postinstallation Tasks

You have finished installing Windows Server 2008 on the new server for Cool Gadgets. Next, you need to decide what to name the server and how it will participate in the existing domain: as a domain controller, a member server, or a stand-alone server. The server will be located near the existing server, named CG-Server1-DC, in the equipment closet. Make a list of the postinstallation tasks to perform on this server, including details on the server name and its role in the domain (if any). Don't include installing specific server roles just yet.

Case Project 2-4: Server Roles on the Second Server

You have finished postinstallation tasks for the new server, and now you need to decide which server roles you will install on it. Reread Case Project 2-1 carefully, which provides most of the information you need to make an informed decision. List which server roles you will install and explain why.

Introducing Active Directory

After reading this chapter and completing the exercises, you will be able to:

- Describe the role of a directory service and the physical and logical Active Directory structure
- Install Active Directory
- Describe the main Active Directory objects
- Explain configuring and applying group policies

Windows Server 2008 Active Directory is the core component in a Windows domain environment. The Active Directory Domain Services role provides a single point of user, desktop, and server administration. To understand Active Directory and its role in a network, you need to know what a directory service is and how it's used to manage resources and access to resources on a network. Before administrators can use Active Directory to manage users, desktops, and servers in a network, they need a good understanding of Active Directory's structure and underlying components and objects, which are covered in this chapter. You also learn about installing Active Directory and using the powerful Group Policy tool to set consistent security, user, and desktop standards throughout your organization.

The Role of a Directory Service

A network **directory service**, as the name suggests, stores information about a computer network and offers features for retrieving and managing that information. Essentially, it's a database composed of records or objects describing users and available network resources, such as servers, printers, and applications. Like a database for managing a company's inventory, a directory service includes functions to search for, add, modify, and delete information. Unlike an inventory database, a directory service can also manage how its stored resources can be used and by whom. For example, a directory service can be used to specify who has the right to log on to a computer or restrict what software can be installed on a computer.

A directory service is often thought of as an administrator's tool, but users can use it, too. Users might need the directory service to locate network resources, such as printers or shared folders, by performing a search. They can even use the directory service as a phone book of sorts to look up information about other users, such as phone numbers, office locations, and e-mail addresses.

Whether an organization consists of a single facility or has multiple locations, a directory service provides a centralized management tool for users and resources in all locations. This capability does add a certain amount of complexity, so making sure the directory service is structured and designed correctly before using it is critical.

Windows Active Directory

Windows Active Directory became part of the Windows family of server OSs starting with Windows 2000 Server. Before Windows 2000, Windows NT Server had a directory service that was little more than a user manager; it included centralized logon and grouped users and computers into logical security boundaries called domains. The Windows NT domain system was a flat database of users and computers with no way to organize users or resources by department, function, or location, no matter how many users you had. This single, unstructured list made managing large numbers of users cumbersome.

Active Directory's hierarchical database enables administrators to organize users and network resources to reflect the organization of the environment in which it is used. For example, if a company identifies its users and resources primarily by department or location, Active Directory can be configured to mirror that structure. You can structure Active Directory and organize the objects representing users and resources in a way that makes the most sense. Active Directory offers the following features, among others, that make it a highly flexible directory service:

- *Hierarchical organization*—This structure makes management of network resources and administration of security policies easier.
- *Centralized but distributed database*—All network data is centrally located, but it can be distributed among many servers for fast, easy access to information from any location. Automatic replication of information also provides load balancing and fault tolerance. **Active Directory replication** is the transfer of information among domain controllers to make sure all domain controllers have consistent and up-to-date information.
- *Scalability*—Advanced indexing technology provides high-performance data access, whether Active Directory consists of a few dozen or few million objects.

- **Security**—Fine-grained access controls enable administrators to control access to each directory object and its properties. Active Directory also supports secure authentication protocols to maximize compatibility with Internet applications and other systems.
- **Flexibility**—Active Directory is installed with some predefined objects, such as user accounts and groups, but their properties can be modified, and new objects can be added for a customized solution.
- **Policy-based administration**—Administrators can define policies to ensure a secure and consistent environment for users yet maintain the flexibility to apply different sets of rules for departments, locations, or user classes as needed.



Overview of the Active Directory Structure

As with most things, the best way to understand how Active Directory works is to install it and start using it, but first, knowing the terms used to describe its structure is helpful. There are two aspects of Active Directory's structure:

- Physical structure
- Logical structure

Active Directory's Physical Structure The physical structure consists of sites and servers configured as domain controllers. An Active Directory **site** is nothing more than a physical location in which domain controllers communicate and replicate information regularly. Specifically, Microsoft defines a site as one or more IP subnets connected by high-speed LAN technology. A small business with no branch offices or other locations, for example, consists of a single site. However, a business with a branch office in another part of the city connected to the main office through a slow WAN link usually has two sites. Typically, each physical location with a domain controller operating in a common domain connected by a WAN constitutes a site. The main reasons for defining multiple sites are to control the frequency of Active Directory replication and to assign policies based on physical location. Chapters 4 and 10 discuss sites in more detail.

Another component of the physical structure is a server configured as a domain controller, which is a computer running Windows Server 2008 with the Active Directory Domain Services role installed. Although an Active Directory domain can consist of many domain controllers, each domain controller can service only one domain. Each domain controller contains a full replica of the objects that make up the domain and is responsible for the following functions:

- Storing a copy of the domain data and replicating changes to that data to all other domain controllers throughout the domain
- Providing data search and retrieval functions for users attempting to locate objects in the directory
- Providing authentication and authorization services for users who log on to the domain and attempt to access network resources

Active Directory's Logical Structure The logical structure of Active Directory makes it possible to pattern the directory service's look and feel after the organization in which it runs. There are four organizing components of Active Directory:

- Organizational units (OUs)
- Domains
- Trees
- Forests

These four components can be thought of as containers and are listed from most specific to broadest in terms of what they contain. To use a geographical analogy, an OU represents a city, a domain is the state, a tree is the country, and a forest is the continent.

An **organizational unit (OU)** is an Active Directory container used to organize a network's users and resources into logical administrative units. An OU contains Active Directory objects, such as user accounts, groups, computer accounts, printers, shared folders, applications, servers, and domain controllers. The OU structure often mimics a company's internal administrative structure, although this structure isn't required. For example, a corporation might create an OU for each department, but an educational institution might create separate OUs for students, faculty, and administration or for campus sites. You can use a combination of structures, too, because OUs can be nested as many levels as necessary. Besides being an organizational tool, OUs can represent policy boundaries, in which different sets of policies can be applied to objects in different OUs. Figure 3-1 depicts OUs and the types of objects in them.

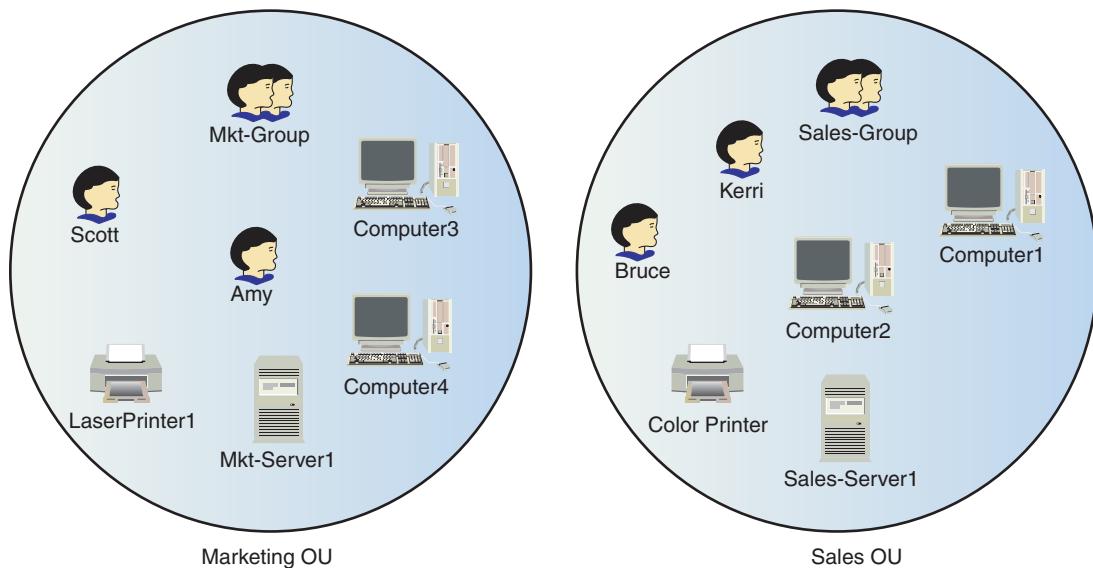


Figure 3-1 Active Directory organizational units

A **domain** is Active Directory's core structural unit. It contains OUs and represents administrative, security, and policy boundaries. A small to medium company usually has one domain with a single administrative group. However, a large company or a company with several locations might benefit from having multiple domains to separate administration or accommodate widely differing network policies. For example, a company with major branches in the United States and Europe might want to divide administrative responsibilities into domains based on location, such as US.coolgadgets.com and UK.coolgadgets.com domains, each with a separate administrative group and set of policies. This arrangement addresses possible language and cultural barriers and takes advantage of the benefit of proximity. Figure 3-2 shows the relationship between domains and OUs.

An Active Directory **tree** is less a container than it is simply a grouping of domains that share a common naming structure. A tree consists of a parent domain and possibly one or more child domains that have the same second-level and top-level domain names as the parent domain. For example, US.coolgadgets.com and UK.coolgadgets.com are both child domains of the parent domain coolgadgets.com. Furthermore, child domains can have child domains, as in phoenix.US.coolgadgets.com. Figure 3-3 depicts domains in an Active Directory tree.

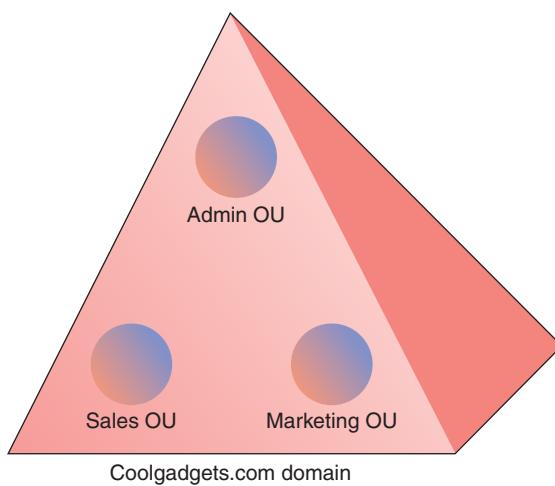


Figure 3-2 An Active Directory domain and OUs

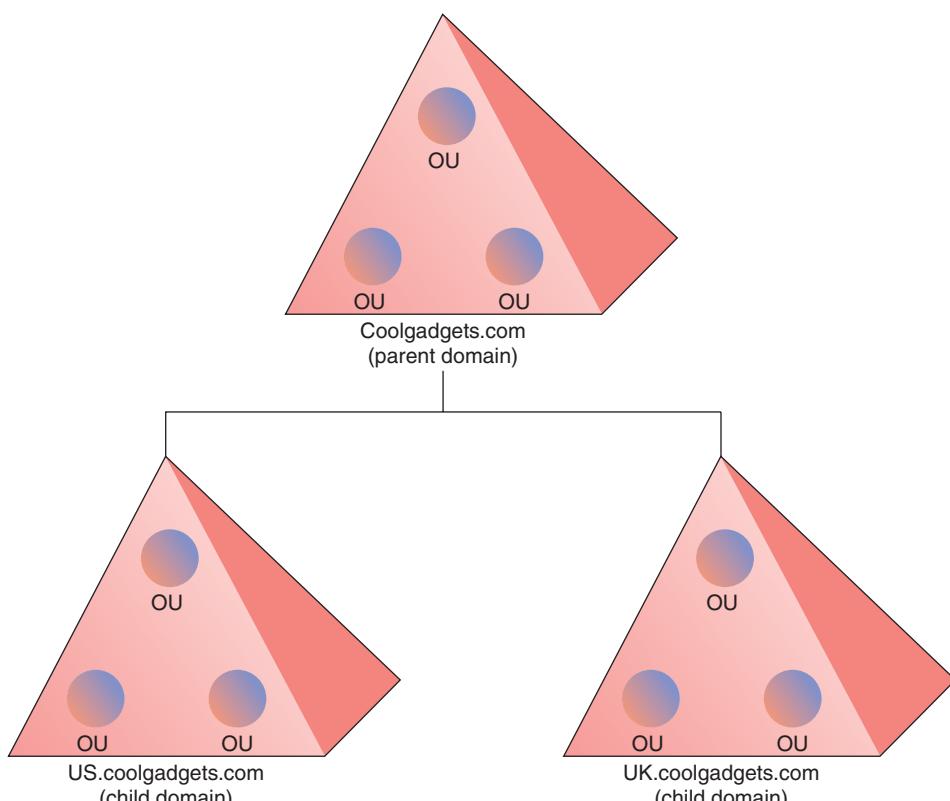


Figure 3-3 An Active Directory tree

An Active Directory **forest** is a collection of one or more trees. A forest can consist of a single tree with a single domain, or it can contain several trees, each with a hierarchy of parent and child domains. Each tree in a forest has a different naming structure, so although one tree might have coolgadgets.com as the parent, another tree in the forest might have niftytools.com as its parent domain. A forest's main purpose is to provide a common Active Directory environment, in which all domains in all trees can communicate with one another and share information yet allow independent operation and administration of each domain. Figure 3-4 shows an Active Directory forest and the trees and domains it contains.

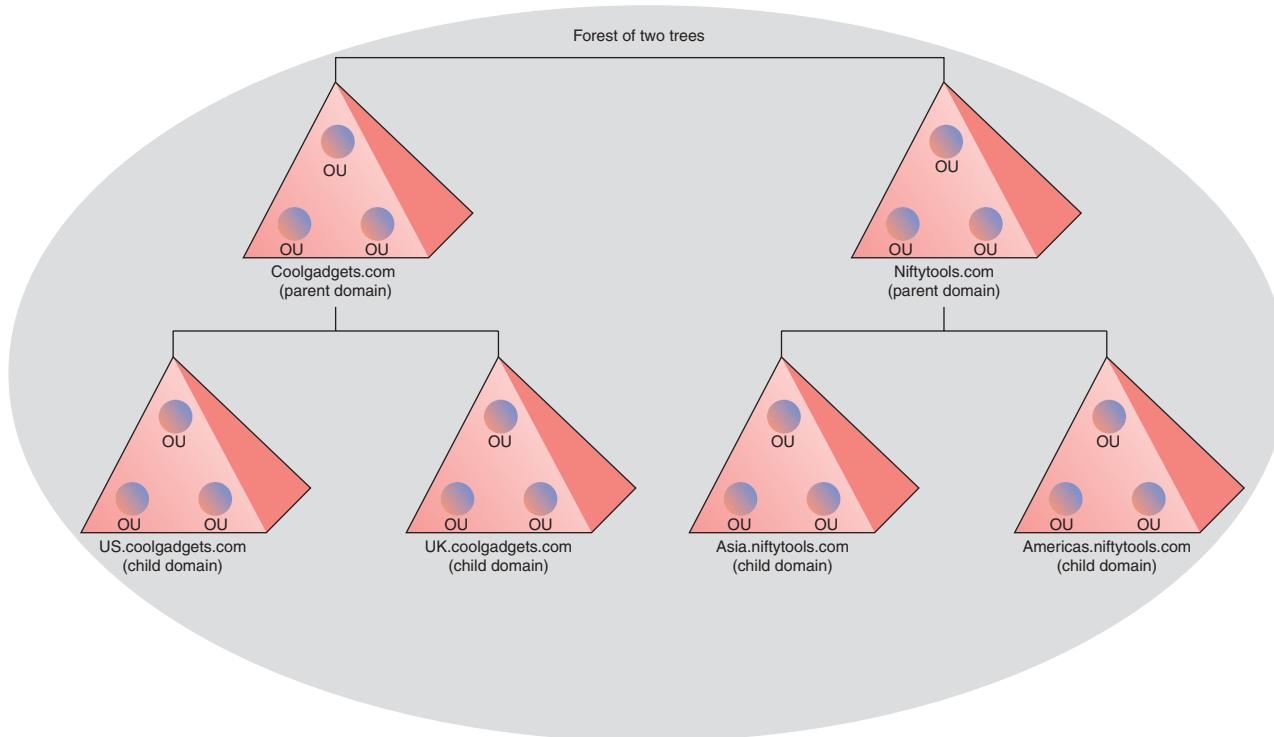


Figure 3-4 An Active Directory forest

This section has given you an overview of Active Directory components, and you explore them in more depth in Chapters 4, 5, 9, and 10. For now, to understand its features and structure, in the next section you install and work with Active Directory.

Installing Active Directory

The Windows Active Directory service is commonly referred to as Active Directory Domain Services (AD DS). You must install this role for Active Directory to be part of your network. As with installing Windows Server 2008, installing AD DS is fairly straightforward, with the real work in the planning and postinstallation tasks.

To begin installing AD DS on a full Windows Server 2008 installation, you use Server Manager. After selecting the role to install, you follow a wizard. The first window provides information about Active Directory and explains that you must install the DNS Server role if DNS isn't already installed on the network. In addition, you're informed that you must run Dcpromo.exe to make the server a fully functional domain controller (DC). After the wizard is finished, Server Manager displays another reminder to run Dcpromo.exe. You can do this from the Start menu, or you can click Active Directory Domain Services in the Roles summary section of Server Manager to see a link for running Dcpromo.exe. When you run Dcpromo.exe, a new wizard starts.

The first question you must answer is whether the domain controller will be part of an existing forest or a new domain in a new forest should be created. For the first domain controller in the network, a new domain in a new forest should be created. Next, you're prompted for the **fully qualified domain name (FQDN)** for the new forest root domain. An FQDN is a domain name that includes all parts of the name, including the top-level domain. Examples include coolgadgets.com or americas.niftytools.com.



The first domain in a new forest is also the name of the forest. The wizard checks to be sure the forest name doesn't already exist.

NOTE

The next step is to choose the forest functional level. Microsoft has expanded Active Directory's functionality with each successive server OS since Windows 2000. For the most advanced features and security, you should choose the Windows Server 2008 functional level. For the most backward compatibility with older domain controllers on the network, you should choose Windows 2000. If you choose the Windows Server 2008 level, you can't run Windows Server 2003 or Windows 2000 domain controllers. You can, however, still run older servers as member servers.

You then have three additional options for the domain controller:

- *DNS server*—For the first domain controller in a new domain, DNS should be installed, and this check box should be selected in most circumstances.
- *Global catalog*—For the first DC in a forest, this check box is selected and disabled because the first DC in a new forest must also be a global catalog server (discussed in Chapters 4 and 10).
- *Read-only domain controller (RODC)*—This check box is not selected by default, and it's disabled for the first DC in the domain.

After you have made your choices, Windows might warn you about a DNS server not being found, which is okay if you're going to install DNS during the Active Directory installation. Next, you're asked for the location of the Active Directory database, log files, and Sysvol folder. The **Sysvol folder** is a shared folder that stores the information from Active Directory that's replicated to other domain controllers. Storing the database and log files on separate disks, if possible, is best for optimal performance. Next, you're asked to enter a password for **Directory Services Restore Mode**. This boot mode is used to perform restore operations on Active Directory if it becomes corrupted or parts of it are deleted accidentally. That's it—Windows is then ready to finish the AD DS installation. If you know you'll be installing other DCs, you can export your answers to a file for use in an unattended installation. When the installation is finished, your server restarts, and then you have some new MMCs in the Administrative Tools folder for configuring and managing Active Directory.

Activity 3-1: Installing Active Directory Domain Services

 **Time Required:** 15 minutes

Objective: Install AD DS as a new domain controller in a new forest.

Description: After installing Windows Server 2008 successfully and completing the immediate postinstallation tasks, you decide to install Active Directory Domain Services. This server will be the first DC in a new forest. (Because the entire class is also installing AD DS, make sure your domain names don't conflict.) In addition, you decide to install the DNS Server role as part of the installation because DNS is required for Active Directory functionality.



Server and domain names are indicated in several activities with "XX" as part of the name. Whenever you see the "XX," replace it with your student number, which your instructor assigns.

NOTE

1. Start your server and log on as Administrator, if necessary. If the Initial Configuration Tasks applet starts, click the **Do not show this window at logon** check box, and then close the window. Server Manager should start. If it doesn't, click the **Server Manager** icon on the Quick Launch toolbar.
2. In the Server Summary section of Server Manager, verify that your server name is ServerXX.
3. Click the **Roles** node in the left pane, and then click **Add Roles**. The next window is informational and warns you to be sure the Administrator account has a strong password, your network settings are configured, and the latest security updates are installed. Click **Next**.
4. In the Select Server Roles window, click **Active Directory Domain Services**, and then click **Next**.

5. Read the information in the next window, which explains that having two domain controllers is optimal, DNS must be installed on the network, and you must run Dcpromo.exe to complete the AD DS installation. Click **Next**.
6. A message is displayed stating that the server might need to restart and reminding you that Dcpromo.exe must be run after the wizard is finished. Click **Install**.
7. The Installation Results window tells you what roles were installed and displays status messages for services that were installed. Click **Close**.
8. Click **Start**, type **dcpromo** in the Start Search text box, and press **Enter**. The Active Directory Domain Services Installation Wizard starts. Click **Next**.
9. Next, you might see a window with compatibility information that explains older OSs could have difficulty authenticating to a Windows Server 2008 domain controller. If so, click **Next**.
10. Click the **Create a new domain in a new forest** option button, and then click **Next**.
11. Next, you name the forest root domain by entering the new domain's FQDN. Type **W2k8adXX.com**, and then click **Next**.
12. Next, you select the forest functional level. To take advantage of new features in Windows Server 2008, you must select the Windows Server 2008 level. Click the list arrow, click to select **Windows Server 2008**, and then click **Next**.
13. In the Additional Domain Controller Options window, you choose whether to install DNS. You can also decide whether this DC should be a global catalog server or an RODC as well. These options are disabled for the first DC in a new domain, however. Click **Next**.
14. In the message box explaining that a DNS server can't be found, click **Yes**.
15. You can choose locations for the database folder, log files, and Sysvol folder. Specifying different disks for the database and log files is ideal, but leave the defaults for now. Click **Next**.
16. When asked for a Directory Services Restore Mode password, enter **Password01** in both places. You can use a different password from the Administrator password, if you like. Click **Next**.
17. Review your choices in the next window, and go back and make changes if necessary. Otherwise, click **Next**.
18. In the next window, click **Finish**, and then click **Restart Now** when prompted.
19. After your computer restarts, log on as Administrator. Open Server Manager, if necessary, and verify the domain information that's displayed. Some new messages have been created during installation. If they are warning messages, you can ignore them for now.
20. Click **Start** and point to **Administrative Tools**. Note the new MMCs that have been added: Active Directory Domains and Trusts, Active Directory Sites and Services, Active Directory Users and Computers, ADSI Edit, and DNS.
21. Close all open windows.

Now that Active Directory is installed, you can examine the types of objects it contains.

What's Inside Active Directory?

After Active Directory is installed, you can explore it by using the Active Directory Users and Computers MMC via Administrative Tools or Server Manager. Active Directory Users and Computers is the main tool for managing Active Directory, although quite a few command-line tools are available, too. Shown in Figure 3-5, Active Directory Users and Computers has two panes. The top node in the left pane shows the server and domain being managed. The next folder, Saved Queries, contains a list of Active Directory queries you can save to repeat Active Directory searches easily. The third node represents the domain and contains all the objects that make up the domain. In Figure 3-5, the domain being managed is called W2k8ad99.com. In this figure, the Users container is open, and objects in this container are displayed in the right pane.

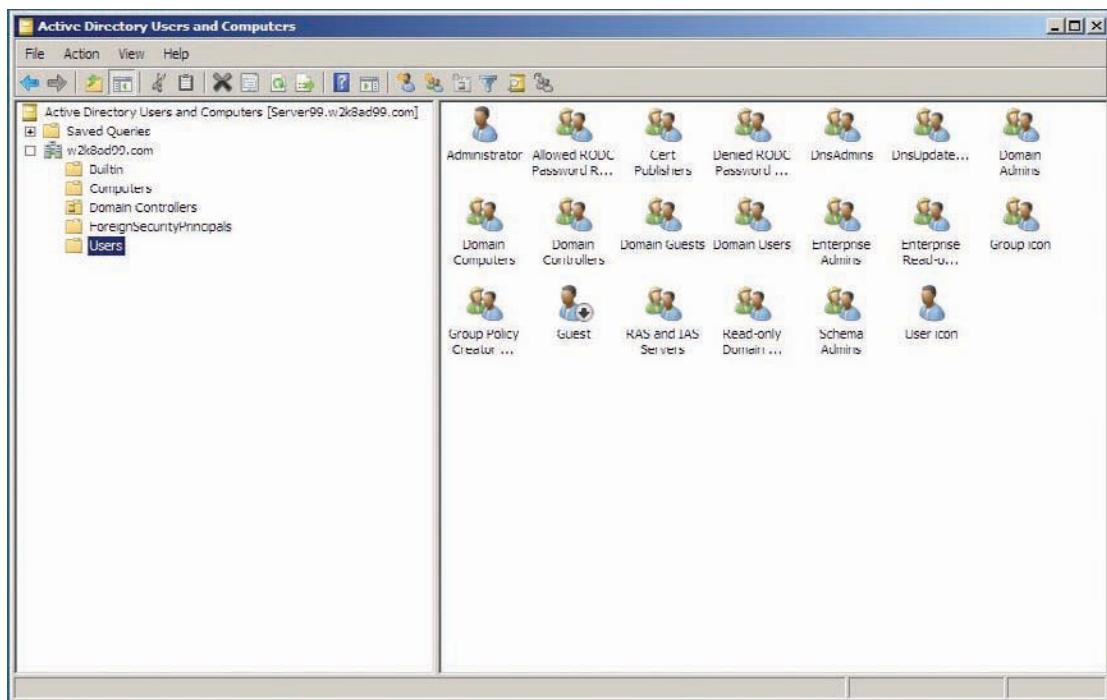


Figure 3-5 The Active Directory Users and Computers window

Before you can go too far in working with Active Directory, knowing something about the information you find in the database is helpful. Active Directory's contents and the functions it performs in your network are defined by the schema, objects, and Group Policy Objects (GPOs, discussed later in this chapter in “Introducing Group Policy”).

The Active Directory Schema

All information in the Active Directory database is organized as objects. An **object** is a grouping of information that describes a network resource, such as a shared printer, or an organizing structure, such as a domain or OU. The **schema** defines the type, organization, and structure of data stored in the Active Directory database and is shared by all domains in an Active Directory forest. The information the schema defines is divided into two categories: schema classes and schema attributes. **Schema classes** define the types of objects that can be stored in Active Directory, such as user or computer accounts. **Schema attributes** define what type of information is stored in each object, such as First name, Last name, and Password for a user account object. The information stored in each attribute, such as “Mary” in the First name attribute, is called the **attribute value**.

Figure 3-6 shows the relationship between schema classes, attributes, and Active Directory objects. As you can see, some schema attributes, such as the Description attribute used for both objects, can be shared by more than one Active Directory object. When Active Directory is first installed, a default schema describes all available default objects, but you can extend this schema to add attributes to existing object classes or create new object classes.

This discussion of Active Directory refers to several different object classes in Active Directory. Figure 3-7 shows object classes and their associated icons in Active Directory Users and Computers. Active Directory objects can be organized into two basic groups, discussed in the next sections: container objects and leaf objects.

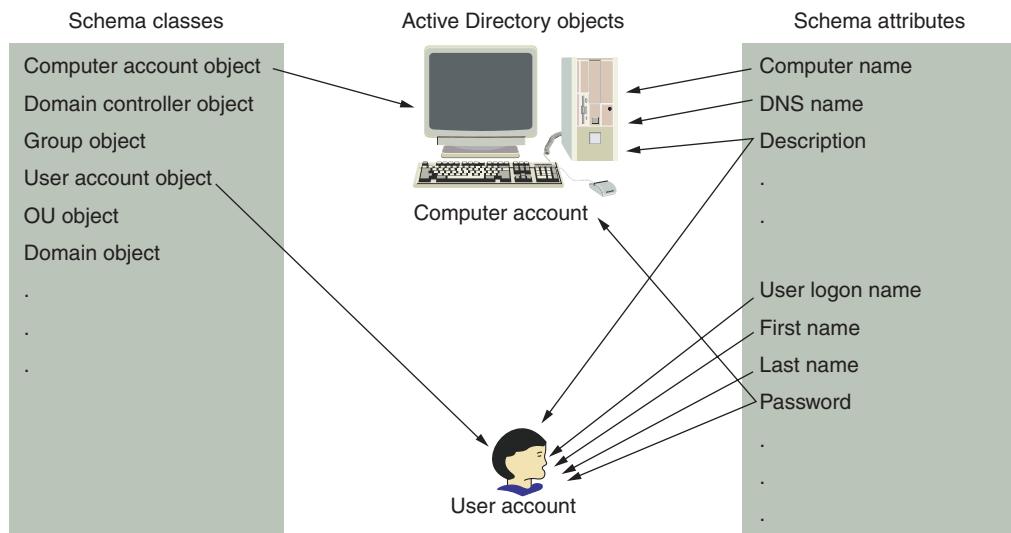


Figure 3-6 Schema classes, schema attributes, and Active Directory objects



Figure 3-7 Icons in Active Directory Users and Computers

Active Directory Container Objects

A container object, as the name implies, contains other objects. Container objects are used to organize and manage users and resources in a network. They can also act as administrative and security boundaries or a way to group objects for applying policies. Three container objects, explained in the following sections, are used in Active Directory Users and Computers: OU, folder, and domain.

Organizational Units An OU is the primary container object for organizing and managing resources in a domain. Administrators can use OUs to organize objects into logical administrative groups, which makes it possible to apply policies to the OU that affect all objects in it. For example, you could apply a policy that prohibits access to Control Panel for all users in that OU. In addition, you can delegate administrative authority for an OU to a user, thereby allowing that user to manage objects in the OU without giving the user wider authority. Object types typically found in an OU include user accounts, group accounts, computer accounts, shared folders, shared printers, published applications, and other OUs. By nesting OUs, administrators can build a hierarchical Active Directory structure that mimics the corporate structure for easier object management.

In Active Directory Users and Computers, an OU is represented by a folder with a book inside, as shown previously in Figure 3-7. When Active Directory is first installed, a single OU called Domain Controllers is created and contains a computer object representing the domain controller. When a new DC is installed in the domain, a new computer object representing it is placed in the Domain Controllers OU by default. A GPO is linked to the Domain Controllers OU and can be used to set security and administrative policies that apply to all DCs in the domain.

Folder Objects

When Active Directory is installed, four folder objects are created:

- **Builtin**—Houses default groups created by Windows and is mainly used to assign permissions to users who have administrative responsibilities in the domain
- **Computers**—The default location for computer accounts created when a new computer or server becomes a domain member
- **ForeignSecurityPrincipals**—Initially empty but later contains user accounts from other domains added as members of the local domain's groups
- **Users**—Stores two default users (Administrator and Guest) and several default groups



These folder objects are represented in Active Directory Users and Computers with a folder icon, but unlike an OU, a folder object's icon doesn't include the book icon. You can't create new folder objects, nor can you apply group policies to folder objects. You can delegate administrative control on all but the Builtin folder. All objects in a folder are subject to group policies defined at the domain level. You can move objects from the default folders (except the Builtin folder) into OUs you have created. For example, because all computer accounts are created in the Computers folder by default, they are subject to the same policies defined at the domain level. If you want to apply different policies to different computers in your domain, you create one or more OUs, move the computer accounts to the new OUs, and apply group policies to these OUs.

Domain Objects The domain is the core logical structure container in Active Directory. Domains contain OU and folder container objects but can also contain leaf objects, such as users, groups, and so forth. A domain typically reflects the organization of the company in which Active Directory is being used, but in large or geographically dispersed organizations, you can create multiple domains, each representing a business unit or location. The main reasons for using multiple domains are to allow separate administration, define security boundaries, and define policy boundaries. Each domain object has a default GPO linked to it that can affect all objects in the domain. The domain object in Active Directory Users and Computers is represented by an icon with three tower computers (refer back to Figure 3-7).



Activity 3-2: Exploring Active Directory Container Objects

Time Required: 10 minutes

Objective: Explore Active Directory container objects.

Description: After installing Active Directory, you want to view its structure by exploring the default container objects in Active Directory Users and Computers.

1. Log on to the server where you just installed Active Directory as Administrator.
2. Open Active Directory Users and Computers by clicking **Start**, pointing to **Administrative Tools**, and clicking **Active Directory Users and Computers**.
3. Click the domain object in the left pane (w2k8ad99.com in Figure 3-5).
4. If necessary, click **View**, **Detail** from the menu so that objects are displayed in the right pane with their name, type, and description.
5. Right-click the domain object and click **Properties**. Click the **General** tab, if necessary, and verify that both the domain functional level and forest functional level are Windows Server 2008.
6. Enter a description for your domain, such as Windows Server 2008 Domain XX, and then click **OK**.
7. Click to expand the domain node, if necessary. Click the **Builtin** folder in the left pane to view its contents in the right pane: a list of group accounts created when Active Directory was installed.
8. Click the **Computers** folder in the left pane. This folder should be empty.

9. Click the **Domain Controllers** OU in the left pane. A computer object representing your domain controller is displayed in the right pane.
10. Right-click the **Domain Controllers** OU and click **Properties**. If you have worked with Active Directory Users and Computers in Windows Server 2003, you might notice that the Group Policy tab is missing. In Windows Server 2008, all group policy management is done with the Group Policy Management MMC. Click **Cancel**.
11. Click the **Users** folder in the left pane. The right pane displays a list of groups and two user accounts created by default when Active Directory is installed.
12. Leave Active Directory Users and Computers open for the next activity.

Active Directory Leaf Objects

A leaf object doesn't contain other objects and usually represents a security account, network resource, or GPO. Security account objects include users, groups, and computers. Network resource objects include servers, domain controllers, file shares, printers, and so forth. GPOs aren't viewed as objects in the same way as other Active Directory objects. In Windows Server 2008, GPOs are managed by the Group Policy Management MMC, discussed later. The following paragraphs explain some common leaf objects in Active Directory.

User Accounts A user account object contains information about a network user. Typically, when a user account is created, the administrator enters at least the user's name, logon name, and password. However, the user account object contains much more information, such as group memberships, account restrictions (allowed logon hours and account expiration date, for example), profile path, and dial-in permissions. In addition, administrators can fill in descriptive fields, such as office location, job title, and department. The main purpose of a user account is to allow a user to log on to a Windows computer or an Active Directory domain to access computer and domain resources. By supplying a user logon name and password, a user is authenticated on the computer or network. **Authentication** confirms a user's identity, and the account is then assigned permissions and rights that authorize the user to access resources and perform certain tasks on the computer or domain.

Windows Server 2008 defines three user account types: local user accounts, domain user accounts, and built-in user accounts. A **local user account** is defined on a local computer and is authorized to access resources only on that specific computer. Local user accounts are mainly used on stand-alone computers or in a workgroup network with computers that aren't part of an Active Directory domain. A **domain user account** is created in Active Directory and provides a single logon for users to access all resources in the domain for which they have been authorized. Windows creates two **built-in user accounts** automatically: Administrator and Guest. They can be local user accounts or domain user accounts, depending on the computer where they're created. On a workgroup or stand-alone Windows computer, these two accounts are created when Windows is installed, and they are local accounts that have access to resources only on the local computer. When Active Directory is installed on a Windows Server 2008 computer, these two accounts are converted from local user accounts to domain user accounts. User accounts are discussed in more detail in Chapter 5.

Groups A group object represents a collection of users with common permissions or rights requirements on a computer or domain. **Permissions** define which resources users can access and what level of access they have to resources. For example, a user might have permission to open and read a certain document but not to change it. A **right** specifies what types of actions a user can perform on a computer or network. For example, a user might have the right to log on to and log off a computer but not shut down the computer. Groups are used to assign members permissions and rights. This method is more efficient than assigning permissions and rights to each user account separately because you have to perform the assignment task only once. For example, if all users in the Accounting Department need access to a shared folder, you can create a group containing all users in this department as members and assign permission to access the shared folder to the group as a whole. In addition, if a user leaves the department, you can remove his

or her account as a group member, and the user loses all rights and permissions assigned to that group. Groups are explained in more detail in Chapter 5.

Computer Accounts A computer account object represents a computer that's a domain controller or domain member and is used to identify, authenticate, and manage computers in the domain. Computer accounts are created automatically when Active Directory is installed on a server or when a server or workstation becomes a domain member. Administrators can also create computer accounts manually if automatic account creation is undesirable. By default, domain controller computer accounts are placed in the Domain Controllers OU, and domain member computer accounts are placed in the Computers folder.

The computer account object's name must match the name of the computer that the account represents. Like user accounts, computer accounts have a logon name and password, but a computer account password is managed by Active Directory instead of an administrator. A computer must have a computer account in Active Directory for users to log on to that computer with their domain user accounts. You learn about managing computer accounts in Chapter 5.

Other Leaf Objects The following list describes other leaf objects that are commonly created in Active Directory:

- *Contact*—A person who is associated with the company but is not a network user. You can think of a contact object as simply being an entry in an address book, used purely for informational purposes.
- *Printer*—Represents a shared printer in the domain. Printers shared on Windows 2000 or later computers that are domain members can be added to Active Directory automatically. If a printer is shared on a non-domain member or a pre-Windows 2000 computer, you must create the printer object manually and specify the path to the shared printer.
- *Shared folder*—Represents a shared folder on a computer in the network. Shared folder objects can be added to Active Directory manually or by using the publish option when creating a shared folder with the Shared Folders MMC snap-in.

Both printer and shared folder objects enable users to access shared printers and folders on any computer in the domain without knowing exactly which computer the resource was created on. Users can simply do a search in Active Directory to find the type of resource they want. In a large network, shared printers and folders could be located on any one of dozens or hundreds of servers. Publishing these resources in Active Directory makes access to them easier.



There are other leaf objects, but the previous sections cover the most common objects you find in Active Directory.

NOTE



Activity 3-3: Viewing Default Leaf Objects

Time Required: 15 minutes

Objective: View the properties of a variety of leaf objects.

Description: You want to learn more about Active Directory objects, so you view the properties of several default leaf objects.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Click to expand the domain node so that folders and OUs are displayed under it, and then click the **Builtin** folder.
3. In the right pane, right-click the **Administrators** group and click **Properties** (or double-click the **Administrators** group).

4. Click the **General** tab, if necessary. Note that the option buttons under Group scope and Group type are disabled because you can't change this information for built-in groups. (You learn more about group scope and group type in Chapter 5.)
5. Click the **Members** tab. You should see one user and two groups listed as members (see Figure 3-8). The Name column displays the name of the user or group member, and the Active Directory Domain Services Folder column displays the domain and folder or OU where the member is located. Note that groups can be nested, as shown here; the Domain Admins and Enterprise Admins groups are members of the Administrators group.

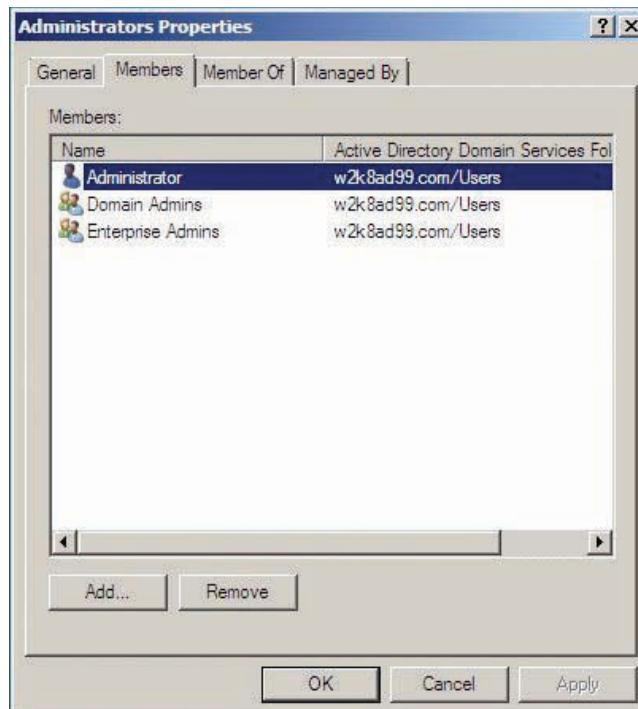


Figure 3-8 Viewing properties of the Administrators group

6. Click the **Member Of** tab. Because built-in groups can't be members of any other group, the Add and Remove buttons are disabled.
7. Click the **Managed By** tab. An administrator can specify another user or group that has the right to manage this group. Click **OK**.
8. In the left pane of Active Directory Users and Computers, click the **Domain Controllers** OU. Double-click the **ServerXX** computer object in the right pane to open its Properties dialog box.
9. If necessary, click the **General** tab. Note that only the Description text box can be changed for this object.
10. Click the **Operating System** tab, which displays the name, version, and service pack (if any) installed on the computer that this computer object represents.
11. Click the **Member Of** tab. Because this computer object represents a domain controller, it's a member of the Domain Controllers group. (If this computer object represents a domain member, it's a member of the Domain Computers group.) Click **OK**.
12. In the left pane of Active Directory Users and Computers, click the **Users** folder. Double-click the **Administrator** user to open its Properties dialog box.

13. If necessary, click the **General** tab. The information here is optional for user accounts but can be used as part of an employee directory. Enter your first name and last name in the corresponding text boxes.
14. Click the **Account** tab, where you can specify the user logon name, logon restrictions, and account options.
15. Click the **Member Of** tab. Note the groups the Administrator account belongs to, and then click **OK**.
16. Find the Guest user, and notice the down arrow on its icon. Double-click the **Guest** user to open its Properties dialog box.
17. Click the **Account** tab. In the Account options list box, scroll down to view the options that can be selected. Which option is responsible for the down arrow on the Guest user icon? The Guest user is disabled by default because it's created with a blank password, which can pose a security risk. Click **OK**.
18. Leave Active Directory Users and Computers open for the next activity.



Activity 3-4: Creating New Objects in Active Directory

Time Required: 15 minutes

Objective: Create a new OU and add some objects to it.

Description: You want to learn more about Active Directory objects, so you create an OU and add a user object and a group object.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Click to expand the domain node so that folders and OUs are displayed under it.
3. Right-click the domain node, point to **New**, and click **Organizational Unit**. In the Name text box, type **TestOU**. Click to clear the **Protect container from accidental deletion** check box, and then click **OK**.
4. Make sure **TestOU** is selected in the left pane, and then right-click in the right pane, point to **New**, and click **User**.
5. In the First name text box, type **Test**, and in the Last name text box, type **User1**. Notice that the Full name text box is filled in automatically.
6. In the User logon name text box, type **testuser1**. The User logon name (pre-Windows 2000) text box is filled in automatically. (A user logon name longer than 20 characters is truncated to 20 characters in this text box.)
7. Click **Next**. In the Password text box, type **mypassword**, and type it again in the Confirm password text box. Note that the User must change password at next logon check box is selected by default. Click **Next**, and then click **Finish**.
8. If you get an error message, read it carefully. By default, Windows Server 2008 requires a complex password, meaning the password must be of a minimum length and have at least three characters of the following types: uppercase letters, lowercase letters, numbers, and special characters. Click **OK**.
9. Click **Back**. In the Password text box, type **Password01**, making sure the P is capitalized and the last two characters are 0 and 1. Retype the password in the Confirm password text box. Click **Next**, and then click **Finish**.
10. Right-click in the right pane of Active Directory Users and Computers, point to **New**, and click **Group**.
11. Type **TestGroupG** in the Group name text box (see Figure 3-9). Verify that the Group scope setting is **Global** and the Group type setting is **Security**, and then click **OK**.

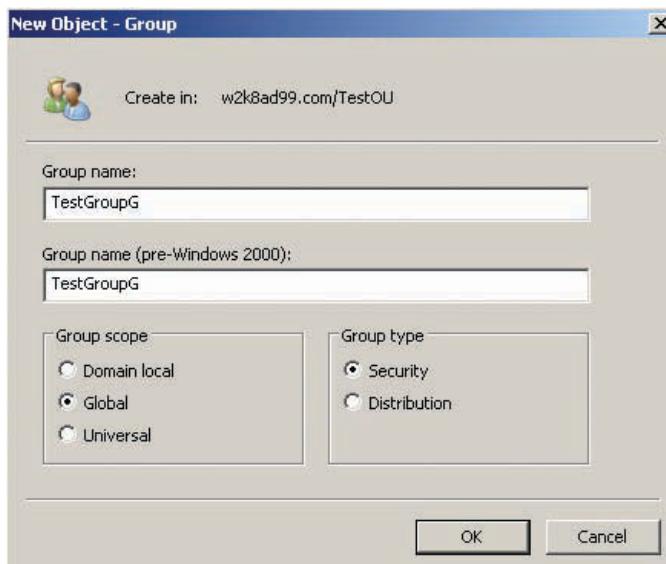


Figure 3-9 Creating a new group

12. Double-click **Test User1** to open its Properties dialog box.
13. Click the **Member Of** tab. This user account is already a member of the Domain Users group; all new users are members of this group by default.
14. Click the **Add** button to open the Select Groups dialog box. In the Enter the object names to select text box, type **TestGroupG**, as shown in Figure 3-10, and then click the **Check Names** button. Active Directory verifies that the group name you entered exists and underlines it if it does. If the group doesn't exist, a Name Not Found message box is displayed, where you can correct the group name. Click **OK**, and then click **OK** again.

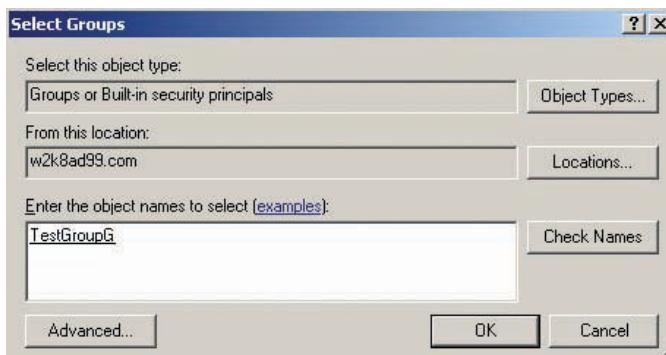


Figure 3-10 The Select Groups dialog box

15. Double-click **TestGroupG** to open its Properties dialog box. Click the **Members** tab to verify that Test User1 has been added as a member. Users can be added to groups in the Member Of tab of the user account's Properties dialog box or the Members tab of the group's Properties dialog box. Click **OK**.
16. Close Active Directory Users and Computers.

As you can tell, Active Directory Users and Computers is a fairly straightforward, easy-to-use tool for managing Active Directory objects, but not every administrator wants to use a graphical utility to create and modify Active Directory objects. Sometimes using command-line tools is easier or even necessary. Although this topic is explored more thoroughly in Chapters 5 and 13, the following activity introduces you to the DSADD command-line tool used to create new objects in Active Directory.

3



Activity 3-5: Using DSADD to Create New Objects

Time Required: 10 minutes

Objective: Create a new user with the DSADD command-line tool.

Description: You want to get more practice creating Active Directory objects, so you decide to create a test user by using the DSADD command-line tool and add that user to the group you created earlier.

1. Log on to your server as Administrator, if necessary, and open a command prompt window by clicking **Start**, **Command Prompt**.
2. At the command prompt, type `dsadd user "cn=Test User2, ou=TestOU, dc=W2k8adXX, dc=com" -upn testuser2@w2k8adXX -Samid testuser2 -fn Test -ln User2 -pwd Password01 -memberof "cn=TestGroupG, ou=TestOU, dc=W2k8adXX, dc=com"` (replacing XX with your student number) and press **Enter**. If you get any response other than “dsadd succeeded: cn=Test User2,ou=TestOU,dc=W2k8adXX,dc=com,” check the command for typos and try again.
3. This complex command creates a user named Test User2 with a logon name of testuser2 and a password of Password01, places the user in TestOU, and makes the user a member of TestGroupG. Close the command prompt window.
4. Open Active Directory Users and Computers, and click **TestOU** in the left pane.
5. Verify that Test User2 is there. Double-click **TestGroupG** to open its Properties dialog box, and then click the **Members** tab to verify that this new user is a member. Click **OK**.
6. Leave Active Directory Users and Computers open for the next activity.

These steps might seem like a lot of work to create a single user, but as you learn in Chapter 5, you can create several users at once quickly and easily with command-line tools and a text file. Microsoft has placed an increased emphasis on command-line tools, especially with Server Core and the new PowerShell suite of tools. You explore many of the command-line tools for server management in Chapter 13.

Locating Active Directory Objects

In a large Active Directory environment with hundreds or thousands of users, groups, computers, and other domain objects, locating objects can be difficult for administrators and users alike. Luckily, Active Directory Users and Computers has a search function for administrators, and Windows Explorer incorporates an Active Directory search function for users.

You search for Active Directory objects by first selecting the type of object you’re searching for. For example, you can search for users, contacts, groups, computers, printers, shared folders, and so forth. In a multidomain environment, you can search in a single domain or in the entire directory (all domains). You can also limit your search to a folder or an OU in a domain. The Find dialog box shown in Figure 3-11 is identical whether you’re searching for objects with Active Directory Users and Computers or Windows Explorer. However, not all objects are available to all users, depending on the object’s security settings and its container.



Figure 3-11 The Find Users, Contacts, and Groups dialog box



Activity 3-6: Locating Objects with Active Directory Users and Computers

Time Required: 10 minutes

Objective: Search for user and group objects by using Active Directory Users and Computers.

Description: Before Active Directory grows too large, you need to experiment with the search feature in Active Directory Users and Computers so that you're comfortable finding objects.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Right-click the domain node in the left pane and click **Find**.
3. Click the **Find** list arrow and verify that **Users, Contacts, and Groups** is selected. In the **In** text box, make sure the domain is selected. You could click **Find Now**, but if you do, all users, contacts, and groups in the entire domain are displayed. You want to narrow down the choices first.
4. In the **Name** text box, type **test**. By specifying this name, all users, groups and contacts starting with “test” are displayed. Click the **Find Now** button. You should see results similar to Figure 3-12.

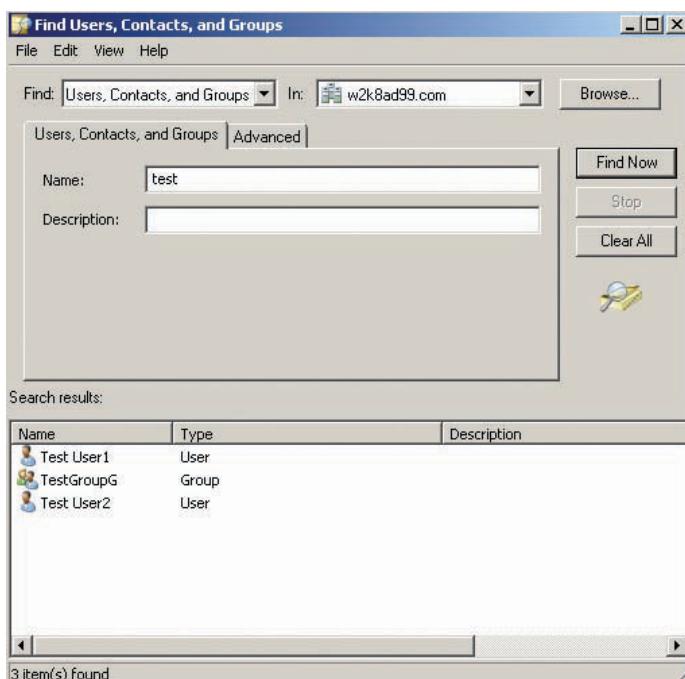


Figure 3-12 Results from an Active Directory find operation

5. In the Search results section, you can double-click any entry to access its properties. Close the Find dialog box and Active Directory Users and Computers.



Activity 3-7: Locating Objects with Windows Explorer

Time Required: 10 minutes

Objective: Search for user and group objects by using Windows Explorer.

Description: Part of your job as network administrator is assisting users in using Active Directory, so you want to familiarize yourself with the Active Directory search tool in Windows Explorer.



These instructions work in both Windows Server 2008 and Windows Vista. In Windows XP, the instructions differ slightly.

NOTE

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, **Network**. You should get a Windows Explorer window similar to Figure 3-13.

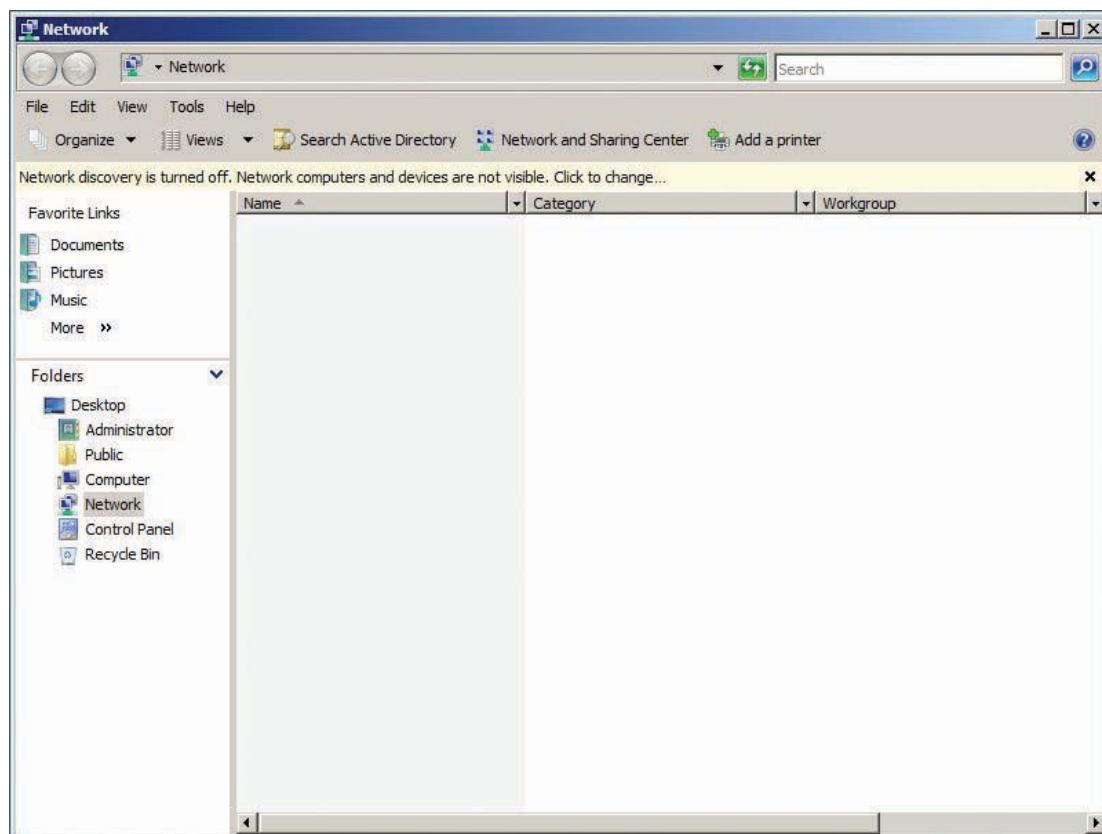


Figure 3-13 The Network window

3. Click the **Search Active Directory** toolbar icon. The resulting Find dialog box is identical to the one in Activity 3-6.
4. In the Find drop-down list, click **Computers**.
5. In the Role drop-down list that's displayed, click **All Active Directory Domain Controllers**.
6. Click the **Find Now** button.
7. Your server name should be returned in the results. Close all open windows.



Activity 3-8: Publishing a Shared Folder in Active Directory

Time Required: 25 minutes

Objective: Publish a shared folder in Active Directory and then find the folder.

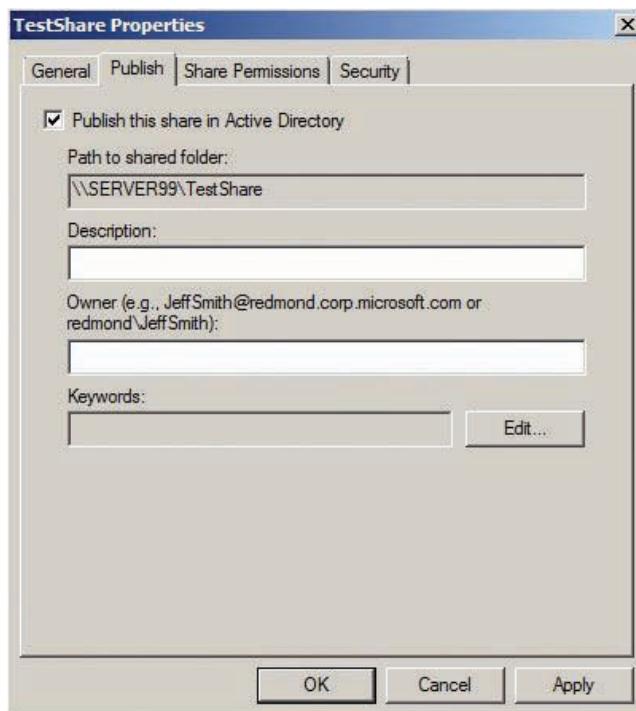
Description: You have heard that users can access shared folders by locating them in Active Directory. You decide to create a shared folder and then publish it in Active Directory. Then you use the find feature in Windows Explorer to locate the shared folder in Active Directory.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, **Computer**. Double-click the C drive to open a Windows Explorer window.
3. Create a folder in the root of the C drive by right-clicking an empty space in the right pane, pointing to **New**, and clicking **Folder**. Type **TestShare** for the name of the new folder, and then press **Enter**.
4. Make sure the folder you just created is selected, and then click the **Share** toolbar icon to start the File Sharing Wizard (see Figure 3-14).



Figure 3-14 The File Sharing Wizard

5. Click the list arrow at the top, and then click **Everyone**. Click the **Add** button to share the folder with all users and grant Read permission for the folder's contents.
6. Click the **Share** button, and then click **Done**.
7. Click **Start**, point to **Administrative Tools**, and click **Computer Management**.
8. Click to expand the **Shared Folders** node, and then click the **Shares** folder.
9. In the right pane, double-click **TestShare** to open its Properties dialog box.
10. Click the **Publish** tab (see Figure 3-15), and then click the **Publish this share in Active Directory** check box.



3

Figure 3-15 The Publish tab of a shared folder's Properties dialog box

11. In the Description text box, type **A share to test publishing in Active Directory**.
12. Click the **Edit** button. In the Edit Keywords dialog box, type **Testing**, and then click **Add**. Click **OK** twice.
13. Close all open windows. Click **Start, Network**.
14. Click the **Search Active Directory** toolbar icon.
15. In the Find drop-down list, click **Shared Folders**.
16. In the Keywords text box, type **test**, and then click **Find Now**.
17. In the Search results section, right-click **TestShare** and click **Explore**. A Windows Explorer window opens, showing the contents of the TestShare shared folder (currently empty).
18. Close all open windows.
19. Open Active Directory Users and Computers.
20. When you publish a shared folder by using Computer Management, the published share appears as a child object of the server on which the share is located. To view child objects of servers, click **View, Users, Contacts, Groups, and Computers as containers** from the menu.
21. Click to expand the **Domain Controllers** OU, and then click the server icon. You should see the share you published in the right pane (see Figure 3-16).

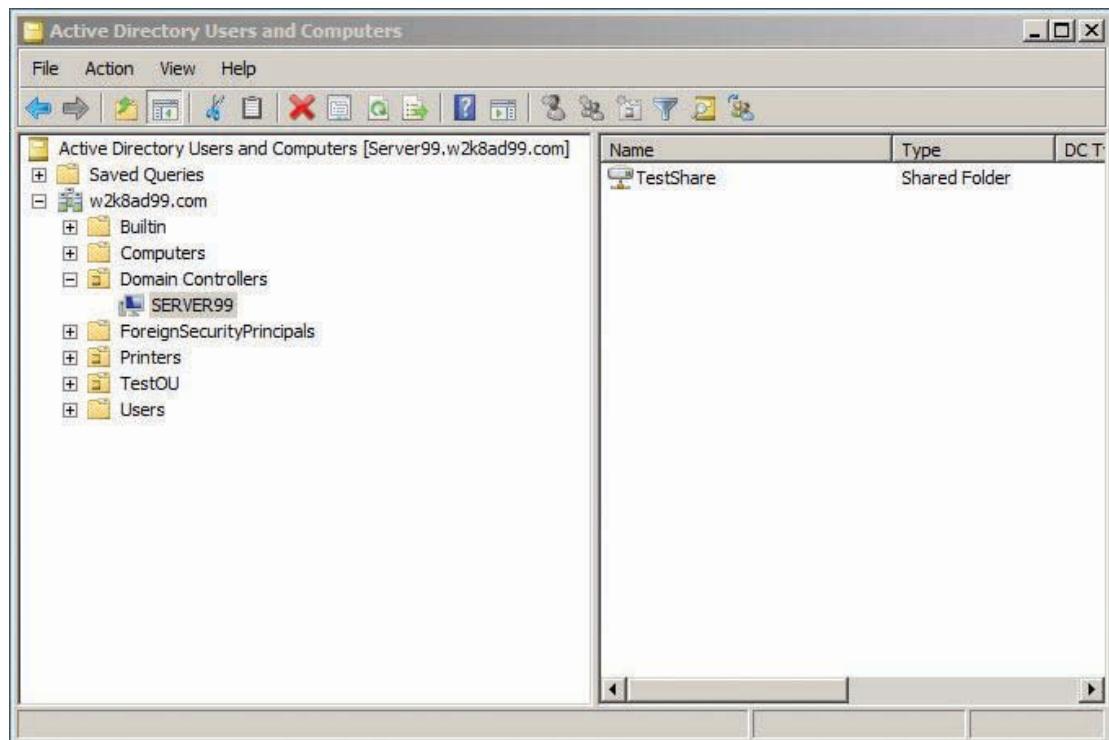


Figure 3-16 A published share in Active Directory Users and Computers

22. Click **View, Users, Contacts, Groups, and Computers as containers** from the menu again to disable this feature, and then close Active Directory Users and Computers.

The last of the Active Directory objects that you explore in this chapter is the GPO, discussed in the following section.

Introducing Group Policies

A **Group Policy Object (GPO)** is a list of settings that administrators use to configure user and computer operating environments remotely. Group policies can specify security settings, deploy software, and configure a user's desktop, among many other computer and network settings. They can be configured to affect an entire domain, a site, and, most commonly, users or computers in an OU. The objects a GPO affects are said to be within that GPO's scope.

Despite the name, GPOs don't apply to group objects. You can link GPOs to sites, domains, and OUs, and GPOs linked to these containers affect only user or computer accounts in the containers. When Active Directory is installed, two GPOs are created and linked to two containers:

- *Default Domain Policy*—This GPO is linked to the domain object and specifies default settings that affect all users and computers in the domain. The settings in this policy are related mainly to account policies, such as password and logon requirements, and some network security policies.
- *Default Domain Controllers Policy*—This GPO is linked to the Domain Controllers OU and specifies default policy settings for all domain controllers in the domain (provided the computer objects representing domain controllers aren't moved from the Domain Controllers OU). The settings in this policy pertain mainly to user rights assignments, which specify the types of actions users can perform on a domain controller.

These default policies don't define any user-specific policies; rather, they are designed to provide default security settings for all computers, including domain controllers, in the domain. You

can view and edit default GPOs as well as create and manage GPOs by using the Group Policy Management MMC, shown in Figure 3-17.

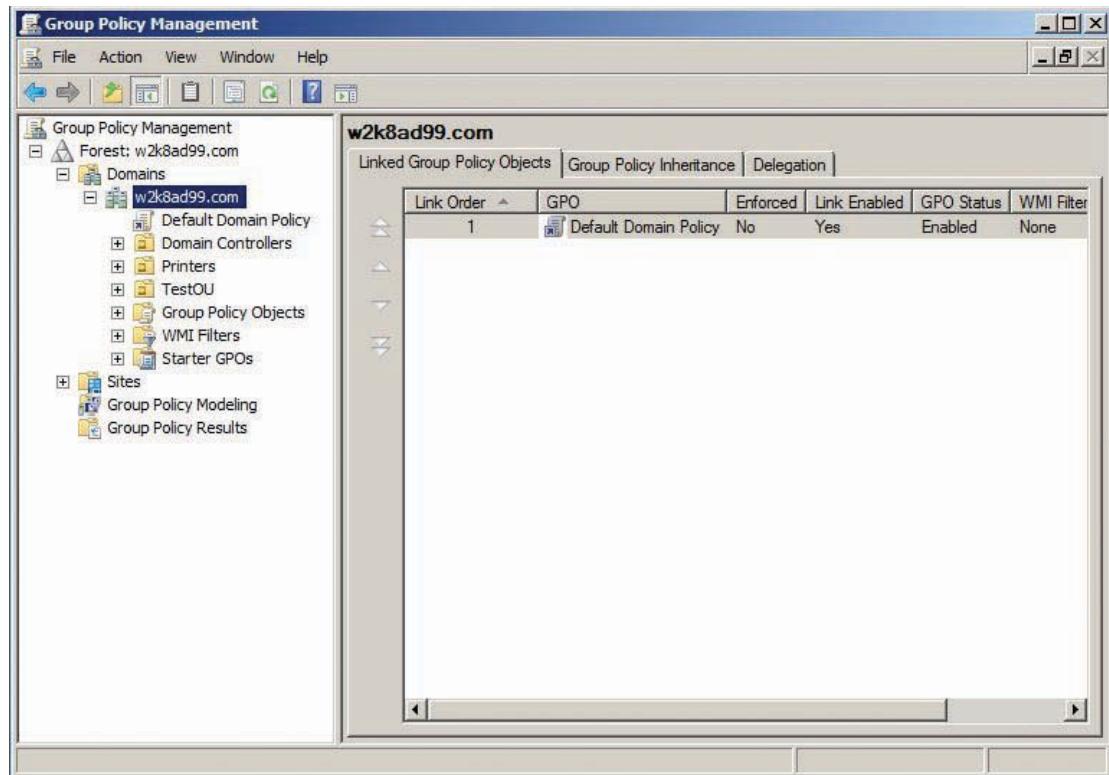


Figure 3-17 The Group Policy Management MMC

In the Group Policy Management MMC, there are two nodes for every GPO:

- *Computer Configuration*—Used to set policies that apply to computers within the GPO’s scope. These policies are applied to a computer when the computer starts.
- *User Configuration*—Used to set policies that apply to all users within the GPO’s scope. User policies are applied when a user logs on to any computer in the domain.

Each node contains a Policies folder and a Preferences folder. Settings configured in the Policies folder are applied to users or computers and can’t be overridden by users. Settings in the Preferences folder are applied to users or computers but are just that: preferences. Therefore, users can change settings configured in the Preferences folder. The idea of group policy preferences is a new feature in Windows Server 2008. To use this feature, you must install the Group Policy Preference Client Side Extensions (GPP CSE) package on computers in the domain. You can download the GPP CSE package from the Microsoft Web site.

The Policies folder under both the Computer Configuration and User Configuration nodes contains three folders: Software Settings, Windows Settings, and Administrative Templates. They can store different information, depending on whether they’re under Computer Configuration or User Configuration.

The Computer Configuration Node

In the Computer Configuration node, the three folders under the Policies folder contain the following information:

- *Software Settings*—This folder contains an item (an extension) called Software Installation, which enables administrators to install and manage applications remotely. Application

installation packages can be configured so that the next time a computer in the GPO’s scope starts, the application is installed automatically. This feature is called “assigning” the application to the computer.

- *Windows Settings*—This folder contains the Scripts extension, the Security Settings node, and the Policy-based QoS node. Administrators can use the Scripts extension to create scripts that run at computer startup or shutdown. The Security Settings node contains the lion’s share of policies that affect computer security, including account policies, user rights, Registry and file system permissions, and network communication policies. The Policy-based QoS node, new in Windows Server 2008, can be used to prioritize and control outgoing network traffic from a computer.
- *Administrative Templates*—This folder contains Control Panel, Network, Printers, System, and Windows Components folders. The settings in these folders affect computer settings that apply to all logged-on users. For example, the Network folder contains settings for configuring Windows Firewall, and Windows Components contains settings for configuring Windows Update. You can control hundreds of computer settings with the Administrative Templates folder.

Remember that policies configured in the Computer Configuration node affect all computers in the container to which the GPO is linked. So a policy set in the Computer Configuration node of a GPO linked to the domain object affects all computers in the domain, including all computers in the Domain Controllers OU and the Computers folder.

The User Configuration Node

In the User Configuration node, the Policies folder contains the same three folders as in the Computer Configuration node. However, the policies defined here affect domain users within the GPO’s scope, regardless of which computer the user logs on to. The following list describes other differences from folders under the Computer Configuration node:

- *Software Settings*—This folder also contains the Software Installation extension. However, application packages configured here can be assigned or published. An assigned application is made available as an icon on the Start menu the next time a user affected by the policy logs on to a computer in the domain. The first time the user tries to run the application or open a document associated with it, the application is installed. A published application is made available for a user to install by using Programs and Features in Control Panel.
- *Windows Settings*—This folder contains six items: the Remote Installation Services extension, the Scripts extension, the Security Settings node, the Folder Redirection node, the Policy-based QoS node, and the Internet Explorer Maintenance node. The Scripts extension enables administrators to create scripts that run at user logon and logoff. The Security Settings node contains policies for configuring certificates and controlling what software users can run. Administrators can use the Folder Redirection node to redirect users’ personal folders to a network share. The Policy-based QoS node provides the same functions as in the Computer Configuration node, except the policy is applied to a computer when a user affected by the policy logs on to the computer. With the Internet Explorer Maintenance node, administrators can control aspects of Internet Explorer, such as security settings, the home page, and the Favorites folder.
- *Administrative Templates*—This folder contains a host of settings that enable administrators to tightly control users’ computer and network environments. For example, Control Panel can be completely hidden from a user, specific Control Panel items can be made available, or items on a user’s desktop and Start menu can be hidden or disabled.

Group Policy is a powerful tool, but with that power comes complexity. This chapter serves as an introduction to group policies, and you learn more about working with their complexities in Chapter 7. For now, take the time to explore the default GPOs in Active Directory in the following activity.



Activity 3-9: Exploring Default GPOs

Time Required: 30 minutes

Objective: Explore the two default GPOs in Active Directory.

Description: You want to begin using GPOs to manage users and computers in your network, so as a first step, you decide to familiarize yourself with the default GPOs linked to the domain and the Domain Controllers OU.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Group Policy Management**.
3. In the left pane, click to expand the **Forest** and **Domains** nodes, if necessary.
4. Click to expand your domain name under the Domains node, if necessary. You should see a window similar to Figure 3-17, shown previously.
5. Click **Default Domain Policy**. If a Group Policy Management Console message appears, read the message, click the **Do not show this message again** check box, and then click **OK**.
6. In the right pane, click the **Scope** tab, if necessary (see Figure 3-18). The Links section shows you which container objects are linked to this GPO. In this case, your domain should be the only container linked. All objects in a container linked to the GPO are affected by that GPO.

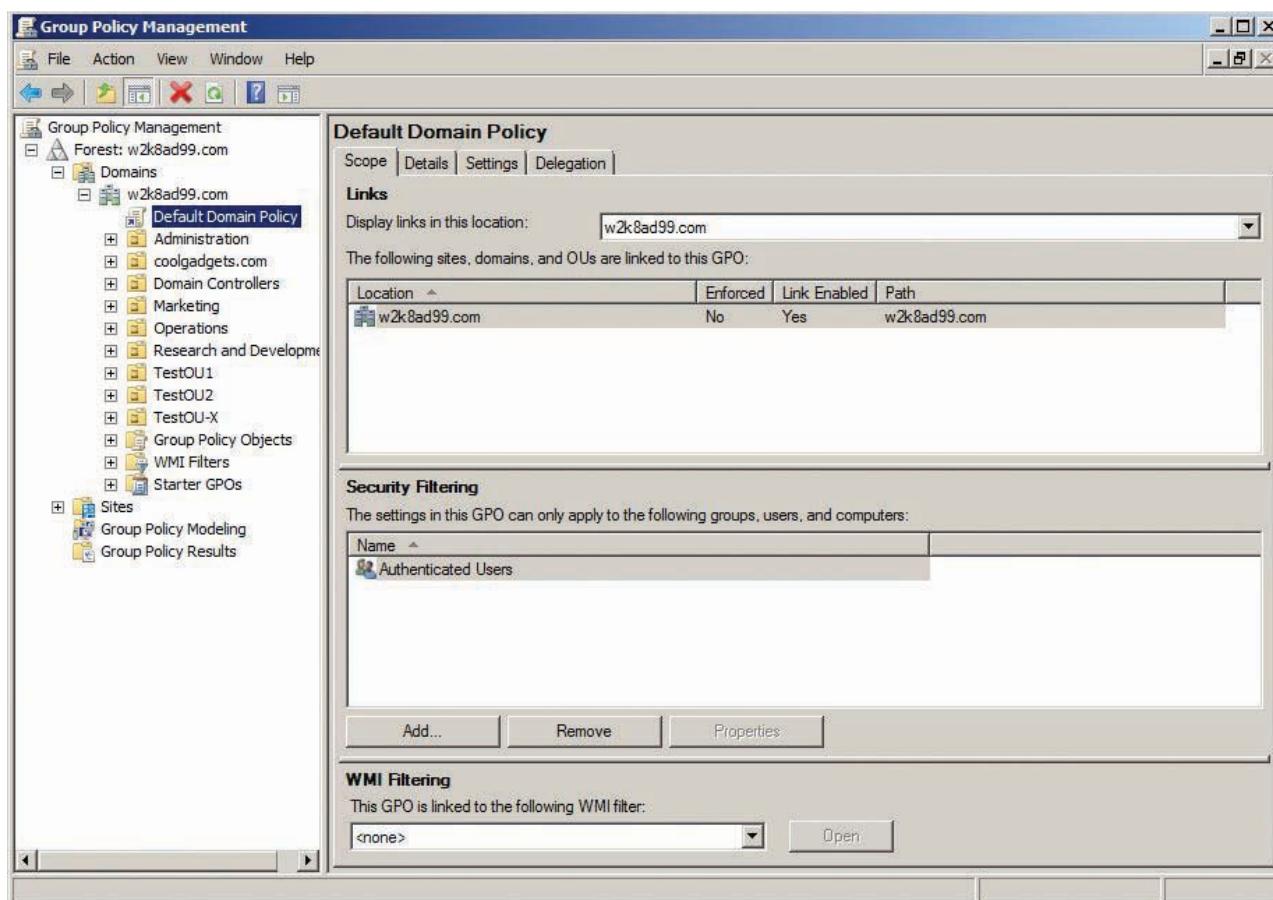


Figure 3-18 The Scope tab

7. Click the **Settings** tab, shown in Figure 3-19. (The settings might take a few seconds to be displayed.) You can view GPO settings here, but you can't change them.

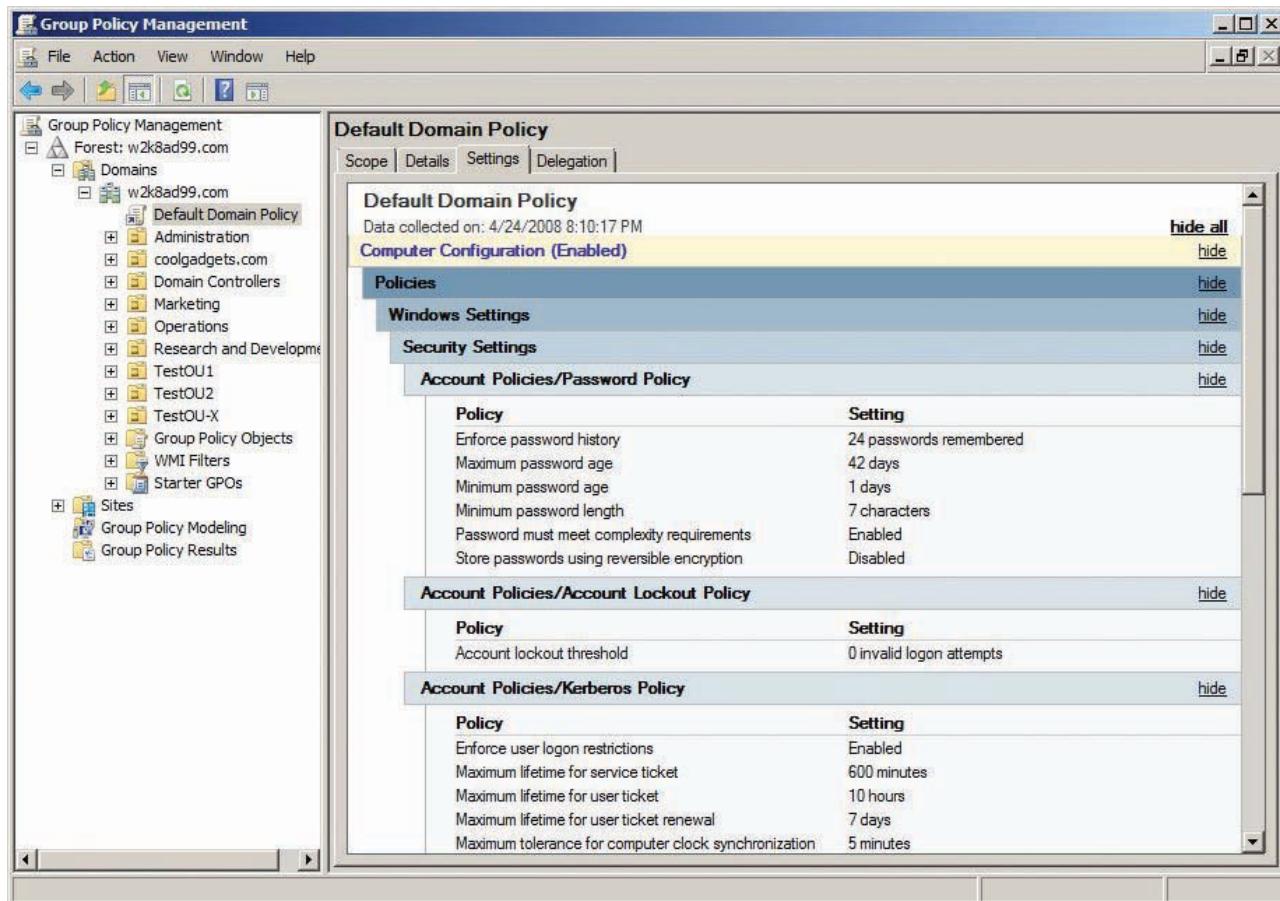


Figure 3-19 The Settings tab

8. Two primary nodes are highlighted: Computer Configuration and User Configuration. Click the **show all** link to expand the settings.
9. Scroll through the settings for the Default Domain Policy, which pertain to user account settings, such as password policies, or security. Note that no settings are displayed under the User Configuration node.
10. Click to expand **Domain Controllers** in the left pane, and then click **Default Domain Controllers Policy**.
11. In the right pane, click the **Settings** tab, if necessary, and then click **show all**.
12. Scroll through the settings for the Default Domain Controllers Policy. Most pertain to user rights assignments, such as which users are allowed to log on to the computer locally or change the system time.
13. Right-click **Default Domain Policy** in the left pane and click **Edit**. The Group Policy Management Editor opens (see Figure 3-20).

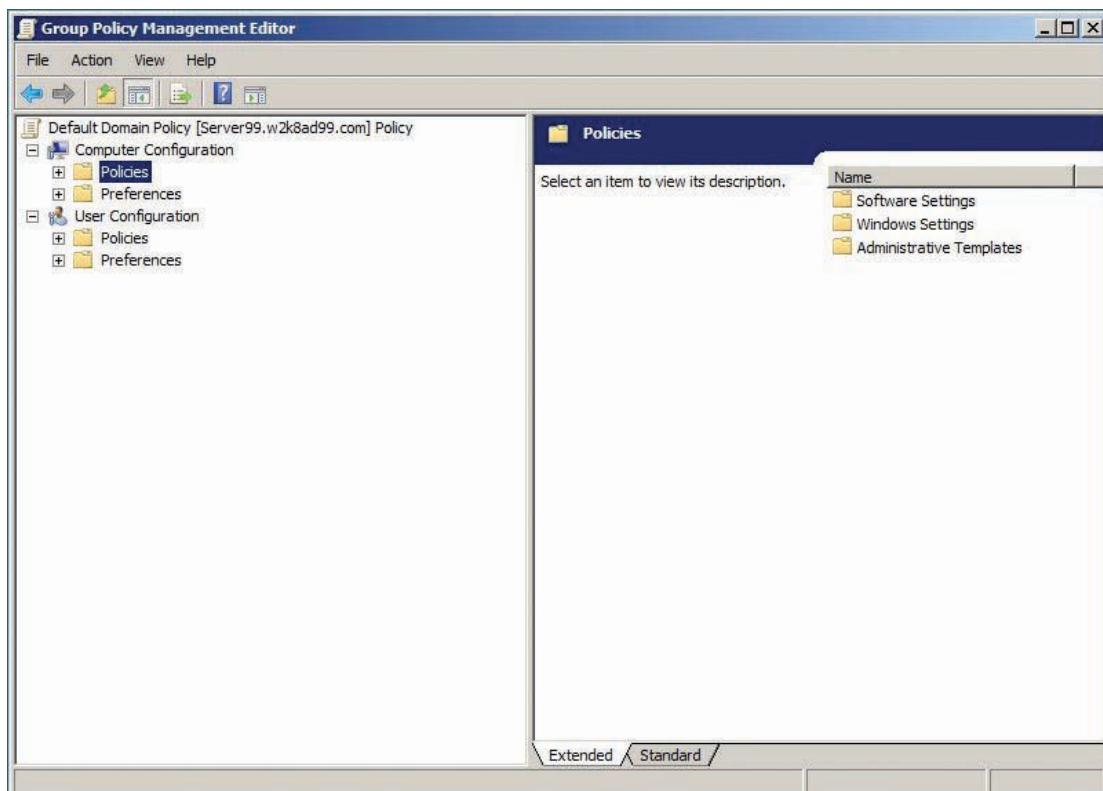


Figure 3-20 The Group Policy Management Editor

14. If necessary, click to expand **Computer Configuration** and **User Configuration**.
15. Under Computer Configuration, click to expand the **Policies** folder.
16. Click to expand **Windows Settings** and then **Security Settings**.
17. Click to expand the **Account Policies** node, and explore the settings in this node and the nodes under it. By default, account policies are defined only in the Default Domain Policy, and all domain users are subject to these settings.
18. Click to expand the **Local Policies** node, and explore the three nodes under it. Most settings in Local Policies are displayed as Not Defined. In fact, only three policies in the Local Policies node are defined. Can you find them?
19. Browse through nodes in the Policies folder under User Configuration. No policies are configured in this node.
20. Close the Group Policy Management Editor. In the Group Policy Management MMC, click to expand **Domain Controllers** if necessary, and then right-click **Default Domain Controllers Policy** and click **Edit**.
21. Under the Computer Configuration node, click to expand the **Policies** folder if necessary, and then click to expand **Windows Settings** and then **Security Settings**. Click to expand **Account Policies** and **Local Policies**, and explore the settings in these nodes. Notice that no account policies are defined but a number of user rights assignments are.
22. Take some time to explore several GPOs to familiarize yourself with what's available. Leave the Group Policy Management MMC open for the next activity.

How Group Policies Are Applied

After reading about group policies and examining the two default policies, you might wonder how the Default Domain Policy can affect all computers in the domain when domain controllers have their own default policy. You might have noticed that the Default Domain Policy defines

several account policies, such as password and account lockout settings, but no user rights assignment policies; the Default Domain Controllers Policy defines user rights assignment policies but no account policies. In addition, many policies are left undefined or not configured because GPOs, like Active Directory, work in a hierarchical structure.

GPOs can be applied in four places: local computer, site, domain, and OU. Policies are applied in this order, too. Policies that aren't defined or configured are not applied at all, and the last policy to be applied is the one that takes precedence. For example, a GPO linked to a domain affects all computers and users in the domain, but a GPO linked to an OU overrides the domain policies if there are conflicting settings. You learn more about using GPOs in Chapter 7.



You can remember the order in which GPOs are applied with the acronym LSDOU: local computer, site, domain, and OU.



Activity 3-10: Working with Group Policies

Time Required: 30 minutes

Objective: Create a GPO and see how policies you configure affect user objects in the OU to which the GPO is linked.

Description: You want to see how some group policy settings affect users in your domain. You know that you want to restrict some users' access to Control Panel, so you decide to start with that policy. Because you want the policy to affect individual users, you configure it in the User Configuration node.

1. If necessary, log on to your server as Administrator, and open the Group Policy Management MMC by clicking **Start**, pointing to **Administrative Tools**, and clicking **Group Policy Management**.
2. Click to expand the **Forest** and **Domains** nodes and then your domain node.
3. Right-click **TestOU** (created earlier) and click **Create a GPO in this domain, and Link it here**.
4. In the New GPO dialog box, type **TestOUGPO** in the Name text box, and then click **OK**.
5. In the left pane, click the **TestOUGPO** you just created. In the right pane, right-click **TestOUGPO** and click **Edit** to open the Group Policy Management Editor.
6. Under User Configuration, click to expand **Policies** and then **Administrative Templates**.
7. Click the **Control Panel** node. In the right pane, double-click the **Prohibit access to the Control Panel** policy to open its Properties dialog box.
8. Click the **Explain** tab, and read the description of this policy.
9. Click the **Setting** tab. Click the **Enabled** option button, and then click **OK**. Note that the State column for the policy you changed now shows Enabled.
10. Close the Group Policy Management Editor and Group Policy Management MMC.
11. Log off your server by clicking **Start**, clicking the arrow next to the padlock icon, and clicking **Log Off**.
12. Log on to your server as **testuser1**. After you press **Ctrl+Alt+Delete**, click the **Switch User** button, and then click **Other User**. Type **testuser1** in the User name text box and **Password01** in the Password text box.
13. In the message box stating that the user's password must be changed before logging on the first time, click **OK**.
14. In the New Password text box, type **Password02**, and then type it again in the Confirm password text box. Click the arrow to log on. Click **OK** when you get the message that the password has been changed.

15. If you get a message stating that the user isn't allowed to log on because of a policy that prevents regular users from logging on locally to a server, click **OK**, and then click **Switch User**.
16. Log back on to your server as Administrator.
17. Open the Group Policy Management MMC. Click to expand the **Domain Controllers** OU. Right-click **Default Domain Controllers Policy** and click **Edit** to open the Group Policy Management Editor.
18. Under Computer Configuration, click to expand **Policies**, **Windows Settings**, and then **Security Settings**.
19. Click to expand **Local Policies**, and then click **User Rights Assignment**. You should see a list of User Rights Assignment policies in the right pane (see Figure 3-21).

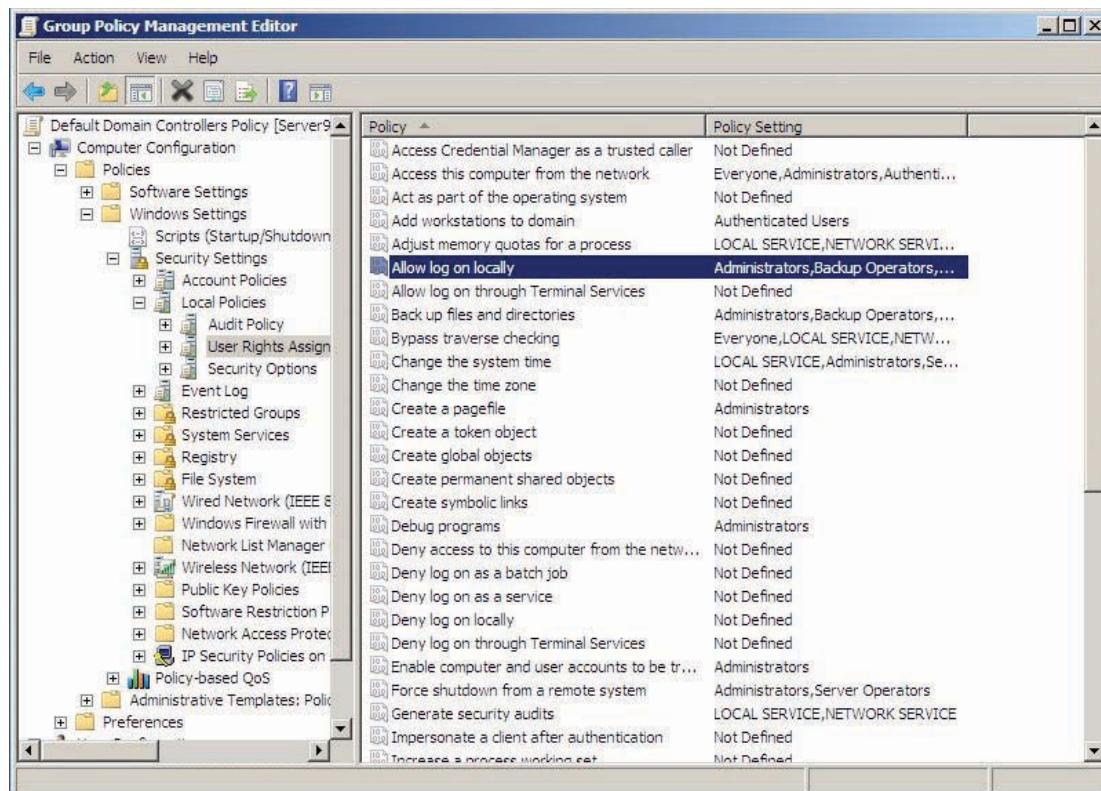


Figure 3-21 User Rights Assignment policies

20. In the right pane, double-click the **Allow log on locally** policy. Click **Add User or Group**. In the Add User or Group dialog box, type **Domain Users**, and then click **OK** twice.
21. Close all windows, and log off. Log on as **testuser1** by following Step 12, but use **Password02** as the password. If you still can't log on, you might need to wait a few minutes and try again. Group policies take some time to take effect.
22. After you're logged on, click **Start**. Note that Control Panel isn't an option on the Start menu. Close the Start menu.
23. Right-click the desktop and click **Personalize**. You see an error message stating that the operation has been canceled because of restrictions. Click **OK**. Your policy has clearly taken effect.
24. Log off the server.

In Activity 3-10, you might have noticed a delay between setting a policy and the policy taking effect. You can run the command-line program Gpupdate.exe, which applies the group policy immediately to the computer on which Gpupdate.exe is running and to the currently logged-on user. Gpupdate.exe is an invaluable tool for testing GPOs because it saves considerable time. As mentioned, computer policies are applied when a computer restarts, which can take some time, and user policies are applied when a user logs on. GPOs are also updated on domain controllers every 5 minutes and on workstations and servers every 90 minutes, even if the computers don't restart.

Chapter Summary

- A directory service is a database that stores network resource information and can be used to manage users, computers, and resources throughout the network. A directory service provides network single sign-on for users and centralizes management in geographically dispersed networks.
- Active Directory is the Windows directory service and has been part of the Windows Server family since Windows 2000 Server. Active Directory is a hierarchical, distributed database that's scalable, secure, and flexible. Active Directory's physical structure is composed of sites and domain controllers, and the logical structure is composed of organizational units, domains, trees, and forests.
- You use Server Manager to install the Active Directory Domain Services role. After running the wizard in Server Manager, you must finish the Active Directory installation by running Dcpromo.exe. After Active Directory is installed, a number of new MMCs are added to the Administrative Tools folder. The main tool for managing an Active Directory domain is Active Directory Users and Computers.
- The data in Active Directory is organized as objects. Available objects and their structure are defined by the Active Directory schema, which is composed of schema classes and schema attributes. The data in a schema attribute is called an attribute value.
- There are two types of objects in Active Directory: container objects and leaf objects. Container objects contain other objects and include domains, folders, and OUs. OUs are the primary organizing container in Active Directory. Domains represent administrative, security, and policy boundaries. OUs are organizing and management containers mainly used to mimic a company's structure and apply group policies to collections of users or computers.
- Leaf objects generally represent security accounts, network resources, and GPOs. Security accounts include users, groups, and computers. There are three categories of user account objects: local user accounts, domain user accounts, and built-in user accounts. Groups are used to assign rights and permissions to collections of users. Computer account objects are used to identify computers that are domain members. Other leaf objects include contacts, printers, and shared folders.
- Active Directory objects can be located easily with search functions in Active Directory Users and Computers and Windows Explorer. Users can use the Active Directory search function to find network resources (such as shared printers and folders), other users, and contacts, among many other items.
- GPOs are lists of settings that enable administrators to configure user and computer operating environments remotely. GPOs have two main nodes: Computer Configuration and User Configuration. Each node contains a Policies folder and a Preferences folder. Under the Policies folder are three additional folders called Software Settings, Windows Settings, and Administrative Templates.
- Policies defined in the Computer Configuration node affect all computers in the Active Directory container to which the GPO is linked. Policies defined in the User Configuration node affect all users in the Active Directory container to which the GPO is linked. Group

objects aren't affected by GPOs. GPOs can be applied in these four places in order: local computer, site, domain, and OU. User policies are applied when a user logs on, and computer policies are applied when a computer restarts.



Key Terms

Active Directory replication The transfer of information among domain controllers to make sure all domain controllers have consistent and up-to-date information.

attribute value Information stored in each attribute. *See also* schema attributes.

authentication A process that confirms a user's identity; the account is then assigned permissions and rights that authorize the user to access resources and perform certain tasks on the computer or domain.

built-in user accounts User accounts created by Windows automatically during installation.

directory service A database that stores information about a computer network and includes features for retrieving and managing that information.

Directory Services Restore Mode A boot mode used to perform restore operations on Active Directory if it becomes corrupted or parts of it are deleted accidentally.

domain The core structural unit of Active Directory; contains OUs and represents administrative, security, and policy boundaries.

domain user account A user account created in Active Directory that provides a single logon for users to access all resources in the domain for which they have been authorized.

forest A collection of one or more Active Directory trees. A forest can consist of a single tree with a single domain, or it can contain several trees, each with a hierarchy of parent and child domains.

fully qualified domain name (FQDN) A domain name that includes all parts of the name, including the top-level domain.

Group Policy Object (GPO) A list of settings that administrators use to configure user and computer operating environments remotely through Active Directory.

local user account A user account defined on a local computer that's authorized to access resources only on that computer. Local user accounts are mainly used on stand-alone computers or in a workgroup network with computers that aren't part of an Active Directory domain.

object A grouping of information that describes a network resource, such as a shared printer, or an organizing structure, such as a domain or OU.

organizational unit (OU) An Active Directory container used to organize a network's users and resources into logical administrative units.

permissions Settings that define which resources users can access and what level of access they have to resources.

right A setting that specifies what types of actions a user can perform on a computer or network.

schema Information that defines the type, organization, and structure of data stored in the Active Directory database.

schema attributes A category of schema information that defines what type of information is stored in each object.

schema classes A category of schema information that defines the types of objects that can be stored in Active Directory, such as user or computer accounts.

site A physical location in which domain controllers communicate and replicate information regularly.

Sysvol folder A shared folder that stores information from Active Directory that's replicated to other domain controllers.

tree A grouping of domains that share a common naming structure.

Review Questions

1. Which of the following best describes a directory service?
 - a. Similar to a list of information in a text file
 - b. Similar to a database program but with the capability to manage objects in it
 - c. A program for managing the user interface on a server
 - d. A program for managing folders, files, and permissions on a distributed server
2. Which of the following is a feature of Active Directory? (Choose all that apply.)
 - a. Fine-grained access controls
 - b. Can be distributed among many servers
 - c. Can have only one server
 - d. Has a fixed schema
3. What term is used for transferring Active Directory information among domain controllers?
4. Which of the following is a component of Active Directory's physical structure?
 - a. Organizational units
 - b. Domains
 - c. Sites
 - d. Folders
5. Which of the following is the responsibility of domain controllers? (Choose all that apply.)
 - a. Storing a copy of the domain data
 - b. Providing data search and retrieval functions
 - c. Servicing multiple domains
 - d. Providing authentication services
6. Groups are considered an organizing component of Active Directory. True or False?
7. Which of the following is *not* associated with an Active Directory tree?
 - a. A group of domains
 - b. A container object that can be linked to a GPO
 - c. A common naming structure
 - d. Parent and child domains
8. Which of the following is associated with an Active Directory forest? (Choose all that apply.)
 - a. Contains trees with different naming structures
 - b. Allows independent domain administration
 - c. Contains domains with different schemas
 - d. Represents the broadest element in Active Directory
9. Which of the following is associated with installing the first domain controller in a forest?
 - a. RODC
 - b. Child domain
 - c. Global catalog
 - d. DHCP
10. The Active Directory database and log files should always be located on the same disk. True or False?

11. Which MMCs are added after Active Directory installation? (Choose all that apply.)
- Active Directory Domains and Trusts
 - Active Directory Groups and Sites
 - ADSI Edit
 - Active Directory Restoration Utility
12. You run the Add Roles Wizard in Server Manager to add the AD DS role. After the wizard is finished, you check the Administrative Tools folder but don't find any of the Active Directory management tools. What should you do?
13. Which of the following defines the types of objects in Active Directory?
- GPOs
 - Attribute values
 - Schema attributes
 - Schema classes
14. Which of the following defines the types of information stored in an Active Directory object?
- GPOs
 - Attribute values
 - Schema attributes
 - Schema classes
15. "John Doe" is an example of which of the following?
- GOPO
 - Attribute value
 - Schema attribute
 - Schema class
16. Which of the following is a container object? (Choose all that apply.)
- Domain
 - Group
 - GPO
 - OU
17. Which of the following is a default folder object?
- Computers
 - Domain Controllers
 - Groups
 - Sites
18. Which type of account is *not* found in Active Directory?
- Domain user account
 - Local user account
 - Built-in user account
 - Computer account
19. You have just created a shared folder on your domain controller. You publish the share in Active Directory by using the Shared Folders snap-in in Computer Management. To make sure the shared folder was published correctly, you use the Search Active Directory tool in Windows Explorer. You can find the shared folder, but when you open Active Directory

Users and Computers, you can't locate the object representing the shared folder. What should you do so that you can see this object in Active Directory Users and Computers?

20. To which of the following can a GPO be linked? (Choose all that apply.)
 - a. Trees
 - b. Domains
 - c. Folders
 - d. Sites
21. Which container has a default GPO linked to it?
 - a. Users
 - b. Printers
 - c. Computers
 - d. Domain
22. When are policies set in the User Configuration node applied?
 - a. Every 5 minutes
 - b. Immediately
 - c. At user logon
 - d. At computer restart
23. Users can override settings in the Preferences folder of a GPO. True or False?
24. Which of the following is a folder under the Computer Configuration node? (Choose all that apply.)
 - a. Administrative Templates
 - b. Users and Computers
 - c. Domain Controllers
 - d. Windows Settings
25. If a policy is defined in a GPO linked to a domain, and that policy is defined with a different setting in a GPO linked to an OU, which is true by default?
 - a. The policy setting in the GPO linked to the OU is applied.
 - b. The policy setting in the GPO linked to the domain is applied.
 - c. Neither policy setting is applied, and an error message is generated.
 - d. The policy in both GPOs defaults to Not Defined so that no conflict exists.

Case Projects



Case Project 3-1: Configuring Active Directory

When Cool Gadgets first started its Windows network almost a year ago, the network was small enough that you simply used the default Users and Computers containers for the user account and computer account objects you created. However, now that the company has grown to more than 50 users and computers, you decide that some structure is needed. You talk to the owner to understand how the business is organized and learn that there are four main departments: Executive, Marketing, Engineering, and Operations. Draw a diagram of your Active Directory structure based on this information, including the types of objects in each container. Include the objects that you know about and where those objects should be located, and state whether you need to move any existing objects. Use triangles and circles to represent container objects in your diagram, as shown in Figures 3-2 through 3-4.

Case Project 3-2: Explaining GPOs

The owner of Cool Gadgets has told you he needs to lock down some desktops so that these users can't access certain Windows components, such as Control Panel. He also wants some standardization in the look of users' desktops, such as wallpaper and so forth. However, he's not sure how to make these changes without affecting all users and computers. Write a short explanation of how GPOs can be applied. Include information about how policies defined in one place can take precedence over policies defined elsewhere.



Case Project 3-3: Creating the Group Policy Structure

After explaining to the owner of Cool Gadgets how GPOs work, you sit down with him to work out the details of the policies he wants enacted. He says he wants all users locked out of Control Panel except users in the Engineering Department, who should have normal access to Control Panel. In addition, he wants all computers in the domain to have auditing enabled for all logon events. Finally, users in the Marketing Department should have a new application made available to them on any computer in the company where they log on. For each requirement, indicate whether a new GPO needs to be created. Also, include where any new GPO will be applied, the path to the policy, and the policy setting to be applied. Use the following format (the answer to the first requirement is given):

Policy requirement: Lock out all users from Control Panel with the exception of Engineering Department users

GPO required: Default Domain Policy applied to the domain

Path to policy: User Configuration\Policies\Administrative Templates\Control Panel\Prohibit access to the Control Panel

Policy setting: Enabled

GPO required: New, applied to the Engineering OU

Path to policy: User Configuration\Policies\Administrative Templates\Control Panel\Prohibit access to the Control Panel

Policy setting: Disabled

This page intentionally left blank

Active Directory Design and Security Concepts

After reading this chapter and completing the exercises, you will be able to:

- Work with organizational units
- Work with forests, trees, and domains
- Describe the components of a site

A directory service should be thought of as a tool to help administrators

manage network resources. Like any tool, the better designed it is, the more useful it will be. In its default configuration, Active Directory is a useful directory service, but its real power is apparent when thought has been put into its design and configuration. In this chapter, you learn that Active Directory is based on a standard for storing and accessing directory service information, which makes integrating it with other vendors' systems possible. Knowing that non-Windows systems might need to access Active Directory information can influence your design decisions.

An efficient Active Directory design that reflects how a business is organized improves the ease and efficiency of managing a Windows network. Likewise, proper configuration of Active Directory is paramount to a smoothly running and secure network. This chapter delves into the architecture of Active Directory with discussion that goes beyond a simple one-domain environment. You learn more about organizational units (OUs) and domains along with Active Directory trees and forests. You also learn about Active Directory sites and their importance in efficient Active Directory design. Your understanding of these concepts will guide you in making wise decisions as you design and implement an Active Directory infrastructure.

Working with Organizational Units

Before delving into working with OUs, you need to know that Active Directory is based on standards for defining, storing, and accessing directory service objects. X.500, a suite of protocols the International Telecommunications Union (ITU) developed, is the basis for the hierarchical structure of Active Directory information and for how Active Directory objects are named and stored. **Lightweight Directory Access Protocol (LDAP)**, created by the Internet Engineering Task Force (IETF), is based on the X.500 Directory Access Protocol (DAP). DAP required the seldom used, high-overhead Open Systems Interconnection (OSI) protocol stack for accessing directory objects. LDAP became a streamlined version of DAP, using the more efficient and widely used TCP/IP—hence the term *lightweight* in the protocol's name.

So why is knowledge of LDAP important? You run across references to LDAP periodically when reading material about Active Directory, and as an administrator, you'll be using tools that incorporate LDAP definitions and objects, such as ADSI Edit, or running programs that use LDAP to integrate with Active Directory. In addition, integrating other OSs, such as Linux, into an Active Directory network requires using LDAP. In fact, you already used a tool that incorporates LDAP terminology when you ran the DSADD command in Chapter 3. LDAP and its syntax are covered in more detail when you work with command-line tools in Chapters 5 and 13 and explore roles such as Active Directory Lightweight Directory Services in Chapter 12. For now, turn your attention to Active Directory design concepts, starting with OUs.

As you learned in Chapter 3, OUs are the building blocks of the Active Directory structure in a domain. Thoughtful planning of the OU structure eases managing users and computers and applying group policies and makes Active Directory a friendlier place for users and technical staff alike. Here are some benefits of using OUs:

- You can create a familiar hierarchical structure based on the organizational chart that enables users and administrators to locate network users and resources quickly.
- You can delegate administration of network resources to other IT staff without assigning more comprehensive administrative permissions.
- You can change the OU structure easily to accommodate corporate reorganizations.
- You can group users and computers for the purposes of assigning administrative and security policies with the Group Policy tool.
- You can hide Active Directory objects for confidentiality or security reasons by configuring access permissions on OUs.



An OU can't be used to assign permissions to objects it contains. Groups, not OUs, are used for permission assignments and are discussed in more detail in Chapter 5.

NOTE

OUS are containers holding objects such as user and computer accounts, but they can also contain other OUs. This ability to nest OUs gives you the flexibility to create a hierarchy with as many levels as needed for your environment. Take a look at a fictitious company, *Fakebusiness.com*, with this top-level organizational structure:

- Administration
- Marketing
- Research and Development (R&D)
- Operations

4

This organization will likely have a single-level OU structure, as shown on the left in Figure 4-1. Dividing R&D into the Engineering and Research departments and Marketing into Sales and Advertising creates the multilevel OU structure shown on the right in Figure 4-1.

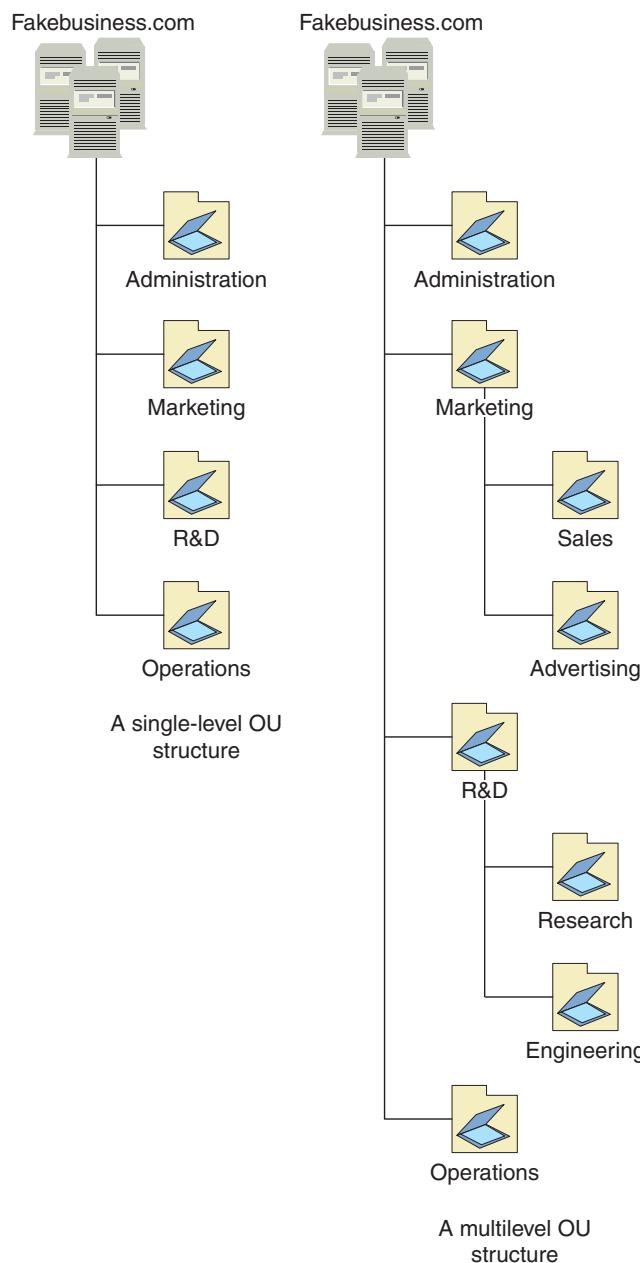


Figure 4-1 Single-level and multilevel OU structures

Now look at a larger organization with departments in different locations. If the company uses department rather than location for identification purposes, the OU structure could reflect that focus, as shown on the left in Figure 4-2. The top-level structure remains intact, but under each department is an OU for each location. Conversely, if the business is organized mainly by location, the OU structure looks like the one on the right in Figure 4-2. Notice that some OUs have the same name, which is allowed as long as they are in different parts of the Active Directory hierarchy. For example, the R&D OU is under both the Boston and Seattle OUs.



There are other approaches to OU hierarchy design. For example, a current trend is designing OUs based on grouping users and resources according to their security levels.

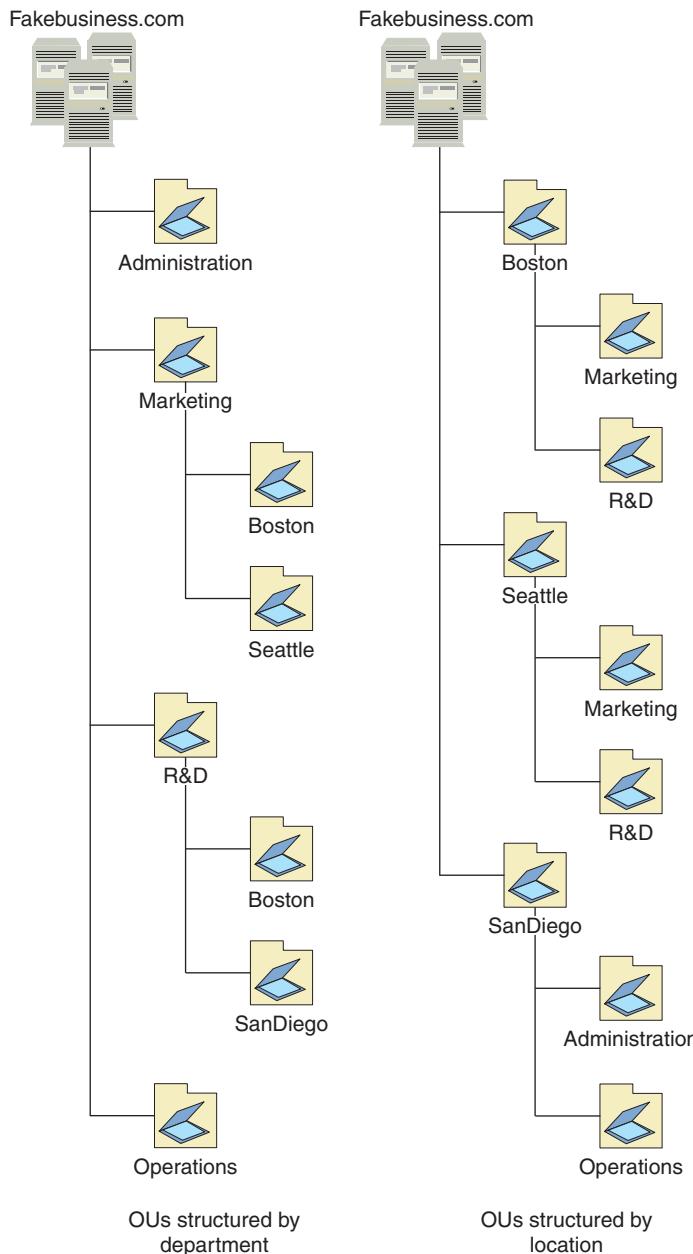


Figure 4-2 A multilocation domain organized by department and location

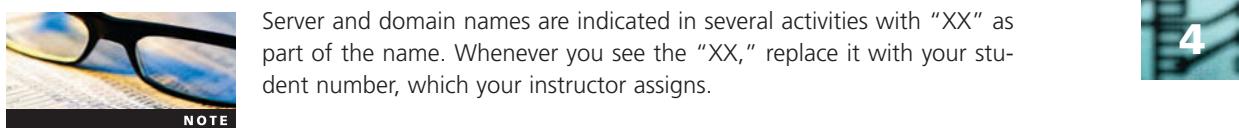


Activity 4-1: Creating a Single-Level OU Structure

Time Required: 10 minutes

Objective: Create a series of OUs to reflect a company's departmental structure.

Description: You have been asked to create the OU structure for a business with four main departments: Administration, Marketing, Research and Development, and Operations. You will create a single-level OU structure based on these requirements.



NOTE

4

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
3. Right-click the domain node (w2k8adXX.com), point to **New**, and click **Organizational Unit**.
4. In the Name text box, type **Administration**. Leave the **Protect container from accidental deletion** check box selected, and then click **OK**.
5. Repeat Steps 3 and 4 to create the **Marketing**, **Research and Development**, and **Operations** OUs. When finished, your OU structure should be similar to Figure 4-3.
6. Leave Active Directory Users and Computers open for the next activity.

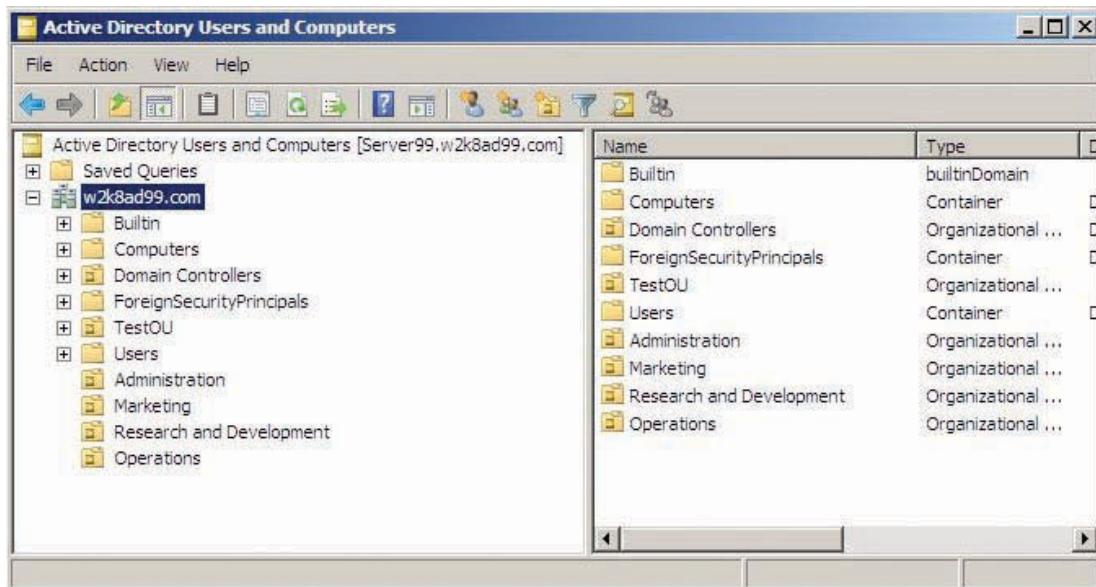


Figure 4-3 A single-level OU structure

OU Delegation of Control

As you've learned, one benefit of using OUs is that you can delegate administration of the OU and its contents to other users without giving them broader administrative capability. **Delegation of control**, in the context of Active Directory, means a person with higher security privileges assigns authority to a person of lesser security privileges to perform certain tasks. Delegation of control of an OU is not an all-or-nothing proposition. You can assign specific tasks the user can

perform on objects in that OU and even delegate other tasks to different users or groups. The following are the most common tasks that can be delegated:

- Create, delete, and manage user accounts.
- Reset user passwords and force password change at next logon.
- Read all user information.
- Create, delete, and manage groups.
- Modify the membership of a group.
- Manage group policy links.
- Generate Resultant Set of Policy (Planning).
- Generate Resultant Set of Policy (Logging).



Three more predefined tasks can be delegated for the object class `inetOrgPerson`, which is a user and contact class defined in Active Directory for LDAP compatibility.

NOTE

In addition to these predefined tasks, you can define custom tasks, which allow fine-grained control over the management tasks a user can perform in an OU. When you create a custom task, you must fully understand the nature of objects, permissions, and permission inheritance. Even if you delegate control only by using predefined tasks, your understanding of how permissions and permission inheritance work is important. After all, the Delegation of Control Wizard does nothing more than assign permissions for Active Directory objects to selected users or groups.



Activity 4-2: Delegating Control of an OU

Time Required: 10 minutes

Objective: Create a user and delegate control of an OU to that user.

Description: Your responsibilities as IT administrator have been keeping you busy, and you're trying to focus on plans for a sizable network expansion. You have been slowed considerably because the Marketing Department is expanding, and you're fielding frequent requests to create users and groups and reset forgotten passwords. You have hired a new technician and think he's ready for additional responsibilities, so you decide to delegate control of user accounts to him.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Right-click the **Operations** OU you created in Activity 4-1, point to **New**, and click **User**.
3. Type **Joe** in the First name text box, **Tech1** in the Last name text box, and **jtech1** in the User logon name text box. Click **Next**.
4. Type **Password01** in the Password text box and again in the Confirm password text box. Click to clear the **User must change password at next logon** check box. Click **Next**, and then click **Finish**.
5. Right-click the **Marketing** OU and click **Delegate Control** to start the Delegation of Control Wizard. Click **Next**.
6. Click **Add**. In the Enter the object names to select text box, type **jtech1**. Click **Check Names**, and then click **OK**. Click **Next**.
7. Click the **Create, delete, and manage user accounts** check box. Click **Next**, and then click **Finish**.
8. Leave Active Directory Users and Computers open for the next activity.

After you have delegated control to a user, there's no clear indication that this change has been made. By default, the OU's properties don't show that another user has been delegated control. To verify who has been delegated control of an OU, you must view the OU's permissions, as explained in the following section.

Active Directory Object Permissions

Three types of objects can be assigned permission to access an Active Directory object: users, groups, and computers. These object types are referred to as **security principals**. An Active Directory object's security settings are composed of three components collectively referred to as the object's security descriptor:

- *Discretionary access control list (DACL)*—A list of security principals, with each having a set of permissions that define access to the object. Each entry in the DACL is referred to as an access control entry (ACE). If a security principal or a group the security principal belongs to isn't in the DACL, the security principal has no access to the object.
- *Object owner*—Usually the user account that created the object or a group or user who has been assigned ownership of the object. An object owner has special authority over that object. Most notably, even if the owner isn't in the object's DACL, the owner can still assign permissions to the object.
- *System access control list (SACL)*—Defines the settings for auditing access to an object.



A fourth component of the security descriptor is the primary group, which has importance only for POSIX compatibility.

NOTE

Every Active Directory object has a list of standard permissions and a list of special permissions that can be assigned to a security principal. For simplicity's sake, the term "users" is used when discussing permissions, but keep in mind that permissions can be assigned to any of the three security principals: users, groups, and computers. Each permission can be set to Allow or Deny, and five standard permissions are available for most objects:

- *Full control*—Users can perform all actions granted by all the standard permissions, change permissions, and take ownership of the object.
- *Read*—Users can view objects and their attributes and permissions.
- *Write*—Users can change the object's attributes.
- *Create all child objects*—Users can create new child objects in the parent object.
- *Delete all child objects*—Users can delete child objects in the parent object.



Permissions and permission inheritance for Active Directory objects work almost identically to NTFS file and folder permissions, discussed in Chapter 6.

TIP

In addition, different object types have other standard and special permissions. For example, a user object has the Reset password and Read logon information permissions; an OU object has the Create Account objects and Create Printer objects permissions.

Users can be assigned permission to an object in three different ways:

- The user's account is added to the object's DACL. This method is referred to as an explicit permission.
- A group the user belongs to is added to the object's DACL.
- The permission is inherited from a parent object's DACL to which the user or group account has been added.

When a user has been assigned permission to an object through a combination of these methods, the user's **effective permissions** are a combination of the assigned permissions. For example, if Joe Tech1's account has been added to an object's DACL and assigned the Allow Read permission, and a group that Joe Tech1 belongs to has been added to the same object's DACL and assigned the Allow Write permission, Joe Tech1 has both Read and Write permissions for the object.

As a rule, a Deny permission overrides an Allow permission. For example, a group Joe Tech1 belongs to has been added to an object's DACL and assigned the Allow Full control permission, and Joe Tech1's account has been added to the same object's DACL and assigned the Deny Write permission. In this case, Joe Tech1 could perform all actions on the object that Full control allows, except actions requiring the Write permission.

There's an exception to this rule: If the Deny permission is inherited from a parent object, and the Allow permission is explicitly added to the object's DACL, the Allow permission takes precedence if there's a conflict.

Using Deny in an ACE As stated, if a security principal isn't represented in an object's DACL, it doesn't have access to the object. For this reason, you don't need to add Deny ACEs to every object to prevent users from accessing those objects. However, the Deny permission does have its place, usually when an exception is needed. For example, Bill is a member of the ITSupport group, which has been given access to the Accounting OU so that group members can manage objects in the OU. Bill is a new employee, so until he's fully trained, you don't want him to be able to delete objects in the OU. You can add Bill's user account to the Accounting OU's DACL and assign the Deny Delete all child objects permission to his account. Using Deny in this way enables you to assign broad permissions to groups, yet make exceptions for certain group members. Another common use of the Deny permission is to override a permission inherited from a parent object, as explained in the following section.

Permission Inheritance in OUs Generally speaking, **permission inheritance** defines how permissions are transmitted from a parent object to a child object. For example, an OU containing other objects is the parent object, and any objects contained in the OU, including other OUs, are considered child objects. All objects in Active Directory are child objects of the domain. By default, permissions applied to the parent OU with the Delegation of Control Wizard are inherited by all child objects of that OU. So if a user has been given permissions to manage user accounts in an OU, these permissions apply to all existing and future user accounts in that OU, including user accounts created in child OUs. In the OU design structured by department in Figure 4-2, if a user is delegated control to create, delete, and manage user accounts in the R&D OU, that user could perform those actions on users in the R&D OU as well as the Boston and San Diego OUs.

Advanced Features Option in Active Directory Users and Computers The default display settings in Active Directory Users and Computers hide some system folders and advanced features, but you can display them by enabling the Advanced Features option from the View menu. After selecting this option, four new folders are shown under the domain node:

- *LostAndFound*—Contains objects created at the same time that their container is deleted, perhaps by another administrator on another domain controller
- *Program Data*—Initially empty; is available to store application-specific objects
- *System*—Used by various Windows system services that are integrated with Active Directory
- *NTDS (NT Directory Service) Quotas*—Stores quota information that limits the number of Active Directory objects a user, group, computer, or service can create

In addition, the Properties dialog box of domain, folder, and OU objects has three new tabs:

- *Object*—Used to view detailed information about a container object, such as the object class, created and modified dates, and sequence numbers for synchronizing replication. It also includes a check box you can select to protect an object from accidental deletion.

- **Security**—Used to view and modify an object’s permissions.
- **Attribute Editor**—Used to view and edit an object’s attributes, many of which aren’t available in standard Properties dialog boxes.

For now, you’re most interested in the Security tab of an OU’s Properties dialog box (see Figure 4-4). The top section lists all accounts (user, group, and computer) that have an ACE in the DACL. The bottom section lists the permission settings for each ACE. In Figure 4-4, Joe Tech1’s ACE is selected, and the bottom section shows Allow Special permissions for his permission settings. To view details for this permission, click the Advanced button.

4

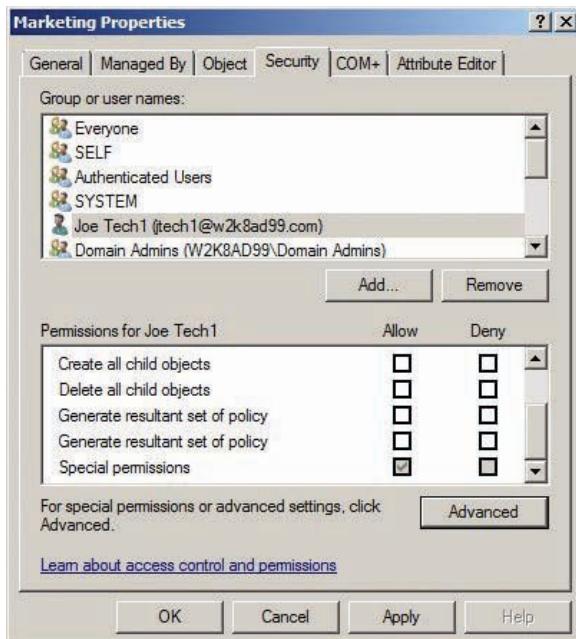


Figure 4-4 The Security tab of an OU’s Properties dialog box

Activity 4-3: Viewing Object Permissions

Time Required: 15 minutes

Objective: Explore the Advanced Features option in Active Directory Users and Computers.

Description: You have just delegated control of the Marketing OU to one of your technicians and are curious to see how the OU’s DACL has changed. To view the settings, you need to enable the Advanced Features option in Active Directory Users and Computers.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Right-click the **Marketing** OU and click **Properties**. Note the three tabs: General, Managed By, and COM+. Click **Cancel**.
3. Click **View, Advanced Features** from the menu, and verify that Advanced Features is selected with a check mark. The display changes to include four new folders: LostAndFound, Program Data, System, and NTDS Quotas.
4. Right-click the **Marketing** OU and click **Properties**. Note the three additional tabs: Object, Security, and Attribute Editor.
5. Click the **Object** tab. The information displayed is useful in troubleshooting. In addition, when the Protect object from accidental deletion check box is selected, the object can’t be deleted unless permissions are changed manually.

6. Click the **Security** tab. Scroll through the list of group and user names so that you know what ACEs are in the DACL. Click each ACE to view its permission settings in the bottom section.
7. Click the **Joe Tech1** ACE, and scroll the permissions list at the bottom. Note that the Allow Special permissions check box is selected.
8. Click the **Advanced** button to open the Advanced Security Settings for Marketing dialog box (see Figure 4-5).

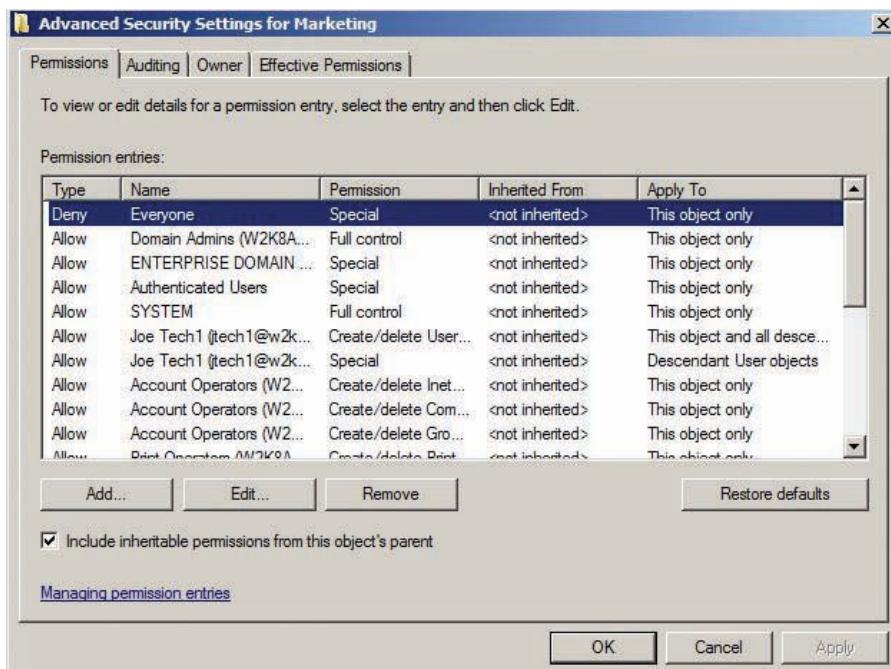


Figure 4-5 An OU's Advanced Security Settings dialog box

9. Double-click the first **Joe Tech1** entry. The Create User objects and Delete User objects check boxes are selected in the Allow column, so Joe Tech1 has permission to create and delete users in the Marketing OU. The “This object and all descendant objects” option in the Apply to list means Joe Tech1 can create and delete users in any OUs under Marketing.



The term “descendant” means that all objects underneath the object are also affected by the permission settings.

10. Click **Cancel**, and then double-click the next **Joe Tech1** entry. Note that all check boxes in the Allow column of the permissions list are selected. In addition, the Descendant User objects option is selected in the Apply to list, which means Joe Tech1 has all permissions for all new and existing user objects in the Marketing OU.
11. Click **Cancel** three times, until only the Active Directory Users and Computers window is open. Leave this window open for the next activity.

Effective Permissions As discussed, effective permissions for an object are a combination of the allowed and denied permissions assigned to a security principal. These permissions can come from assignments made directly to a user account or to a group the user belongs to. Before examining the nuances of object permissions, take a look at some examples of how to determine a user’s effective permissions for an object. Table 4-1 lists two groups with the group members, and Table 4-2 lists the ACEs for an OU.

Table 4-1 Group membership

Group	Members
Group1	Bill, Tom, Mary, Susan
Group2	Bill, Mary, Jane, Alex

Table 4-2 ACEs for an OU: Example 1

ACE	Permission	How assigned
Bill	Allow Read	Explicit
Tom	Allow Full control	Explicit
Group1	Allow Write	Inherited
Group2	Allow Create all child objects	Inherited

The effective permissions are as follows:

- Bill: Allow Read, Write, and Create all child objects
- Tom: Allow Full control
- Mary: Allow Write and Create all child objects
- Susan: Allow Write
- Jane and Alex: Allow Create all child objects

All the permissions assigned are Allow permissions, so you just add them together to arrive at the effective permissions for each user. Tom is granted Full control, which encompasses all other permissions. Take a look at another example with the same group memberships but using the ACEs in Table 4-3.

Table 4-3 ACEs for an OU: Example 2

ACE	Permission	How assigned
Bill	Deny Delete all child objects	Inherited
Mary	Deny Full control	Inherited
Group1	Allow Full control	Inherited
Group2	Allow Create all child objects	Inherited

The effective permissions are as follows:

- Bill: Allow Full control, except for deleting all child objects
- Tom: Allow Full control
- Mary: Deny Full control
- Susan: Allow Full control
- Jane and Alex: Allow Create all child objects

The Deny permission overrides the Allow permission, so although Bill, as a member of Group1, inherited Full control, the Deny Delete all child objects entry prevents him from deleting objects in the OU. Mary inherited Full control because of her membership in Group1, but the Deny Full control entry for her user account overrides the inherited permission. Look at the next example with the same group memberships but using the ACEs in Table 4-4.

Table 4-4 ACEs for an OU: Example 3

ACE	Permission	How assigned
Bill	Allow Full control	Explicit
Jane	Allow Create all child objects	Explicit
Group1	Deny Full control	Inherited
Group2	Deny Create all child objects	Inherited

The effective permissions are as follows:

- Bill: Allow Full control
- Jane: Allow Create all child objects
- Tom, Mary, Susan, Alex: Denied access

In this example, the Deny permissions are inherited, so any explicitly assigned Allow permissions take precedence. Remember, this is the exception to the rule that Deny permissions override Allow permissions. So although Bill and Jane are denied permission because of their group memberships, those permissions are inherited, and the Allow permissions for their user accounts are assigned explicitly.

Now take a closer look at permission inheritance. As stated, permissions for an object are inherited from its parent automatically. In Active Directory, the domain is the top-level object for permission inheritance. So the domain object doesn't inherit any permission settings because it has no parent container from which to inherit settings. OUs inherit some permissions from the domain object or, with nested OUs, from their parent OU. In addition, several permissions are added to an OU's DACL by default when it's created. You can see which permissions are inherited and which have been added to a DACL by viewing the Advanced Security Settings dialog box, shown previously in Figure 4-5. The Inherited From column shows “<not inherited>” or the complete path to the object from which permission was inherited. The Apply To column shows whether the permission is set to be inherited by child objects. The following are some of the most common settings for permission inheritance:

- *This object only*—The permission setting isn't inherited by child (descendant) objects. This setting is the default when a new ACE is added to an object's DACL manually instead of with the Delegation of Control Wizard.
- *This object and all descendant objects*—The permission setting applies to the current object and is inherited by all child objects.
- *All descendant objects*—The permission setting doesn't apply to the selected object but is inherited by all child objects.
- *Descendant [object type] objects*—The permission is inherited only by specific child object types, such as user, computer, or group objects.

Permission inheritance is enabled by default on child objects but can be disabled. Inherited permissions can't be changed or removed without disabling permission inheritance first. However, you can add permissions to an object without disabling inheritance. In Figure 4-5, note the “Include inheritable permissions from this object's parent” check box. By default, it's selected, which means the object does inherit permissions from its parent object. Clearing this check box blocks permission inheritance, and you're prompted to copy inheritable permissions from the parent object, remove inherited permissions, or cancel the operation. Selecting the option to copy inheritable permissions is a good idea so that you have a starting point for your DACL. After you have disabled inheritance, you can always remove or change the copied permissions.

Use caution before changing permissions and permission inheritance. Incorrect settings can cause Active Directory access problems, so be sure you know what effect your changes will have on Active Directory before applying them. If your changes cause problems, you can click the

Restore defaults button in the Advanced Security Settings dialog box, which resets permissions for the object to the default security settings defined in the Active Directory schema.



Activity 4-4: Working with Permission Inheritance

Time Required: 15 minutes

Objective: Create two OUs under an existing OU and view the effect of different permission inheritance settings.

Description: You have been told that the Marketing Department is growing to the point that Sales and Advertising departments will be added under it to make management easier. You decide to create two OUs to reflect this organizational structure.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Right-click the **Marketing** OU, point to **New**, and click **Organizational Unit**. In the Name text box, type **Sales**, and then click **OK**. Repeat this procedure, but type **Advertising** in the Name text box.
3. Click to expand the **Marketing** OU, if necessary. Right-click the **Sales** OU and click **Properties**. Click the **Security** tab.
4. Scroll down in the Group or user names list box, and click **Enterprise Admins**. Note that the check boxes in the Allow column of the Permissions section are disabled.
5. Click the **Remove** button. A Windows Security message box opens, explaining that you can't remove the Enterprise Admins entry because the permission was inherited from the parent object. You must disable inheritance if you want to remove the entry. Click **OK**.
6. Click **Joe Tech1**, and click **Remove**. You see the same message as in Step 5. Click **OK**, and then click **Advanced**.
7. Click one of the **Joe Tech1** entries in the Permission entries list box. Place your mouse pointer over the **Inherited From** column to see the full path of the object from which the permission was inherited. In this case, the path is the Marketing OU in your domain.
8. Click to clear the **Include inheritable permissions from this object's parent** check box. The Windows Security message box shown in Figure 4-6 is displayed. Note that disabling inheritance applies to all entries in the permissions list, not just the selected entry. If you want to enable inheritance again, simply select the check box again.

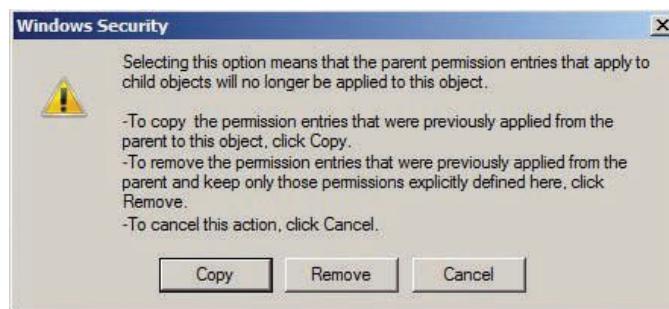


Figure 4-6 The Windows Security message shown when you disable inheritance

9. Click **Copy**. The Inherited From column for all entries changes to "<not inherited>." Click **OK**. You see a warning message explaining that permissions are being added to the DACL. These "added" permissions are simply ones that have been changed from inherited to not inherited. When permissions are added to a DACL, Windows must apply those permissions to all child objects, if required by the permission's Apply To setting. Windows is informing you that if many child objects are present, the process can take more time and storage. Click **Yes**.



10. Click **Joe Tech1** in the Sales Properties dialog box, and then click **Remove**. Because you have disabled inheritance, you can now remove or edit any permissions that were previously inherited and couldn't be removed or changed. Click **OK**.
11. Right-click the **Advertising** OU and click **Properties**. Click the **Security** tab. Click **Joe Tech1**, and then click **Remove**. Note that disabling inheritance on the Sales OU doesn't affect the Advertising OU. Click **OK**, and then click **Cancel**.
12. Leave Active Directory Users and Computers open for the next activity.

One challenge an administrator faces when dealing with permissions and permission inheritance is determining who has access to which objects. With the Advanced Security Settings dialog box, you can determine what permissions a user or group has to an object. Click the Effective Permissions tab, and then select a user or group whose effective permissions you want to view, as shown in Figure 4-7. You can only view permissions here; you can't change them.

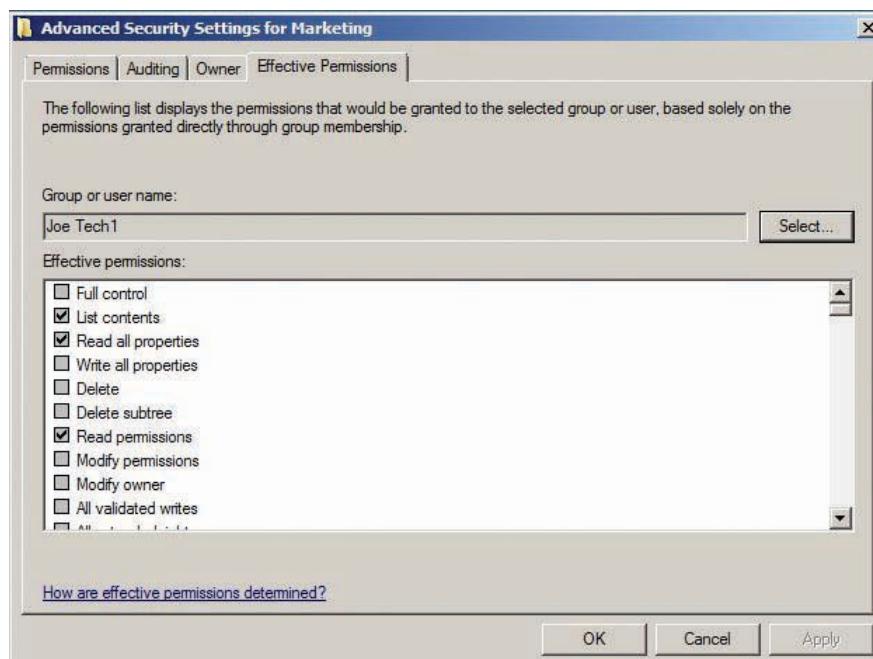


Figure 4-7 The Effective Permissions tab



Activity 4-5: Determining Effective Permissions

Time Required: 15 minutes

Objective: Set up different permissions and then verify the results by checking effective permissions.

Description: A junior administrator has some questions about how permissions work. You create an account for her to use and delegate control of a test OU to her so that she can work with some different permission situations and use the Effective Permissions tab to verify her results.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Create an OU under the domain node named **TestOU1**.
3. Create a user under the Operations OU with a logon name of **jradmin**, full name of **Jr Admin**, and password of **Password01**. Make sure the user's password never expires.
4. Right-click **TestOU1** and click **Delegate Control**. Click **Next**.
5. Click **Add** to open the Select Users, Computers, or Groups dialog box. Type **jradmin**, click **OK**, and then click **Next**.

6. Click the **Create a custom task to delegate** option button, and then click **Next**.
7. Click the **This folder, existing objects in this folder, and creation of new objects in this folder** option button, and then click **Next**.
8. Click the **Full Control** check box in the Permissions list box. Click **Next**, and then click **Finish**.
9. Right-click **TestOU1** and click **Properties**. Click the **Security** tab, and then click the **Jr Admin** ACE. Verify that the **Full control** check box in the Allow column is selected.
10. Click the **Advanced** button. Click the **Effective Permissions** tab, and then click the **Select** button.
11. Type **jradmin**, and then click **OK**. The effective permissions for jradmin are less than Full control because the Everyone group has a Deny Delete permission for this OU. The Deny Delete permission is added to every new OU by default and can be removed by clearing the Protect object from accidental deletion check box in the Object tab. Click **OK** twice.
12. Log off and log on as **jradmin**. Open Active Directory Users and Computers. If you see the UAC prompt to enter your password, enter **Password01**, and then click **OK**.
13. Create an OU named **TestOU1-L2** under TestOU1 and an OU named **TestOU1-L3** under TestOU1-L2 so that the OU structure looks like Figure 4-8.

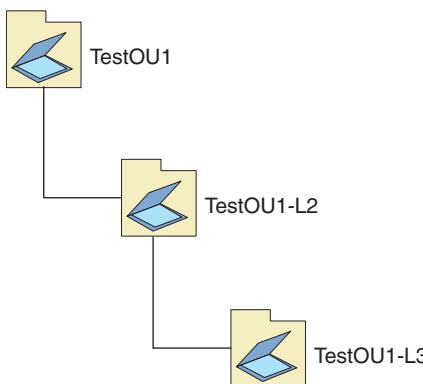


Figure 4-8 The Test OU structure

14. In the TestOU1 container, create a user named **jrttest1**. Create a global security group called **jrgroup1** in TestOU1, and add jrttest1 as a member of this group.
15. Click **View, Advanced Features** from the menu. Right-click **TestOU1-L2** and click **Properties**.
16. Click the **Security** tab, and then click the **Advanced** button. In the Advanced Security Settings dialog box, click the **Owner** tab. Note that jradmin is the owner of this OU because the jradmin user created the OU. Click **OK**.
17. Click the **Add** button. Type **jrgroup1**, and then click **OK**. By default, the ACE for jrgroup1 has the Allow Read permission.
18. Click **jrgroup1** in the Group or user names list box, and then click the **Write** and **Create all child objects** check boxes in the Allow column. Click to clear the **Read** check box in the Allow column, and then click **Apply**.
19. Click the **Advanced** button, and then click the **Effective Permissions** tab. Click the **Select** button, type **jrttest1**, and then click **OK**. In the Effective permissions list box, note that jrttest1 gets the Write and Create objects permissions because jrttest1 is a member of jrgroup1. As a member of the special group Authenticated Users (discussed in Chapter 5), jrttest1 also gets the Read permission. Click **OK**.
20. Click the **Add** button. Type **jrttest1**, and then click **OK**.
21. Click **jrttest1** in the Group or user names list box, and then click the **Write** check box in the Deny column. Click to clear the **Read** check box in the Allow column, and then click **Apply**.

22. Click the **Advanced** button, and then click the **Effective Permissions** tab. Click the **Select** button, type **jrttest1**, and then click **OK**. Scan the Effective permissions list. Note that jrttest1 no longer has the Write permission because you applied the Deny permission. Click **OK** twice.
23. Right-click the **TestOU1-L3** OU and click **Properties**. Click the **Security** tab.
24. Scroll through the Group or user names list box. There are no entries for jrttest1 and jrgroup1 because when you add an ACE to a DACL manually, the default inheritance setting is for the ACE to apply to “This object only.” This setting can be changed, however. Click **Cancel**.
25. Click **TestOU1-L2** to select it, and then open its Properties dialog box. Click the **Security** tab, and then click the **Advanced** button. Double-click the **jrttest1** entry. In the Apply to list, change the setting to **This object and all descendant objects**, and then click **OK**. Double-click the **jrgroup1** entry. In the Apply to list, change the setting to **This object and all descendant objects**, and then click **OK**. Click **OK** twice.
26. Right-click the **TestOU1-L3** OU and click **Properties**. Click the **Security** tab. Notice that there are entries for jrttest1 and jrgroup1 now. Click the **Advanced** button. Click the **Effective Permissions** tab, and then click **Select**. Type **jrttest1**, and then click **OK**. Note that jrttest1’s permissions are the same as for the TestOU1-L2 OU. Click **OK**.
27. Click **jrttest1** in the Group or user names list box, and then click the **Write** check box in the Allow column. The Write check box in the Deny column is disabled because the permission was inherited. Click **Apply**, and then click the **Advanced** button.
28. Click the **Effective Permissions** tab, and then click **Select**. Type **jrttest1**, and then click **OK**. The Write check box is selected now because the explicit Allow Write permission you added overrides the inherited Deny Write permission. Click **OK** twice.
29. Close Active Directory Users and Computers and log off.

Working with Forests, Trees, and Domains

In the day-to-day administration of an Active Directory domain, most administrators focus on OUs and their child objects. In a small organization, a solid understanding of OUs and leaf objects might be all that’s needed to manage a Windows domain successfully. However, in large organizations, building an Active Directory structure composed of several domains, multiple trees, and even a few forests might be necessary.

When the first domain controller is installed in a network, the structure you see in Active Directory Users and Computers—a domain object and some folder and OU containers—isn’t all that’s created. In addition, the root of a new tree and the root of a new forest are created, along with elements that define a new site. As a business grows or converts an existing network structure to Active Directory, there might be reasons to add domains to the tree, create new trees or forests, and add sites to the Active Directory structure. This section starts by describing some helpful terms for understanding how Active Directory operates and is organized. Next, the forest’s role in Active Directory is explained, along with using multiple forests in an Active Directory structure. Then you examine trust relationships and domains, particularly situations involving multiple domains and multiple trees.

Active Directory Terminology

A number of terms are used to describe Active Directory’s structure and operations. In the following sections, you examine terms associated with directory partitions, operations masters, replication, and trust relationships.

Directory Partitions An Active Directory database has many sections stored in the same file on a domain controller’s hard drive. These sections must be managed by different processes and replicated to other domain controllers in an Active Directory network. Each section of an Active Directory database is referred to as a **directory partition**. There are five directory partition types in the Active Directory database:

- **Domain directory partition**—Contains all objects in a domain, including users, groups, computers, OUs, and so forth. There’s one **domain directory partition** for each domain in

the forest. Changes made to objects in domain directory partitions are replicated to each domain controller in the domain. Some object attributes are also replicated to global catalog servers (described later in “The Importance of the Global Catalog Server”) in all domains. Changes to the domain directory partition can occur on any domain controller in the domain except read-only domain controllers.

- *Schema directory partition*—Contains information needed to define Active Directory objects and object attributes for all domains in the forest. The **schema directory partition** is replicated to all domain controllers in the forest. One domain controller in the forest is designated as the schema master domain controller (discussed in the next section) and holds the only writeable copy of the schema.
- *Global catalog partition*—The **global catalog partition** holds the global catalog, which is a partial replica of all objects in the forest. It stores the most commonly accessed object attributes to facilitate object searches and user logons across domains. The global catalog is built automatically by domain replication of object attributes flagged for inclusion. Administrators can’t make changes to this partition.
- *Application directory partition*—Used by applications and services to hold information that benefits from automatic Active Directory replication and security. DNS is the most common service to use an **application directory partition** for the DNS database. The information in an application directory partition can be configured to replicate to specific domain controllers rather than all domain controllers, thereby controlling replication traffic. There can be more than one application directory partition.
- *Configuration partition*—By default, the **configuration partition** holds configuration information that can affect the entire forest, such as details on how domain controllers should replicate with one another. Applications can also store configuration information in this partition. This partition is replicated to all domain controllers in the forest, and changes can be made to information stored in this partition on all domain controllers.



Operations Master Roles A number of operations in a forest require having a single domain controller, called the **operations master**, with sole responsibility for the function. In most cases, the first domain controller in the forest takes on the role of operations master for these functions. However, you can transfer the responsibility to other domain controllers when necessary. There are five operations master roles, referred to as **Flexible Single Master Operation (FSMO) roles** (discussed more in Chapter 10), in an Active Directory forest:

- *Schema master*—As mentioned, the schema partition can be changed on only one domain controller, the schema master. This domain controller is responsible for replicating the schema directory partition to all other domain controllers in the forest when changes occur.
- *Infrastructure master*—This domain controller is responsible for ensuring that changes made to object names in one domain are updated in references to these objects in other domains. For example, if a user account in Domain A is a member of a group in Domain B and the user account name is changed, the infrastructure master in Domain A is responsible for replicating the change to Domain B. By default, the first domain controller in each domain is the infrastructure master for that domain.
- *Domain naming master*—This domain controller manages adding, removing, and renaming domains in the forest. There’s only one domain naming master per forest, and the domain controller with this role must be available when domains are added, deleted, or renamed.
- *RID master*—All objects in a domain are identified internally by a **security identifier (SID)**. An object’s SID is composed of a domain identifier, which is the same for all objects in the domain, and a **relative identifier (RID)**, which is unique for each object. Because objects can be created on any domain controller, there must be a mechanism that keeps two domain controllers from issuing the same RID, thereby duplicating an SID. The RID master is responsible for issuing unique pools of RIDs to each domain controller, thereby guaranteeing unique SIDs throughout the domain. There’s one RID master per domain.

- **PDC emulator master**—This role provides backward compatibility with Windows NT servers configured as Windows NT backup domain controllers or member servers. In addition, the PDC emulator master manages password changes to help ensure that user authentication occurs without lengthy delays. When a user account password is changed, the change is replicated to all domain controllers but can take several minutes. Meanwhile, the user whose password was changed might be authenticated by a domain controller that hasn't yet received the replication, so the authentication fails. To reduce this problem, password changes are replicated immediately to the PDC emulator master, and if authentication fails at one domain controller, the attempt is retried on the PDC emulator master.

Active Directory uses a multimaster method for replicating Active Directory object data (such as user and computer accounts), as discussed in the next section. However, because domain controllers that manage FSMO role data are, by definition, single masters, special attention must be paid to them. When removing domain controllers from a forest, make sure these roles aren't removed from the network accidentally. Domain administrators should keep track of which server holds each role and move the role to another domain controller if that machine is to be taken offline.



Activity 4-6: Viewing the Operations Master Roles

Time Required: 15 minutes

Objective: Discover where operations master roles are configured.

Description: You're a consultant called in to document the Active Directory configuration for a company, in particular the operations master roles. You use Active Directory Users and Computers, Active Directory Domains and Trusts, and Active Directory Schema to view these roles.

1. Log on to your server as Administrator, if necessary, and open Active Directory Users and Computers.
2. Right-click **Active Directory Users and Computers** [serverXX.w2k8adXX.com], point to **All Tasks**, and click **Operations Masters**.
3. The RID tab shows which domain controller performs the RID master role. Click the **Change** button. The error message tells you that the DC you're connected to is the operations master, and you must first connect to the domain controller to which you want to transfer the operations master role. Click **OK**.
4. Click the **PDC** tab to view the DC that's the PDC emulator master. Click the **Infrastructure** tab to view the DC that's the infrastructure master. These operations master roles are performed by only one DC per domain. Click **Close**.
5. Right-click **Active Directory Users and Computers** [serverXX.w2k8adXX.com] and click **Change Domain Controller**. If your domain had more than one DC, you could connect to any of them here, and then change the operations master role to the chosen DC. Click **Cancel**. Close Active Directory Users and Computers.
6. Click **Start**, point to **Administrative Tools**, and click **Active Directory Domains and Trusts**.
7. Right-click **Active Directory Domains and Trusts** [serverXX.W2k8adXX.com] and click **Operations Master**. Here's where you can find which DC is the domain naming master. Note that only one DC in the forest performs this function. Click **Close**. Close Active Directory Domains and Trusts.
8. To view the schema master, you must use a different process because this role isn't shown in any of the standard MMCs. Click **Start**, **Run**, type **regsvr32 schmmgmt.dll** in the Open text box, and click **OK**. In the message box stating that DllRegisterServer in schmmgmt.dll succeeded, click **OK**.



This command is necessary to register, or activate, certain commands that aren't normally available in Windows—in this case, the Active Directory Schema snap-in.

9. Click **Start, Run**, type **MMC** in the Open text box, and click **OK**.
10. Click **File, Add/Remove Snap-in** from the MMC menu.
11. In the Available snap-ins list box, click **Active Directory Schema**. Click **Add**, and then click **OK**.
12. Right-click **Active Directory Schema** and click **Operations Master**. Note that only one DC in the entire forest performs the schema master role. Click **Close**. When prompted to save your console settings, click **No**. Close all open windows.

Active Directory Replication Replication is the process of maintaining a consistent database of information when the database is distributed among several locations. Active Directory contains several databases called partitions that are replicated between domain controllers by using intrasite replication or intersite replication. **Intrasite replication** is replication between domain controllers in the same site; **intersite replication** occurs between two or more sites. (Sites are discussed in more detail later in “Understanding Sites.”) The replication process differs in these two types, but the goal is the same—to maintain a consistent set of domain directory partitions.

Active Directory uses **multimaster replication** for replicating Active Directory objects, such as user and computer accounts, which means changes to these objects can occur on any domain controller and are propagated, or replicated, to all other domain controllers. Intrasite replication occurs between replication partners in an Active Directory site; a replication partner is a pair of domain controllers configured to replicate with one another. A process called the **Knowledge Consistency Checker (KCC)** runs on every domain controller to determine the replication topology, which defines the domain controller path that Active Directory changes flow through. This path is configured as a ring (or multiple rings, if there are enough domain controllers), with each domain controller in the path constituting a hop. The KCC is designed to ensure no more than three hops between any two domain controllers, which can result in multiple rings, as shown in Figure 4-9.

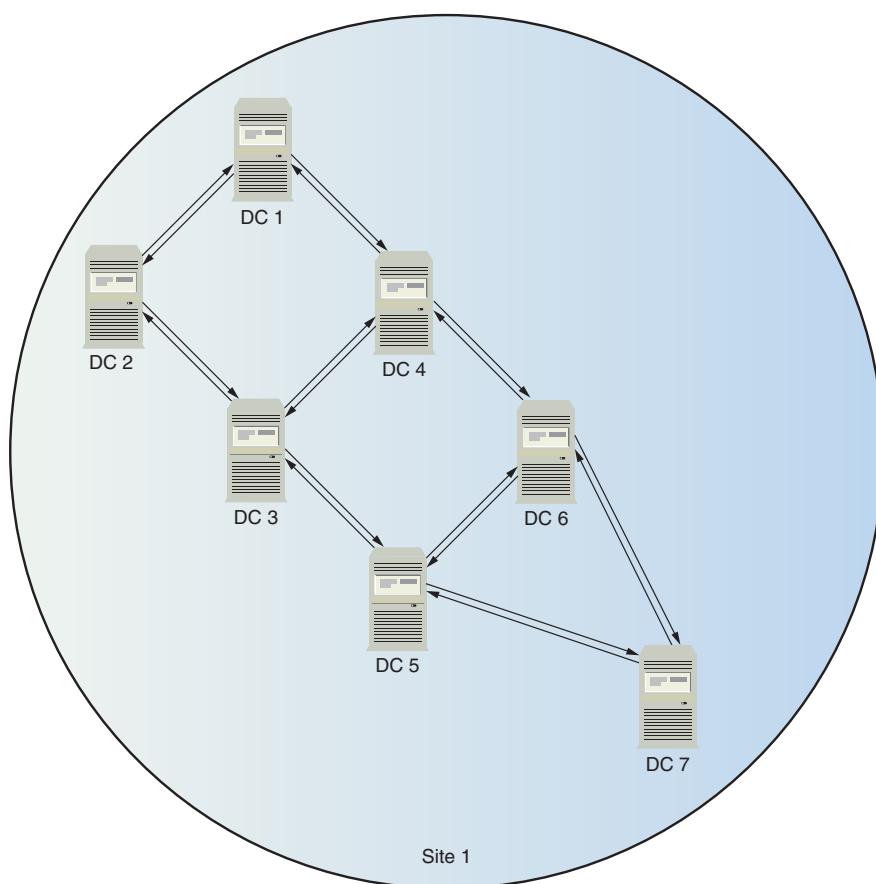


Figure 4-9 Replication topology

Intrasite replication occurs 15 seconds after a change is made on a domain controller, with a 3-second delay between each replication partner. The KCC also configures the topology for intersite replication, but it's different from intrasite replication's topology (discussed later in "Understanding Sites").

Trust Relationships In Active Directory, a **trust relationship** defines whether and how security principals from one domain can access network resources in another domain. Windows NT domains must be specifically configured with trust relationships before users in one domain can access resources in another domain. Starting with Windows 2000 and Active Directory, trust relationships are established automatically between all domains in the forest. Therefore, when a user authenticates to one domain, the other domains in the forest accept, or trust, the authentication.



Although trusts between domains in the same forest are created automatically, there's no automatic trust between domains in separate forests.

NOTE

Don't confuse trusts with permissions. Permissions are still required to access resources, even if a trust relationship exists. When there's no trust relationship between domains, however, no access across domains is possible. Because all domains in a forest have trust relationships with one another automatically, trusts must be configured only when your Active Directory environment includes two or more forests or when you want to integrate with other OSs. Trusts are discussed in more detail later in "Understanding Trusts."

The Role of Forests

The Active Directory forest is the broadest logical component of the Active Directory structure. Forests contain domains that can be organized into one or more trees. All domains in a forest share some common characteristics:

- *A single schema*—The schema defines Active Directory objects and their attributes and can be changed by an administrator or an application to best suit the organization's needs. All domains in a forest share the same schema, so a change to the schema affects objects in all domains. This shared schema is one reason that large organizations or conglomerates with diverse business units might want to operate as separate forests. With this structure, domains in different forests can still share information through trust relationships, but changes to the schema—perhaps from installing an Active Directory-integrated application, such as Microsoft Exchange—don't affect the schema of domains in a different forest.
- *Forestwide administrative accounts*—Each forest has two groups defined with unique rights to perform operations that can affect the entire forest: Schema Admins and Enterprise Admins. Members of Schema Admins are the only users who can make changes to the schema. Members of Enterprise Admins can add or remove domains from the forest and have administrative access to every domain in the forest. By default, only the Administrator account for the first domain created in the forest is a member of these two groups.
- *Operations masters*—As discussed, certain forestwide operations can be performed only by a domain controller designated as the operations master. Both the schema master and the domain naming master are forestwide operations masters, meaning only one domain controller in the forest can perform these roles.
- *Global catalog*—There's only one global catalog per forest, but unlike operations masters, multiple domain controllers can be designated as global catalog servers. Because the global catalog contains information about all objects in the forest, it's used to speed searching for objects across domains in the forest and to allow users to log on to any domain in the forest.
- *Trusts between domains*—These trusts allow users to log on to their home domains (where their accounts are created) and access resources in domains throughout the forest without having to authenticate to each domain.

- *Replication between domains*—The forest structure facilitates replicating important information among domain controllers throughout the forest. Forestwide replication includes information stored in the global catalog, schema directory, and configuration partitions.

The Importance of the Global Catalog Server The first domain controller installed in a forest is designated as a global catalog server, but you can use Active Directory Sites and Services to configure additional domain controllers as global catalog servers for redundancy. The following are some vital functions the global catalog server performs:

- *Facilitates domain and forestwide searches*—As discussed, the global catalog is contacted to speed searches for resources across domains.
- *Facilitates logon across domains*—Users can log on to computers in any domain by using their **user principal name (UPN)**. A UPN follows the format *username@domain*. Because the global catalog contains information about all objects in all domains, a global catalog server is contacted to resolve the UPN. Without a global catalog server, users could log on only to computers that were members of the same domain as their user accounts.
- *Hold universal group membership information*—When a user logs on to the network, all the user's group memberships must be resolved to determine rights and permissions. Global catalog servers are the only domain controllers that hold universal group membership information, so they must be contacted when a user logs on. A universal group (discussed in Chapter 5) is the only type of group that can contain accounts from other domains, which is why this information must be stored in the global catalog.

4

Because of the critical functions a global catalog server performs, having at least one domain controller configured as a global catalog server in each corporate location is a good idea to speed logons and directory searches for users in all locations.



Activity 4-7: Configuring a Global Catalog Server

Time Required: 5 minutes

Objective: Use Active Directory Sites and Services to see how to configure a global catalog server.

Description: You have installed a domain controller at a branch office. You have heard about the importance of having a global catalog server at all locations. A junior administrator is currently at the branch office, and you want to be able to instruct her on how to configure the domain controller.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Active Directory Sites and Services**.
3. Click to expand the **Sites** node, if necessary. Click to expand **Default-First-Site-Name**, **Servers**, and then **ServerXX**. Your screen should look similar to Figure 4-10.

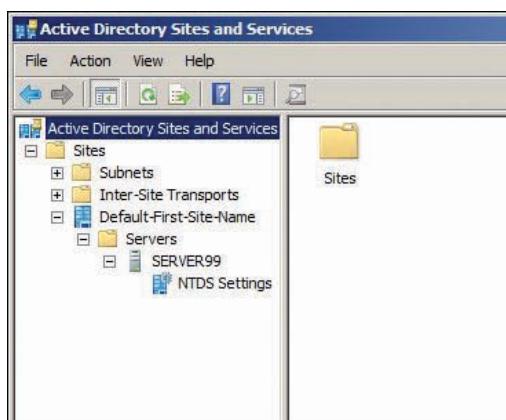


Figure 4-10 Active Directory Sites and Services

4. Right-click **NTDS Settings** under ServerXX and click **Properties**. Click the **General** tab, if necessary. When the Global Catalog check box is selected, the domain controller is a global catalog server. Because it's the only global catalog server in the forest, clearing the check box generates a warning message stating that users can't log on if there's no global catalog server. Click **Cancel**.
5. Right-click **ServerXX** and click **Properties**. Click the **General** tab, if necessary. Note that Global Catalog is specified in the DC Type text box. Click **Cancel**. Close Active Directory Sites and Services.

Forest Root Domain As discussed, when the first domain is created in a Windows network, the forest root is also created. In fact, the first domain *is* the forest root and is referred to as the **forest root domain**. It has a number of important responsibilities and serves as an anchor for other trees and domains added to the forest. Certain functions that affect all domains in the forest are conducted only through the forest root domain, and if this domain becomes inoperable, the entire Active Directory structure ceases functioning. Figure 4-11 shows the forest root domain with multiple domains and trees. In Chapter 3, Figure 3-4 showed the same structure, but for simplicity, it didn't show one of the domains as the forest root.

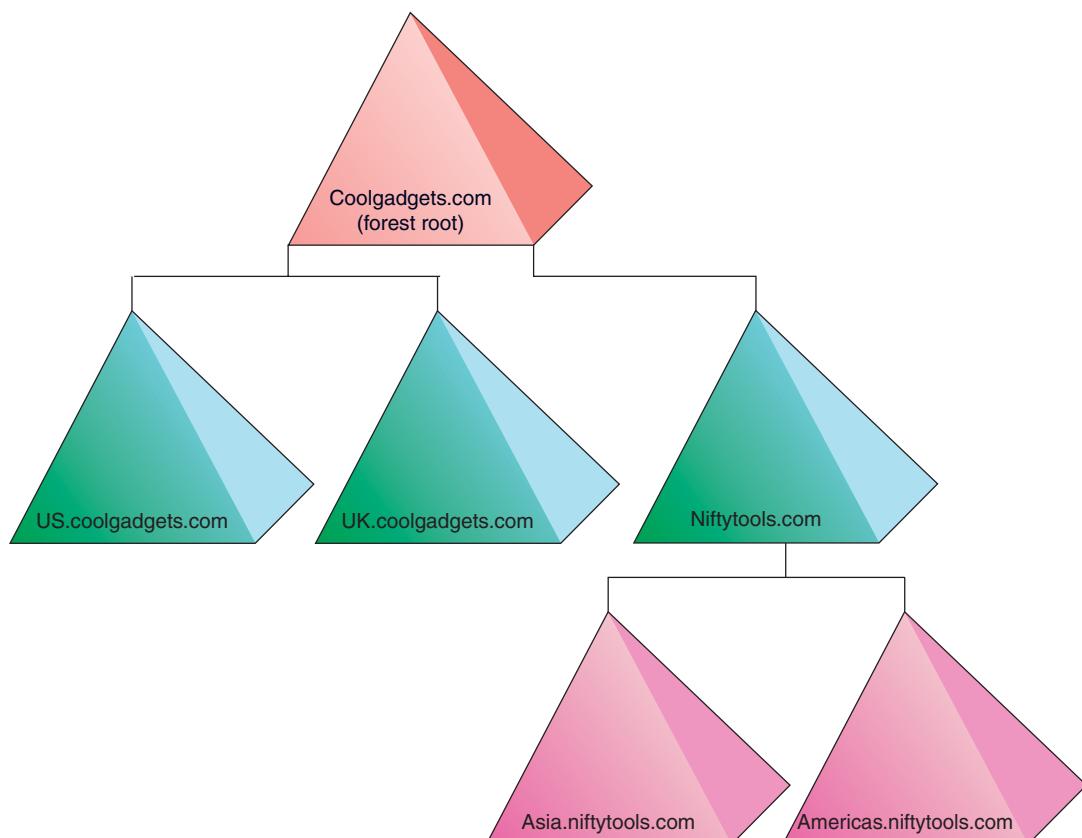


Figure 4-11 The forest root domain

What makes the forest root domain so important? It provides functions that facilitate and manage communication between all domains in the forest as well as between forests, if necessary. Some functions the forest root domain usually handles include the following:

- DNS server
- Global catalog server
- Forestwide administrative accounts
- Operations masters

The DNS server and global catalog server functions can be installed on other servers in other domains for fault tolerance. However, the forestwide operations masters and forestwide administrative accounts can reside only on a domain controller in the forest root domain. For these reasons, the forest root domain is a critical component of the Active Directory structure.

Because of the forest root domain's functionality and security, some organizations choose a **dedicated forest root domain**, which contains only the forestwide administrative accounts and domain controllers needed to run the forestwide operations master roles. No additional OUs or server roles are installed. The advantages of running a dedicated forest root domain include the following:

- **More secure**—Limiting who can make forestwide changes, such as adding and deleting domains and modifying schemas, is easier. Only members of the forestwide administrative accounts can make these changes, and having a dedicated domain makes restricting membership in these groups easier.
- **More manageable**—The directory database is small because of the limited number of objects it holds, making backups and restores easier and faster. A small directory that requires few changes also makes replication fast because little traffic is generated. Reduced traffic makes it easy to place domain controllers for the forest root domain in multiple locations for redundancy.
- **More flexible**—In the event of a company name change that can result in a domain name change, the forest root domain need not be disturbed. You can use a generic name for the forest root domain because it doesn't contain any resources that users will access. For example, you could add a dedicated forest root domain to the forest in Figure 4-11, giving it a generic name that isn't used on the Internet or in the company to access network resources. The resulting forest might look like Figure 4-12.

4

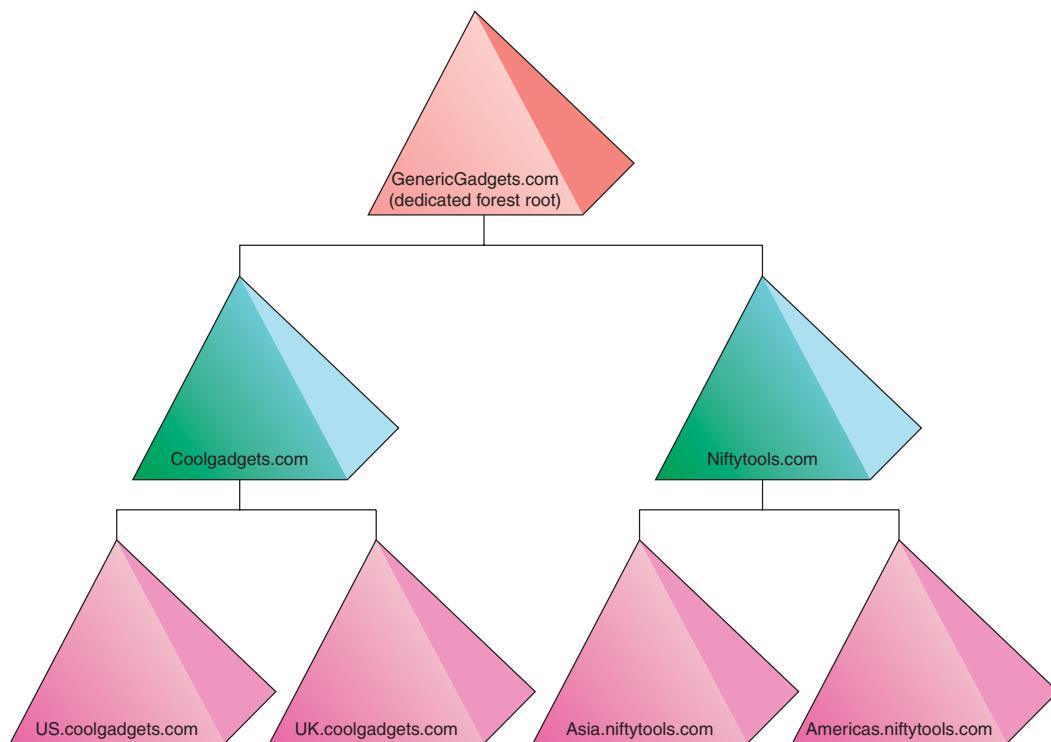


Figure 4-12 A dedicated forest root domain

The advantages of having a dedicated forest root are compelling, particularly for organizations with a multiple domain structure. Whether the forest root is dedicated or not, its importance to the overall health of the Active Directory structure can't be overstated. Membership in forestwide groups should be restricted to only the most knowledgeable administrators, and regular backup and maintenance of domain controllers is paramount.

Choosing a Single or Multiple Forest Design

Most organizations operate under a single Active Directory forest, which has a number of advantages:

- *A common Active Directory structure*—Forestwide replication and a single schema for the forest provide a consistent, reliable directory service.
- *Easy access to network resources*—The global catalog and forestwide trusts make finding and accessing resources across domains easy.
- *Centralized management*—A single administrative unit to manage all aspects of the directory simplifies administering and implementing network policies.

Ironically, the advantages of a single forest structure entail limitations that might lead an organization to design its Active Directory structure around multiple forests. Some large organizations can consist of a collection of diverse business units. Companies merge, are taken over, reorganize, open foreign offices, and so forth, creating what amounts to several businesses under the umbrella of a single corporation. Each business unit might have widely differing management policies and be running different business applications. Having this amount of diversity with a single Active Directory forest often requires a high level of cooperation or might be technically unfeasible. Some reasons, technical and administrative, that a company might choose a multiple forest design include the following:

- *The need for differing schemas*—For example, when two businesses merge, each might have an existing Active Directory structure with customized schema elements that are incompatible with one another.
- *Security boundaries*—By default, directory information in one forest isn't accessible, or even visible, to users in a different forest, which makes the forest a security boundary. However, trusts can be configured between domains in different forests so that administrators can control cross-forest access.
- *Separate administration*—When multiple business units have separate IT administration, there might be disagreement on policies that affect the entire forest. Whether differences are technical or political, a multiple forest design could be the best solution.

Organizations that do use multiple forests usually must configure trusts between the forests, as you learn in the following section.

Understanding Trusts

Active Directory trusts can exist between domains and between forests. With a trust relationship between domains in the same forest or in different forests, users can access resources across domains without having to log on more than once. Moreover, a user account needs to exist in only one domain, which simplifies user management.

To say that Domain A trusts Domain B means that users in Domain B can be given permission to access resources in Domain A. Domain A is referred to as the trusting domain, and Domain B is referred to as the trusted domain. In Active Directory design documentation, a trust relationship is drawn with an arrow pointing from the trusting domain to the trusted domain, as shown in Figure 4-13. There are a number of trust relationship types, explained in the following sections: one-way and two-way trusts, transitive trusts, shortcut trusts, forest trusts, external trusts, and realm trusts.

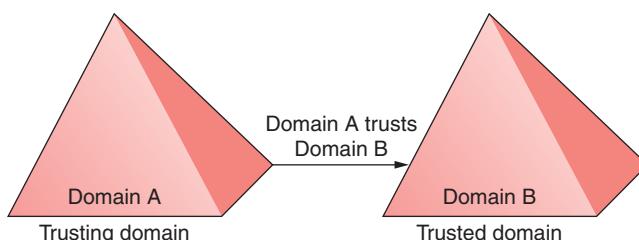


Figure 4-13 A trust relationship

One-Way and Two-Way Trusts A **one-way trust** exists when one domain trusts another, but the reverse is not true, as in Figure 4-13. Domain A trusts Domain B, but Domain B doesn't trust Domain A. So although Domain B's users can be given access to Domain A's resources, Domain A's users can't be given access to Domain B's resources. More common is the **two-way trust**, in which users from both domains can be given access to resources in the other domain.

Transitive Trusts A **transitive trust** is named after the transitive rule of equality in mathematics: If $A=B$ and $B=C$, then $A=C$. When applied to domains, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C. The automatic trust relationships created among domains in a forest are transitive two-way trusts. These trusts in a forest follow the domain parent-child relationship in a tree and flow from the forest root domain to form the trust relationship between trees. Figure 4-14 shows two-way transitive trusts between all domains in a forest. The trust relationship between branches of the tree (US.coolgadgets.com and UK.coolgadgets.com) and between trees flows through the forest root domain.

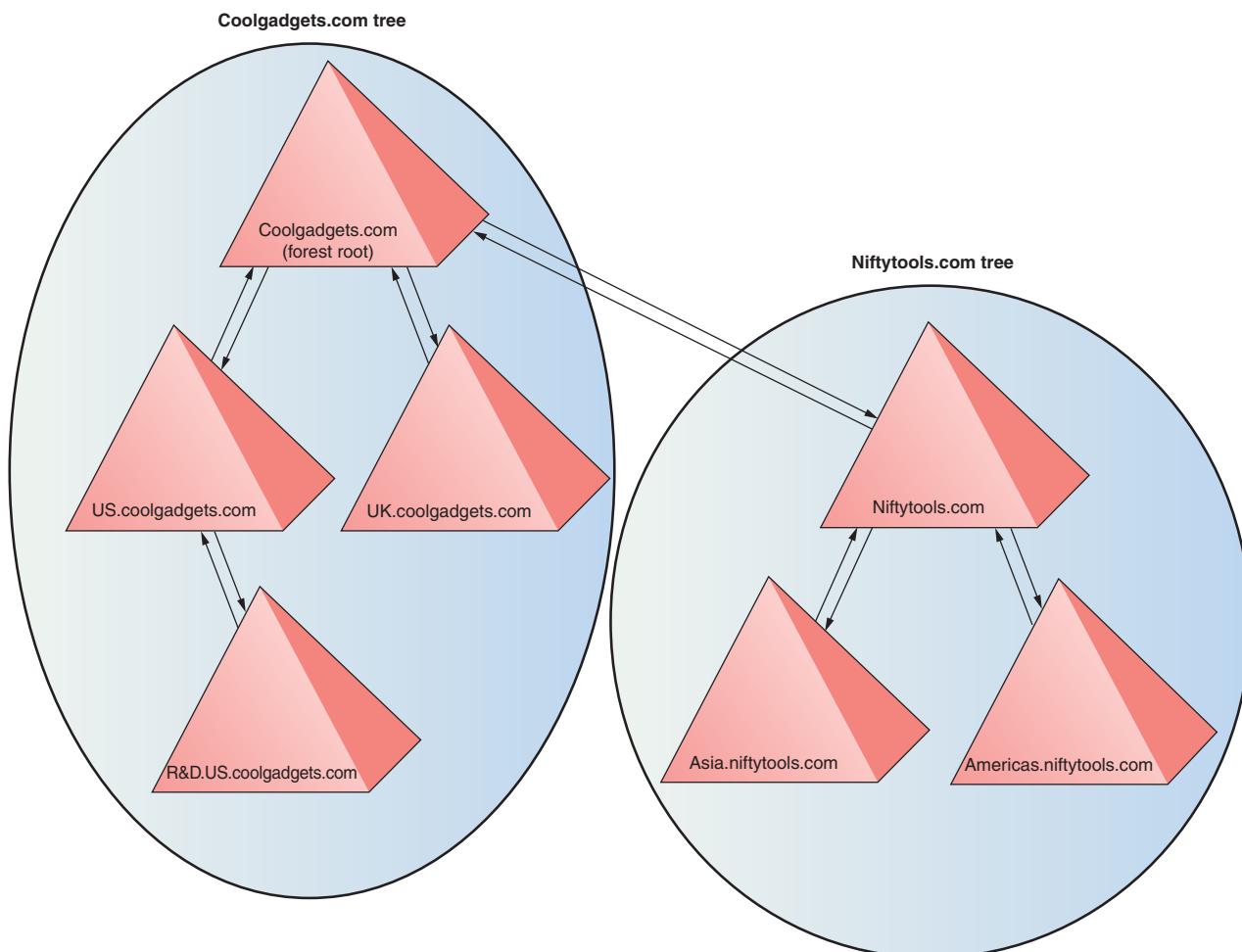


Figure 4-14 Transitive two-way trusts in a forest

The transitive nature of these trust relationships means that R&D.US.coolgadgets.com trusts Asia.niftytools.com because R&D.US.coolgadgets.com trusts US.coolgadgets.com, which trusts Coolgadgets.com, which in turn trusts Niftytools.com, which trusts Asia.niftytools.com. Because the trusts are two-way, the reverse is also true. Unfortunately, for the trust between R&D.US.coolgadgets.com and Asia.niftytools.com to work, authenticating a user in R&D.US.coolgadgets.com must be referred to a domain controller in each domain in the path to Asia.niftytools.com. This authentication referral process can cause substantial delays when a

user wants to access resources in a domain that's several referrals away. Fortunately, there's a solution to this problem in the form of shortcut trusts.

Shortcut Trusts A **shortcut trust** is configured manually between domains to bypass the normal referral process. Figure 4-15 shows the same forest as Figure 4-14 but with a manually configured two-way shortcut trust between R&D.US.coolgadgets.com and Asia.niftytools.com.

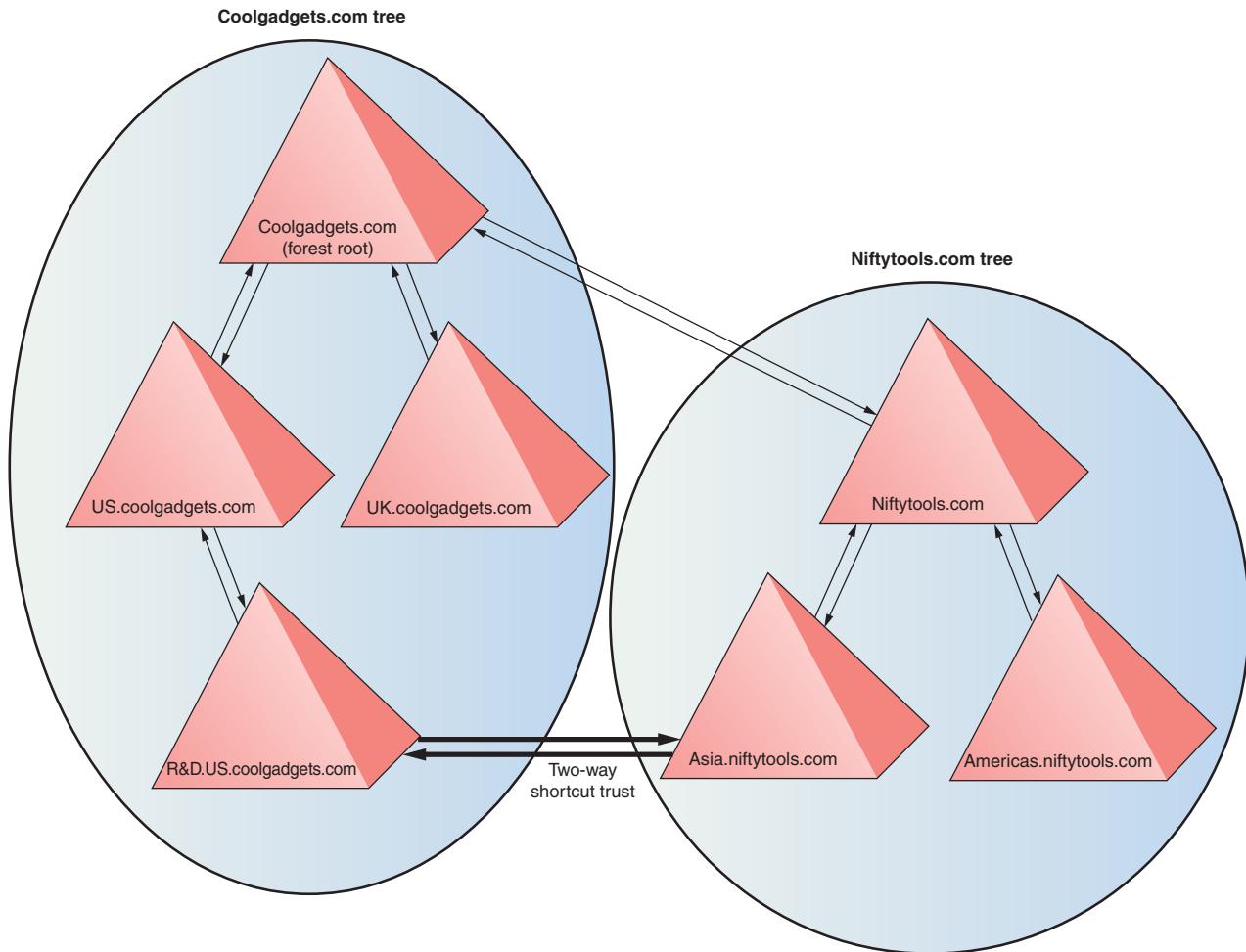


Figure 4-15 A two-way shortcut trust

Shortcut trusts are transitive and can be configured as one-way or two-way trusts between domains in the same forest. Generally, they're configured when user accounts often need to access resources in domains that are several referrals away. If the Active Directory design includes multiple forests, older Windows OSs, or non-Windows OSs in which resources must be shared, additional trust options are available: forest trusts, external trusts, and realm trusts.

Forest Trusts A **forest trust** provides a one-way or two-way transitive trust between forests that allows security principals in one forest to access resources in any domain in another forest. It's created between the forest root domains of two Windows Server 2008 or Windows Server 2003 forests. Forest trusts aren't possible in Windows 2000 forests. A forest trust is transitive to the extent that all domains in one forest trust all domains in the other forest. However, the trust isn't transitive from one forest to another. For example, if a forest trust is created between Forest A and Forest B, all domains in Forest A trust all domains in Forest B. If there's a third forest, Forest C, and Forest B trusts Forest C, a trust relationship isn't established automatically between Forest A and Forest C. A separate trust must be configured manually between these two forests.

A forest trust is a powerful tool when having a trust relationship between all domains in two separate forests is an advantage. If the need for a trust relationship is limited to just a few domains in different forests, however, an external trust is required.

External Trusts An **external trust** is a one-way or two-way nontransitive trust between two domains that aren't in the same forest. External trusts are generally used in these circumstances:

- *To create a trust between two domains in different forests*—If no forest trust exists, an external trust can be created to allow users in one domain to access resources in another domain in a different forest. If a forest trust does exist, an external trust can still be used to create a direct trust relationship between two domains. This option can be more efficient than a forest trust when access between domains is frequent, much like a shortcut trust is used in a forest.
- *To create a trust with a Windows 2000 or Windows NT domain*—You can't create a forest trust between a Windows Server 2008 or 2003 forest and a Windows 2000 forest or Windows NT domain. An external trust must be used to create the trust relationship between domains.

Realm Trusts Today's networks are often composed of systems running different OSs, such as Windows, Linux, UNIX, and Mac OS. A **realm trust** can be used to integrate users of other OSs into a Windows Server 2008 domain or forest. It requires the OS to be running the Kerberos V5 authentication system that Active Directory uses. **Kerberos** is an open-standard security protocol used to secure authentication and identification between parties in a network.



Activity 4-8: Configuring Trusts

Time Required: 5 minutes

Objective: Perform the beginning steps of creating a forest trust relationship with a partner.

Description: Before a forest trust can be created, you need more knowledge of DNS and how to configure additional DNS zones or DNS forwarders. The actual building of the trust is done in Chapter 10. For now, you explore Active Directory Domains and Trusts to become familiar with this tool.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Active Directory Domains and Trusts**.
3. Right-click the domain node in the left pane and click **Properties**. Click the **Trusts** tab, shown in Figure 4-16.

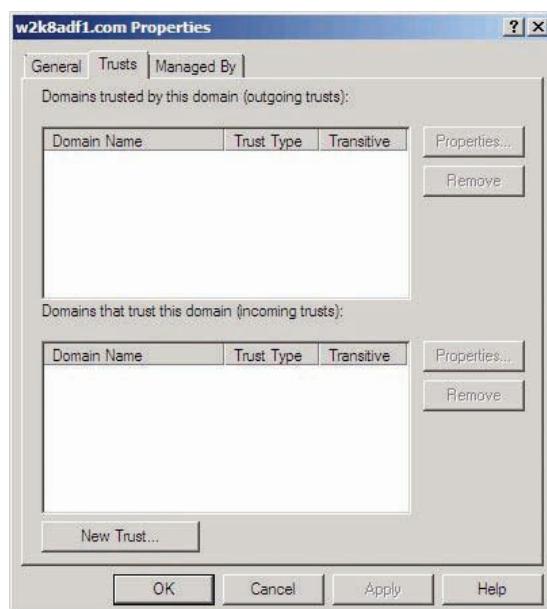


Figure 4-16 The Trusts tab

4. Click the **New Trust** button to start the New Trust Wizard. Note the types of trusts you can create with the wizard, and then click **Next**.
5. At this point, you enter the name of the forest with which you want to create a trust. However, for this step to work, the DNS server in your domain must be able to resolve the other forest name. This capability requires additional configuration of your DNS server, which is covered in Chapter 9. For now, click **Cancel**, and then click **Cancel** again. Close Active Directory Domains and Trusts.

Understanding Domains and Trees

As discussed in Chapter 3, an Active Directory tree is a grouping of domains that share a common naming structure. A tree can consist of a single domain or a parent domain and one or more child domains, which can also have child domains of their own. An Active Directory tree is said to have a contiguous namespace because all domains in the tree share at least the last two domain name components: the second-level domain name and the top-level domain name. For example, coolgadgets.com has a second-level domain name of coolgadgets and a top-level domain name of com.

Organizations operating under a single name internally and to the public are probably best served by an Active Directory forest with only one tree. However, when two companies merge or a large company splits into separate business units that would benefit from having their own identities, a multiple tree structure makes sense. As you've learned, there's no major functional difference between domains in the same tree or domains in different trees, as long as they're part of the same forest. They're all covered by the same transitive two-way trust afforded by the forest structure. The only operational difference is the necessity of maintaining multiple DNS zones (discussed in Chapter 9).

Designing the Domain Structure The domain is the primary identifying and administrative unit in Active Directory. A unique name is associated with each domain and used to access network resources. A domain administrator account has full control over objects in the domain, and certain security policies apply to all accounts in a domain. Additionally, most replication traffic occurs between domain controllers within a domain. Any of these factors can influence your decision to use a single or multidomain design. Most small and medium businesses choose a single domain for reasons that include the following:

- *Simplicity*—The more complex something is, the easier it is for things to go wrong. Unless your organization needs multiple identities, separate administration, or differing account policies, keeping the structure simple with a single domain is the best choice.
- *Lower costs*—Every domain must have at least one domain controller and preferably two or more for fault tolerance. Each domain controller requires additional hardware and software resources, which increases costs.
- *Easier management*—Many management tasks are easier in a single-domain environment:
 - Having a single set of administrators and policies prevents conflicts caused by differing viewpoints on operational procedures and policies.
 - Object management is easier when personnel reorganizations or transfers occur. Moving user and computer accounts between different OUs is easier than moving them between different domains.
 - Managing access to resources is simplified when you don't need to consider security principals from other domains.
 - Placement of domain controllers and global catalog servers is simplified when your organization has multiple locations because you don't need to consider cross-domain replication.
- *Easier access to resources*—A single domain provides the easiest environment for users to find and access network resources. In a multi domain environment, mobile users who

frequent branch offices with different domains must authenticate to their home domain. If their home domain isn't available for some reason, they can't log on to the network.

Although a single domain structure is usually easier and less expensive than a multidomain structure, it's not always better. Using more than one domain makes sense or is even a necessity in the following circumstances:

- *Compatibility with a Windows NT domain*—If you need to maintain an existing Windows NT domain structure, the easiest option is to use multiple domains and create an external trust between them.
- *Need for differing account policies*—Account policies that govern password and account lockout policies apply to all users in a domain. If you need to have differing policies for different business units, using separate domains is the best way to meet this requirement. A new feature in Windows Server 2008 called fine-grained password policies can be used to apply different password policies for users or groups in a domain, but this feature can be difficult to manage when many users are involved.
- *Need for different name identities*—Each domain has its own name that can represent a separate company or business unit. If each business unit must maintain its own identity, child domains can be created in which part of the name is shared, or multiple trees with completely different namespaces can be created.
- *Replication control*—Replication in a large domain maintaining several thousand objects can generate substantial traffic. When multiple corporate locations are connected through a WAN, the amount of replication traffic could be unacceptable. Replication traffic can be reduced by creating separate domains for key locations because only global catalog replication is required between domains.
- *Need for internal versus external domains*—Companies that run public Web servers often create a domain used only for publicly accessible resources and another domain used for internal resources.
- *Need for tight security*—With separate domains, stricter resource control and administrative permissions are easier. If a business unit prefers to have its own administrative staff, separate domains must be created.



Understanding Sites

As discussed in Chapter 2, a site is one of Active Directory's physical components, along with a domain controller. An Active Directory site represents a physical location where domain controllers are placed and group policies can be applied. When you're designing the logical components of Active Directory, such as domains and OUs, you don't need to consider the physical location of objects. In other words, an OU named Accounting could contain user accounts from both Chicago and New Orleans, and the domain controllers holding the Active Directory database could be located in San Francisco and New York. As long as there's a network connection between the location where a user logs on and the location of the domain controller, the system works.

Having said that, having a domain controller near the accounts using it makes sense. Authentication and resource access works fine across a WAN link, but if a corporate location contains several users, placing domain controllers in that location is more efficient. Performance and reliability are less predictable on slower WAN links than on LAN links. So the extra cost of additional domain controllers can be outweighed by the productivity gained from faster, more reliable network access.

When the first domain controller of a forest is installed, a site is created named Default-First-Site-Name. Any additional domain controllers installed in the forest are assigned to this site until additional sites are created. Figure 4-17 depicts a single-site domain in two locations at the top and the same domain defined as two sites at the bottom.

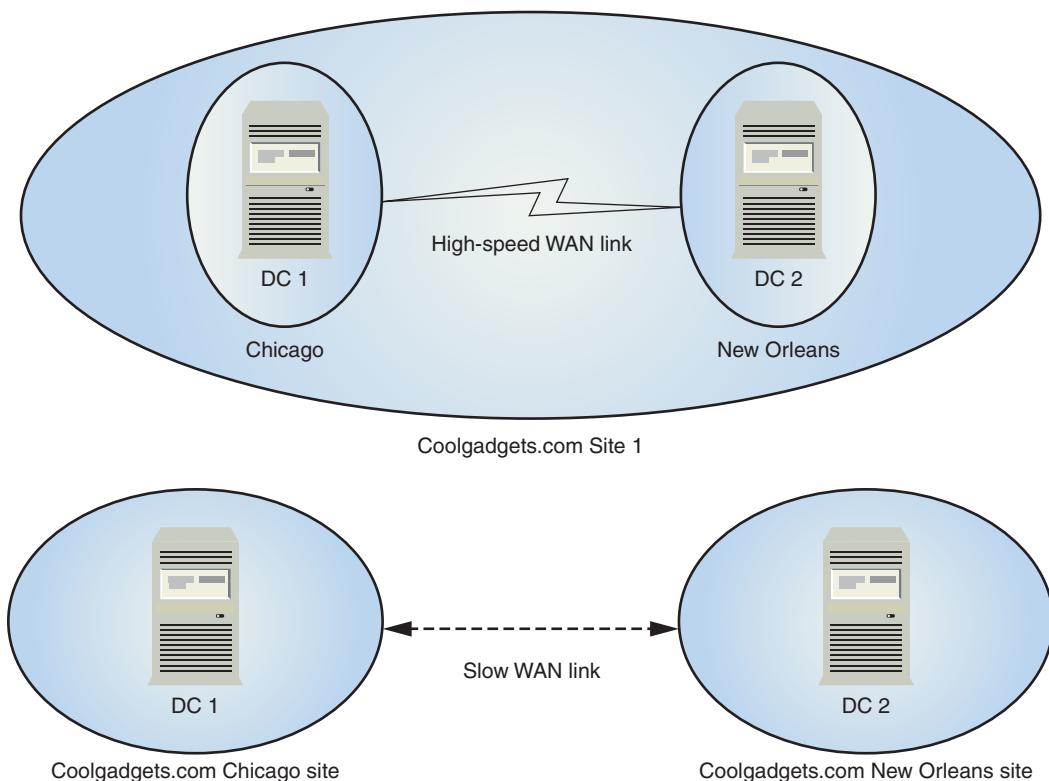


Figure 4-17 Active Directory sites

There are three main reasons for establishing multiple sites:

- *Authentication efficiency*—When a user logs on to a domain, the client computer always tries to authenticate to a domain controller in the same site to ensure that logon traffic is kept in the same site and off slower WAN links.
- *Replication efficiency*—A domain controller in every branch office facilitates faster and more reliable network access, but domain controllers must communicate with one another to replicate the Active Directory database. Using the default replication schedule, however, can create considerable replication traffic. Replication between domain controllers occurs within 15 seconds after a change is made and once per hour when no changes have occurred. In databases with several thousand objects, this schedule can take a toll on available bandwidth needed for other network operations. With multiple sites, intersite replication can be scheduled to occur during off-peak hours and at a frequency that makes most sense. For example, a small branch office site with a limited bandwidth connection to the main office can be configured to replicate less often than a larger branch office that requires more timely updates.
- *Application efficiency*—Some distributed applications, such as Exchange Server (an e-mail and collaboration application) and Distributed File System (DFS), use sites to improve efficiency. These applications ensure that client computers always try to access data in the same site before attempting to use the WAN link.

Sites are created by using Active Directory Sites and Services. A site is linked to an IP subnet that reflects the IP addressing scheme used at the physical location the site represents. A site can encompass one or more IP subnets, but each site must be linked to at least one IP subnet that doesn't overlap with another site. IP subnets are explained more in Chapter 8. When a new domain controller is created and assigned an IP address, it's assigned to a site based on its address automatically. Figure 4-18 shows the relationship between sites and IP subnets.

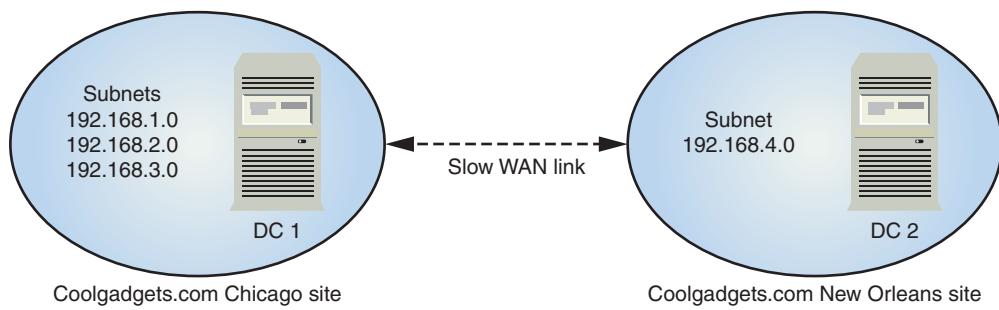


Figure 4-18 Sites and subnets

4

Site Components

Sites and connections between sites are defined by a number of components that can be created and configured in Active Directory Sites and Services. They include subnets, site links, and bridgehead servers, discussed in the following sections.

Subnets As discussed, each site is associated with one or more IP subnets. In short, an IP subnet is a range of IP addresses that a group of computers share. All computers assigned an address in the subnet can communicate with one another without requiring a router. By default, no subnets are created in Active Directory Sites and Services. When a new site is created, all subnets used by the default site should be created and associated with the default site. Then the subnets for the new site should be created and associated with the new site. Figure 4-19 shows Active Directory Sites and Services with the Default-First-Site-Name Properties dialog box open.

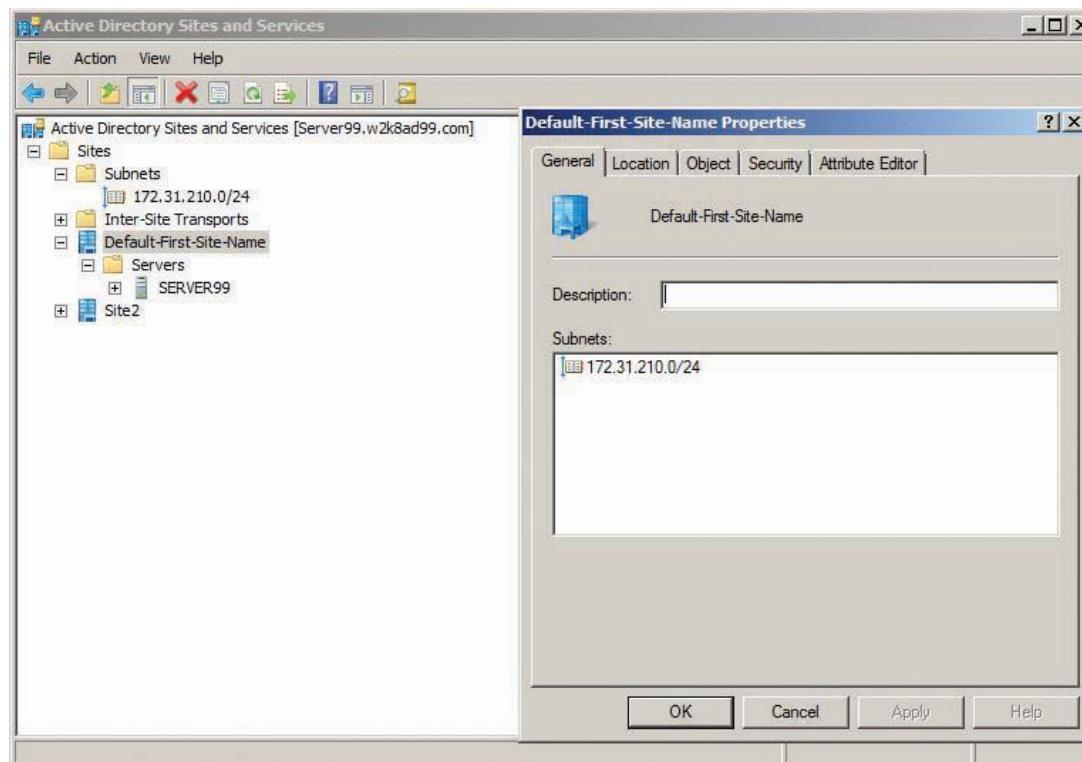


Figure 4-19 The Default-First-Site-Name Properties dialog box



Activity 4-9: Creating a Subnet in Active Directory Sites and Services

Time Required: 5 minutes

Objective: Create a subnet in Active Directory Sites and Services and associate the subnet with a site.

Description: You're creating multiple sites for your Active Directory structure. Before you create the second site, however, you must configure the existing site to use the subnets already in use in your network.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Active Directory Sites and Services**.
3. Double-click to expand **Sites**, if necessary. Right-click **Subnets**, point to **New**, and click **Subnet**.
4. In the Prefix text box, type **192.168.100.0/24** (assuming you're following the IP address scheme used in this book; otherwise, ask your instructor what to enter).
5. In the Select a site object for this prefix list box, click **Default-First-Site-Name**, and then click **OK**.
6. In the left pane, click **Subnets**. Right-click **192.168.100.0/24** and click **Properties**. In the General tab, you can give the subnet a description and change the site the subnet is associated with.
7. Click **Cancel**. Close Active Directory Sites and Services.

Site Links A **site link** is needed to connect two or more sites for replication purposes. When Active Directory is installed, a default site link called **DEFAULTTIPSITELINK** is created. Until new site links are created, all sites that are added use this site link. Site links determine the replication schedule and frequency between two sites. If all locations in an organization are connected through the same WAN link or WAN links of equal bandwidth, a single site link might be suitable. If the locations use different WAN connections at differing speeds, however, additional links can be created to configure differing replication schedules. Site links have three configuration options, as shown in Figure 4-20.

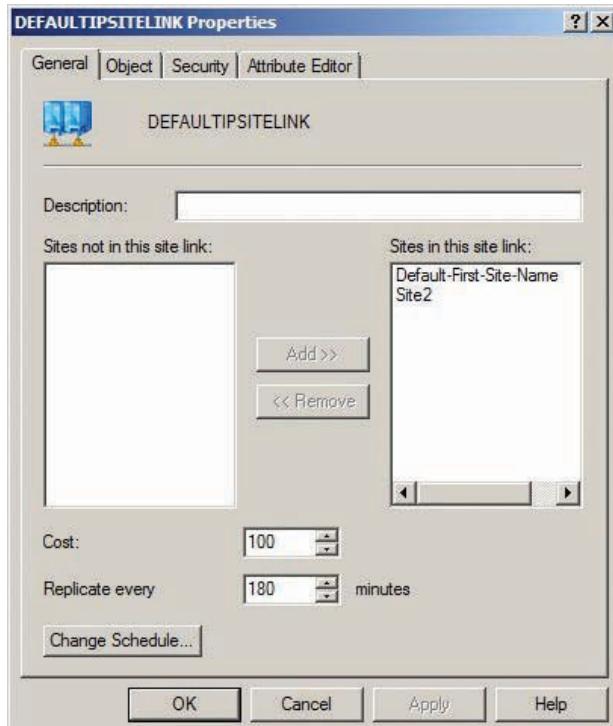


Figure 4-20 The default site link's Properties dialog box

The Cost field is an administrator-assigned value that represents the bandwidth of the connection between sites. The default value is 100. An administrator can alter this value to influence which path is chosen when more than one path exists between two sites. As shown in Figure 4-21, Site A replicates with Site B and Site C through the corresponding site links, but Site A has two options for replicating with Site D: the link with Site B or the link with Site C. The site link cost determines that Site A will use the link with Site B. Site link costs are additive, so the total cost for Site A to replicate with Site D through Site C is 400; the total cost to replicate with Site D via Site B is only 300. When you have more than one path option between two sites, the lower cost path is always used unless links in the path become unavailable. In this case, the replication process reconfigures itself to use the next lower cost path, if available. Site links are transitive by default, which means Site A can replicate directly with Site D, and Site C can replicate directly with Site B, without creating an explicit link between the two sites.

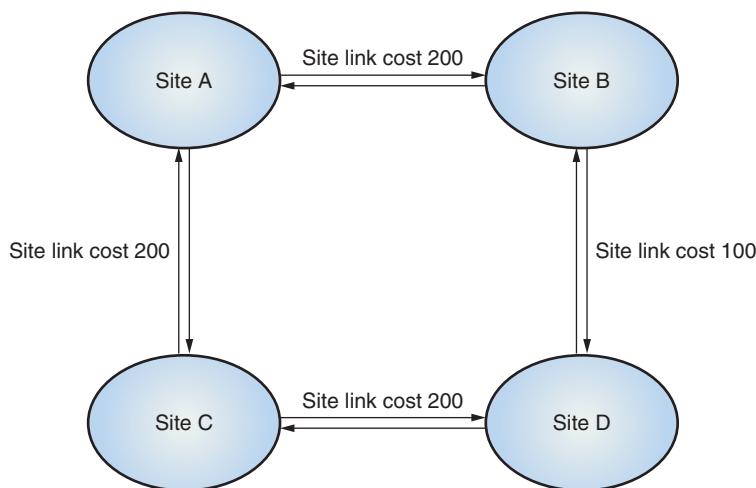


Figure 4-21 Site replication topology

Bridgehead Servers You learned that intrasite replication occurs among several domain controllers after the KCC creates the topology. Intersite replication occurs between bridgehead servers. When the KCC detects that replication must occur between sites, one domain controller in each site is designated as the Inter-Site Topology Generator (ISTG). The ISTG then designates a bridgehead server to handle replication for each directory partition. Because bridgehead servers perform such a vital function in multisite networks, and this function can consume considerable server resources, the administrator can override automatic assignment of a bridgehead server and assign the role to a specific domain controller. Configuration of bridgehead servers is discussed in Chapter 10.

Chapter Summary

- Active Directory is based on the X.500 and LDAP standards, which are standard protocols for defining, storing, and accessing directory service objects.
- OUs, the building blocks of the Active Directory structure in a domain, can be designed to mirror a company's organizational chart. Delegation of control can be used to give certain users some management authority in an OU. You need to be familiar with OU permissions and permission inheritance to understand delegation of control.
- Large organizations might require multiple domains, trees, and forests. Some terms for describing the Active Directory structure include directory partitions, operations master roles, Active Directory replication, and trust relationships.

- Directory partitions are sections of the Active Directory database that hold varied types of data and are managed by different processes. Directory partitions can be replicated from one domain controller to another. FSMO roles are functions carried out by a single domain controller per domain or forest and perform vital functions that affect Active Directory operations.
- The forest is the broadest logical Active Directory component. All domains in a forest share some common characteristics, such as a single schema, the global catalog, and trusts between domains. The global catalog facilitates several important functions, such as cross-domain logon and forestwide searching. The forest root domain is the first domain created in a forest.
- Trusts permit domains to accept user authentication from another domain and facilitate cross-domain and cross-forest resource access with a single logon. The types of trusts an administrator can create include shortcut trusts, forest trusts, realm trusts, and external trusts.
- A domain is the primary identifying and administrative unit of Active Directory. Each domain has a unique name, and there's an administrative account with full control over objects in the domain. Some organizations can benefit by using multiple domains when different security or account policies are required, among other reasons. A tree consists of one or more domains with a contiguous namespace. An Active Directory forest might require multiple trees when an organization is composed of companies with a noncontiguous namespace.
- An Active Directory site represents a physical location where domain controllers reside. Multiple sites are used for authentication efficiency, replication efficiency, and application efficiency. Site components include subnets, site links, and bridgehead servers.

Key Terms

application directory partition A directory partition that applications and services use to store information that benefits from automatic Active Directory replication and security.

configuration partition A directory partition that stores configuration information that can affect the entire forest, such as details on how domain controllers should replicate with one another.

dedicated forest root domain The first domain in a forest; contains only the forestwide administrative accounts and domain controllers needed to run the forestwide operations master roles.

delegation of control The process of a user with higher security privileges assigning authority to perform certain tasks to a user with lesser security privileges; usually used to give a user administrative permission for an OU.

directory partition A section of an Active Directory database stored on a domain controller's hard drive. These sections are managed by different processes and replicated to other domain controllers in an Active Directory network.

domain directory partition A directory partition that contains all objects in a domain, including users, groups, computers, OUs, and so forth.

effective permissions A combination of a user's assigned permissions through group membership, an explicit user permission assignment, and inherited permissions.

external trust A one-way or two-way nontransitive trust between two domains that aren't in the same forest.

Flexible Single Master Operation (FSMO) roles Specialized domain controller tasks that handle operations that can affect the entire domain or forest. Only one domain controller can be assigned a particular FSMO.

forest root domain The first domain created in a new forest.

forest trust A trust that provides a one-way or two-way transitive trust between forests, which enables security principals in one forest to access resources in any domain in another forest.

global catalog partition A directory partition that stores the global catalog, which is a partial replica of all objects in the forest. It contains the most commonly accessed object attributes to facilitate object searches and user logons across domains.

intersite replication Active Directory replication that occurs between two or more sites.

intrasite replication Active Directory replication between domain controllers in the same site.

Kerberos An open-standard security protocol used to secure authentication and identification between parties in a network.

Knowledge Consistency Checker (KCC) A process that runs on every domain controller to determine the replication topology.

Lightweight Directory Access Protocol (LDAP) A protocol that runs over TCP/IP and is designed to facilitate access to directory services and directory objects. LDAP is based on a suite of protocols called X.500, developed by the International Telecommunications Union.

multimaster replication The process for replicating Active Directory objects in which changes to the database can occur on any domain controller and are propagated, or replicated, to all other domain controllers.

one-way trust A trust relationship in which one domain trusts another, but the reverse is not true.

operations master A domain controller with sole responsibility for certain domain or forestwide functions.

permission inheritance The process of transmitting permissions from a parent object to a child object.

realm trust A trust used to integrate users of other OSs into a Windows Server 2008 domain or forest; requires the OS to be running Kerberos V5 authentication.

relative identifier (RID) The part of the SID that's unique for each Active Directory object. *See also* security identifier (SID).

schema directory partition A directory partition containing the information needed to define Active Directory objects and object attributes for all domains in the forest.

security identifier (SID) A numeric value assigned to each object in a domain that uniquely identifies the object; composed of a domain identifier, which is the same for all objects in a domain, and the RID. *See also* relative identifier (RID).

security principals An Active Directory object that can be assigned permissions or rights to Active Directory objects and network resources.

shortcut trust A manually configured trust between domains in the same forest for the purpose of bypassing the normal referral process.

site link A logical connection between two sites that determines the replication schedule and frequency between the sites.

transitive trust A trust relationship based on the transitive rule of mathematics; therefore, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C.

trust relationship An arrangement that defines whether and how security principals from one domain can access network resources in another domain.

two-way trust A trust in which both domains in the relationship trust each other, so users from both domains can access resources in the other domain.

user principal name (UPN) A user logon name that follows the format *username@domain*.

Users can use their UPNs to log on to their own domain from a computer that's a member of a different domain.

Review Questions

1. The protocol for accessing Active Directory objects and services is based on which of the following standards?
 - a. DNS
 - b. LDAP
 - c. DHCP
 - d. ICMP

2. Which MMC do you use to create OUs?
 - a. Active Directory Sites and Services
 - b. Active Directory Domains and Trusts
 - c. Active Directory Users and Computers
 - d. Computer Management
3. Which wizard is used to assign users the authority to perform certain tasks on Active Directory objects?
4. User, computer, and group accounts can be referred to as which of the following?
 - a. Discretionary access accounts
 - b. Security descriptors
 - c. Local objects
 - d. Security principals
5. Which of the following must you modify if you want to change an Active Directory object's permissions?
 - a. DACL
 - b. SACL
 - c. Object attributes
 - d. Object schema
6. An object's owner automatically has Full control permission for the object. True or False?
7. JDoe is a member of a group that has Full control permission for an OU, which the group inherited from a parent OU. What is the best way to stop JDoe from having Write permission to this OU without affecting any other permissions?
 - a. Remove JDoe from the group.
 - b. Add a Deny ACE for JDoe to the parent OU.
 - c. Add an explicit Deny ACE for JDoe to the OU.
 - d. Add a Deny ACE for the group to the parent OU.
8. You're logged on as Administrator to a domain controller and are trying to troubleshoot a problem with a user's access to Active Directory objects. You open Active Directory Users and Computers to access an object's properties. However, you can't view the object's permissions. What is the most likely problem?
 - a. You don't have sufficient permissions to view the object's permissions.
 - b. You need to open Active Directory Domains and Trusts.
 - c. You need to enable Advanced Features.
 - d. You need to run the View Object Permissions Wizard.
9. A user's permissions to an object that are a combination of inherited and explicit permissions assigned to the user's account and groups the user belongs to are referred to as which of the following?
 - a. Inherited permissions
 - b. Effective permissions
 - c. Explicit permissions
 - d. Access permissions
10. Inherited permissions always override explicit permissions. True or False?
11. You're viewing the DACL for an OU and notice an inherited ACE for a user account that gives the account permission to the OU that it shouldn't have. You want to remove the

ACE from the OU, but you get an error message when you attempt to do so. What do you need to do?

- a. Open Active Directory Users and Computers in administrative mode.
 - b. Use ADSI Edit to remove permissions.
 - c. Disable inheritance on the OU.
 - d. Add an explicit Deny ACE for the user account.
12. A user is having trouble accessing an OU, so you need to determine the user's permissions to the OU. You log on to the domain controller as Administrator and view the Security tab of the OU's Properties dialog box. What do you do next?
13. Which of the following is a directory partition? (Choose all that apply.)
- a. Domain directory partition
 - b. Group policy partition
 - c. Schema directory partition
 - d. Configuration partition
14. Which is responsible for management of adding, removing, and renaming domains in a forest?
- a. Schema master
 - b. Infrastructure master
 - c. Domain naming master
 - d. RID master
15. Which is responsible for determining the replication topology?
- a. GPO
 - b. PDC
 - c. RID
 - d. KCC
16. Your company has merged with another company that also uses Windows Server 2008 and Active Directory. You want to give the other company's users access to your company's domain resources and vice versa without duplicating account information and with the least administrative effort. How can you accomplish this?
17. Which of the following do all domains in the same forest have in common? (Choose all that apply.)
- a. The same domain name
 - b. The same schema
 - c. The same user accounts
 - d. The same global catalog
18. Which of the following is *not* a function of the global catalog?
- a. Facilitates forestwide searches
 - b. Keeps universal group memberships
 - c. Facilitates intersite replication
 - d. Facilitates forestwide logons
19. You have an Active Directory forest of two trees and eight domains. You haven't changed any of the operations master domain controllers. On which domain controller is the schema master?
- a. All domain controllers
 - b. The last domain controller installed
 - c. The first domain controller in the forest root domain
 - d. The first domain controller in each tree

20. Which of the following is a valid reason for using multiple forests?
 - a. Centralized management
 - b. Need for different schemas
 - c. Easy access to all domain resources
 - d. Need for a single global catalog
21. What can you do to reduce the delay caused by authentication referral?
 - a. Create a forest trust.
 - b. Create an external trust.
 - c. Create a shortcut trust.
 - d. Create a transitive trust.
22. What can you do to integrate user authentication between Linux and Active Directory?
 - a. Create a realm trust.
 - b. Create an external trust.
 - c. Create a one-way trust.
 - d. Create a transitive trust.
23. Trust relationships between all domains in a forest are two-way transitive trusts. True or False?
24. Which of the following is a reason to use multiple domains? (Choose all that apply.)
 - a. Need for different name identities
 - b. Replication control
 - c. Need for differing account policies
 - d. Easier access to resources
25. Which of the following is a reason for establishing multiple sites? (Choose all that apply.)
 - a. Improving authentication efficiency
 - b. Enabling more frequent replication
 - c. Reducing traffic on the WAN
 - d. Having only one IP subnet

Case Projects



Case Project 4-1: Creating an OU Structure

In Case Project 3-1, you outlined the OU structure for Cool Gadgets. Now it's time to put it into practice. Because you're unlikely to have a domain controller to dedicate to these activities, your OU structure will simulate the `coolgadgets.com` domain. If you recall, Cool Gadgets has four main departments: Executive, Marketing, Engineering, and Operations. Create this OU structure on your domain controller after creating an OU named `coolgadgets.com` to simulate the domain container. When you're finished, your OU structure should look like Figure 4-22.

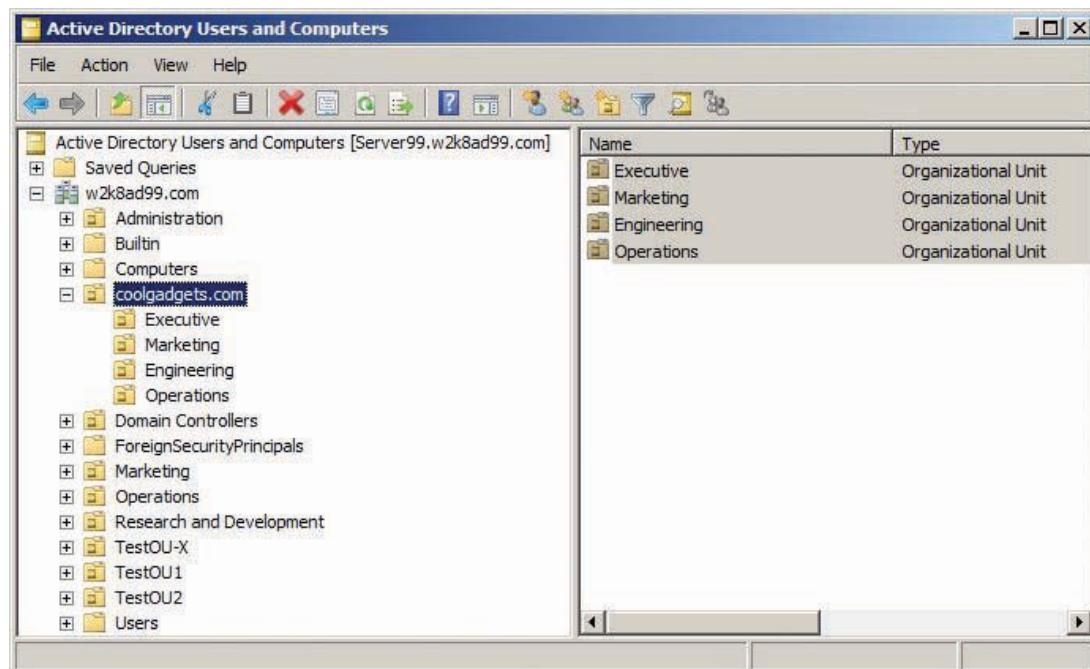


Figure 4-22 The coolgadgets.com OU structure

Case Project 4-2: Expanding the OU Structure

Because Cool Gadgets has expanded over the past year, two departments were added under the Marketing Department: Sales and Advertising. In addition, Operations has two new departments under it: Manufacturing and Testing. Create these additional OUs where appropriate, and write a short explanation of how an OU structure that mirrors a company's organizational structure can be beneficial.

Case Project 4-3: Determining Effective Permissions

The following list shows two groups and their members:

- Group1: Bill, Tom, Mary, Susan
- Group2: Bill, Mary, Jane, Alex

The following tables, labeled Problem 1, Problem 2, and Problem 3, show the DACLs for an OU. In these DACLs, a special group called Everyone has an implied membership of all users. Determine the effective permissions for each user in these three tables.

Problem 1

ACE	Permission	How assigned
Everyone	Allow Read	Inherited
Bill	Allow Full control	Explicit
Tom	Deny Read	Explicit
Group1	Allow Write	Inherited
Group2	Allow Create all child objects	Inherited

Problem 2

ACE	Permission	How assigned
Everyone	Allow Read	Inherited
Bill	Deny Delete all child objects	Explicit
Tom	Allow Read	Explicit
Group1	Allow Write	Inherited
Group2	Allow Full control	Inherited

Problem 3

ACE	Permission	How assigned
Everyone	Read	Inherited
	Deny Delete all child objects	Explicit
Bill	Allow Delete all child objects	Explicit
Tom	Allow Read	Explicit
Group1	Allow Delete all child objects	Inherited
	Allow Create all child objects	Inherited
Group2	Allow Full control	Inherited

Case Project 4-4: Solving an Active Directory Design Puzzle

You have been asked to consult on a job at BigCorp, which uses Windows Server 2008 and Active Directory. This company has several thousand users and multiple domains in a single forest. You arrive on site, sit down at a domain controller, and open Active Directory Users and Computers to review the Active Directory design. You find that there are no OUs, except the default Domain Controllers OU, and only a couple of accounts besides the default users and groups in the Users and BuiltIn folders. The domain object is named TopDomain. You have been assured that the domain controller is an operational and critical part of the Active Directory network. After a while, you realize what domain component of the forest you're looking at. What type of domain are you looking at and what are its key functions?

Account Management

After reading this chapter and completing the exercises, you will be able to:

- Explain how to manage user accounts
- Work with user profiles
- Describe factors in managing group accounts
- Work with computer accounts
- Describe tools for automating account management

A primary task of an Active Directory domain administrator is managing user, group, and computer accounts. Users are hired, leave the company, change departments, and change their names. Passwords are forgotten and must be reset. New resources become available to which users or, more likely, groups of users must be given access. New computers are installed on the network and must be added to the domain. All these tasks, particularly in large networks, keep administrators busy.

This chapter discusses GUI and command-line tools for creating and managing all aspects of Active Directory accounts. You examine user account properties and user profiles, including roaming and mandatory profiles. Finally, you learn about group account types and group scopes, including how to use groups to maintain secure access to resources in a multidomain environment.

Managing User Accounts

Working with user accounts is one of the most important Active Directory administrative tasks. User accounts are the main link between real people and network resources, so user account management requires not only technical expertise, but also people skills. When users can't log on or access a needed resource, they often turn to the administrator to solve the problem. Fortunately, an administrator's understanding of how user accounts work and how to best configure them can reduce the need to exercise people skills with frustrated users.

User accounts have two main functions in Active Directory:

- *Provide a method for user authentication to the network*—The user logon name and password serve as a secure method for users to log on to the network to access resources. A user account can also contain account restrictions, such as when and where a user can log on or an account expiration date.
- *Provide detailed information about a user*—For use in a company directory, user accounts can contain departments, office locations, addresses, and telephone information. You can modify the Active Directory schema to contain just about any user information a company wants to keep.

As you learned in Chapter 3, Windows OSs have three categories of user accounts: local, domain, and built-in. Local user accounts are found in Windows client OSs, such as Windows XP and Vista, as well as Windows Server OSs on systems that aren't configured as domain controllers. These accounts are stored in the Security Accounts Manager (SAM) database on local computers, and users can log on to and access resources only on the computer where the account resides. A network running Active Directory should limit the use of local user accounts on client computers, however, as they can't be used to access domain resources. Local user accounts are mainly used in a peer-to-peer network where Active Directory isn't running. Administrators can also log on to a computer with a local Administrator account for the purposes of joining the computer to a domain or troubleshooting access to the domain. Local user accounts are usually created in Control Panel's User Accounts applet or the Computer Management MMC's Local Users and Groups snap-in. Because these accounts don't participate in Active Directory, they can't be managed from Active Directory or be subject to group policies. The number of attributes in a local user account pales in comparison to those in Active Directory user accounts, as shown in Figure 5-1.

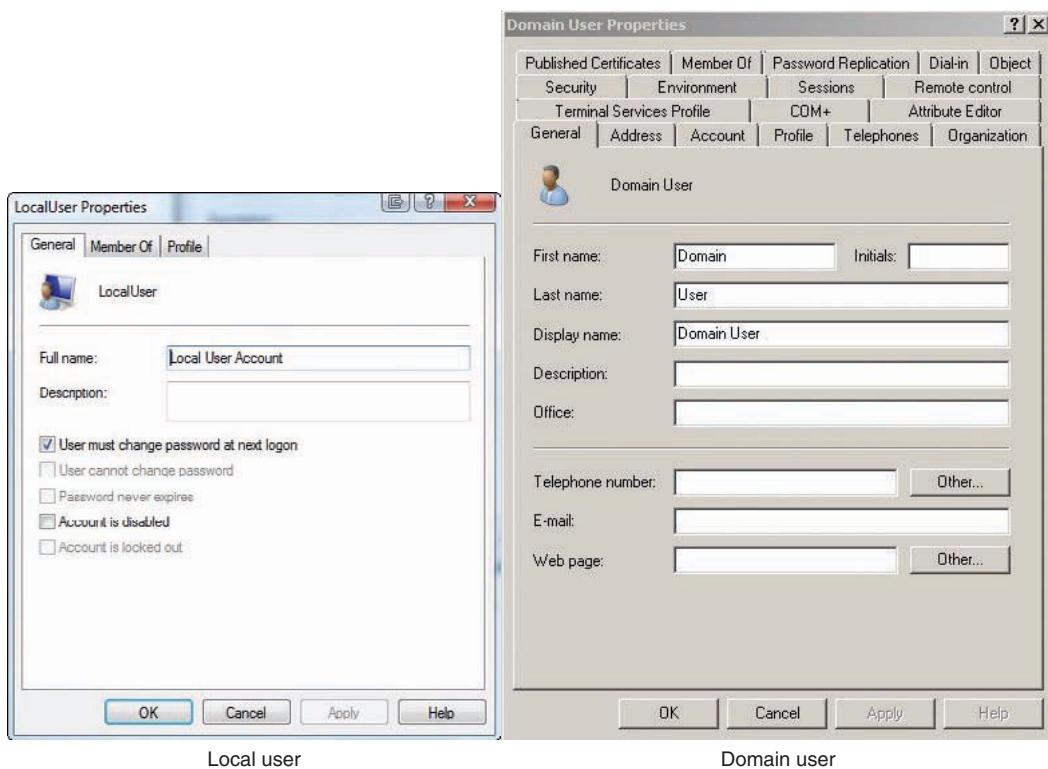


Figure 5-1 Local and domain user accounts

User accounts created in Active Directory are referred to as domain user accounts. Generally, these accounts enable users to log on to any computer that's a domain member in the Active Directory forest. They also provide single sign-on access to domain resources in the forest and other trusted entities to which the account has permission. Domain user accounts can be managed by group policies and are subject to account policies linked to the domain.

Built-in user accounts include the Administrator and Guest accounts created during Windows installation. They can be local or domain user accounts, depending on whether they're stored in the computer's SAM database or in Active Directory. Built-in accounts have the same qualities as regular local or domain accounts, except they can't be deleted. When Active Directory is installed on a Windows Server 2008 computer, the Administrator and Guest accounts are converted from local user to domain user accounts. These accounts require special handling because of their unique role in being the two accounts on every Windows computer. The following guidelines apply to the built-in Administrator account:

- The local Administrator account has full access to all aspects of a computer, and the domain Administrator account has full access to all aspects of the domain.
- Because the Administrator account is created on every computer and domain, it should be renamed and given a very strong password to increase security. With these measures in place, a user attempting to gain unauthorized access has to guess not only the administrator's password, but also the logon name.
- The Administrator account should be used to log on to a computer or domain only when performing administrative operations is necessary. Network administrators should use a regular user account for logging on to perform nonadministrative tasks.
- The Administrator account can be renamed or disabled but can't be deleted.

The following guidelines apply to the built-in Guest account:

- After Windows installation, the Guest account is disabled by default and must be enabled by an administrator before it can be used to log on.

- The Guest account can have a blank password, so if you enable this account, be aware that anybody can log on with it without needing a password. The Guest account should be assigned a password before it's enabled.
- Like the Administrator account, the Guest account should be renamed if it's going to be used.
- The Guest account has limited access to a computer or domain, but it does have access to any resource for which the Everyone group has permission.

Creating and Modifying User Accounts

User accounts are created primarily with Active Directory Users and Computers but can also be created with command-line tools, as you did in Chapter 3 with the DSADD command. Using command-line tools to create and manage accounts is discussed later in “Automating Account Management.” When you create a user account in an Active Directory domain, keep the following considerations in mind:

- Other Active Directory objects must be unique only in their container, but a user account must be unique throughout the domain because it's used to log on to the domain.
- User account names aren't case sensitive. They can be from 1 to 20 characters and use letters, numbers, and special characters, with the exception of ", [], :, ;, <, >, ?, *, +, @, |, ^, =, and ,.
- Devise a naming standard for user accounts, which makes creating users easier and can be convenient when using applications, such as e-mail, that include the username in the address. The downside of using a predictable naming standard is that attackers can guess usernames easily to gain unauthorized access to the network. Common naming standards include a user's first initial plus last name (for example, kwilliams for Kelly Williams) or a user's first name and last name separated by a special character (for example, Kelly.Williams or Kelly_Williams). In large companies where names are likely to be duplicated, adding a number after the username is common.
- By default, a complex password is required, as described in Chapter 3. Passwords are case sensitive.
- By default, only a logon name and password are required to create a valid user, but descriptive information, such as first and last name, should be included to facilitate Active Directory searches.

You have created a few users already, but take a closer look at the process, particularly some of the fields you encounter in Active Directory Users and Computers. Figure 5-2 shows the New Object - User dialog box.

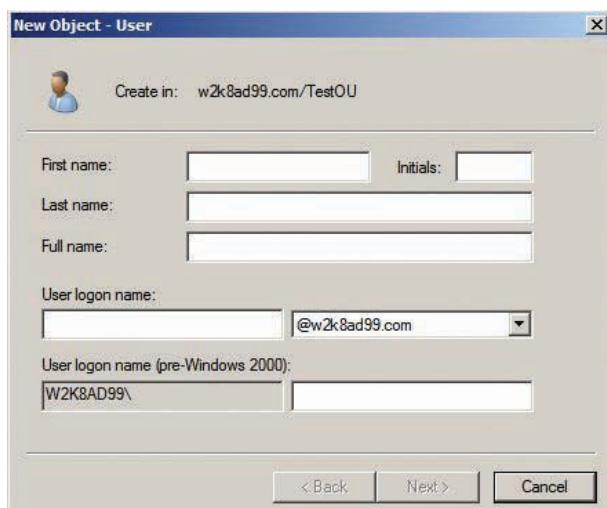


Figure 5-2 The New Object - User dialog box

As mentioned, the only fields *required* for a valid user are a user logon name (pre-Windows 2000) and a password. However, you can get away with specifying only these two fields when you're using DSADD. When you use Active Directory Users and Computers, you must enter a value for the following attributes:

- *Full name*—This field is normally a composite of the First name, Initials, and Last name fields, but you can enter a name that's different from what's in these three fields.
- *User logon name*—This field is referred to as the user principal name (UPN). As you learned in Chapter 4, the UPN format is *logon name@domain*. The “@domain” part is called the UPN suffix. You can fill in the logon name and select the domain in the drop-down list, which is set to the current domain controller's domain by default. By using the UPN, users can log on to their home domains from a computer that's a member of a different domain.
- *User logon name (pre-Windows 2000)*—Generally, this field is the same as User logon name but need not be. It consists of the domain name (without the top-level domain), a backslash, and the user logon name. Computers running OSs before Windows 2000 can't be domain members, so users of these older OSs must log on to a Windows 2000 or later domain with the format *domain\user*. Although the User logon name and User logon name (pre-Windows 2000) fields can be different, it's not recommended.
- *Password and Confirm password*—These fields (see Figure 5-3) are required by default because account policies in a Windows Server 2008 domain don't allow blank passwords. The default password policy requires a minimum length of 7 characters and a maximum of 127, and the password must meet complexity requirements. You can change this password policy, however.



Figure 5-3 Password fields

The four check boxes in Figure 5-3 are as follows:

- *User must change password at next logon*—This option, enabled by default, requires users to create a new password the next time they log on. Typically, you use this option when users are assigned a generic password at account creation for logging on to the domain for the first time. After the first logon, the user is prompted to change the password so that it complies with the password policy. This option is also used when an existing user's password is reset.

- *User cannot change password*—This option is useful when multiple users log on with the same user account, a practice common with part-time employees or guests who need access to the network. However, this option can't be set if “User must change password at next logon” is already selected. If you attempt to set both options, Windows displays a message stating that only one can be set.
- *Password never expires*—This option overrides the password policy that sets a maximum password age to force users to change their passwords periodically. It applies only to password expiration, not to account expiration, and can't be set when “User must change password at next logon” is already selected. Later in “Understanding Account Properties,” you see how to set an expiration date for a user account.
- *Account is disabled*—This option, which prevents using the user account, is sometimes used when user accounts are created before users require them, such as when you've hired a new employee who hasn't started yet. You can also set this option on existing user accounts when a user goes on extended leave or leaves the company, and the account will be renamed and assigned to a replacement.



Activity 5-1: Creating User Accounts

Time Required: 15 minutes

Objective: Create user accounts with different account options.

Description: You want to experiment with some user account options that can be set during account creation.

1. Log on to your server as Administrator, if necessary, and open Active Directory Users and Computers.
2. Click to expand the domain node, click **TestOU**, and then click the **New User** toolbar icon. (*Hint:* Hover your mouse pointer over toolbar icons to see their descriptions.) Type **testuser3** in the User logon name text box. The User logon name (pre-Windows 2000) text box is filled in automatically. However, the Next button is still disabled, which means you haven't filled in all the required fields. Type **Test** in the First name text box and **User3** in the Last name text box. Now the Full name text box is filled in automatically, and the Next button is enabled. Click **Next**.
3. In the Password text box, type **p@\$\$word**. Type **p@\$\$word** again in the Confirm password text box.
4. Click to select the **User cannot change password** check box. Read the warning message, and then click **OK**. Click to clear the **User must change password at next logon** check box, and then click **User cannot change password**. Click **Next**, and then click **Finish**.
5. Read the error message. What can you do to change the password you typed in Step 4 so that it meets complexity requirements? Click **OK**, and then click **Back**.
6. Type **p@\$\$word1** in the Password and Confirm password text boxes. Adding a number at the end meets complexity requirements, but you could also change one letter to uppercase, such as **p@\$\$Word**. Click **Next**, and then click **Finish**.
7. Log off, and then log on as **testuser3** with the password you just set.
8. Press **Ctrl+Alt+Delete**, and then click **Change a password**.
9. In the Old password text box, type **p@\$\$word1**. In the New password text box, type **p@\$\$word2**, and type it again in the Confirm password text box. Click the **arrow** icon. You get an “Access is denied” message because the account is prohibited from changing the password. Click **OK**, and then click **Cancel**. Click **Log off**.
10. Log on as Administrator, and open Active Directory Users and Computers.
11. Create a user in the TestOU OU with the logon name **testuser4** and the first and last names **Test User4**. Enter an appropriate password, and then click **Account is disabled**. Click **Next**, and then click **Finish**.

12. In Active Directory Users and Computers, notice that testuser4's icon has a down arrow to indicate that the account is disabled. If you open the Users folder, you'll see the Guest user has this icon, too, to indicate its disabled status.
13. Leave Active Directory Users and Computers open for the next activity.

Using User Templates Creating users can be a repetitive task, especially when you're creating several users with similar group memberships, account options, and descriptive fields. Fortunately, you can reduce some of this repetition by using a **user template**, which is simply a user account that's copied to create users with common attributes. You can copy many user account attributes in this template to accounts you're creating, except for name, logon name, password, and some contact and descriptive fields (such as phone number and e-mail address) that are generally unique for each user. When you copy a user account, the same wizard for creating a user runs so that you can fill in the name, logon name, password, and other unique fields.

Here are some tips for creating user templates:

- Create one template account for each department or OU, as users in the same department often have several common attributes.
- Disable the template account so that it doesn't pose a security risk.
- Add an underscore or other special character to the beginning of a template account's name so that it's easily recognizable as a template and is listed first in an alphabetical list of accounts.
- Fill in as many common attributes as you can so that after each account is created, less customizing is necessary.

5

Activity 5-2: Creating a User Template



Time Required: 10 minutes

Objective: Create a user template for populating the Sales OU with users.

Description: You need to create several users for the Sales Department and want to minimize the work involved by using a user template.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Click to expand the **Marketing** OU and then click the **Sales** OU.
3. In the Sales OU, create a group named **Sales-G** with the default group scope and group type. You'll add the user template to this group so that all Sales OU users belong to this group by default.
4. In the Sales OU, create a user with the full name **_Sales Template**, the logon name **_SalesTemplate**, and the password **Password01**. Make sure the **Account is disabled** and **User must change password at next logon** check boxes are selected.
5. Right-click the **_Sales Template** user and click **Properties**.
6. If necessary, click the **General** tab. Type **Sales Template User Account** in the Description text box, **Building 1** in the Office text box, **555-5555** in the Telephone number text box, and **www.coolgadgets.com** in the Web page text box.
7. Click the **Address** tab. Type **555 First St.** in the Street text box, **Metropolis** in the City text box, **AZ** in the State/province text box, and **12121** in the Zip/Postal Code text box. Click **United States** in the Country/region drop-down list.
8. Click the **Organization** tab. Type **Salesperson** in the Job Title text box, **Sales** in the Department text box, and **Cool Gadgets** in the Company text box.
9. Click the **Member Of** tab. Click **Add** to open the Select Groups dialog box. Type **Sales-G** in the Enter the object names to select text box, click **Check Names**, and then click **OK** twice.

10. In the right pane of Active Directory Users and Computers, right-click the **_Sales Template** user and click **Copy**. Type **Sales** in the First name text box, **Person1** in the Last name text box, and **salesperson1** in the User logon name text box, and then click **Next**.
11. Type **Password01** in the Password and Confirm password text boxes. Click to clear the **Account is disabled** check box, and then click **Next**. Click **Finish**.
12. Right-click **Sales Person1** and click **Properties**. Arrange the Properties dialog box so that you can see the **_Sales Template** user in Active Directory Users and Computers. Right-click **_Sales Template** and click **Properties**. Arrange the two Properties dialog boxes side by side so that you can compare them (see Figure 5-4). Make sure the General tab is visible in both.

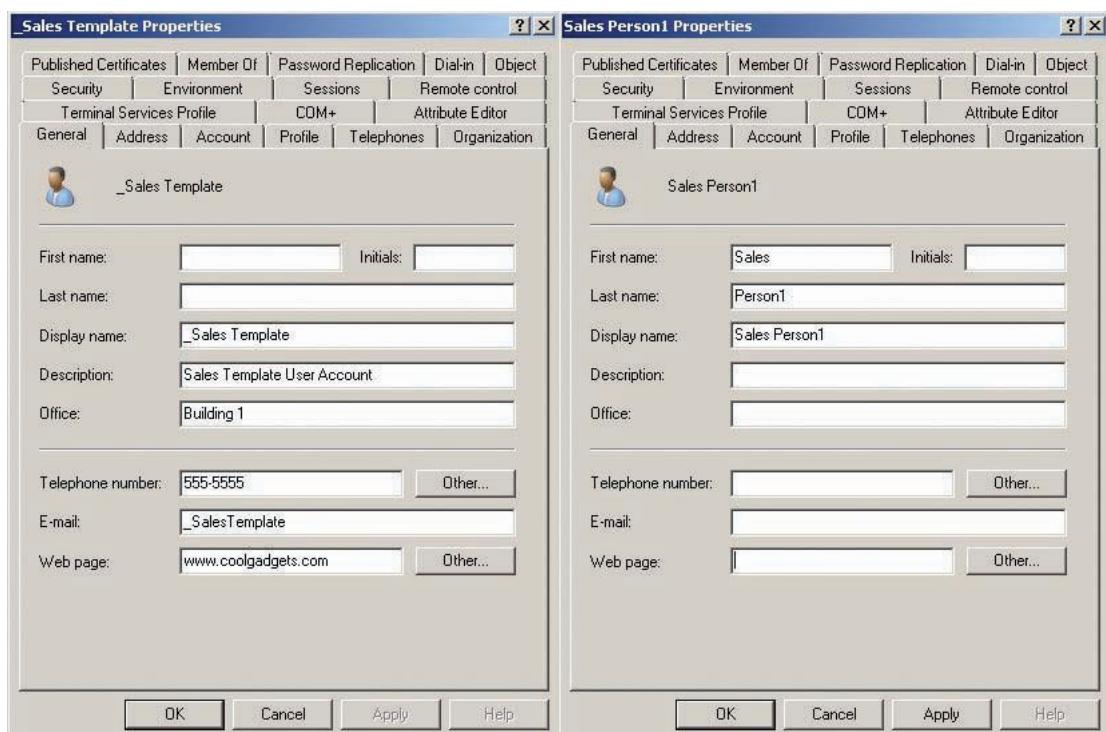


Figure 5-4 Comparing user properties

13. Notice that no fields in the template's General tab were copied to the Sales Person1 user. Click the **Address** tab in both Properties dialog boxes, and notice that the Street field wasn't copied. Click the **Organization** tab, and notice that the Job Title field wasn't copied.
14. Click the **Member Of** tab in both Properties dialog boxes, and notice that the group membership *was* copied.
15. Click **Cancel** to close both Properties dialog boxes, and leave Active Directory Users and Computers open.

User templates are useful for creating several users with a number of similar attributes. Unfortunately, some attributes aren't copied to the new user account, such as the Description, Office, Telephone number, Web page, and other fields. In addition, if one of the attributes that is copied changes, quite a bit of manual configuration might be required. However, there's a way to work around these limitations, discussed in the following section.



You can use the Active Directory Schema snap-in to change whether an attribute is copied when the user is copied. Load the snap-in into an MMC, double-click the attribute, and click the "Attribute is copied when duplicating a user" check box. In Activity 4-6, you registered the DLL needed to use this snap-in.

Modifying Multiple Users As you learned in Activity 5-2, user templates don't copy all the common attributes you might want to set for multiple users, such as department members who have the same telephone number or office location. In addition, you might need to add several users to a group after the users are created. Fortunately, Active Directory Users and Computers supports making changes to several accounts simultaneously. To select multiple accounts, hold down Ctrl and click each one separately. If the accounts are listed consecutively, click the first one, hold down Shift, and click the last account in the list, or drag over the accounts to select them. After making a selection, right-click it or click Action on the menu bar to perform the following actions on all selected accounts simultaneously:

- *Add to a group*—Adds the selected accounts to a group you specify
- *Disable Account*—Disables the selected accounts
- *Enable Account*—Enables the selected accounts
- *Move*—Moves the selected accounts to a new OU or folder
- *Send Mail*—Opens the configured e-mail application and places each user's e-mail address in the To field
- *Cut*—Cuts the selected accounts so that you can paste them into another OU or folder
- *Delete*—Deletes the selected accounts
- *Properties*—Opens the Properties for Multiple Items dialog box, where you can edit certain attributes of the selected accounts



Activity 5-3: Editing Multiple Accounts



Time Required: 10 minutes

Objective: Create users and change attributes on several accounts simultaneously.

Description: You need to change some attributes on several users in your Sales OU, so you decide to use the Properties for Multiple Items dialog box to make this task easier.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Click to expand the **Marketing** OU, if necessary, and then click the **Sales** OU.
3. Create two user accounts by using the **_Sales** Template account. The accounts should have the first and last names **Sales Person2** and **Sales Person3** and logon names **salesperson2** and **salesperson3**. Enter **Password01** for the password on both accounts. Make sure the **Account is disabled** check box is selected. Click to clear the **User must change password at next logon** check box so that they *don't* have to change their passwords. Click **Next** and then **Finish** for each account.
4. In Active Directory Users and Computers, click **Sales Person 1**, and then hold down **Shift** and click **Sales Person3**. Release **Shift**, and then click **Action**, **Properties** from the menu to open the Properties for Multiple Items dialog box (see Figure 5-5).
5. Click the **Description** check box, and then type **Cool Gadgets Sales Person** in the text box. Click the **Web page** check box, and then type **www.coolgadgets.com** in the text box.
6. Click the **Account** tab. Scroll down in the Account options list box, and click to clear the **Account is disabled** check box. Click **Apply**.
7. Click the **Address** and **Profile** tabs to see which attributes you can change.
8. Click the **Organization** tab. Click the **Job Title** check box, type **Sales Associate** in the text box, and then click **OK**.
9. Open the Properties dialog box for each Sales Person user to verify that the changes were made for all. When you're finished, click **OK** to close them.
10. Leave Active Directory Users and Computers open for the next activity.

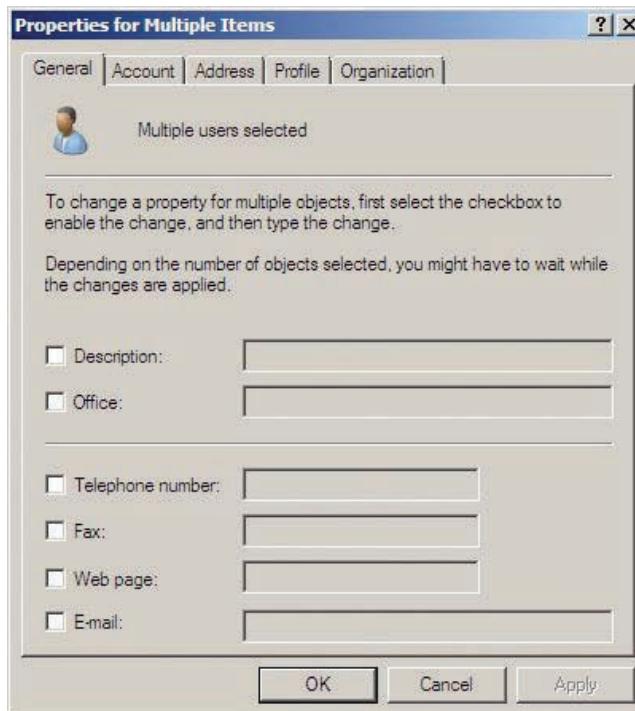


Figure 5-5 The Properties for Multiple Items dialog box

Editing multiple items isn't limited to user accounts, although it's most useful with these objects. You can edit multiple computer and group accounts and even objects of differing types, but the only attribute you can edit for these object types is the Description field.

Understanding Account Properties

After an account is created, your work as an administrator is just beginning. User account properties aren't static and require modification from time to time. Users might need their password changed, their group memberships altered, their logon restrictions modified, and other account changes. You explore user account properties in this section by examining some tabs in a user account's Properties dialog box. However, some account changes can be made only by right-clicking a user account or using the Action menu of Active Directory Users and Computers:

- *Reset a password*—If users forget their passwords or are prohibited from changing them, administrators can reset a password by right-clicking the user account and clicking Reset Password or using the Action menu.
- *Rename an account*—The object name shown in the Name column of Active Directory Users and Computers is referred to as the common name (CN). For example, the CN of the user you created in Activity 5-2 is Sales Person1. A user account's CN is taken from the Full name field when the user is created. You can change a user account's CN only by right-clicking the account or using the Action menu. Changing the name fields in the General tab of the account's Properties dialog box doesn't change the CN.
- *Move an account*—You can move a user account, or any Active Directory object, with one of three methods:
 - Right-click the user and click Move. (You can also click Action, Move from the menu.) You're then prompted to select the container to which you're moving the object.
 - Right-click the user and click Cut. (You can also click Action, Cut from the menu.) Then open a container object and paste the user into the container.
 - Drag the user from one container to another.

The General Tab The General tab of a user account's Properties dialog box contains descriptive information about the account, none of which affects a user account's logon, group memberships, rights, or permissions. However, some fields in the General tab do bear mentioning:

- *Display name*—The value in this field is taken from the Full name field during account creation and is usually the same as the CN. However, changing the display name doesn't change the CN, and changing the CN doesn't affect the display name. This field can be used in Active Directory searches.
- *E-mail*—You can use the value in this field to send an e-mail to the user associated with the account. If you right-click the user account and click Send Mail, the default mail application starts, and the value in this field is entered in the e-mail's To field.
- *Web page*—This field can contain a URL. If this field is configured, you can right-click the user account and click Open Home Page, and a Web browser opens the specified Web page.

The remainder of the fields in the General tab can be used to locate an object with an Active Directory search.

The Account Tab The Account tab (see Figure 5-6) contains the information that most affects a user's logon to the domain. Aside from a password reset, this tab is the best place to check when a user is having difficulty with the logon process.

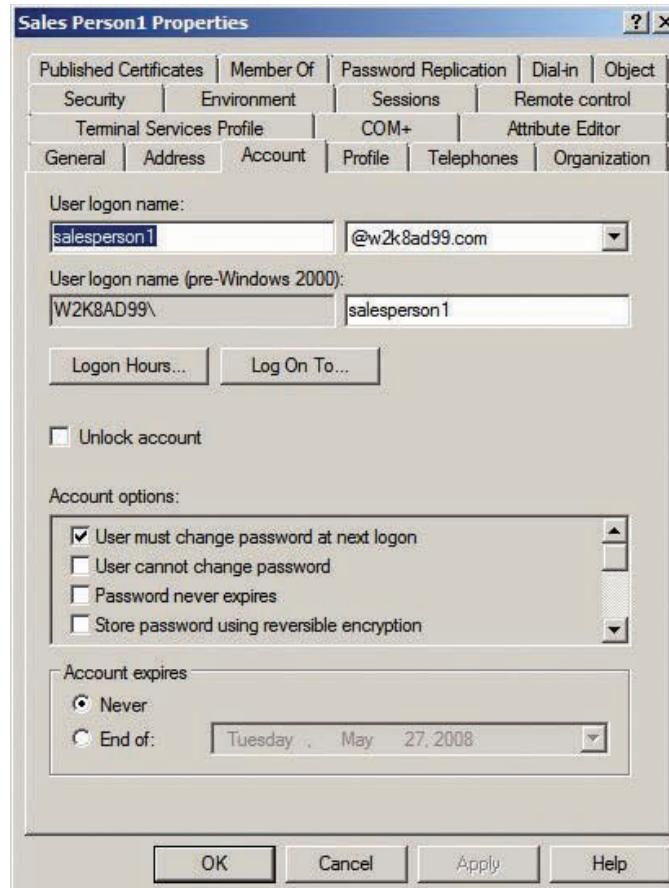


Figure 5-6 The Account tab

- *User logon name* and *User logon name (pre-Windows 2000)*—These fields were described previously in “Creating and Modifying User Accounts.”

- **Logon Hours**—Clicking this button opens a dialog box (see Figure 5-7) where administrators can restrict days and hours that users can log on to the domain. By default, all days and all hours are permitted. To exclude hours, click the Logon Denied option button and select the boxes for the hours you want to exclude; each box represents one hour. You can drag over the hour boxes to select several days or hours at a time. In Figure 5-7, logging on is denied to Sales Person1 every day from 12:00 a.m. to 3:00 a.m. The default behavior of this feature denies new attempts to log on during logon denied hours but doesn't affect a user who's already logged on. However, you can set a group policy to force a user to be disconnected when logon hours expire.

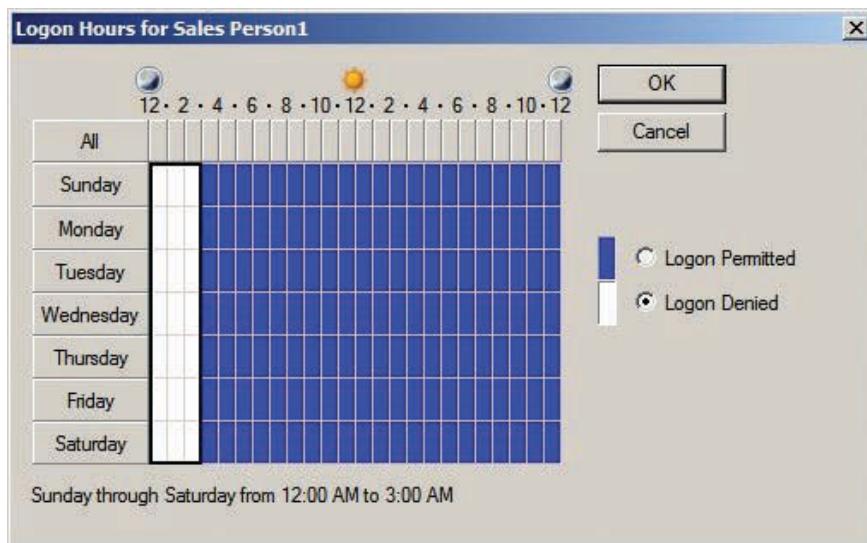


Figure 5-7 Setting logon hours

- **Log On To**—Click this button to specify by computer name which computers the user account can use to log on to the domain. By default, a user can use all computers in the domain.
- **Unlock account**—If this check box is selected, the user has too many failed logon attempts. In this case, the account is locked out and the user can't log on. Clearing the check box unlocks the account.
- **Account options**—Five of these options were described previously. Most account options pertain to the user's password and Kerberos authentication properties, but a few warrant more explanation:
 - **Store password using reversible encryption**: Allows applications to access an account's stored password for authentication purposes. Enabling this option poses a considerable security risk and should be used only when no other authentication method is available.
 - **Smart card is required for interactive logon**: Requires a smart card for the user to log on to a domain member. When this option is enabled, the user's password is set to a random value and never expires.
 - **Account is sensitive and cannot be delegated**: Used to prevent a service from using an account's authentication credentials to access a network resource or another service. This option increases security and is most often set on Administrator accounts.
 - **Account expires**—An administrator uses this option to set a date after which the account can no longer log on.

The Profile Tab The Profile tab (see Figure 5-8) is used to specify the location of files that make up a user's profile, a logon script, and the location of a home folder:

- *Profile path*—Used to specify the path to a user's profile. By default, a user's profile is stored on the computer where the user is currently logged on. In Windows Vista or Server 2008, the profile is in the C:\Users\username directory. In Windows XP, it's in the C:\Documents and Settings\username directory. When you're creating a user template, you can use the %username% variable instead of the actual username. User profiles are discussed later in “Working with User Profiles.”
- *Logon script*—Used to specify a script that runs when the user logs on. The preferred method for specifying a logon script is using a group policy, but in older OSs, such as Windows NT and Windows 9x, group policies aren't used.
- *Home folder*—Used to specify the path to a user's home folder. In general, the home folder has been replaced by the Documents or My Documents folder. Some older applications use this field as the default location for storing user documents, however. You can also use this field to specify the location on a terminal server where user documents are stored during Terminal Services sessions. The home folder can be a local path or a drive letter that points to a network share.

5

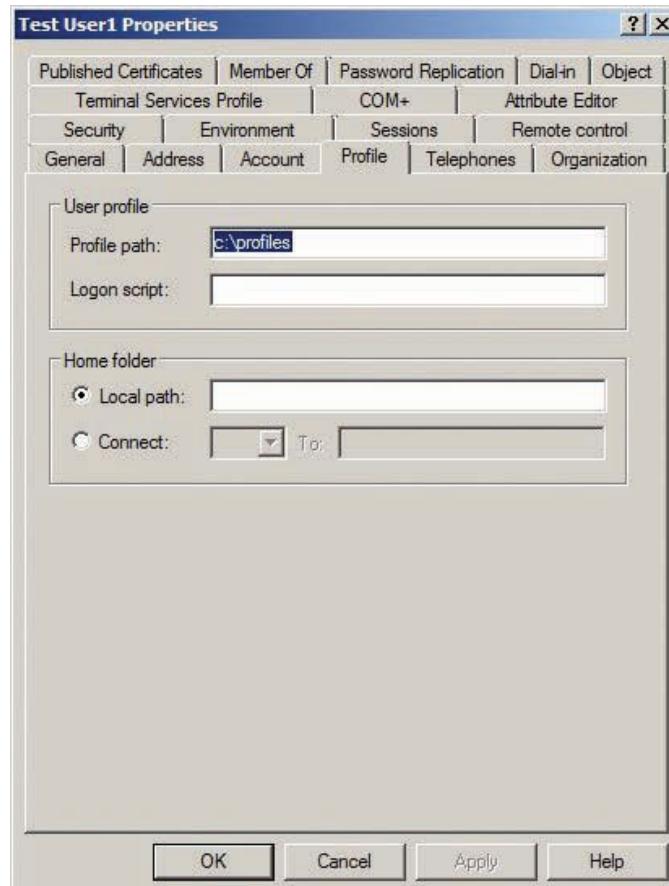


Figure 5-8 The Profile tab

The Member Of Tab The Member Of tab lists groups the user belongs to and can be used to change group memberships. Every new user is added to the Domain Users group automatically. You can remove a user from Domain Users, but it's not recommended because

membership in this group is one way to give users default rights and permissions. The Set Primary Group button in this tab is needed only when a user is logging in to a Macintosh, UNIX, or Linux client computer.

Terminal Services Tabs Four tabs in a user account's Properties dialog box are related to Terminal Services. The settings in these tabs affect a user's session and connection properties when connecting to a Windows Server 2008 Terminal Services server:

- *Terminal Services Profile*—This tab is similar to the Profile tab, in defining where a user's profile and home folder are located. However, the settings here are used only when a user is logged on to a terminal server or to prevent a user from logging on to a terminal server.
- *Remote control*—You use this tab to configure a user's Terminal Services remote control settings (see Figure 5-9). When remote control is enabled, an administrator can observe or interact with a user's Terminal Services session by using the Remote Desktop client. If the Require user's permission check box is selected, Windows prompts the user to allow the administrator to view or interact with the session. You use options in the Level of control section to specify whether you can view a user's session or interact with it.

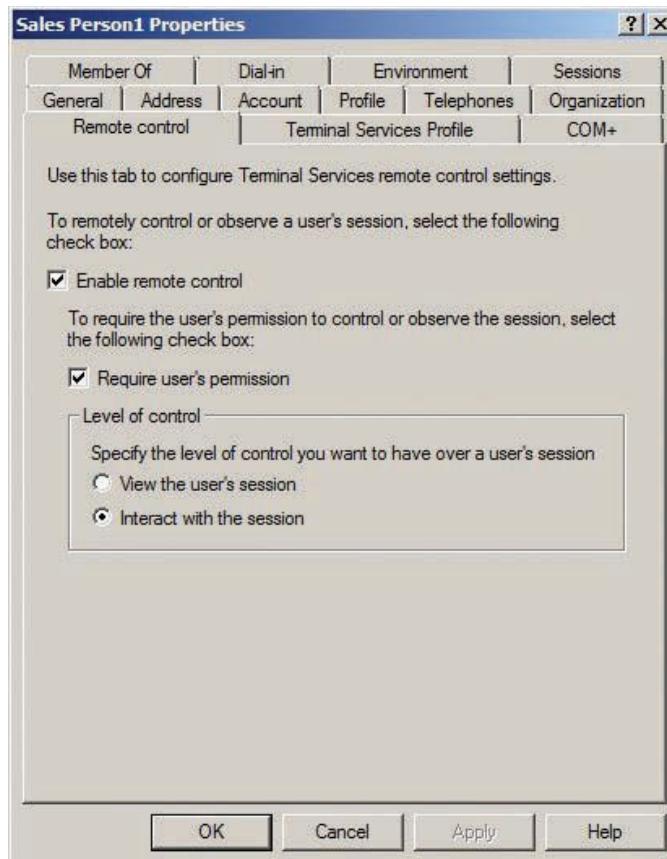


Figure 5-9 The Remote control tab

- *Environment*—You use this tab to configure the Terminal Services startup environment. You can specify a program to run when the user logs on to a terminal server and determine whether a user's local drives and printers should be available during a Terminal Services session.

- **Sessions**—You configure timeout and reconnection settings for Terminal Services in this tab (see Figure 5-10), such as how long a session can be active and what actions to take when the session limit has been reached or the session has been disconnected.

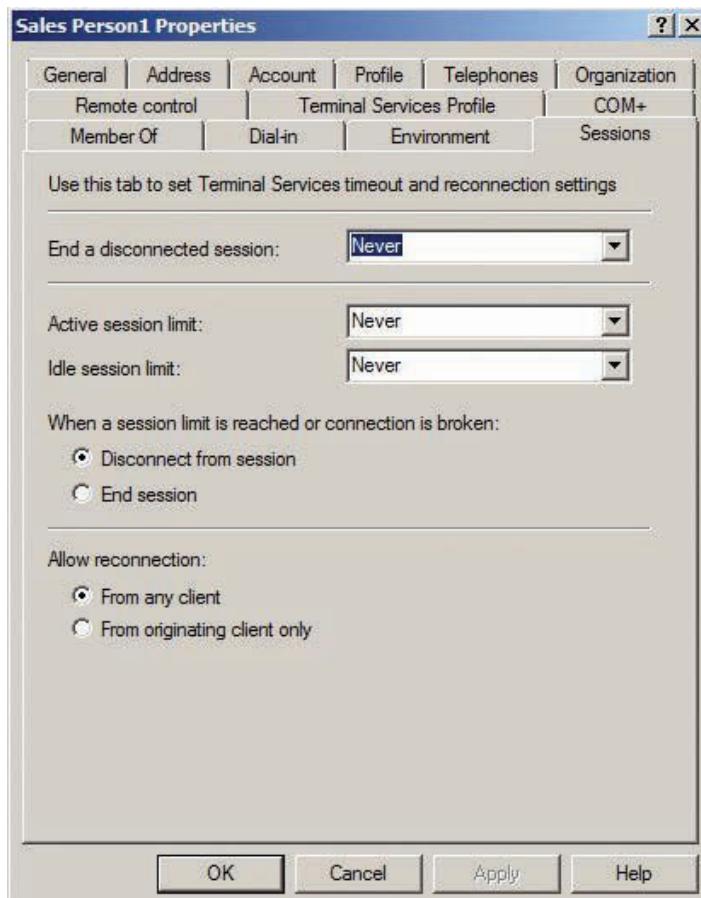


Figure 5-10 The Sessions tab

User accounts are security principals, which means permissions and rights can be assigned to them so that users can access network resources and perform certain operations on their computers. You can create two other user-related accounts: contacts and distribution lists, explained in the following section.

Using Contacts and Distribution Lists

A **contact** is an Active Directory object that usually represents a person for informational purposes only, much like an address book entry. Like a user account, a contact is created in Active Directory Users and Computers, but a contact isn't a security principal and, therefore, can't be assigned permissions or rights. The most common use of a contact is for integration into Microsoft Exchange's address book. The Full name field is the only information required to create a contact, but a contact's Properties dialog box has General, Address, Telephones, Organization, and Member Of tabs (see Figure 5-11) for adding detailed information about the contact. You use the Member Of tab to add a contact to a group or a distribution list.

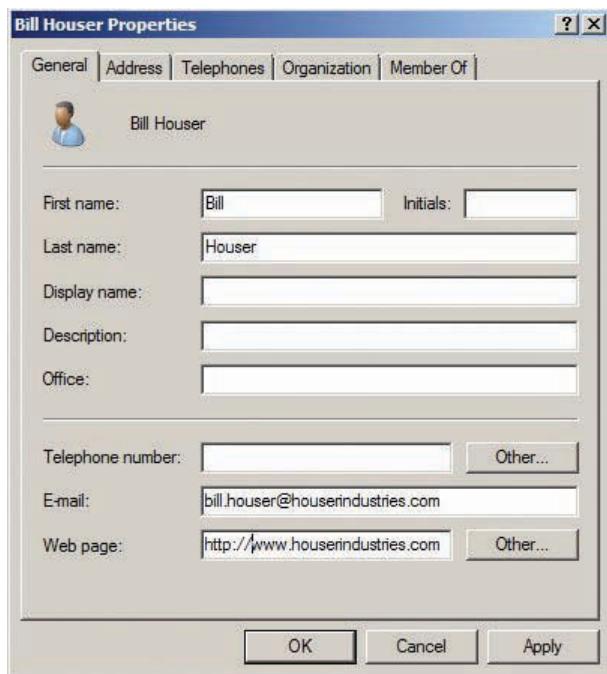


Figure 5-11 The Properties dialog box for a contact

Distribution lists are created in the same way as groups. The only real difference is the group type, which is distribution rather than security (explained later in “Managing Group Accounts”). Like a contact, a distribution list is used primarily with Microsoft Exchange for sending e-mails, but to several people at once. Both regular user accounts and contacts can be added as members of a distribution list.



Activity 5-4: Creating a Contact and a Distribution List

Time Required: 10 minutes

Objective: Create a contact and a distribution list.

Description: You need to have a marketing business partner’s contact information readily available. Because your users are well versed in using Active Directory to find other directory information, you decide to create contact and distribution list objects in Active Directory for outside business contacts. For organizational purposes, you place outside contacts in separate OUs.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. If necessary, click to expand the **Marketing** OU, and then create a new OU called **External** under it.
3. Click the **External** OU you just created. Right-click a blank spot in the right pane, point to **New**, and click **Contact**.
4. Type **Partner** in the First name text box and **One** in the Last name text box, and then click **OK**.
5. Right-click a blank spot in the right pane, point to **New**, and click **Group**.
6. In the Group name text box, type **MktEmail**. Under Group type, click the **Distribution** option button, and then click **OK**.
7. Right-click **Partner One** and click **Properties** to open its Properties dialog box. Click each tab to view the information you can enter for a contact.

8. Click the **Member Of** tab. Click **Add** to open the Select Groups dialog box. Type **MktEmail** in the Enter the object names to select text box, click **Check Names**, and then click **OK** twice.
9. Close Active Directory Users and Computers.

Working with User Profiles

A **user profile** is a collection of a user's personal files and settings that define his or her working environment. By default, a user profile is created when a user logs on to a computer for the first time; the profile is stored in a folder that usually has the user's logon name. On a Windows Server 2008 or Vista computer, the profile is created as a subfolder of the Users folder, which is on the same drive as the Windows folder (referred to as %SYSTEMDRIVE%), usually C. Figure 5-12 shows the profile folder hierarchy on a typical Vista system.

5

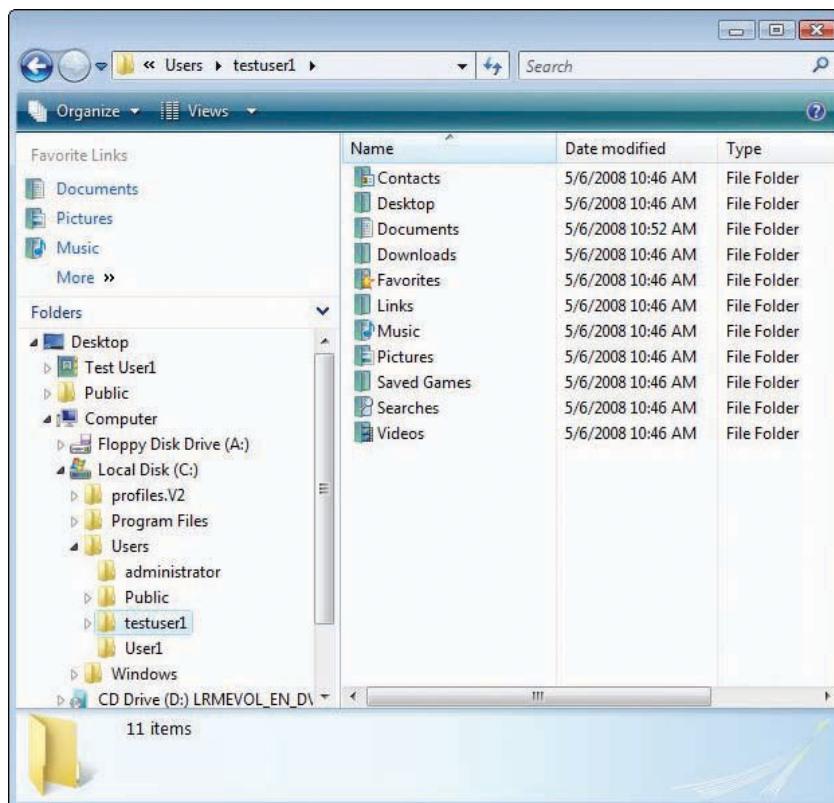
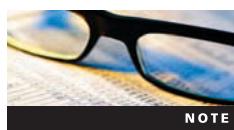


Figure 5-12 The location of user profile folders



In Windows XP and Server 2003, the folder containing user profiles is Documents and Settings rather than Users.

NOTE

The profile contains personal data folders a user maintains as well as files and folders containing user and application settings. Some files and folders in the profile are hidden or system files that can't be viewed with the default Windows Explorer settings. To view all files in the profile, you must enable the option to view hidden and system files in Windows Explorer. The following list describes some key files and folders in a user's profile. Because some folder names

have changed in Windows Vista and Server 2008, the Windows XP name is in parentheses. If the folder doesn't exist in a Windows XP profile, N/A is noted in parentheses.

- *AppData (N/A)*—A hidden folder that's the default location for user application data
- *Desktop*—Contains desktop items, such as shortcuts and files
- *Documents (My Documents)*—The default location applications use to store saved documents
- *Downloads (N/A)*—The default location for files downloaded via a Web browser
- *Favorites*—Bookmarks from Internet Explorer
- *Music (My Music)*—The default location for saved music files
- *Pictures (My Pictures)*—The default location for saved picture files
- *Ntuser.dat*—A hidden system file containing user preferences for Windows and application settings; merged with the Registry when a user logs on to Windows

A user profile stored on the same system where the user logs on is called a **local profile**. As stated, a local profile is created from a hidden profile called Default the first time a user logs on to a system; to see this profile, you must enable the option for viewing hidden and system files in Windows Explorer. When users log off, their profile settings are saved in their local profiles so that the next time they log on, all their settings are preserved. However, if a user logs on to a different computer, the profile is created again from the Default profile. If administrators want to make users' profiles available on any computer they log on to, they can set up roaming profiles, discussed next.

Roaming Profiles

A **roaming profile** follows the user no matter which computer he or she logs on to. It's stored on a network share so that when a user logs on to any computer in the network, the profile is copied from the network share to the profile folder on the local computer. This local copy of the roaming profile is referred to as the profile's cached copy. Any changes the user makes to the profile are replicated from the locally cached copy to the profile on the network share when the user logs off.



Windows Server 2008/Vista roaming profiles aren't compatible with roaming profiles from earlier OSs.

NOTE

If a user's account is configured to use roaming profiles but the profile hasn't been created yet, the roaming profile is created from one of two locations:

- *The NETLOGON share*—This system folder is shared by default. A customized default profile can be stored in this share in a folder named Default User.V2. The V2 at the end indicates a Windows Server 2008/Vista default roaming profile. The NETLOGON share is located in %SYSTEMDRIVE%\Windows\SYSVOL\sysvol\domain\Scripts; *domain* is the domain name.
- *The Default profile on the local system*—If there's no Default User.V2 folder in the NETLOGON share, a user's initial roaming profile is copied from the Default profile in %SYSTEMDRIVE%\Users\Default, in the same way as a local profile.

The general steps for customizing the default roaming profile (covered in Activity 5-7) are as follows:

1. Create a user, making sure the profile is local.
2. Log on to a system as the user you created.
3. Customize your environment with, for example, a screen saver, a background, desktop items, and Start menu items. You can even load some documents in the Documents folder or on the desktop.

4. Log off and log on as Administrator.
5. Use Control Panel's User Profiles applet to copy the user's profile to the NETLOGON share on your domain controller in a folder named Default User.V2.

You can also use this method to customize a default local profile. The only difference is that you copy the customized profile to the %SYSTEMDRIVE%\Users\Default folder instead of the network share.

Configuring Roaming Profiles There are two parts to configuring roaming profiles: configuring a shared folder to hold roaming profiles and configuring each user account's properties to specify the roaming profile's location. The following steps outline this process:

1. Create a folder on the server for storing roaming profiles. The server should have the File Services role installed. The folder is usually called Profiles or Users.
2. Share this folder and give the Domain Users group the Full control share permission. If only some users will have roaming profiles stored on this server, however, you can create a group with these users as members and give this group Full control for the share. The default NTFS permissions should suffice. (NTFS permissions are covered in Chapter 6.)
3. Edit the Profile path text box in the Profile tab of each user account's Properties dialog box. The path should be similar to \\server\profiles%\username%. As shown in Figure 5-13, you can use %username% in place of the user's logon name so that you can fill in the profile path when you create a user template or edit multiple accounts simultaneously.

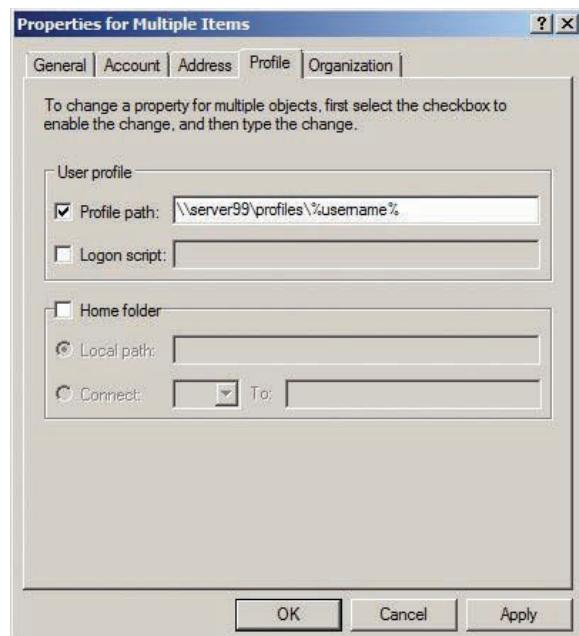


Figure 5-13 Editing the profile path on multiple accounts

After roaming profiles are configured, the next time the user logs on to a computer, the default or existing local profile is copied to the roaming profile. The folder with the user's logon name and .V2 at the end is created automatically with the appropriate permissions set. The .V2 distinguishes a roaming profile from a pre-Vista roaming profile.

Mandatory Profiles

The previous method for creating roaming profiles works great when you want users to have control over their profiles. Suppose you want certain users to have a profile that can't be changed, or can be changed during the session but reverts to the original profile the next time

the user logs on? This type of profile is called a **mandatory profile**. It works much like a regular roaming profile, except changes to the profile aren't copied to the server.

Mandatory profiles are sometimes used when users are assigned a generic logon shared by several employees. For example, a company might have a class of user referred to as Night Administrator. If several full-time or part-time employees share this designation, they can all be assigned the logon name "nightadmin." The network administrator can keep a tight rein on these users by creating a mandatory profile for the nightadmin user account with these steps:

1. Create the nightadmin account and log on as that account.
2. Configure the desktop and Start menu settings as necessary.
3. Log off as nightadmin and back on as Administrator.
4. Copy the nightadmin profile to the Shared Profiles folder on the server by using the User Profiles dialog box (opened from the Advanced tab of the System Properties dialog box), shown in Figure 5-14. When you click the Copy To button, you're prompted for the path to the server.

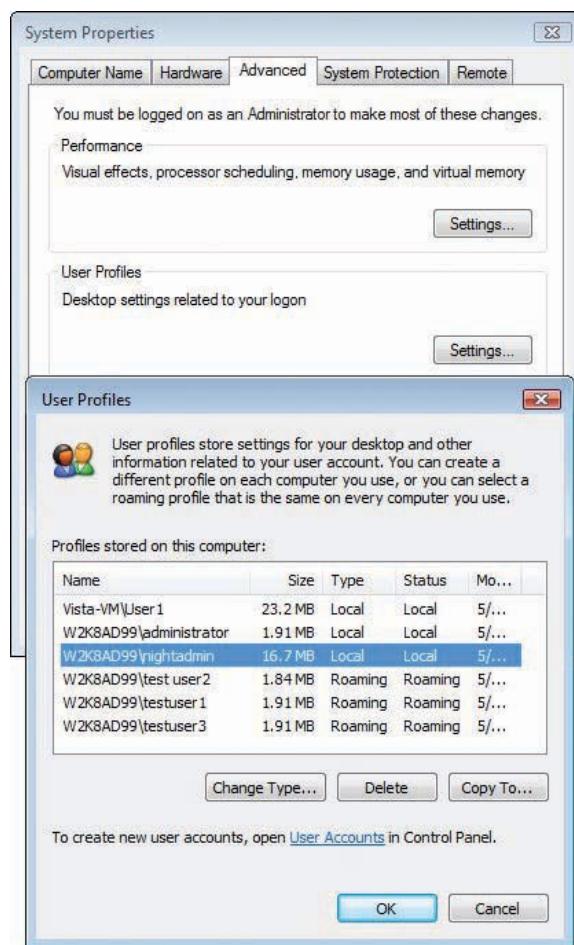


Figure 5-14 The User Profiles dialog box

5. Rename the Ntuser.dat file in the nightadmin profile as Ntuser.man, and mark the file as Read-only.
6. Configure the profile path in the nightadmin user account's Properties dialog box.

You can also use these steps to have multiple user accounts use a single mandatory profile. In Step 4, after you copy the profile, click the Change button and select the users who should

have access to the profile. Then configure each user account's profile path to point to the same folder on the server (rather than %username%).



In the next activity, you add a Vista client computer to your domain. Normally, this task is done earlier, when you set up the network. However, you haven't needed a client computer until this point in the book, when you work with user profiles.



Activity 5-5: Adding a Vista Computer to the Domain

Time Required: 10 minutes

Objective: Make a Vista computer a member of the domain.

Description: To test user profiles and other user-related activities, you realize that being able to log on and log off the domain from a member Vista computer is ideal. The Vista computer can be implemented as a virtual machine so that you don't need so many physical computers.



See Appendix D for information on using virtual machines. You can download a preconfigured 30-day evaluation of a Vista virtual machine from the Microsoft Web site. Go to www.microsoft.com/downloads and search on "vista 30 day eval."

1. Log on to your Vista computer as Administrator, if necessary.
2. Click **Start**, right-click **Computer**, and click **Properties**.
3. In the Computer name, domain, and workgroup settings section, click the **Change settings** link. If necessary, click **Continue** in the User Account Control (UAC) message box.
4. In the System Properties dialog box, click the **Computer Name** tab, if necessary, and then click the **Change** button. In the Computer name text box, type **VistaXX**. Under Member of, click the **Domain** option, type **W2k8adXX.com**, and then click **OK**.



Remember to replace XX in activities with your student number.

5. Type the domain Administrator username and password when prompted. Click **OK** when you get a message welcoming you to the domain. When prompted to restart your computer, click **OK**, and then click **Close**.
6. Click **Restart Now**. While Vista is restarting, log on to your server as Administrator, and open Active Directory Users and Computers.
7. Click the **Computers** folder, which contains a computer object with the name of the Vista computer you just joined to the domain.
8. When Vista restarts, log on to the domain as Administrator. (If necessary, click **Switch User** at the logon prompt so that you can enter the username and password to log on to the domain.) Enter the username in the format **W2k8adXX\Administrator** or **Administrator@W2k8adXX** because Vista assumes you're logging on to the local computer instead of the domain when you log on as Administrator.
9. Stay logged on to Vista for the next activity.

Activity 5-6: Creating a Roaming Profile

Time Required: 10 minutes

Objective: Create a roaming profile for a user.

Description: You want a user to have a roaming profile. This user has never logged on to the domain before and receives the default profile on the Vista system as the initial profile.

1. If necessary, log on to your server as Administrator, and open Active Directory Users and Computers.
2. Click to expand the **Marketing** OU, and then click the **Sales** OU. Click the **Sales Person1** user, and then open the Properties dialog box.
3. Click the **Profile** tab. In the Profile path text box, type **\serverXX\Profiles\salesperson1**, and then click **OK**.
4. Click **Start, Computer**. Click the C drive, and create a folder named **Profiles** in the root of this drive.
5. Right-click the **Profiles** folder and click **Properties**. Click the **Sharing** tab.
6. The Sharing tab has two buttons. If you click the Share button, the Sharing Wizard guides you through the process. Because you need to do advanced sharing, click the **Advanced Sharing** button.
7. Click the **Share this folder** check box. Notice that the share name, which is what users see on the network, defaults to the folder name.
8. Click the **Permissions** button. Click **Add**, type **Domain Users**, and then click **Check Names** to verify. Click **OK**.
9. Click **Domain Users**, and then click the **Full control** check box in the Allow column.
10. Click **Everyone**, and then click **Remove**. The only entry in the Group or user names list box should be Domain Users. Click **OK** twice, and then click **Close**.
11. Log on to the domain from your Vista computer as **salesperson1** with the password **Password01**. When you're prompted to change the password, change it to **Password02**.
12. After you have logged on, go to your server (physical or virtual). Open Windows Explorer, click the **Profiles** share, and verify that a new folder named **salesperson1.V2** has been created. It's the roaming profile for salesperson1. You can't navigate this folder, however, because by default, only the user whose profile it is can access the profile.
13. Go to your Vista computer (physical or virtual). Click **Start**, and then right-click **Computer** and click **Properties**.
14. Click the **Advanced system settings** link. In the UAC message box, type the Administrator's username and password for the domain (should be **Administrator** and **Password01**).
15. In the User Profiles section, click the **Settings** button. View the list of profiles, and notice that the profile type for salesperson1 is roaming. Click **Cancel** twice.
16. Leave Active Directory Users and Computers open for the next activity.



Activity 5-7: Configuring a Roaming Profile for Multiple Users and Customizing the Default Roaming Profile

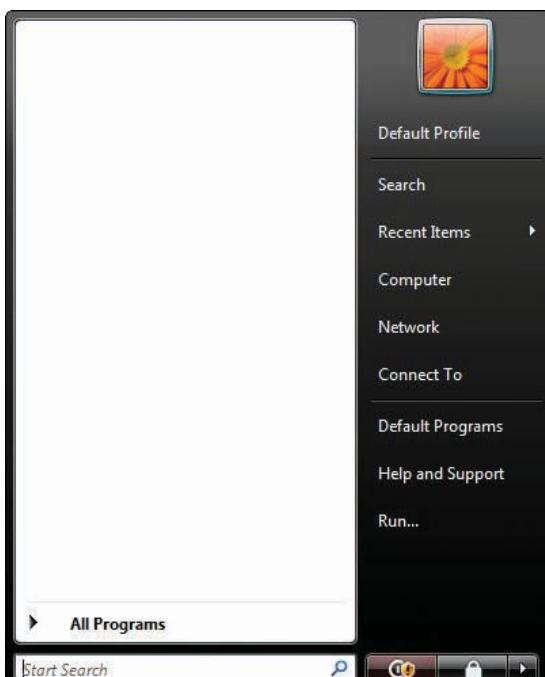
Time Required: 30 minutes

Objective: Configure a roaming profile for multiple users and customize the default roaming profile.

Description: You need to configure roaming profiles for several users. To do this, you edit the profile path on all users simultaneously. You want to customize desktop and Start menu settings for the default roaming profile, too.

1. If necessary, log on to your server as Administrator and open Active Directory Users and Computers.
2. Click to expand the **Marketing** OU, if necessary, and then click the **Sales** OU. In the right pane, click **Sales Person2**, and then hold down **Ctrl** and click **Sales Person3**. Release the **Ctrl** key. Right-click **Sales Person3** and click **Properties**.
3. Click the **Profile** tab. Click the **Profile path** check box, type **\serverXX\profiles\%username%** in the Profile path text box, and then click **OK**.

4. Click the **TestOU1** OU you created in Chapter 4. Create a user with the full name **Default Profile**, a logon name of **defprofile**, and a password of **Password01**. Configure the account so that the password doesn't have to be changed at the next logon.
5. Log off the Vista computer, if necessary, and log on to the domain as the **defprofile** user you just created.
6. Right-click the desktop and click **Personalize**. Click **Desktop Background**. In the Picture Location drop-down list, click **Solid Colors**. Click to select a color, and then click **OK**. Close the Personalization window.
7. Right-click **Start** and click **Properties**. Click the **Customize** button. Click the **Don't display this item** option button for the following items: Control Panel, Documents, Games, Music, and Pictures. Click the **Run command** check box, and then click **OK**. Click **OK** again.
8. Click **Start** to verify your choices. For each item in the left pane of the Start menu, right-click it and click **Remove from this list**. Your Start menu should look similar to Figure 5-15 when you're finished.



5

Figure 5-15 A customized Start menu

9. Log off Vista and then log back on as Administrator. Remember to use **W2k8adXX\Administrator** as the logon name.
10. Click **Start**, right-click **Computer**, and click **Properties**. Click the **Advanced system settings** link. If necessary, click **Continue** in the UAC message box.
11. In the User Profiles section, click the **Settings** button. Click the **W2K8ADXX\defprofile** entry, and then click the **Copy To** button. In the Copy profile to text box, type **\serverXX\netlogon\Default User.V2**. Don't click **OK** yet.
12. Click the **Change** button. Type **Everyone**, and then click **Check Names**. Click **OK**, and then click **OK** again. Click **OK** two more times.
13. Log off Vista. Log on to Vista as **salesperson2** with the password **Password01**. Check your Start menu. It should look just as it did for the defprofile user after your customization in Steps 6 and 7.
14. Log off Vista again, and leave Active Directory Users and Computers open on your server for the next activity.



Activity 5-8: Creating a Mandatory Profile

Time Required: 15 minutes

Objective: Create a mandatory profile based on the roaming profile you created previously.
Description: Users can change profiles as they see fit, but you want to prevent a specific user from changing the default profile you assigned. After creating the user profile, you decide to make it mandatory.

1. Log on to the domain from your Vista computer as Administrator.
2. Click **Start**, right-click **Computer**, and click **Properties**. Click the **Advanced system settings** link. If necessary, click **Continue** in the UAC message box.
3. In the User Profiles section, click **Settings**. Click the **W2K8ADXX\defprofile** entry, and then click the **Copy To** button. In the Copy profile to text box, type **\serverXX\Profiles\salesperson3.V2**. Don't click **OK** yet.
4. Click the **Change** button. Type **salesperson3**, and then click **Check Names**. Click **OK**, and then click **OK** again. Click **OK** two more times. Log off the Vista computer.
5. Log on to your server as Administrator, if necessary.
6. Open Windows Explorer, and navigate to the **C:\Profiles** folder. Click the **salesperson3.V2** folder. By default, you can't see Ntuser.dat because it's a hidden system file.
7. In Windows Explorer, click **Organize** on the toolbar, and then click **Folder and Search Options**.
8. Click the **View** tab. Click the **Show hidden files and folders** option button, and then click to clear the **Hide protected operating system files (Recommended)** check box. In the warning message, click **Yes**, and then click **OK**.
9. Right-click the **ntuser.dat** file in the **salesperson3.V2** folder and click **Rename**. Rename the file as **ntuser.man**. If necessary, click **Yes** in the message box about changing the file extension and **Yes** in the message box about being sure you want to rename this system file. Right-click **ntuser.man** and click **Properties**. Click **Read-only** at the bottom of the General tab, and then click **OK**. Close Windows Explorer.
10. Log on to the domain from the Vista computer as **salesperson3** with the password **Password01**.
11. Right-click the desktop, point to **New**, and click **Text Document** to create a file called New Text Document on your desktop.
12. Right-click the desktop again and click **Personalize**. Click **Desktop Background**. In the Picture Location drop-down list, click **Windows Wallpapers**. Click to select a wallpaper, and then click **OK**. Close the Personalization window.
13. Right-click **Start** and click **Properties**. Click the **Customize** button. Click the **Display as a link** option button under Control Panel and Documents, and then click **OK**. Click **OK** again.
14. Log off and log on again as **salesperson3**. Notice that the document you created on your desktop is no longer there, your wallpaper isn't displayed, and your Start menu reverted to the previous settings.
15. Log off Vista.

Super Mandatory Profiles If a user's roaming or mandatory profile isn't available because of a network error, a temporary profile based on the default profile is created and then deleted when the user logs off. When you don't want users with mandatory profiles to receive the default profile, you can use a **super mandatory profile**, which prevents a user from logging on to the domain when the mandatory profile is unavailable. To configure a super mandatory profile, rename the user's existing profile folder to include .man after the username, such as salesperson3.man.V2. Then configure the profile path in the user account's Properties dialog box in the same manner, such as **\serverXX\profiles\salesperson3.man**. You don't need to include the .V2 at the end of the path, as Windows appends it automatically for Vista clients. After configuring a super mandatory profile, if the user's mandatory profile is unavailable, the user is prohibited from logging on.

Managing Profiles

As you saw in previous activities, user profiles can be managed in the User Profiles dialog box (shown previously in Figure 5-14) with these three buttons:

- *Change Type*—Click to change a profile from roaming to local. This setting applies only when the user logs on to the computer where the profile has been changed. In other words, changing the profile from roaming to local makes the profile local only on that computer. The user's profile remains roaming on every other computer. If the profile had been roaming but is now local on the computer, it can be changed back to roaming (unless the profile path has been deleted from the user account's properties). Mandatory profiles can't be changed here.
- *Delete*—Click to delete the profile from the local computer; if the profile is roaming, its cached copy on the local computer is deleted. Roaming profile files on the server aren't deleted.
- *Copy To*—Click to copy a profile, whether local, roaming, or mandatory, to a new location, usually a network server. By default, only the user whose profile you copy has access to the profile. However, you can use the Change button in the Copy To dialog box to specify other users or groups allowed to use the profile. If multiple users will use the same copy of the profile, you should configure the profile as mandatory. Specifying users who can use the profile sets permissions for only those users to access the profile. You must still set the path in the Profile tab of the user account's Properties dialog box.

5

You can also manage many aspects of user profiles by using group policies. For example, certain computers can be configured to always use local profiles, and the profile's locally cached copy can be deleted automatically when the user logs off the computer. More than 20 profile settings can be configured with group policies. Many of them are covered in Chapter 7.

The Cost of Roaming Profiles

Roaming profiles are a convenient way to provide a consistent working environment for users. However, they come with a cost. Profiles can grow to be very large when users store a lot of files in different document folders. When a user logs on to a computer for the first time or if Windows detects that the profile on the server is newer than the locally cached copy, the profile must be copied from the server to the local computer. Similarly, if a user makes changes to his or her profile, the profile must be copied to the server when the user logs off. Whether the profile is copied to the workstation or the server (or both), profiles containing a lot of data can use considerable network bandwidth and cause long delays during logon and logoff.

Folder redirection can reduce some problems caused by roaming profiles. This feature redirects certain folders normally contained in the profile to a network server location. It effectively takes the folders out of the profile, excluding them from the copying process that takes place when a user logs on or off. For example, a network share called Redirected contains a folder for each user, and under each user folder are the user's redirected folders. Folders that can be redirected include Desktop, Start Menu, Documents, Pictures, Music, Videos, Download, and Favorites. Other folders can be redirected, and Chapter 7 covers redirection more thoroughly.

Managing Group Accounts

Active Directory group objects are the main security principal administrators use to grant rights and permissions to users. Using groups to assign user rights and permissions is preferable to using separate user accounts, mainly because groups are easier to manage. Users with similar access requirements to resources can be made members of a group, and instead of creating ACEs for each user in a network resource's DACL, you can make a single entry for the group. Furthermore, if a user changes departments or positions in the company, you can remove the user from one group and place the user in another group that meets his or her new access requirements. With a single administrative action, you can completely alter a user's access to resources. If permissions are assigned to a single user account, the administrator must find each resource for which the user has an ACE, make the necessary changes, and then add the user account to the DACL for each resource the new department or position requires.

When an administrator creates a group in Active Directory Users and Computers, aside from assigning a name, there are two additional settings, discussed in the following sections: group type and group scope.

Group Types

There are two group types: security groups and distribution groups. A **distribution group** is used to group users together mainly for sending e-mails to several people at once with an Active Directory-integrated e-mail application, such as Microsoft Exchange. Distribution groups aren't security principals and, therefore, can't be used to assign rights and permissions to their members. A distribution group can have the following objects as members: user accounts, contacts, other distribution groups, security groups, and computers.

Because you can mix user accounts and contacts, you can build useful distribution lists that include people outside your organization. You can also nest groups, which makes organizing users and contacts more flexible. However, because distribution groups aren't used for security and are useful only with certain applications, their use in Active Directory is more limited than security groups.

Security groups are the main Active Directory object administrators use to manage network resource access and grant rights to users. Most discussions about groups focus on security groups rather than distribution groups, and in general, when the term "group" is used without a qualifier, a security group should be assumed. Security groups can contain the same types of objects as distribution groups. However, if a security group has a contact as a member and the security group is granted permission to a resource, the permission doesn't extend to the contact because a contact isn't a security principal. Security groups can also be used as distribution groups by applications such as Microsoft Exchange, so re-creating security groups as distribution groups isn't necessary for e-mail purposes.

Converting Group Type You can change the group type from security to distribution and vice versa. However, only a security group can be added to a resource's DACL. If a security group is an entry in the DACL for a shared folder, for example, and the security group is converted to a distribution group, the group remains in the DACL but has no effect on access to the resource for any of its members.

The need to convert group type isn't all that common, but when it's necessary, usually a distribution group is converted to a security group. This conversion might be necessary when, for example, a group of users is assigned to collaborate on a project. Initially, distribution groups composed of team members might be created for the purpose of e-mail communication, but later, it's determined that the project requires considerable network resources to which team members need access. The distribution group could be converted to a security group for the purpose of assigning rights and permissions, and the security group could still be used as an e-mail distribution list.

Group Scope

The **group scope** determines the reach of a group's application in a domain or a forest: which security principals in a forest can be group members and to which forest resources a group can be assigned rights or permissions. Three group scope options are possible in a Windows Server 2008 forest: domain local, global, and universal. A fourth scope called local applies only to groups created in the SAM database of a member computer or stand-alone computer. Local groups aren't part of Active Directory.

The functionality of groups depends on the domain functional level. In Chapter 3, when you installed Active Directory, you had the option to choose the forest and domain functional level. When a DC in the domain runs Windows Server 2008, you can choose from three domain functional levels: Windows 2000 native, Windows Server 2003, and Windows Server 2008. Windows Server 2003 and Windows 2000 Server support another domain functional level called Windows 2000 mixed, which allows Windows NT DCs to participate in the domain. This functional level isn't supported in Windows Server 2008, however. The following discussion about group scopes applies to domains running at the Windows 2000 native functional level or higher.

Table 5-1 summarizes for each group scope possible group members, which groups the scope can be a member of, and to which resources permissions or rights can be assigned.

Table 5-1 Group scope membership and resource assignment

Group scope	Possible members	Can be a member of	Permissions and rights assignments
Domain local	User accounts, global groups, and universal groups from any domain in the forest	Domain local groups in the same domain Local groups on domain member computers; domain local groups in the BuiltIn folder can be members only of other domain local groups	Resources on any DC or member computer in the domain; domain local groups in the BuiltIn folder can be added to DACLs only on DCs, not on member computers
	Other domain local groups from the same domain		
	User accounts, global groups, and universal groups from trusted domains in another forest		
Global	User accounts and global groups (nested) in the same domain	Global groups in the same domain Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest
Universal	User accounts, global groups, and universal groups from any domain in the forest	Universal groups from any domain in the forest Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest

5

Domain Local Groups A **domain local group** is the main security principal recommended for assigning rights and permissions to domain resources. Although both global and universal groups can also be used for this purpose, Microsoft best practices recommend using these groups to aggregate users with similar access or rights requirements. Global and universal groups should then be added as members of domain local groups, which are added to a resource’s DACL. The process can be summarized with the acronyms AGDLP and AGGUDLP. In single-domain environments or when users from only one domain are assigned access to a resource, use AGDLP:

Accounts are made members of

Global groups, which are made members of

Domain Local groups, which are assigned

Permissions to resources

In multidomain environments where users from different domains are assigned access to a resource, use AGGUDLP:

Accounts are made members of

Global groups, which when necessary are nested in other

Global groups, which are made members of

Universal groups, which are then made members of

Domain Local groups, which are assigned

Permissions to resources

The repeating theme is that permissions should be assigned to as few different security principals as possible, namely domain local groups. Using this method to assign permissions keeps the list of ACEs short, making resource access management considerably easier. This rule isn’t hard and fast, as there are circumstances in which other group scopes and individual user accounts should be assigned permissions. Whenever possible, however, these rules should be followed.

Some administrators create a domain local group for each level of access to each shared resource. For example, you have a shared folder called SalesDocs that requires two levels of access by different groups: Read access and Modify access. You could create two domain local groups named SalesDocs-Read-DL, with Read permission, and SalesDocs-Mod-DL, with Modify permission. By using this group-naming standard, you have identified the resource, access level, and group scope. Next, you need only add the global or universal groups containing users to the correct domain local group. Keep in mind that the “local” in domain local refers to where resources this group scope is assigned to can be located. You can’t, for example, add a domain local group from Domain A to the DACL of a resource in Domain B.

Global Groups As mentioned, a **global group** is used mainly to group users from the same domain with similar access or rights requirements. A global group’s members can be user accounts and other global groups from the same domain. However, a global group is considered global because it can be made a member of a domain local group in any domain in the forest or trusted domains in other forests. Global groups can also be assigned permissions to resources in any domain in the forest or trusted domains in other forests.

A common use of global groups is creating one for each department, location, or both. In a single-domain environment, global groups are added to domain local groups for assigning resource permissions. You might wonder why user accounts aren’t simply added directly to a domain local group, bypassing global groups altogether. In a single-domain environment, you can do this, but this approach has some drawbacks:

- Domain local group memberships can become large and unwieldy, particularly for resources to which many users from several departments must have access. Examine Figure 5-16 and consider which group you would rather manage.

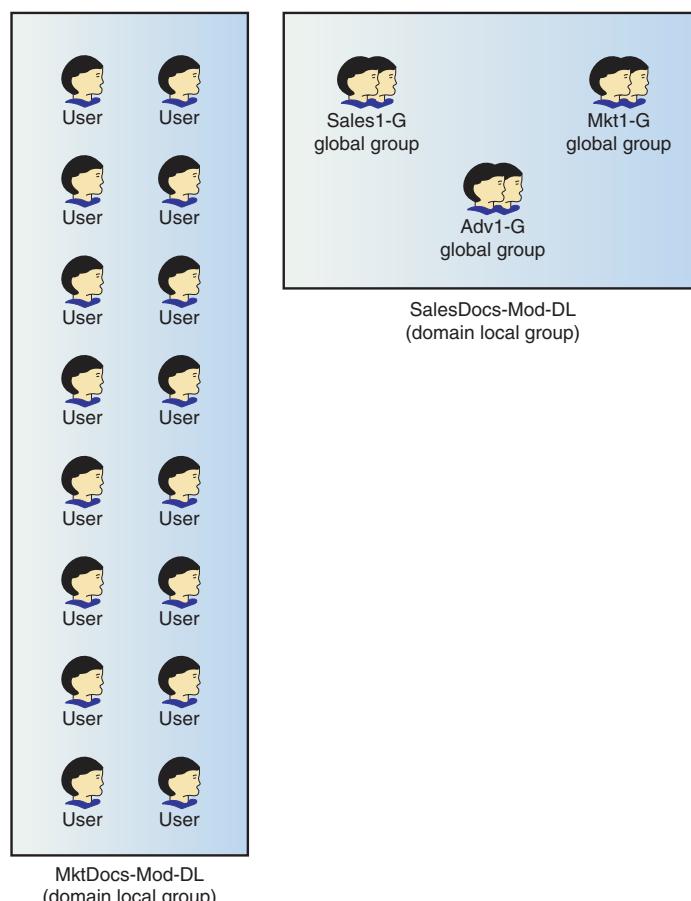


Figure 5-16 Global groups are easier to manage

- If the company ever adds a domain, you need to redesign group memberships to grant permissions to cross-domain resources. This task is necessary because a domain local group can't be a member of a group or assigned permission to a resource in another domain.

In multidomain environments where departments are represented in more than one domain, departmental global groups from each domain can be aggregated into a universal group, which is then made a member of a domain local group for resource access. For example, in Figure 5-17, both the US and UK coolgadgets.com domains have a global group called Sales. These global groups are added to the universal group Sales-U in the coolgadgets.com parent domain; Sales-U is then made a member of the domain local group assigned permissions to the shared folder. Keep in mind that the shared resource could be located in any of the three domains, as long as the domain local group is in the same domain as the shared resource. The universal group in this example can be added to a domain local group in any domain in the forest as well as trusted domains in other forests.

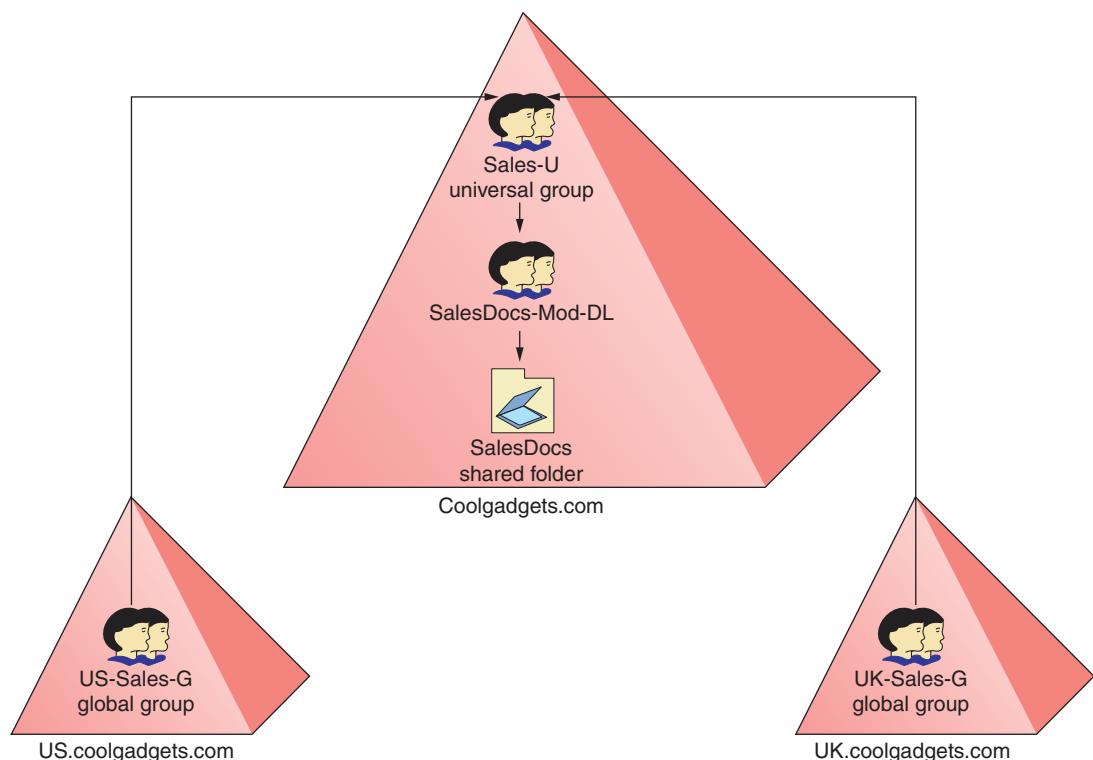


Figure 5-17 Using global and universal groups

Universal Groups A **universal group** is special in a couple of ways. First, a universal group's membership information is stored only on domain controllers configured as global catalog servers. Second, they are the only type of group with a truly universal nature:

- User accounts, global groups, and universal groups from any domain in the forest can be a member.
- They can be a member of other universal groups or domain local groups from any domain in the forest.
- They can be assigned permissions to resources in any domain in the forest.

Because universal groups' membership information is stored only on global catalog servers, plan the placement of domain controllers configured as global catalog servers carefully. When users log on, a global catalog server must be available to determine their memberships in any

universal groups. For that reason, a remote office with many users should have at least one domain controller configured as a global catalog server to reduce WAN traffic during user logons.

An alternative to having a global catalog server at each site is enabling caching of universal group membership information on a remote office's domain controller. With caching enabled, a domain controller queries a global catalog server to determine universal group membership, and then keeps a local copy of that information to use for future logons.

Universal group membership changes require replication to all global catalog servers. In a forest operating at the Windows 2000 functional level, replicating universal groups can create considerable network traffic because the entire group membership is copied. Windows Server 2003 and later forest functional levels include a feature called linked value replication, which allows replicating only group membership changes instead of the entire membership list. Having said that, there's still a benefit to keeping group membership lists short by nesting groups.



Universal groups didn't exist in Windows NT domains. The domain functional level must be at least Windows 2000 native to support universal groups.

NOTE

Local Groups A **local group** is created in the local SAM database on a member server or workstation or a stand-alone computer. Because groups and users created on a stand-alone computer can't interact with Active Directory, this discussion focuses on local groups created on computers that are members of an Active Directory domain.

Local groups can be found on any Windows computer that isn't a domain controller, and you manage them with the Local Users and Groups snap-in in the Computer Management MMC. Using local groups to manage resources on a member computer is generally discouraged because it decentralizes resource management. Assigning permissions and rights on member computers to domain local groups is better. However, when a Windows computer becomes a domain member, Windows changes the membership of two local groups automatically:

- **Administrators**—The Domain Admins global group is made a member of this local group, so any Domain Admins group member has administrative access to every member computer in the domain.
- **Users**—The Domain Users global group is made a member of this local group, giving Domain Users group members a set of default rights and permissions appropriate for a regular user on every member computer in the domain.

Local groups can have the following account types as members:

- Local user accounts created on the same computer
- Domain user accounts from any domain in the forest or trusted domains in another forest
- Domain local groups from the same domain (except domain local groups in the BuiltIn folder)
- Global or universal groups from any domain in the forest or trusted domains in another forest

Local groups can be assigned permissions only to resources on the local computer. The most common use of local groups, besides the Administrators and Users local groups, is in a workgroup environment on non-domain computers. However, when a member computer's user requires considerable autonomy for managing local computer resources, you can grant the user enough rights on the local computer for this autonomy.

Nesting Groups

Nesting groups is exactly what it sounds like: making one group a member of another group. In a Windows NT domain, the only group nesting allowed is to make a global group a member of a domain local group. However, in Windows 2000 and later, there are few restrictions on group nesting, as long as you follow the group scope's membership rules. Group nesting is often used

to group users who have similar roles but work in different departments. For example, you can create a global group for supervisors in each department and place users in each department with a supervisory role in this group. Next, create a SuperAll global group and place the departmental supervisor groups in this group (see Figure 5-18). In this way, all departmental supervisors can easily be assigned the rights and permissions their role specifies. Furthermore, in a multidomain environment, a similar group configuration can be developed for each domain. The SuperAll global groups from each domain can then be added to a universal supervisors group for assigning permissions and rights throughout the forest. This example follows the AGGUDLP rule described earlier.

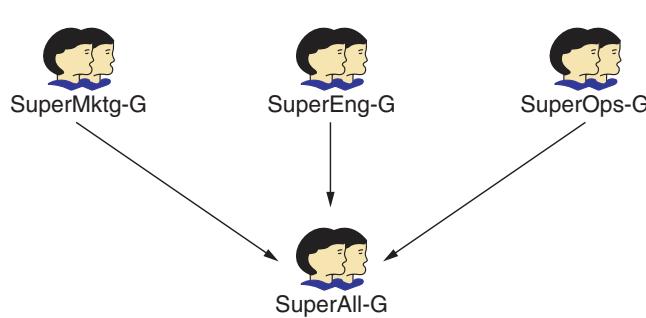


Figure 5-18 Nesting global groups

5

Although there are few restrictions on group nesting in a Windows 2000 native or higher domain functional level, the complexity of tracking and troubleshooting permissions increases as the number of levels of nested groups increases. Like OUs, groups can be nested an unlimited number of levels, but that doesn't mean you should. In most circumstances, one level of nesting groups of the same type should suffice, as in Figure 5-18. An additional level, such as aggregating nested global groups into a universal group, should work for most designs. The last step is to put your group of groups, whether global or universal, into a domain local group for resource access.

Converting Group Scope

When you create a group, the default setting is a security group with global scope. However, just as you can convert group type from security to distribution and vice versa, you can convert the group scope, with some restrictions, as explained in the following list:

- Universal to domain local, provided it's not a member of another universal group
- Universal to global, provided no universal group is a member
- Global to universal, provided it's not a member of another global group
- Domain local to universal, provided no domain local group is a member



Activity 5-9: Creating Groups with Different Scopes

Time Required: 20 minutes

Objective: Create groups with different scopes.

Description: You want to experiment to see how nesting groups and converting group scope work.

1. If necessary, log on to your server as Administrator and open Active Directory Users and Computers.
2. Click **TestOU**, and create the following security groups with the indicated scope: **Group1-G** (global), **Group2-G** (global), **Group1-DL** (domain local), **Group2-DL** (domain local), **Group1-U** (universal), **Group2-U** (universal).

3. In the right pane of Active Directory Users and Computers, click **Group1-G**, and open its Properties dialog box. Click the **General** tab, if necessary. In the Group scope section, notice that the Domain local option is disabled because converting from global to domain local isn't allowed.
4. Click the **Members** tab, and then click **Add**. Type **Group2-G**, click **Check Names**, and then click **OK**.
5. Click **Add**. Type **Group1-DL** and click **Check Names**. The Name Not Found message box is displayed because domain local groups can't be members of global groups. Click **Cancel**.
6. Click **Advanced**, and then click **Find Now**. Active Directory displays only valid objects that can be made a group member, so no domain local or universal groups are listed. Click **Cancel** twice, and then click **OK**.
7. Click **Group2-G**, and open its Properties dialog box. In the Group scope section, click the **Universal** option button, and then click **OK**. You should get an error message stating that a global group can't have a universal group as a member. Because Group2-G is a member of Group1-G, attempting to convert it to universal violates that rule. Click **OK**, and then click **Cancel**.
8. Click **Group1-DL**, and open its Properties dialog box. In the Group scope section, the Global option is disabled because you can't convert a domain local group to a global group.
9. Click the **Members** tab, and then click **Add**. Type **Group1-G** and click **Check Names**. Adding a global group as a member of a domain local group is in line with the AGDLP best practice. Click **OK** twice.
10. Click **Group1-U**, and open its Properties dialog box. Add **Group2-U** as a member, and then click **OK**. Click **Group2-U**, and open its Properties dialog box. In the Group scope section, click **Domain local**, and then click **OK**. You get an error message, which reinforces the rule that universal groups can be converted to domain local groups only if they aren't already a member of another universal group. Click **OK**, and then click **Cancel**.
11. Click **Group1-U**, and open its Properties dialog box. Try to add **Group1-DL** as a member. Nesting domain local groups in universal groups isn't permitted. Add **Group1-G** as a member. Success!
12. Leave Active Directory Users and Computers open for the next activity.

Default Groups in a Windows Domain

When an Active Directory domain is created, some default groups are created automatically to establish a framework for assigning users rights and permissions to perform common tasks and access default resources. Windows assigns default groups a variety of rights and permissions so that users can carry out certain tasks simply by being added to the appropriate group. For example, the default Backup Operators group is assigned the right to back up all files and directories on all computers in the Domain Controllers OU. To give users this capability, simply add them as members of the Backup Operators group.

There are three categories of default groups in a Windows domain: groups in the **Builtin** folder, groups in the **Users** folder, and special identity groups that don't appear in Active Directory Users and Computers and can't be managed there. A fourth category, the default local groups in the SAM database on member computers, corresponds roughly to groups in the **Builtin** folder.

Default Groups in the Builtin Folder All default groups in the **Builtin** folder are domain local groups used for assigning rights and permissions in the local domain. Neither the group scope nor type can be converted. Each group in this folder has a brief description that can be seen in Active Directory Users and Computers. Table 5-2 lists fuller descriptions for the most prominent of these groups.

Table 5-2 Default groups in the Builtin folder

Group	Description
Account Operators	Members can administer domain user, group, and computer accounts, except computers in the Domain Controllers OU and the Administrators, Domain Admins, Enterprise Admins, Schema Admins, and Read-Only Domain Controllers groups. Members can log on locally and shut down domain controllers in the domain. There are no default members.
Administrators	Members have full control of all DCs in the domain and can perform almost all operations on DCs. Default members are Domain Admins, Enterprise Admins, and the Administrator user account.
Backup Operators	Members can back up and restore all files and directories on DCs in the domain with an Active Directory-aware backup program. Members' ability to access all files and folders doesn't extend beyond their use of backup software. Members can log on locally to and shut down DCs. There are no default members.
Guests	This group has no default rights or permissions. The Domain Guests group and Guest user account are default members.
IIS_IUSRS	Internet Information Services uses this group to allow anonymous access to Web resources.
Network Configuration Operators	Members can change TCP/IP settings and release and renew DHCP-assigned addresses on DCs. There are no default members.
Print Operators	Members can manage all aspects of print jobs and printers connected to DCs. Members can log on locally to and shut down DCs in the domain. There are no default members.
Remote Desktop Users	Members can log on remotely to DCs with the Remote Desktop client. There are no default members.
Server Operators	Members can log on locally to DCs, manage some services, manage shared resources, back up and restore files, shut down DCs, format hard drives, and change the system time. There are no default members.
Users	Members can run applications and use local printers on member computers, among other common tasks. Members of this group can't, by default, log on locally to DCs. Domain Users and the special identity Authenticated Users and Interactive groups are members of the Users group by default. Because all user accounts created in a domain are automatically members of the Domain Users global group, all domain users become members of this group as well.

5

Default Groups in the Users Folder The default groups in the Users folder are a combination of domain local, global, and, in the forest root domain, universal scope. User accounts are generally added to global and universal groups in this folder for assigning permissions and rights in the domain and forest. Table 5-3 describes several groups in the Users folder.

Table 5-3 Default groups in the Users folder

Group/scope	Description
Allowed RODC Password Replication Group	Members can have their passwords replicated to RODCs. There are no default members.
Denied RODC Password Replication Group	Members can't have their passwords replicated to RODCs, so this group is a security measure to ensure that passwords for sensitive accounts don't get stored on RODCs. Default members include Domain Admins, Enterprise Admins, and Schema Admins.
DnsAdmins/domain local	This group is created when DNS is installed in the domain. Members have administrative control over the DNS Server service. There are no default members.
Domain Admins/global	Members have full control over domainwide functions. This group is a member of all domain local and local Administrators groups. The domain Administrator account is a member by default.
Domain Computers/global	All computers that are domain members (excluding DCs) are added to this group by default.
Domain Controllers/global	All DCs are members of this group by default.
Domain Users/global	All user accounts in the domain are added to this group automatically. This group is used to assign rights or permissions to all users in the domain, but it has no specific rights by default. This group is a member of the Users domain local group by default.
Enterprise Admins/universal	This universal group is found only on DCs in the forest root domain. Members have full control over forestwide operations. This group is a member of the Administrators group on all DCs. The Administrator account for the forest root domain is a member by default.

(continued)

Table 5-3 Default groups in the Users folder (*continued*)

Group/scope	Description
Group Policy Creator Owners/global	Members can create and modify group policies throughout the domain.
Read-only Domain Controllers/global	RODCs are members by default.
Schema Admins/universal	This universal group is found only on DCs in the forest root domain. Members can modify the Active Directory schema. The Administrator account for the forest root domain is a member by default.

Special Identity Groups Special identity groups, described in Table 5-4, don't appear as objects in Active Directory Users and Computers, but they can be assigned permissions by adding them to resources' DACLs. Membership in these groups is controlled dynamically by Windows, can't be viewed or changed manually, and depends on how an account accesses the OS. For example, membership in the Authenticated Users group is assigned to a user account automatically when the user logs on to a computer or domain. No group scope is associated with special identity groups.

Table 5-4 Special identity groups

Group	Description
Anonymous Logon	Users and services that access domain resources without using an account name or a password. Typically used when a user accesses an FTP server that doesn't require user account logon.
Authenticated Users	Members include any user account (except Guest) that logs on to a computer or domain with a valid username and password. Often used to specify all users in a forest.
Creator Owner	A user becomes a member automatically for a resource he or she created (such as a folder) or took ownership of. Often assigned Full control permission for subfolders and files only on the root of a drive so that a user who creates a file or folder on the drive has full control of the object automatically.
Dial-up	A user logged on through a dial-up connection is a member.
Everyone	Refers to all users who access the system. Similar to the Authenticated Users group but includes the Guest user.
Interactive	Members are users logged on to a computer locally or through Remote Desktop. Used to specify that only a user sitting at the computer's console is allowed to access a resource on that computer.
Network	Members are users logged on to a computer through a network connection. Used to specify that only a user who's trying to access a resource through the network can do so.
Owner Rights	New in Server 2008, it represents the current owner of a folder or file. Permissions set on this group can be used to override implicit permissions granted to the owner of a file, such as Change Permissions and Take Ownership.
Service	Any security principal logged on as a service is a member.
System	Refers to the Windows OS.
Self	Refers to the object for which permissions are being set. If this group is an ACE in the object's DACL, the object can access itself with the specified permissions.



Activity 5-10: Working with Default Groups

Time Required: 20 minutes

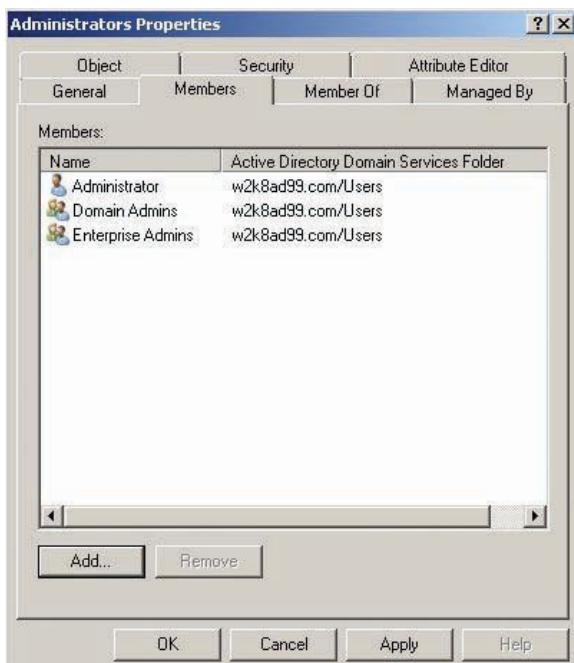
Objective: View properties of default groups.

Description: You want to see the scope and membership of some default groups that Windows creates.

1. If necessary, log on to your server as Administrator and open Active Directory Users and Computers.
2. Click the **Builtin** folder. Click the **Administrators** group, and open its Properties dialog box. Click the **General** tab, if necessary. The options in the Group scope and Group type sections

are disabled because you can't change the scope or type of groups in the Built-in folder. Notice that the selected scope is Built-in local. These groups are considered domain local, but there are some differences between Built-in domain local and other domain local groups, as you'll see.

- Click the **Members** tab to see this group's members (see Figure 5-19), and then click **Cancel**.



5

Figure 5-19 Members of the Administrators group

- Next, view the membership of the **Guests** and **Users** groups. Notice that the **Users** group has two special identities as members. Close both Properties dialog boxes.
- Click the **Users** folder. Click **Domain Admins**, and open its Properties dialog box. Click the **General** tab, if necessary. Notice that you can't change this group's scope or type. Click the **Members** tab to view the group membership, and then click **Cancel**.
- Next, view the membership of the **Domain Users** group. Notice that all the users you have created became members of this group automatically. Close this Properties dialog box.
- View the membership of the **Domain Computers** group. Notice that the Vista computer is a member of this group. Close this Properties dialog box.
- Log on to the domain from your Vista computer as Administrator.
- Open Windows Explorer, and click the C: drive. Create a new folder named **TestScope**.
- Right-click **TestScope** and click **Properties**. Click the **Security** tab. Next to the Administrators and Users ACEs, *computer name\group* in parentheses is displayed. This notation differentiates users and groups on the local computer from users and groups of the same name on the domain.
- Click **Edit**. Click **Add**. In the Select Users, Computers or Groups dialog box, you can click the Locations button to select objects from the local computer or a different domain.
- Click **Advanced**, and then click **Find Now**. Scroll down and click **Group1-DL**, and then click **OK** twice.
- Click **Add**. Type **Users** (the name of the Built-in local group in Active Directory), and then click **Check Names**. You get the Name Not Found message box because even though **Users** is a domain local group, it can't be added to the DACL of member computers because it's a Built-in local group. Built-in local groups can be added only to the DACLs of domain controller resources. The right way to add all users to a member computer's DACL is to add the local

- Users group to the DACL because the local Users group has the Domain Users group as a member by default. Click **Cancel**.
14. Click the **Locations** button. Click the name of your computer, and then click **OK** to have Windows look in the local SAM database for objects. Click **Check Names**. Windows adds *computer name* in front of the Users name you entered in Step 13. Click **OK** three times.
 15. Click **Start**, point to **Administrative Tools**, and click **Computer Management**. Double-click **Local Users and Groups**, and then click **Groups**. (If Administrative Tools isn't on your Start menu, add it as follows: Right-click **Start** and click **Properties**. Click the **Customize** button. Scroll down the list box to System Administrative Tools, click **Display on the All Programs menu and the Start menu**, and then click **OK** twice.)
 16. Click the **Users** group, and open its Properties dialog box to view its membership. Notice that Domain Users is one of the members. When a computer joins a domain, the local Users group gains the Domain Users group as a member, and the local Administrators group gains the Domain Admins group as a member. Click **Cancel**.
 17. Close all open windows, and log off the Vista computer.

Working with Computer Accounts

Computer accounts are created in Active Directory when a workstation becomes a member of the domain. Like a user account, a computer account is a security principal with an SID and a password and must authenticate to the domain. Unlike a user account, an administrator can't manage a computer account's password, which each computer changes automatically every 30 days. Only computers running Windows NT or later can have a computer account in the domain; Windows 9x computers can't have an account.

Don't confuse having a computer account with a user's ability to access domain resources. A user can log on to a workgroup computer with any Windows version installed and still access domain resources. For example, if users log on to a Windows Vista computer that isn't a domain member, they can access domain resources in the usual way, by using the UNC path. However, they must log on to each domain resource they want to access in the format *domain\username*. Just the same, having users log on to computers that are domain members has these advantages:

- *Single sign-on*—Users who log on from domain member computers have access to any permitted resources throughout the forest without needing to authenticate again.
- *Active Directory search*—Users of domain member computers can search Active Directory for objects and resources throughout the forest.
- *Group policies*—Administrators can manage aspects of member computers by using group policies, including security settings and use restrictions.
- *Remote management*—Administrators can right-click a computer object and choose **Manage** to run the Computer Management MMC for member computers.

Creating Computer Accounts

Generally, computer accounts are created when a computer joins the domain. In Activity 5-5, you joined a Vista computer to the domain. When a computer account is created in this way, the account is placed in the Computers folder by default. This behavior also applies to member servers. To gain the full benefit of computer accounts, move them to an OU you have created because the Computers folder can't have a group policy linked to it. Furthermore, because you usually require different policies for servers and user workstations, you can move computer accounts for servers and workstations to separate OUs and link different group policies to these OUs.



You can use the Redircmp command-line program to specify a different default location for computer accounts created when a computer joins the domain.

You can also create computer accounts manually before the computer joins the domain. When a computer attempts to join a domain, it automatically uses a computer account matching its computer name, if one exists in Active Directory. Some administrators prefer the manual method so that computer accounts can be created in an OU that already has a group policy linked to it. By doing so, the computer or server is subject to group policies immediately on joining the domain, and the administrator doesn't have to move the computer account later. Additionally, by creating the account manually, the administrator doesn't have to give the "Add workstations to domain" right to users.

By default, the Authenticated Users group is granted the "Add workstations to domain" right so that users need only a valid username and password to join their computers to the domain. This right permits users to join computers to the domain and create up to 10 computer accounts in the domain. If administrators don't want users to have this right, they can change it through group policies. Other groups that can add workstations to a domain are Domain Admins, Account Operators, and Enterprise Admins.



Managing Computer Accounts

Computer account objects are, for the most part, a set-it-and-forget-it proposition. After creating them and possibly moving them to another OU, you might not need to do anything with these objects. However, sometimes administrators must attend to computer accounts—usually when something has gone wrong.

As mentioned, a computer account has an associated password and must log on to the domain. The computer changes this password automatically every 30 days by default. If the password becomes unsynchronized between the computer and the computer account in Active Directory, the computer can no longer access the domain. Sometimes the password can become unsynchronized if a computer has been turned off or is otherwise unable to contact a domain controller for an extended period and, therefore, can't change its password. In effect, the password expires, and the only solution is to reset the computer account by right-clicking the computer object in Active Directory Users and Computers and clicking Reset Account. After resetting, the computer must leave the domain (by joining a workgroup) and then join it again. You can also use the Netdom command-line program on member servers with an unsynchronized account. This program resets the password on the local server and the corresponding computer account, so the server doesn't have to leave and rejoin the domain.



If the computer does become unsynchronized with its account in Active Directory, users get a message stating that the trust relationship between the workstation and the domain failed.

TIP

Another reason for an administrator to access a computer account is to run the Computer Management MMC remotely on a member computer. As mentioned, clicking Manage in the right-click menu of a computer account opens Computer Management on that computer. The Computer Management MMC includes the Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Reliability and Performance, Device Manager, Disk Management, and Services and Applications snap-ins—quite a bit of management capability available at a click.

Computer accounts can be deleted or disabled, just as user accounts can be. You might need to delete a computer account if the computer is no longer a member of the domain or, rarely, if resetting the account doesn't solve the problem of a computer not being able to log on to the domain. In these cases, you can delete the account and re-create it. The computer must also leave and rejoin the domain. You might need to disable a computer account if the computer (a laptop, for example) won't be in contact with the domain for an extended period. When the computer needs access to the domain again, you can re-enable the computer account. Note that, unlike a user account with a unique security ID usually tied to security permissions, computer accounts can be deleted and re-created more readily with little (if any) impact on the network or users of the computer.

You might wonder why you would ever want to place computer accounts into groups. The most common reason for creating groups for computer accounts is to use group policy filtering to configure exceptions for a group of users or computers that would normally be affected by a policy. Group policy filtering is discussed in Chapter 7.

Automating Account Management

Account management has been discussed mostly from the standpoint of using Active Directory Users and Computers to work with accounts. When only a few accounts require action, using a GUI tool is convenient. When many accounts require action or certain tasks must be repeated many times, however, a command-line program is often the most efficient tool for the job. Administrators can take advantage of batch files to handle lengthy and cumbersome command-line syntax. A batch file is a text file with the .bat extension that's used to enter a command or series of commands normally typed at the command prompt. Batch files can take arguments to replace variables in the command. Bulk import/export programs also make account management faster and easier. These programs can read an input file (import) to create several Active Directory objects at once or produce an output file (export) from Active Directory objects. In the following sections, examples and activities walk you through using command-line and bulk import/export programs to manage accounts.

Command-Line Tools for Managing Active Directory Objects

The GUI interface of Active Directory Users and Computers is convenient for creating a few accounts or making changes to a few objects. Even with the help of a template, however, quite a bit of manual entry is still required to create a user. Many administrators prefer a command-line program, often used with a batch file, to create or change accounts. The following are the most common command-line tools for managing accounts:

- **DSADD**—Adds objects to Active Directory. Used mainly for adding account objects but can also be used to create OUs and contacts.
- **DSGET**—Displays an object's properties onscreen by default, but the output can be redirected to a file.
- **DSMOD**—Modifies existing Active Directory objects.
- **DSMOVE**—Moves objects in a domain to another folder or OU or renames the object.
- **DSQUERY**—Finds and displays objects in Active Directory that meet specified criteria. The output can be displayed onscreen or sent (piped) to other commands. For example, DSQUERY could find and display a list of all users in an OU, and that list could be piped to a DSMOD command that adds the users to a group.
- **DSRM**—Removes, or deletes, objects from Active Directory.

You can type all these commands followed by “/?” to get help on syntax and use. For example, if you need to know more about the DSADD command, type DSADD /? at the command prompt.

You used DSADD in Chapter 3 to create a user. Now take a closer look at its syntax and how you can use it in a batch file to make account creation easier. The syntax for using DSADD to create objects is as follows:

```
DSADD ObjectType ObjectDN [options]
```

- *ObjectType* is the type of object you want to create, such as a user or group.
- *ObjectDN* is the object's distinguished name (DN), which includes the full path in Active Directory where the object should be created. The path is specified by starting with the object name, followed by each parent container object up to the top-level domain name. Each component of the path is separated by a comma. The components of the DN are as follows:
 - **CN (common name)**—The name of the object as it will be seen in Active Directory.
 - **CN (common name)**—The CN component can be repeated if the object is in a folder, such as the Users or Computers folder, rather than an OU.
 - **OU (organizational unit)**—Use this component if the object is in an OU. It's repeated for as many levels as necessary, starting with the lowest OU level.
 - **DC (domain component)**—Each part of the domain name is specified separately until the top-level domain name is reached.

For example, to create a user account named BSmith in the Sales OU, which is in the Marketing parent OU in the w2k8ad99.com domain, the command is as follows:

```
DSADD user CN=BSmith,OU=Sales,OU=Marketing,DC=w2k8ad99,DC=com
```

To create a computer account named New Computer in the Computers folder in the same domain, the command is as follows:

```
DSADD computer "CN=New Computer,CN=Computers,DC=w2k8ad99,DC=com"
```

The quotation marks around the distinguished name path are required if the path contains any spaces, including after commas. In this example, the computer name New Computer has a space in it.

Following the DN, a command can include options specified with this syntax:

-OptionName OptionValues

For example, if you want to add BSmith and include the first name and last name attributes, the command uses the -fn and -ln options, as shown:

```
DSADD user CN=BSmith,OU=Sales,OU=Marketing,DC=w2k8ad99,DC=com -fn  
Bill -ln Smith
```

The DSADD command's syntax is somewhat intimidating, and if you had to type this entire command over and over, you might start to wonder how useful it is. The command's usefulness is apparent, however, when you have to create several accounts with similar properties except a few that are unique for each user. You can construct the command once in a batch file with a placeholder for the unique information that varies each time the command is used. For example, you could type the following command in a text file saved as uadd.bat:



The variables in this command are indicated with *italics*. When you type the actual command, however, you don't use any text formatting.

```
DSADD user "CN=%1,OU=Sales,OU=Marketing,DC=w2k8ad99,DC=com" -fn %2  
-ln %3 -pwd Password01 -memberof Sales-G -mustchpwd yes
```

This command creates a user in the specified container and domain, assigns the password Password01, places the user in the Sales-G group, and requires that the user change the password at next logon. The %1, %2, and %3 are variables replaced with username, first name, and last name. For example, to run the uadd.bat batch file to create a user named Susan Martin with the username SMartin, you enter the following:

```
uadd SMartin Susan Martin
```

For each user you need to create, you have to specify only the username, first name, and last name. If you have several users with similar properties to create, you could complete the task considerably faster than in Active Directory Users and Computers, even if you used a user template.



Activity 5-11: Creating a Batch File for the DSADD Command

Time Required: 20 minutes

Objective: Create a batch file for the DSADD command.

Description: A new department, Advertising, has been added to your company, and 15 new employees will be hired immediately. You have already created the OU structure to accommodate this new department: the Advertising OU under the Marketing OU. All users will belong to a global group called Advert-G, which you need to create first.

1. If necessary, log on to your server as Administrator and open Active Directory Users and Computers.
2. Click to expand the **Marketing** OU, and then click the **Advertising** OU.

3. Create a security group called **Advert-G** with global scope.
4. Click **Start**, type **Notepad** in the Start Search text box, and press **Enter**.
5. In Notepad, type the following on one line: **DSADD user "CN=%1, OU=Advertising, OU=Marketing, DC=w2k8adXX, DC=com" -fn %2 -ln %3 -upn %1@w2k8adXX.com -pwd Password01 -memberof "CN=Advert-G, OU=Advertising, OU=Marketing, DC=w2k8adXX, DC=com" -mustchpwd yes.**
6. Save the file as **C:\uadd.bat**. Because Notepad adds the .txt extension automatically, enclose the filename in quotation marks to preserve the .bat extension. Exit Notepad.
7. Open a command prompt window. Type **C:\uadd AdvUser1 Advertising User1** and press **Enter**.
8. The last line of the command output should start with “dsadd succeeded.” If DSADD failed, check the syntax in the uadd.bat file. Make sure there’s a space between the option name and the option value, and you replaced XX with your student number in all three places your domain name appears.
9. Refresh the view in Active Directory Users and Computers by clicking **Action, Refresh** from the menu or clicking the **Refresh** toolbar icon. The user you just created should appear in the Advertising OU and be a member of the Advert-G group.
10. Create two more users named **AdvUser2** and **AdvUser3** (with first names and last names in the format shown in Step 7) by using the batch file. Leave Active Directory Users and Computers and the command prompt window open for the next activity.

One benefit of some command-line programs is that you can use the output of one as input to another, called **piping**. You can use piping with the DSQUERY and DSMOD commands, but it’s not unique to directory service commands. One of the most common uses of piping is to send the output of any command displaying more than one screen of information to the more program. You can try it by displaying the help information for a command:

```
DSMOD user /? | more
```

The vertical bar, called a “pipe,” specifies sending the output of DSMOD user /? to the more program, which simply paginates information it receives so that you can view one page of output at a time. In the following activity, you use DSQUERY to find and display Active Directory information and then use a pipe to DSMOD to add users to a group.



Activity 5-12: Using DSQUERY and DSMOD with a Pipe

Time Required: 10 minutes

Objective: Pipe output from DSQUERY to DSMOD to add users to a group.

Description: All users in the Marketing OU and all OUs under it need to be added to a new group called Marketing-G. You create the group and use DSQUERY and DSMOD to assign group memberships.

1. If necessary, log on to your server as Administrator, open a command prompt window, and open Active Directory Users and Computers.
2. At the command prompt, type **DSADD group "CN=Marketing-G, OU=Marketing, DC=w2k8adXX, DC=com"** and press **Enter**.



By default, groups are created as global security groups. Therefore, as shown in the command in Step 2, you don’t need to specify group scope and type unless the group you’re creating has different settings.

3. Type **DSQUERY user OU=Marketing,DC=w2k8adXX,DC=com** and press **Enter**. (You don’t have to use quotation marks if there are no spaces in the DN path.) The output should be a list of all users, shown in DN format, in the Marketing OU and all its child OUs. This data is what’s piped to the DSMOD command in the next step.

4. Type **DSQUERY user OU=Marketing,DC=w2k8adXX,DC=com | DSMOD group CN=Marketing-G,OU=Marketing,DC=w2k8adXX,DC=com -addmbr** and press **Enter**.
5. If you get a message indicating that DSMOD was successful, open Active Directory Users and Computers, if necessary. If you get an error, check the syntax and spelling, and make sure there are no spaces between DN components.
6. In Active Directory Users and Computers, click the **Marketing-G** group in the Marketing OU. (You might need to refresh the view before you can see this group. If so, click **Action, Refresh** from the menu.) Open its Properties dialog box, and then click the **Members** tab. You should see all the users the DSQUERY command displayed in Step 3.
7. At some point, the passwords of most users you have created will expire. To set their passwords to never expire, enter the following command: **DSQUERY user | DSMOD user -pwdneverexpires yes**
8. Close all open windows.

Another feature of many command-line programs is redirecting output to a file instead of displaying it onscreen. The syntax to redirect output is as follows:

command > outputfile

For example, you could use the DSQUERY command from the previous activity to send the results to a file named MktgUsers.txt:

```
DSQUERY user OU=Marketing,DC=w2k8adXX,DC=com > MktgUsers.txt
```

Command-line programs such as DSADD work well when you have many objects to create, especially when used with a batch file. DSQUERY is also useful for displaying a list of objects based on particular criteria or piping the data to programs such as DSMOD for further processing. What if you already have a database or spreadsheet of possibly hundreds of users to create, however? When you have a file with Active Directory objects to create, two programs can import that information into Active Directory: CSVDE and LDIFDE.

Bulk Import and Export with CSVDE and LDIFDE

CSVDE and LDIFDE can bulk import or export Active Directory data; the difference between them is mainly the format of files they use. CSVDE uses the comma-separated values (CSV) format common in database and spreadsheet programs. LDIFDE uses LDAP Directory Interchange Format (LDIF), which isn't as common but is useful when you're working with LDAP applications. Another difference is that CSVDE can only create objects in Active Directory, and LDIFDE can create or modify objects.

Neither program has a simple method for importing a list of people directly from a database or spreadsheet, but with a little database or spreadsheet programming know-how, you can do it without too much trouble. The easiest way to get an idea of the file format these programs use is to use their export functions to create an output file. In CSVDE, the following command creates a file called MktUsers.csv that can be opened in Notepad, as shown in Figure 5-20:

```
csvde -m -f mktusers.csv -d "ou=marketing,dc=w2k8ad99,dc=com" -r
"(objectClass=user)"
```

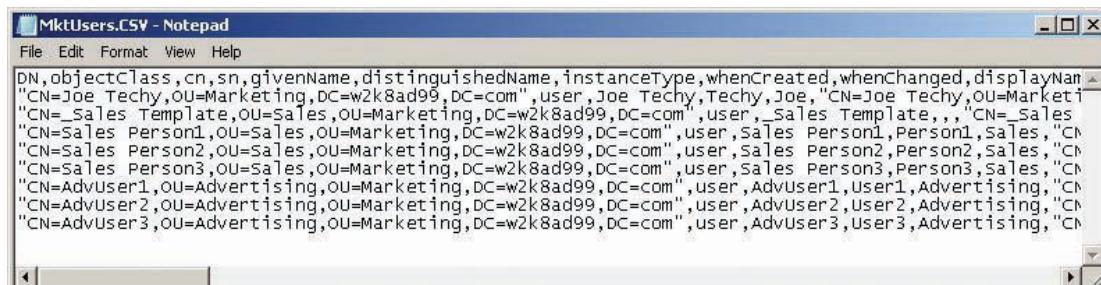


Figure 5-20 An export file created by CSVDE

To see the same output from LDIFDE, use the following command (see Figure 5-21):

```
ldifde -f MktUsers -d "ou=Marketing,dc=w2k8ad99,dc=com" -r
"objectClass=user"
```

```
MktUsers - Notepad
File Edit Format View Help
dn: CN=Joe Techy,OU=Marketing,DC=w2k8ad99,DC=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: user
cn: Joe Techy
sn: Techy
givenName: Joe
distinguishedName: CN=Joe Techy,OU=Marketing,DC=w2k8ad99,DC=com
instanceType: 4
whenCreated: 20080405192527.0Z
whenChanged: 20080405192527.0Z
displayName: Joe Techy
usNCreated: 16648
memberof: CN=Marketing,OU=Marketing,DC=w2k8ad99,DC=com
```

Figure 5-21 An export file created by LDIFDE

As mentioned, LDIFDE is more powerful because of its capability to modify Active Directory objects. One method is exporting the objects you want to modify, making changes to the attributes you’re modifying, and importing the file. Each object in the exported file has an associated action specified by the changetype line (the second line of output in Figure 5-21). To modify objects, change the action in the changetype line to “modify.” LDIFDE is also useful for bulk moving of users from one domain to another. Users can be exported from one domain and imported to the other domain.

Creating Users with CSVDE You can use a regular text file to import users (and other objects) into Active Directory with CSVDE, but the file must be formatted correctly. A CSV file must have a header record (the first line of a file) listing attributes of the object to be imported. For a user, it normally includes at minimum the distinguished name, the SAM account name, the UPN, and the object class attribute. Here’s an example of a header record:

```
dn, SamAccountName, userPrincipalName, objectClass
```



To find a list of any object’s attributes, open the Attribute Editor tab of its Properties dialog box. To see this tab, you must enable Advanced Features on Active Directory Users and Computer’s View menu.

A data record for this CSV file looks like this:

```
"cn>New User, ou=TestOU, dc=w2k8adXX, dc=com", NewUser,
NewUser@w2k8adXX.com, user
```

You add a data record for each user you need to create. Creating this file manually is no time saver compared with using DSADD in a batch file or even using Active Directory Users and Computers. If you have a database of several hundred users you need to create, however, with a little experience in Access or other database programs, you could create this file from the database easily. A major drawback of CSVDE is that you can’t set passwords with it, so all accounts are disabled until you create a password for each account that meets complexity requirements. As a workaround, you can temporarily set the password policy for the domain to allow blank passwords.



Activity 5-13: Using CSVDE to Create Users

Time Required: 10 minutes

Objective: Create a text file to use with CSVDE to import users.

Description: You have a large database of users, and you need to create user accounts for them. You have heard of the CSVDE program but haven’t used it. You want to create a CSV file manually to import a test user before writing code to create the file with a database program.

1. If necessary, log on to your server as Administrator.
2. Click **Start**, type **notepad** in the Start Search text box, and press **Enter**.
3. In Notepad, type the following, pressing **Enter** after each line:



In the following example, take care to type the second and third lines on one line, and then type the fourth and fifth lines on one line.

```
dn, SamAccountName, userPrincipalName, objectClass
"cn=CSV User1,ou=TestOU,dc=w2k8adXX,dc=com", CSVUser1,
CSVUser1@w2k8adXX.com, user
"cn=CSV User2,ou=TestOU,dc=w2k8adXX,dc=com", CSVUser2,
CSVUser2@w2k8adXX.com, user
```

5

4. Click **File**, **Save As** from the menu. In the Save as type list box, click **All Files (*.*)**. In the File name text box, type **C:\csvusers.csv**, and then click **Save**. Exit Notepad.
5. Open a command prompt window. Type **cd ** and press **Enter**. Type **csvde -i -f csvusers.csv** and press **Enter**.
6. Close the command prompt window, and open Active Directory Users and Computers. Click the **TestOU** OU and verify that the users were created. Leave Active Directory Users and Computers open for the next activity.

Creating Users with LDIFDE The LDIF format is considerably different from the CSV format, but the idea is the same. Instead of a header line followed by data records, each object consists of a series of lines, and each line specifies an action or attribute. Following is an example of a file for creating a user:

```
dn: cn=LDF User1,ou=TestOU,dc=w2k8adXX,dc=com
changetype: add
ObjectClass: user
SamAccountName: LDFUser1
UserPrincipalName: LDFUser1@w2k8adXX.com
```

Aside from the format of data in the file, the data is no different from what's in a CSV file, except the changetype entry, which can be add, modify, or delete (depending on what you're doing with objects). One common use of LDIFDE is exporting users from one domain and importing them into another domain.



Activity 5-14: Using LDIFDE to Create Users

Time Required: 10 minutes

Objective: Create a text file to use with LDIFDE to import users.

Description: You have a large database of users, and you need to create user accounts for them. You have heard of the LDIFDE program but haven't used it. You want to create a CSV file manually to import a test user before writing code to create the file with a database program.

1. If necessary, log on to your server as Administrator.
2. Click **Start**, type **notepad** in the Start Search text box, and press **Enter**.
3. In Notepad, type the following, pressing **Enter** after each line:

```
dn: cn=LDF User1,ou=TestOU,dc=w2k8adXX,dc=com
changetype: add
ObjectClass: user
SamAccountName: LDFUser1
UserPrincipalName: LDFUser1@w2k8adXX.com
```

4. Click **File, Save As** from the menu. In the Save as type list box, click **All Files (*.*)**. In the File name text box, type **C:\ldfusers.ldf**, and then click **Save**. Exit Notepad.
5. Open a command prompt window. Type **cd ** and press **Enter**. Type **ldifde -i -f ldfusers.ldf** and press **Enter**.
6. Close the command prompt window, and open Active Directory Users and Computers, if necessary. Click the **TestOU** OU and verify that the user was created. If necessary, refresh the view so that you can see this user.
7. Close all open windows.

Chapter Summary

- User accounts provide a way for users to authenticate to the network and contain user information that can be used in a company directory. There are three categories of users in Windows: local, domain, and built-in. The two built-in accounts are Administrator and Guest.
- Active Directory Users and Computers is the main tool for creating and maintaining user accounts. User account names must be unique in a domain, aren't case sensitive, and must be 20 or fewer characters. A complex password is required by default. A naming standard should be devised before creating user accounts. At the very least, the user's full name, logon name, and password are required to create a user account in Active Directory Users and Computers.
- User templates facilitate creating users who have some attributes in common, such as group memberships. Administrators can use the multiple edit feature of Active Directory Users and Computers to edit certain fields for several users at once.
- The most important user account properties are in the General, Account, Profile, Member Of, and Terminal Services tabs. The Account tab contains information that controls many aspects of logging on to the domain, such as logon name, logon hours, logon locations, account lockout, and account expiration. The Profile tab contains information about where a user's profile data is stored and can specify a logon script.
- A user profile contains personal files and settings that define the user's environment. By default, the profile is local and stored as a subdirectory of the %SYSTEMDRIVE%\Users folder. A profile stored on a network share is called a roaming profile and is configured in the Profile tab of a user account's Properties dialog box. Profiles can be made mandatory by renaming the Ntuser.dat file as Ntuser.man in the user's profile directory.
- Groups are the primary security principal used to grant rights and permissions. The two group types are security and distribution, but only security groups are used to assign permissions and rights. The group type can be converted from security to distribution and vice versa.
- There are three group scopes in Active Directory: domain local, global, and universal. (Local groups are found on domain member computers and stand-alone computers.) The recommended use of groups can be summarized with the acronyms AGDLP and AGGUDLP. Groups can be nested, as long as the rules for group membership are followed. Group scope can be converted, with some restrictions. There are default groups in the Built-in and Users folders, and there are special identity groups with dynamic membership that can't be managed.
- Computers that are domain members have computer accounts in Active Directory. Domain users logging on to member computers can use single sign-on forestwide and perform Active Directory searches. Computers can be managed by using group policies and remote MMCs.
- Computer accounts are created automatically when a computer joins a domain or manually by an administrator. By default, computer accounts are created in the Computers folder, but to use group policies, they must be moved to an OU that has a group policy linked to it.
- You can automate account management by using command-line tools, such as DSADD and DSMOD, and bulk import/export programs, such as CSVDE and LDIFDE. Command-line tools can be simplified by using batch files and piping.

Key Terms

5

contact An Active Directory object that usually represents a person for informational purposes only, much like an address book entry.

distribution group A group type used when you want to group users together, mainly for sending e-mails to several people at once with an Active Directory-integrated e-mail application, such as Microsoft Exchange.

distribution list An Active Directory object consisting of a list of users in a distribution group, used for sending an e-mail to multiple people simultaneously.

domain local group A group scope that's the main security principal recommended for assigning rights and permissions to domain resources.

global group A group scope used mainly to group users from the same domain who have similar access and rights requirements. A global group's members can be user accounts and other global groups from the same domain.

group scope A property of a group that determines the reach of a group's application in a domain or a forest—which security principals in a forest can be group members and to which forest resources a group can be assigned rights or permissions.

local group A group created in the local SAM database on a member server or workstation or a stand-alone computer.

local profile A user profile stored on the same system where the user logs on.

mandatory profile A user profile that can be changed during a user's logon session, but the next time the user logs on, the changes aren't saved, and the profile reverts to its original state.

piping Sending the output of one command as input to another command.

roaming profile A user profile that follows the user no matter which computer he or she logs on to. It's stored on a network share so that when a user logs on to any computer in the network, the profile is copied from the network share to the profile folder on the local computer.

security groups A group type that's the main Active Directory object administrators use to manage network resource access and grant rights to users.

super mandatory profile A user profile type that prevents a user from logging on to the domain when the mandatory profile is unavailable.

universal group A group scope that can contain users from any domain in the forest and be assigned permission to resources in any domain in the forest.

user profile A collection of a user's personal files and settings that define his or her working environment.

user template A user account that's copied to create users with common attributes.

Review Questions

1. Which of the following is a user account category? (Choose all that apply.)

- a. Local
- b. Global
- c. Domain
- d. Universal

2. Which of the following is a built-in user account? (Choose all that apply.)

- a. Administrator
- b. Operator
- c. Anonymous
- d. Guest

3. Sam*Snead is a valid user account name. True or False?
4. Which of the following is true about user accounts in a Windows Server 2008 domain? (Choose all that apply.)
 - a. The name can be from 1 to 20 characters.
 - b. The name is case sensitive.
 - c. The name can't be duplicated in the domain.
 - d. Using default settings, PASSWORD123 is a valid password.
5. Which of the following account options can't be set together? (Choose all that apply.)
 - a. User must change password at next logon
 - b. Store password using reversible encryption
 - c. Password never expires
 - d. Account is disabled
6. Global groups can have domain local groups as members. True or False?
7. Jane has left the company. Her user account is a member of several groups and has permissions and rights to a number of forestwide resources. Jane's replacement will arrive in a couple of weeks and need access to the same resources. In addition, you want the new employee to have access to the files in Jane's profile. What is the best course of action?
 - a. Find all groups Jane is a member of and make a note of them. Delete Jane's user account and create a new account for the new employee. Add the new account to all the groups Jane was a member of.
 - b. Copy Jane's user account and give the copy another name.
 - c. Disable Jane's account. When the new employee arrives, rename Jane's account, assign it a new password, and enable it again.
 - d. Back up Jane's profile and restore it to a folder assigned to the new employee.
8. Over the past several months, Tom, who has access to sensitive company information, has logged on to computers in other departments and left them without logging off. You have discussed the matter with him, but the problem continues to occur. You're concerned that someone could access these sensitive resources easily. What's the best way to solve this problem?
 - a. Ensure that all computers Tom is logging on to have screen savers set to lock the computer after 5 minutes of inactivity.
 - b. Specify which computers Tom can log on to in the domain by using the Log On To option in his account's properties.
 - c. Move Tom's account and computer to another domain, thereby making it impossible for him to log on to computers that are members of different domains.
 - d. Disable local logon for Tom's account on all computers except Tom's.
9. You have noticed inappropriate use of computers for gaming and Internet downloads by some employees who come in after hours and on weekends. These employees don't have valid work assignments during these times. You have been asked to devise a solution for these employees that doesn't affect other employees or these employees' computers during working hours. What's the best solution?
 - a. Install personal firewall software on their computers in an attempt to block the gaming and Internet traffic.
 - b. Request that the Maintenance Department change the locks on their office doors so that they can enter only during prescribed hours.
 - c. Set the Logon Hours options for their user accounts.
 - d. Before you leave each evening and before the weekend, disable these employees' accounts and re-enable them the next working day.

10. The Users domain local group can be a member of the local Administrators group on a Vista computer. True or False?
11. Which of the following is considered a security principal? (Choose all that apply.)
- Contacts
 - Computers
 - User accounts
 - Distribution lists
12. You're trying to troubleshoot a user's profile. When you open the folder containing the profile, you notice that many files and folders you expect to see are missing. The symptoms of the problem don't indicate so many files and folders being missing. What's the likely problem, and how can you solve it?
13. What file do you see in the root of a user's mandatory profile?
- Netlogon.dat
 - Netlogon.man
 - Ntuser.dat
 - Ntuser.man
14. You have just installed 50 new Vista computers. You want to be sure that all users get an initial profile you have created when they first log on to a computer in the domain; they can then customize the profile as needed. Which of the following is a required step for this task?
- Rename Ntuser.dat.
 - Copy the appropriate files to the Default folder on every computer in the domain.
 - Create a folder named Default User.V2.
 - Assign permissions to the NETLOGON share.
15. You want to prevent users from logging on to the domain if their mandatory profiles are unavailable for some reason. Which of the following is a necessary step?
- Configure the Log On To option in the user's account.
 - Add .man to the profile path in their account properties.
 - Add .V2 to the profile path in their account properties.
 - Click the Super Mandatory check box in their account properties.
16. You have configured roaming profiles throughout your company. However, employees are now complaining that logging on and off sometimes take a long time. You have also noticed a spike in overall network traffic, particularly during the beginning and end of shifts. What can you do to reduce the delays and reduce network traffic while maintaining the convenience of roaming profiles?
17. Which of the following is a valid group scope? (Choose all that apply.)
- Global
 - Domain local
 - Forest
 - Domain global
18. What happens if a security group that's an ACE in a shared folder is converted to a distribution group?
- A security group can't be converted to a distribution group if it has already been assigned permissions.
 - The group is removed from the DACL automatically.

- c. The group remains in the DACL, but the ACE has no effect on members' access to the resource.
 - d. The group remains in the DACL, and permissions assigned to the group affect access to the resource as though it were still a security group.
19. Which of the following can be a member of a universal group? (Choose all that apply.)
- a. User accounts from the local domain only
 - b. Global groups from any domain in the forest
 - c. Other universal groups from any domain in the forest
 - d. Domain local groups from the local domain only
20. Which group conversion is allowed?
- a. Domain local to universal, provided no domain local group is already a member
 - b. Global to domain local, without restriction
 - c. Domain local to global, provided no domain local group is already a member
 - d. Universal to global, without restriction
21. Which of the following is true about the Users domain local group?
- a. It's in the Users folder.
 - b. It can be converted to a global group.
 - c. Domain Users is a member.
 - d. Its members can log on locally to a domain controller.
22. A domain user logging on to the domain becomes a member of which special identity group?
- a. Creator Owner
 - b. System
 - c. Authenticated Users
 - d. Anonymous Logon
23. Windows 98 computers can have a computer account in a Windows Server 2008 domain. True or False?
24. A user is having trouble logging on to the domain from a computer that has been out of service for several months. Nobody else can seem to log on from the computer either. What should you try first to solve the problem?
- a. Reinstall Windows on the workstation and create a new computer account in the domain.
 - b. Rename the computer and create a new computer account with the new name.
 - c. Reset the computer account, remove the computer from the domain, and rejoin it to the domain.
 - d. Disable the computer account, remove the computer from the domain, and rejoin it to the domain.
25. Which commands can you use together to change attributes of several users at once?
- a. DSGET and DSADD
 - b. DSGET and DSMOD
 - c. DSQUERY and DSMOD
 - d. DSQUERY and DSGET

Case Projects



Case Project 5-1: Creating Groups for Your Domain

Recall the OU structure you created in Case Projects 4-1 and 4-2 with the coolgadgets.com OU simulating the domain. Create groups in the OUs under coolgadgets.com that are appropriate for the domain structure. The group members are the users in each department the OU represents. Explain your group-naming standard, and specify the group scope you're using for these groups. Are any groups candidates for nesting?

Case Project 5-2: Creating User Templates for Each Department

You know that you'll be creating several users for each department in coolgadgets.com. Users in each department will have some common attributes, specifically membership in their departmental groups and information in the Organization tab's Department and Company fields. Create a user template for each department. What are some best practices you should follow when creating this user template?

Case Project 5-3: Creating Users for Your Departments

Using the user template you created in Case Project 5-2, create two users in each department. For simplicity's sake, name the users *DepartmentUserX* with a full name of *Department UserX*. For example, in the Operations Department, the first user is OperationsUser1 with the full name Operations User1. Assign the password Password01 to each user. Additionally, create a third user in each department named *MgrDepartment*, so for the Operations Department, the user is MgrOperations with a full name of Manager Operations.

Case Project 5-4: Using Command-Line Account Management

Use DSADD to create a Managers group in the coolgadgets.com OU. Next, use DSQUERY and DSMOD with a pipe to add the manager accounts you created in Case Project 5-3 to the Managers group. Write down the commands you used and turn them into your instructor, or take a screen shot of the commands and their output.



This page intentionally left blank

Windows File and Print Services

**After reading this chapter and completing
the exercises, you will be able to:**

- Describe features of the major Windows file systems
- Secure access to files with permissions
- Share folders with Windows file sharing
- Use Windows storage management tools
- Work with Windows printers

The file system is a critical component of all operating systems. The OS and users must be able to retrieve and store files quickly and securely for the network to function smoothly. File access often goes hand in hand with printer access, which is why these two functions are usually coupled.

As network use has grown through the years and storage requirements have exploded, file system management has grown into the broader topic of storage management. This chapter discusses available file systems in Windows Server 2008 and how to secure access to files. It also covers tools and strategies for reliable storage management and using Windows to provide a robust, manageable printing environment for users.



Although File Services and Print Services aren't major objectives of the 70-640 exam (as they are in the 70-642 exam), these topics are central to the reasons for using a computer network, and providing and securing access to file and printer resources is tightly coupled with Active Directory user and group accounts.

Windows File Systems

A **file system** defines the method and format that an OS uses to store, locate, and retrieve files from electronic storage media. On a server, the primary storage medium is a hard disk, so it's the focus of this discussion. Windows supports two file systems for storing files on hard disks: FAT and NTFS. NTFS is by far the more important and dominant in modern versions of Windows. However, FAT is still found on workstations and servers occasionally, and there are valid reasons to use this file system in certain circumstances.

Before going into detail on FAT and NTFS, reviewing the components of a file system is helpful. Modern file systems are composed of some or all of the following components:

- ***Filenaming convention***—All files stored on a disk are identified by name, and the file system defines rules for how a file can be named. These rules include length, special characters that can be used (such as \$, #, %, &, and !), and case sensitivity (differentiating uppercase and lowercase letters).
- ***Hierarchical organization***—Most file systems are organized as an inverted tree structure, with the root of the tree at the top and folders or directories acting as branches. Each folder can be empty or contain a list of files and additional folders. In most file systems, folders or directories don't contain the data that make up an actual file; rather, they contain information about a file along with a pointer to its location on the disk. Information for each file is usually referred to as a directory entry.
- ***Data storage method***—Space on hard disks is divided into one or more partitions, with each partition containing its own file system. Typically, each partition is divided into 512-byte sectors. The file system groups one or more sectors into blocks or clusters, which are used as the basic unit of storage for file data. These blocks are indexed so that the file data they contain can be retrieved easily. A single file can occupy from one to many thousands of blocks. File systems vary in the methods they use for indexing and managing these blocks, which affect the efficiency and reliability of data storage and retrieval.
- ***Metadata***—Metadata is information about a file beyond its name and the data it contains. This information is generally stored by the directory or folder that holds a file's name or in a data structure the directory entry points to. Metadata can include time and date stamps indicating when a file was created, last changed, and last accessed; descriptive information about the file that can be used in searches; file attributes; and access control lists.
- ***Attributes***—Attributes are usually on/off settings, such as Read-only, Hidden, and so forth. Different file systems have different sets of attributes that can be applied to files and folders.
- ***Access control lists (ACLs)***—ACLs determine who can access a file or folder and what can be done with the file (read, write, delete, and so on).

File systems vary in whether and how each component is implemented. Generally, more advanced file systems have flexible filenames, an efficient method of managing data storage, a considerable amount of metadata, advanced attributes, and ACLs. In Chapter 1, you reviewed some basic differences between the FAT and NTFS file systems. Next, you examine these file systems more closely.



There are many more file systems than FAT and NTFS. For more information on other file systems and a comparison of features, see http://en.wikipedia.org/wiki/Comparison_of_file_systems.

NOTE

6

The FAT File System

The File Allocation Table (FAT) file system consists of two variations: FAT16 and FAT32. FAT16 is usually simply referred to as FAT. The name “File Allocation Table” suggests the structure used to manage data storage. FAT16 has been around since the mid-1980s, which is one of its biggest strengths—it’s well known and well supported by most OSs. FAT32 arrived on the scene with the release of Windows 95 OSR2 in 1996.



A third variation of FAT, FAT12, is the original implementation of FAT developed in the late 1970s. It was limited to use on floppy disks.

NOTE

The main difference between FAT16 and FAT32 is the size of the disk partition that can be formatted. FAT16 is limited to 2 GB partitions in most implementations (although Windows NT permits partitions up to 4 GB). FAT32 allows partitions up to 2 TB, but in Windows 2000 and later, Microsoft limits them to 32 GB because the file system becomes noticeably slower and inefficient with larger partition sizes. This 32 GB limitation applies only to creating partitions; Windows can read FAT32 partitions of any size. FAT16 supports a maximum file size of 2 GB, and FAT32 supports files up to 4 GB.



The number in FAT file system names refer to the number of bits available to address disk clusters. FAT16 can address up to 2^{16} disk clusters, and FAT32 can address up to 2^{32} disk clusters. The number of disk clusters a file system can address is directly proportional to the largest partition size it supports.

NOTE

Already, you can see that the FAT file system has severe limitations in today’s computing environment. The file size limitation alone prevents storing a standard DVD image file on a FAT file system. The limitations are even more apparent when you consider reliability and security requirements of current OSs. FAT doesn’t support file and folder permissions for users and groups, so any user logging on to a computer with a FAT disk has full control over every file on that disk. In addition, FAT lacks support for encryption, file compression, disk quotas, and reliability features, such as transaction recovery and journaling, all of which NTFS supports.

You might think that FAT isn’t good for much, especially compared with the more robust NTFS, but FAT still has its place. It’s the only file system option when using older Windows OSs, such as Windows 9x. In addition, FAT is simple and has little overhead, so it’s still the file system of choice on removable media, such as floppy disks and the increasingly popular flash drives. For hard drives, however, particularly on Windows servers, NTFS is unquestionably the way to go.

The NTFS File System

NTFS is a full-featured file system that Microsoft introduced with Windows NT in 1993. Since that time, its features have been expanded to help administrators gain control of ever-expanding storage requirements. NTFS has supported file and folder permissions almost since its inception,

which was a considerable advantage over FAT. Many compelling features have been added, particularly with the release of Windows 2000:

- *Disk quotas*—Enable administrators to limit the amount of disk space that users' files can occupy on a disk volume. Starting with Windows Server 2008, quotas can also be specified for folders.
- *Volume mount points*—Make it possible to associate the root of a disk volume with a folder on an NTFS volume, thereby forgoing the need for a drive letter to access the volume.
- *Shadow copies*—Enable users to keep historical versions of files so that they can revert a file to an older version or restore an accidentally deleted file.
- *File compression*—Allows users to store documents in a compressed format without needing to run a compression/decompression program to store and retrieve the documents.
- *Encrypting File System (EFS)*—Makes encrypted files inaccessible to everyone except the user who encrypted the file, including users who have been granted permission to the file.

Disk Quotas With the number and types of files used today requiring more disk space on corporate servers, **disk quotas** are a welcome tool to help administrators get a handle on server storage. Typically, disk quotas are set on an NTFS volume and, by default, apply to all users except administrators. Quotas are configured in the Quota tab of an NTFS volume's Properties dialog box (see Figure 6-1).

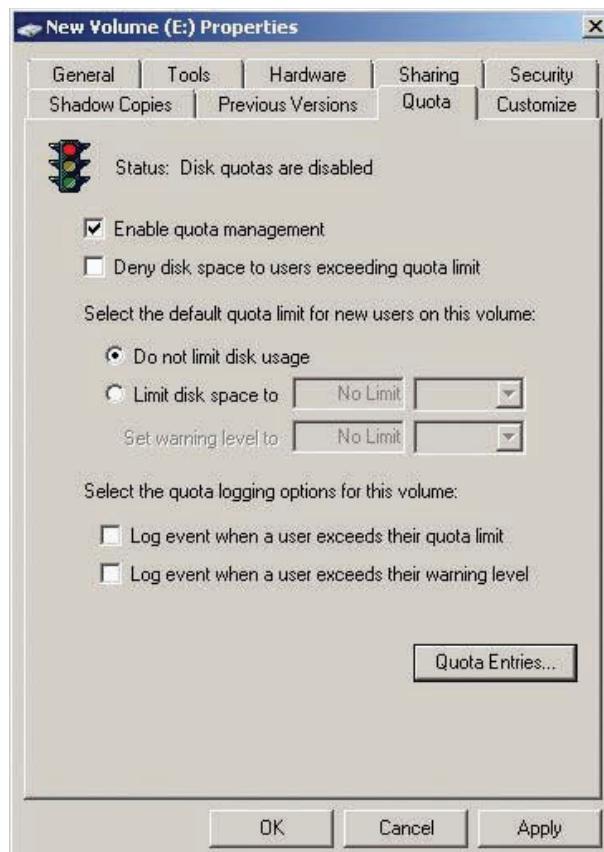
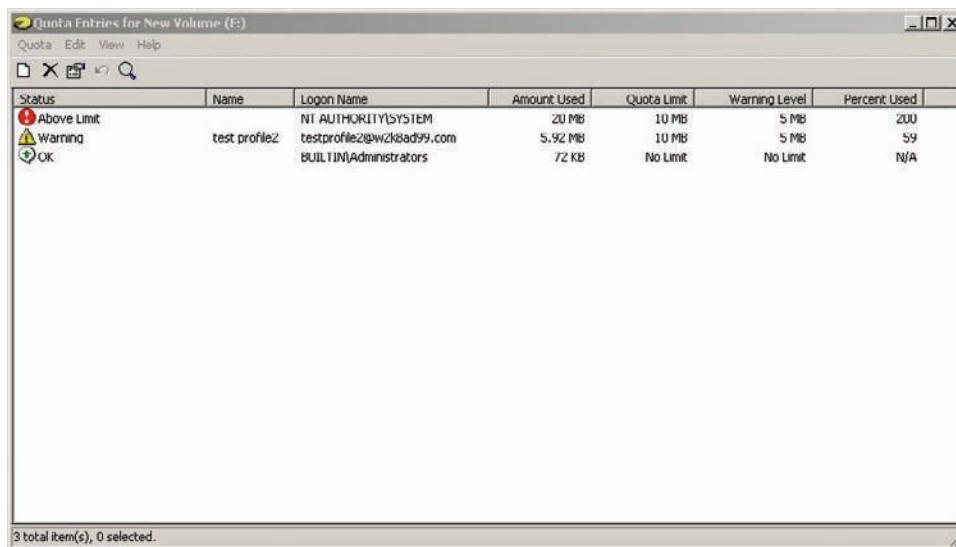


Figure 6-1 The Quota tab

The options for setting quotas are as follows:

- *Enable quota management*—When this check box is selected, quotas are enabled on the volume. (Quotas are disabled by default.) After they're enabled, the quota system begins tracking each user's disk use and creates quota entries with details on usage. To see quota entries, click the Quota Entries button.
- *Deny disk space to users exceeding quota limit*—This option prevents users from saving files to the volume when their limit is exceeded. When this check box is not selected, administrators can still view disk quota entries and use the logging options to monitor how much space each user is using.
- *Do not limit disk usage*—When this option is selected, no disk use limits are set, but the quota system tracks usage for each user.
- *Limit disk space to*—When this option is selected, administrators can specify the maximum amount of space users can occupy and set a warning level that must be less than or equal to the limit. Disk space can be specified in kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).
- *Log event when a user exceeds their quota limit*—Selecting this option creates an entry in the event log when users exceed their quota limits. These events are written only after the NTFS driver scans the disk for quota entries that exceed the limit or warning level. Scanning occurs at one-hour intervals by default.
- *Log event when a user exceeds their warning level*—Selecting this option creates an entry in the event log when users exceed their warning levels.
- *Quota Entries*—Clicking this button opens the Quota Entries window, where you can view users' disk usage information. In addition, the limits specified in the Quota tab can be overridden by editing or creating an entry for a user. Figure 6-2 shows the Quota Entries window.



The screenshot shows a Windows application window titled "Quota Entries for New Volume (E:)". The window has a menu bar with "Quota", "Edit", "View", and "Help". Below the menu is a toolbar with icons for "New", "Edit", "Delete", "Search", and "Help". The main area is a table with the following data:

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
Above Limit		NT AUTHORITY\SYSTEM	20 MB	10 MB	5 MB	200
Warning	test profile2	testprofile2@W2K8AD99.com	5.92 MB	10 MB	5 MB	59
OK		BUILTIN\Administrators	72 KB	No Limit	No Limit	N/A

At the bottom of the window, a status bar displays "3 total item(s), 0 selected.".

Figure 6-2 The Quota Entries window

By default, administrators aren't subject to quota limits. For example, in Figure 6-2, the local Administrators group's entry specifies no limits. If you want to impose quotas on specific administrators, you can create a new quota entry for each of these administrators and set limits. You can create quota entries for regular users as well, if you want to specify a different limit or warning level from those in the volume's Quota tab. Note that quota entries can be created only for user accounts, not groups.

Be aware of how user disk use is calculated. Windows determines each user's disk usage based on the owner of each file on the volume. If ownership of a file changes, disk space use for the previous file owner decreases and increases for the new file owner. By default, the creator of a file is the file's owner, including files created when a user copies a file.



Activity 6-1: Enabling Quotas

Time Required: 10 minutes

Objective: Enable disk quotas on a new volume.

Description: You want to get a handle on server disk use before it gets out of hand, so you decide to enable disk quotas on the volume where most user files are stored.



This activity assumes you have a second, unallocated disk installed on the domain controller. If not, use unallocated disk space from Disk 0 instead of using Disk 1.

NOTE

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Computer Management** to open the Computer Management MMC. Click to expand the **Storage** node, if necessary, and then click **Disk Management**.
3. Right-click the unallocated space of Disk 1 and click **New Simple Volume**. Click **Next**. In the Simple volume size in MB text box, type **2000**, and then click **Next**.
4. In the Assign the following drive letter list box, click **Q** (for quotas), and then click **Next**.
5. Leave the File system and Allocation unit size settings as NTFS and Default, respectively. Type **QData** in the Volume label text box. Click **Next**, and then click **Finish**. Windows formats the partition, and when it's finished, the Disk Management window should look similar to Figure 6-3.

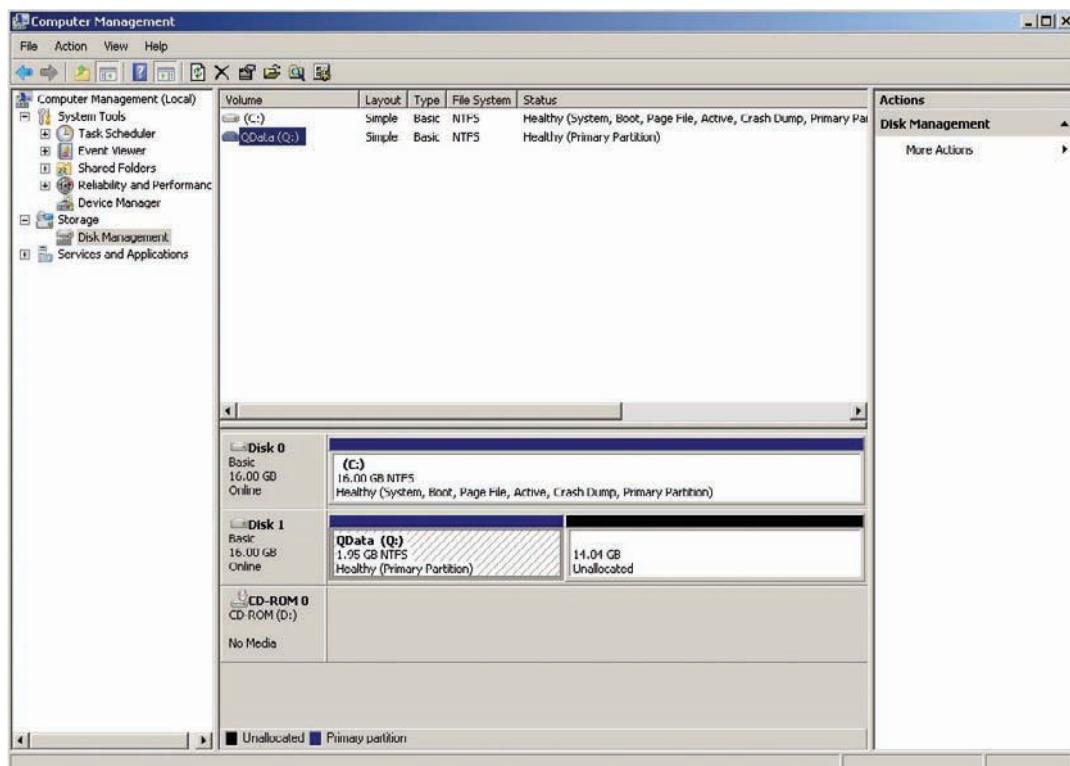


Figure 6-3 Disk Management with a new volume created

6. Right-click the **QData** volume you just created and click **Properties**. Click the **Quota** tab, and then click the **Enable quota management** and **Deny disk space to users exceeding quota limit** check boxes.
7. Click the **Limit disk space to** option button. Type **10** and click **MB**. In the Set warning level to text box, type **5** and click **MB**. These numbers are set very low just for demonstration purposes. Typically, quota limits and warning levels are set much higher.
8. Click both check boxes starting with **Log event when a user exceeds . . .**, and then click the **Quota Entries** button. You see only a single entry, the default Administrators group. Close the Quota Entries window, and then click **OK** to close the Properties dialog box. Click **OK** in the Disk Quota message box to enable the quota system.
9. Right-click the **QData** volume and click **Explore**.
10. Create a folder called **Shared**. Right-click the **Shared** folder you just created and click **Share**. In the list box at the top, click **Everyone**, and then click the **Add** button.
11. Click the **Everyone** entry in the list box at the bottom. Click the list arrow in the Permission Level column, and then click **Contributor** in the list. Click the **Share** button, and then click **Done**.
12. Close all open windows.



Activity 6-2: Working with Quotas

Time Required: 15 minutes

Objective: Test disk quotas.

Description: You want to see how disk quotas work, so you log on to the domain from your Vista computer as a test user. You copy files to the share on the server and examine the results when you exceed the warning level and quota limit.

1. Log on to the domain from your Vista computer as **testuser1** with the password **Password01**.
2. Open Windows Explorer, navigate to **C:\Windows\System32**, and copy the **wmploc.dll** file. You're using this file because its size is larger than the warning level and smaller than the quota limit.
3. Click **Start**, type **\serverXX\Shared** in the Start Search text box, and press **Enter**. When the Windows Explorer window opens, paste the **wmploc.dll** file into the share.
4. Log on to your server as Administrator, if necessary. Click **Start**, **Computer**. Right-click the **QData** volume and click **Properties**. Click the **Quota** tab.
5. Click the **Quota Entries** button. You should see a new quota entry for **testuser1** with a Warning icon in the Status column. Double-click the **testuser1** entry. If necessary, you could assign a different quota limit and warning level for this user or choose not to limit disk space. Click **Cancel**. Close the Quota Entries window.
6. On your Vista computer, copy the **wmploc.dll** file and paste it in the share. You should get a message indicating that there's not enough space to copy the file. Click **Cancel**.
7. On your server, click to clear the **Deny disk space to users exceeding quota limit** check box, and then click **Apply**.
8. On your Vista computer, try to copy and paste the **wmploc.dll** file into the share again. When prompted, click **Copy, but keep both files**. You should be successful this time.
9. On your server, open the Quota Entries window again. Test User1 should now have an Above Limit icon in the Status column. Close the Quota Entries window. In the Quota tab of the volume's Properties dialog box, click to clear the **Enable quota management** check box to disable quotas on the volume. Click **Apply**, and then click **OK**. Click **OK** again.
10. Close all open windows on your server and Vista computer.

Volume Mount Points **Volume mount points** enable you to access a volume as a folder in another volume instead of by using a drive letter. The volume that holds the folder serving as the mount point must be an NTFS volume, and the folder must be empty. In UNIX and Linux, mount points rather than drive letters have always been used to access disk volumes, so users of these OSs should be quite comfortable with mount points. Windows volumes can be assigned both a mount point and a drive letter, if needed. Some reasons for using mount points include the following:

- Extend the apparent amount of free space on an existing volume. For example, a Windows XP or Vista user uses several applications with large multimedia files. These files are stored in the Documents (My Documents in Windows XP) folder in the user's profile on the C drive. The C drive is getting low on disk space, so a new disk is installed. Instead of assigning the disk a drive letter and copying the user's documents to the new volume, you can mount the volume in a folder under the user's Documents (My Documents) folder. New files can be added to this folder, thereby maintaining the user's normal working environment.
- Consolidate frequently accessed volumes. For example, you have a computer with two hard disk volumes, C and D; a DVD volume, E, where you keep a reference DVD; and a flash drive, F, which you use to transfer documents. You can create a folder to act as a mount point for each drive in your Documents folder on the C drive so that you have access to all data in these volumes in a convenient location.
- Consolidate several shared volumes under a single network share. Instead of having several different share names that users must remember, you can have a single shared folder containing each volume as a mount point. In this way, users have access to all shared volumes through a single share.



Activity 6-3: Using a Volume Mount Point

Time Required: 10 minutes

Objective: Make a volume accessible by using a mount point.

Description: You have created a volume to which all users need access. You already have a shared folder that users can access through a mapped drive, and you don't want to complicate matters by adding another mapped drive. The solution is to mount this new volume as a folder in the existing shared folder.

1. Log on to your server as Administrator, if necessary.
2. Open the Computer Management MMC, and then open the Disk Management snap-in. Right-click the **QData** volume and click **Change Drive Letter and Paths**. Click **Add**. Click **Browse**, click to expand the **C** drive, and then click the **TestShare** folder you created in Chapter 3.
3. Click **New Folder**. Type **QData** to change the folder name, and then click **OK** twice. Notice that QData is still assigned the drive letter Q. The drive letter can be unassigned, but as is, the QData volume can be accessed by using both the drive letter and the mount point.
4. Right-click the **C** drive and click **Explore**. Double-click the **TestShare** folder to verify that QData is mounted there. Notice that the mount point is represented as a drive icon with a shortcut arrow.
5. To test network access to the share and mounted volume, log on to your Vista computer as **testuser1** with **Password01**. Click **Start**, type **\serverXX\testshare** in the Start Search text box, and press **Enter**. You should see the QData folder in TestShare. Network users don't see the drive icon, so QData being a mounted volume isn't visible to network users.
6. Close all open windows and log off your Vista computer.

Shadow Copies Like quotas, **shadow copies** are enabled on an entire volume. When this feature is enabled, users can access previous versions of files in shared folders and restore files that have been deleted or corrupted. You configure shadow copies in the Shadow Copies tab of a volume's Properties dialog box (see Figure 6-4). Shadow copies are disabled by default.

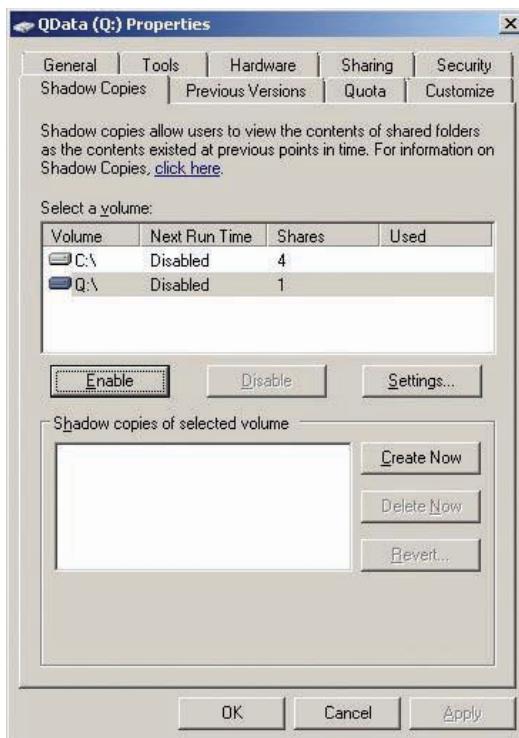


Figure 6-4 The Shadow Copies tab

When you enable shadow copies on a volume, Windows warns you that the default settings aren't appropriate for heavily used servers and recommends configuring the settings manually. The most important setting is the location of shadow copies. By default, Windows allocates space on the same volume where shadow copies are enabled. On servers with a lot of shared files that are accessed and changed frequently, this default setting might not be ideal because of the additional load shadow copies place on the disk system. Volumes used heavily for sharing files should be configured to use a different volume for storing shadow copies—one that doesn't have shadow copies enabled. If you want to change the default volume, you should do so in the Settings dialog box (see Figure 6-5) before enabling shadow copies. Otherwise, you have to disable shadow copies, change the storage volume, and reenable shadow copies.



Figure 6-5 The Settings dialog box for shadow copies



Be aware that disabling shadow copies deletes all previous versions of documents maintained by shadow copies.

The Settings dialog box for shadow copies offers the following options:

- **Located on this volume**—Choose the volume for storing previous versions of files the Shadow Copies service creates. By default, the volume on which shadow copies are enabled is used. The volume must be an NTFS volume.
- **Details**—Click this button to view statistics on how much space shadow copies are using and how much free space is still available on the volume.
- **Maximum size**—By default, the Use limit option is set to 10% of the total volume size, but a minimum of 300 MB is required. You can also specify No limit, but this option is recommended only if you use a separate volume for storing shadow copies.
- **Schedule**—By default, shadow copies are created when they are first enabled on a volume and then two times a day at 7:00 a.m., and 12:00 p.m., Monday through Friday. You can change the schedule to suit your environment. To create shadow copies manually, click the Create Now button in the Shadow Copies tab of the volume’s Properties dialog box (shown previously in Figure 6-4).

When the disk space that shadow copies use reaches the specified limit, or available space on the volume can no longer accommodate a new shadow copy, older copies are deleted. Remember, shadow copies of files aren’t created as each file is changed. Shadow copies are created for the entire volume at once on the prescribed schedule (or manually). So on a volume with many shared files that change frequently, considerable disk space might be required each time the Shadow Copies service runs. Regardless of the disk space available for shadow copies, a maximum of 64 previous versions are kept. When the 65th shadow copy is created, the oldest one is deleted. If necessary, shadow copies can be deleted to free up disk space. In the Shadow Copies tab, select the volume at the top, and the shadow copies for the selected volume are listed at the bottom by the date and time they were created. Select the instance you want to delete, and then click the Delete Now button.

At times, you might need to revert all shared files in a volume to a previous shadow copy instance. The Revert button in the Shadow Copies tab does just that. Select the shadow copy instance you want, and click Revert to restore all shared folders on the volume to an earlier time. Keep in mind that if you use this feature, any files created since the selected shadow copy instance are deleted.



Activity 6-4: Configuring Shadow Copies

Time Required: 15 minutes

Objective: Enable shadow copies on a volume.

Description: You have several shares on a volume that store documents employees use. These documents change frequently and have sometimes been deleted or corrupted accidentally. You have spent quite a bit of time restoring files from backup at users’ requests, so you decide to enable shadow copies on the volume.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, **Computer**. Right-click the **QData** volume and click **Configure Shadow Copies**. (You can also open the volume’s Properties dialog box and click the Shadow Copies tab.)
3. In the Select a volume list box, click **Q:** if it’s not already selected. Each volume on the computer has an entry so that you can configure shadow copies for all volumes in one place. Each volume entry tells you the next scheduled run time for shadow copies, the number of shares on the volume, and how much space shadow copies are currently using.

4. Click the **Settings** button. If necessary, you can change where shadow copies for this volume are stored. The Use limit option is set to 10% of volume size or 300 MB, whichever is higher. Click the **Schedule** button. The schedule currently contains two entries: one for 7:00 a.m. and one for 12:00 p.m. Monday through Friday. You can delete and add entries to the default schedule to create your own schedule. Click **Cancel**, and then click **OK**.
5. To enable shadow copies and create the first shadow copy, click to select the Q:\ volume, and then click the **Enable** button. Read the resulting message and click **Yes**. Click the new entry in the Shadow copies of selected volume list box, and note that the Delete Now and Revert buttons are enabled.
6. Click the **Revert** button, and read the Volume Revert message. Click **Check here if you want to revert this volume**, and then click **Revert Now**. The shadow copy entry is deleted because this instance was used to revert the volume.
7. Click **Create Now**. A new shadow copy entry is created. Click **OK**.
8. Open Windows Explorer, and navigate to the **Shared** folder on the QData volume. Right-click the **Shared** folder in the left pane, point to **New**, and click **Text Document**.
9. Open the volume's Properties dialog box again, and click the **Shadow Copies** tab. If necessary, click the Q:\ volume. Click the entry in the Shadow copies of selected volume list box, and then click **Revert**. Click **Check here if you want to revert this volume**, and then click **Revert Now**. Click **OK**.
10. In Windows Explorer, click to open the **Shared** folder in the left pane, if necessary. Right-click empty space in the Shared folder and click **Refresh**. Notice that the text document you created is gone. Create another text document. Open it in Notepad, type your name and save the file, and exit Notepad.
11. Open the volume's Properties dialog box again, and click the **Shadow Copies** tab. If necessary, click the Q:\ volume. Click **Create Now**, as you need a shadow copy for the next activity, and then click **OK**.

6



Activity 6-5: Using Shadow Copies

Time Required: 10 minutes

Objective: Use shadow copies to revert to a previous version.

Description: You want to test your shadow copies configuration. You access the Shared folder on the QData volume from a network client, make changes to the text document you created, and revert to the saved version.



Vista is configured with the Shadow Copy client needed to access previous versions of files made available with shadow copies. If you're using Windows XP, you must install the client software. You can find instructions and a link to the client at <http://technet.microsoft.com/en-us/windowsserver/bb405951.aspx>.

1. Log on to the domain from your Vista computer as **testuser1** with **Password01**.
2. From Vista, open the **Shared** share located on your server. (If necessary, see Step 3 of Activity 6-2 for a reminder of how to do this.)
3. Open the text document in the Shared share that you created in Activity 6-4; you should see your name in this document. Add your address or anything you like to this file. Save the file, and then exit Notepad.
4. Right-click the text document and click **Restore previous versions**. The file's Properties dialog box opens to the Previous Versions tab. Only one previous version is listed, and you have options to open it to view its contents, copy it so that you don't overwrite the current version, or restore it and overwrite the current version.
5. Click **Restore** twice. You should get a message stating that the file was restored successfully. Click **OK**, and then click **OK** again.

6. Open the text document and verify that it contains only your name. Exit Notepad.
7. Log off Vista, but stay logged on to your server.

File Compression and Encryption File compression and encryption on an NTFS volume are implemented as file attributes, like the Read-only and Hidden attributes. One caveat: These attributes are mutually exclusive, so a file can't be both compressed and encrypted. You can set only one of these two attributes.

Files can be compressed and accessed without users needing to take any explicit action to uncompress them. When a compressed file is opened, the OS uncompresses it automatically. On NTFS volumes, you can enable file compression on the entire volume, a folder and its contents, or a file. You can enable compression on an entire volume at the time you format it or by clicking the "Compress this drive to save disk space" option in the General tab of the volume's Properties dialog box. If you compress a drive when you format it, all files stored on the volume are compressed. When you compress a volume after it has been formatted, you're asked whether you want to compress only the root of the drive or the root of the drive plus all subfolders and files. If you compress just the root, only new files placed in the root of the volume are compressed. If you compress all subfolders and files, all existing files plus new files are compressed on the entire volume.

You can compress a single folder as well. The same rules for the volume apply to a folder. If you compress only a folder, only new files added to the folder are compressed, and existing folders and files are left alone. If you apply changes to this folder, subfolders, and files, all new and existing files in the folder and its subfolders are compressed. By default, compressed folders and files can be identified by their blue filenames. A single file can be compressed by setting its compression attribute.

When copying or moving files, you should be aware of these rules for compression behavior:

- Files *copied* to a new location inherit the compression attribute from the parent container. So whether a file is compressed or not, if it's copied to a folder or volume that has the compression attribute set, the file is compressed. If the destination's compression attribute is not set, the file isn't compressed.
- Files *moved* to a new location on the same volume retain their current compression attributes. Files moved to a different volume inherit the compression attribute from the parent container. This behavior happens because files moved to a different volume are actually copied to the new volume and deleted from the original volume, so the behavior is the same as with copied files.

File encryption on NTFS volumes is made possible by Encrypting File System (EFS) and works in a similar manner to file compression. You can set the encryption attribute on a file or folder but not on a volume. If encryption is set on a folder, as with compression, you're prompted with the option to set the attribute on the folder only or on the folder, subfolders, and files. By default, encrypted folders and files can be identified by their filenames displayed in green.

The rules for encryption behavior when copying and moving files are different from the rules for compression:

- Encrypted files that are copied or moved always stay encrypted, regardless of the destination's encryption attribute. The exception is if the file is copied or moved to a FAT volume, in which case the file is decrypted because FAT doesn't support encryption.
- Unencrypted files that are moved or copied to a folder with the encryption attribute set are always encrypted.

Encrypted files can usually be opened only by the user who encrypted the file. However, this user can designate other users who are allowed to access the file. In addition, in a domain environment, the domain Administrator account is designated as a recovery agent. A designated recovery agent can decrypt a file if the user account that encrypted it can no longer access it. This

can happen if an administrator resets a user's password, the user account is deleted, or the user leaves the company. To encrypt a file, click the Advanced button in the General tab of a file's Properties dialog box, and then click Encrypt contents to secure data (see Figure 6-6). To see the recovery agent and which accounts can access the encrypted file, click the Details button to open the dialog box shown in Figure 6-7.



6

Figure 6-6 The Advanced Attributes dialog box

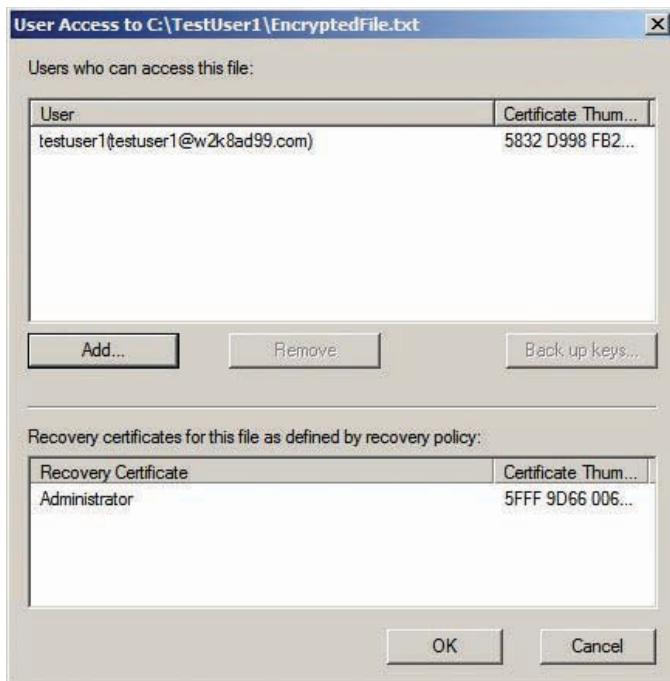


Figure 6-7 Viewing user access to an encrypted file

A user must have a valid EFS certificate to be added to an encrypted file's access list. EFS is set up to issue an EFS certificate automatically to any user who encrypts a file. Users can also be issued a certificate from a certificate server. Recovery agents are identified by certificates, too, but recovery agent certificates can't be used as EFS certificates and vice versa. Certificates and Active Directory Certificate Services are discussed in Chapter 11.



Activity 6-6: Using Disk Compression

Time Required: 10 minutes

Objective: Set the compression attribute on folders and files.

Description: You want to understand the compression attribute on an NTFS volume, so you set the attribute on some files and folders, and then copy and move the files to see how compression behaves.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and click to open the **QData** volume. Create two folders named **Ctest1** and **Ctest2**.
3. Right-click **Ctest1** and click **Properties**. Click **Advanced**. In the Advanced Attributes dialog box, click the **Compress contents to save disk space** check box, and then click **OK** twice. Note that the Ctest1 folder's name is blue.
4. Click to open the **Ctest1** folder, and create a text document in it named **Test1**. Note that the Test1 filename is blue, indicating that it's compressed. Open **Test1**, type your name, and then save and close the file. Access to the compressed file is transparent, meaning you didn't have to do anything special to open it.
5. Copy **Test1** and paste it in the same folder. Rename this file **Test2**.
6. Right-click and drag **Test2** to the Ctest2 folder. Release the right mouse button and click **Move Here**. Click to open the **Ctest2** folder. Note that Test2 is still compressed. Press **Ctrl+Z** to undo the last action. Test2 is moved back to the Ctest1 folder.
7. Right-click and drag **Test2** to the Ctest2 folder. Release the right mouse button and click **Copy Here**. Click the **Ctest2** folder. Notice that Test2 isn't compressed because copied files inherit the compression attribute from their parent folders, and moved files retain their compression attribute (unless moved to a different volume). Close any open windows.



Activity 6-7: Using File Encryption

Time Required: 20 minutes

Objective: Use EFS to protect sensitive files.

Description: You want to instruct users on how to encrypt files on their computers. You decide to perform some tests so that you have a solid understanding of how encryption works.

1. Log on to the domain from your Vista computer as **testuser1** with **Password01**.
2. Click **Start**, **Computer**. In the left pane of Windows Explorer, click to open the **Public** folder under Favorite Links. Double-click the **Public Documents** folder to open it.
3. Create a text file in the Public Documents folder, and name it **Encrypted1**. Open the Advanced Attributes dialog box for Encrypted1, click the **Encrypt contents to secure data** check box, and then click **OK** twice. When you get the Encryption Warning message, click the **Encrypt the file only** option button and **Always encrypt only the file** check box, and then click **OK**.
4. Open Encrypted1 in Notepad, and type your name in it. Save the file, and exit Notepad.
5. Open the Advanced Attributes dialog box for Encrypted1, and click the **Details** button. Notice that testuser1 is listed as a user who can access the file, and Administrator is listed as a recovery agent. Click **Add**. Only testuser1's certificate is listed because no other user has been issued an EFS certificate on this computer. Click **Cancel** twice, and then click **OK** twice.
6. Log off and log on as **testuser2** with **Password01**. Navigate to the **Public Documents** folder. Double-click **Encrypted1** to open it. You get an Access Denied message. Click **OK**, and then exit Notepad.
7. Create a text file named **Encrypted2**. Set the encryption attribute on the file, and then click **OK** until all Properties dialog boxes are closed. Open the Advanced Attributes dialog box

- for Encrypted2. Click **Details**, and then click **Add**. Note that testuser1 and testuser2 are listed. Click **testuser1**, and then click **OK**. Click **OK** three more times.
8. Log off and log on again as **testuser1**. Click to open the **Public Documents** folder. Verify that you can open Encrypted2 without error, and then close the file.
 9. Copy **Encrypted2** to the desktop. Verify that the new file remains encrypted by opening the Advanced Attributes dialog box. Oddly, when an encrypted or compressed file is on the desktop, the filename remains a normal color instead of green (for encrypted) or blue (for compressed).
 10. Log off Vista.

EFS is a valuable feature on an NTFS volume as an extra layer of security for files stored on the hard drive. EFS is particularly important on laptops and other systems that aren't well protected from theft or loss. If a computer or hard drive is stolen, accessing data in an EFS-protected file takes considerable effort. However, NTFS file and folder permissions, discussed in the next section, remain the primary method of controlling access to files on domain controllers and member servers.

6

Securing Access to Files with Permissions

There are two modes for accessing files on a networked computer: network (sometimes called remote) and interactive (sometimes called local). It follows, then, that there are two ways to secure files: share permissions and NTFS permissions. Share permissions are applied when a user attempts network access to shared files. NTFS permissions always apply, whether file access is attempted interactively or remotely, through a share. That last statement might sound confusing, so take a closer look at how permissions work.



NTFS permissions work much like Active Directory object permissions, with concepts such as permission inheritance and special permissions, so much of what you learned about Active Directory permissions in Chapter 4 applies here as well.

Permissions can be viewed as a gatekeeper to control who has access to folders and files. When you log on to a computer or domain, you're issued a ticket containing information such as your username and group memberships. If you attempt to access a file or folder, the gatekeeper examines your ticket and compares your username and group memberships (including special identity groups) to the file or folder's access list. If neither your username nor your groups are on the list, you're denied access. If you or your groups *are* on the list, you're issued an access ticket that combines all your allowed permissions. (Deny permissions are exceptions, as you learned in Chapter 4 and examine again later in this chapter.) You can then access the resource as specified by your access ticket.

At least, that's how the process works when you're attempting interactive access to files. If you're attempting network access, there are two gatekeepers: one that checks your ticket against the share permissions access list and, if you're granted access by share permissions, another that checks your ticket against the NTFS permissions access list. The NTFS gatekeeper is required to examine your ticket only if you get past the share gatekeeper. If you're granted access by share permissions, you're issued an access ticket. Then if you're granted access by NTFS permissions, you're allowed to keep the access ticket that gives you the least permission between the two.

For example, Bill is granted Read access by share permissions and Read and Write access by NTFS permissions. Bill gets to keep only the Read access ticket because it's the lesser of the two permissions. Another example: Neither Bill nor any of Bill's groups are on the share permissions access list. There's no need to even examine NTFS permissions because Bill is denied access at the share permissions gate. As a final example, Bill is granted Full Control access by share permissions and Modify access by NTFS permissions. Bill's access ticket gives him Modify permission because it allows less access than Full Control.

The general security rule for assigning permissions to resources is to give users the least access necessary for their job. This rule is often referred to as the "least privileges principle."

Unfortunately, this axiom can be at odds with another general rule: Keep it simple. Sometimes determining the least amount of access a user requires can lead to complex permission schemes. The more complex a permission scheme is, the more likely it will need troubleshooting, and the more troubleshooting that's needed, the more likely an administrator will assign overly permissive permissions out of frustration.



NOTE

Because FAT volumes don't have permissions, everybody who logs on locally to a computer with a FAT volume has full access to all files on that volume. If a folder is shared on a FAT volume, network users' access is determined solely by share permissions.

Share Permissions

Share permissions apply to folders and files accessed across the network. Before a file can be accessed across the network, it must reside in a shared folder or a subfolder of a shared folder. Share permissions are configured on a shared folder and apply to all files and subfolders of the shared folder. These permissions can't be configured on individual files; NTFS permissions are used for that purpose.

There are three share permissions levels (see Figure 6-8):

- *Read*—Users can view contents of files, copy files, run applications and script files, open folders and subfolders, and view file attributes.
- *Change*—All permissions granted by Read, plus create files and folders, change contents and attributes of files and folders, and delete files and folders.
- *Full Control*—All permissions granted by Change, plus change file and folder permissions as well as take ownership of files and folders. (File and folder permissions and ownership are available only on NTFS volumes.)

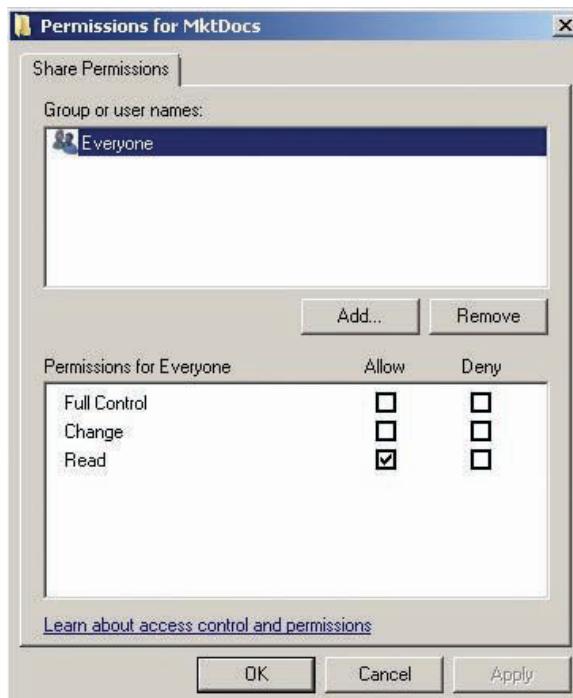


Figure 6-8 The Share Permissions tab

Windows assigns default permissions depending on how a folder is shared. (Several methods for sharing files are discussed later in “Windows File Sharing.”) Generally, the default share permission is Read for the Everyone special identity. On FAT volumes, share permissions are the

only way to secure files accessed through the network. NTFS permissions protect file accesses via the network and interactively.

NTFS Permissions

NTFS permissions give both network users and interactive users fine-grained access control over folders and files. Unlike share permissions, which can be configured only on a shared folder, NTFS permissions can be configured on folders and files. By default, when permissions are configured on a folder, subfolders and files in that folder inherit the permissions. However, inherited permissions can be changed when needed, making it possible to have different permission settings on files in a folder.

Permissions and permission inheritance, as they pertain to Active Directory objects, were discussed in Chapter 4, and they work much the same way when applied to NTFS folders and files. Perhaps the biggest difference between setting Active Directory and NTFS permissions is that there's no Delegation of Control Wizard for NTFS folders. To view or edit permissions on an NTFS folder or file, you simply access the Security tab of the object's Properties dialog box.

Unlike share permissions, which have only three permission levels, NTFS folders have six standard permissions, and NTFS files have five. Folders also have 14 special permissions, and files have 13. Special permissions aren't completely separate from standard permissions, however. Each standard permission is really a grouping of special permissions, as you see later.

NTFS standard permissions for folders and files are as follows (see Figure 6-9):

- **Read**—Users can view file contents, copy files, open folders and subfolders, and view file attributes and permissions. However, unlike the Read permission in share permissions, this permission doesn't allow users to run applications or scripts.
- **Read & execute**—Grants the same permissions as Read and includes the ability to run applications or scripts. When this permission is selected, List folder contents and Read are selected, too.
- **List folder contents**—This permission applies only to folders and grants the same permission as Read & execute. However, because it doesn't apply to files, Read & execute must also be set on the folder to allow users to open files in the folder.

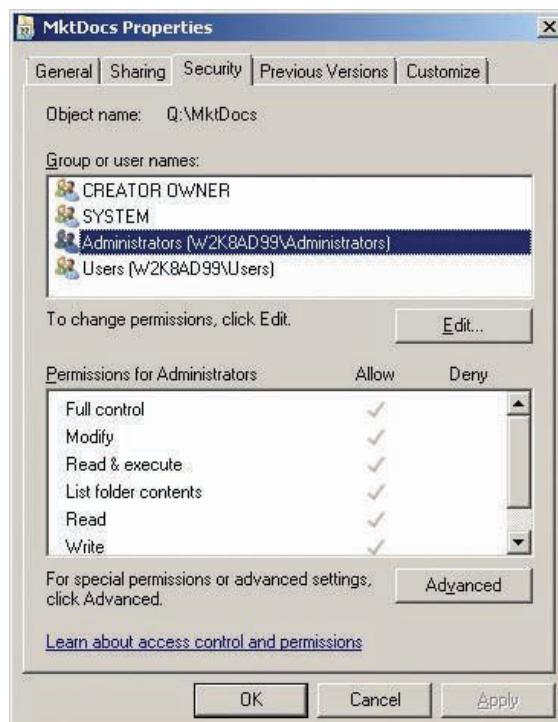


Figure 6-9 NTFS standard permissions

- *Write*—Users can create and modify files and read file attributes and permissions. However, this permission doesn't allow users to read or delete files. In most cases, the Read or Read & execute permission should be given with the Write permission.
- *Modify*—Users can read, modify, delete, and create files. Users can't change permissions or take ownership. Selecting this permission automatically selects Read & execute, List folder contents, Read, and Write.
- *Full control*—Users can perform all actions given by the Modify permission with the addition of changing permissions and taking ownership.

Standard permissions should suffice for most situations. Configuring special permissions should be reserved for, well, special circumstances. The temptation to configure special permissions to follow the least privileges principle can lead to breaking the “keep it simple” rule and result in administrators’ and users’ frustration. However, if you look at the NTFS permissions Windows sets by default on every volume, you see a few ACEs that use special permissions. So although you don’t have to use them often, you need to understand them, particularly to figure out how initial volume permissions are set. Table 6-1 describes each special permission and lists which standard permissions include it.

Table 6-1 NTFS special permissions

Special permission	Description	Included in standard permission
Full control	Same as the standard Full control permission	Full control
Traverse folder/execute file	For folders: Allows accessing files in folders or subfolders even if the user doesn't normally have access to the folder For files: Allows running program files	Full control, Modify, Read & execute, List folder contents
List folder/read data	For folders: Allows users to view subfolders and filenames in the folder For files: Allows users to view data in files	Full control, Modify, Read & execute, List folder contents, Read
Read attributes	Allows users to view file or folder attributes	Full control, Modify, Read & execute, List folder contents, Read
Read extended attributes	Allows users to view file or folder extended attributes	Full control, Modify, Read & execute, List folder contents, Read
Create files/write data	Allows users to create new files and modify the contents of existing files	Full control, Modify, Write
Create folders/append data	Allows users to create new folders and add data to the end of existing files but not change existing data in a file	Full control, Modify, Write
Write attributes	Allows users to change file and folder attributes	Full control, Modify, Write
Write extended attributes	Allows users to change file and folder extended attributes	Full control, Modify, Write
Delete subfolders and files	Allows users to delete subfolders and files in the folder	Full control
Delete	Allows users to delete the folder or file	Full control, Modify
Read permissions	Allows users to read NTFS permissions of a folder or file	Full control, Modify, Read & execute, List folder contents, Read, Write
Take ownership	Allows users to take ownership of a folder or file, which gives the user implicit permission to change permissions on that file or folder	Full control

File and Folder Ownership Every file system object (files and folders) has an owner. The object owner is granted certain implicit permissions, regardless of how permissions are set in the object’s DACL: viewing and changing permissions for the object and transferring

ownership to another user. So it's possible that users can be file owners but not be able to open the files they own. However, because owners can change permissions on files they own, they can grant themselves the permissions they want.

A user can become the owner of a file system object in three ways:

- *Create the file or folder*—The user who creates a file or folder is automatically the owner.
- *Take ownership of a file or folder*—User accounts with Full control permission or the Take ownership special permission for a file or folder can take ownership of the file or folder. Members of the Administrators group can take ownership of all files.
- *Assigned ownership*—An Administrator account can assign another user as the owner of a file or folder.

NTFS Permission Inheritance As mentioned, permission inheritance in the file system behaves like permission inheritance in Active Directory. By default, initial permissions are set at the root of a volume, and all folders and files in that volume inherit these settings unless configured otherwise.



Windows changes the default inheritance settings on many folders created during installation so that they don't inherit all permissions from the root of the volume.

NOTE

One reason you might need to configure special permissions is so that you can define inheritance properties of special permissions on folders. There are seven options for how permissions on a folder apply to other objects in that folder, as shown in Figure 6-10.



Figure 6-10 Apply to options for special permissions

All standard permissions have the Apply to option set to "This folder, subfolders and files," but there might be reasons to change this default setting. For example, you might want users to be able to create and delete files in a folder but not delete the folder itself. To do this, you could

set the standard Read & execute and Write permissions on the folder, and then set the Delete special permission to apply to subfolders and files only.

Subfolders and files are configured to inherit permissions by default; however, as with Active Directory objects, permission inheritance can be disabled. If you need to remove permissions from a file or folder, you must disable inheritance first. You can add new ACEs or add permissions to an existing ACE with inheritance enabled, but you can't remove inherited permissions. To disable permission inheritance, open the Advanced Security Settings dialog box for an object and clear the “Include inheritable permissions from this object's parent” option (see Figure 6-11). When you disable inheritance, you're prompted to copy the previously inherited permissions or remove all permissions. In most cases, copying the permissions is best so that you have a starting point from which to make changes. The “Replace all existing inheritable permissions on all descendants with inheritable permissions from this object” option, also in the Advanced Security Settings dialog box, forces the current folder's child objects to inherit applicable permissions. If a child object has inheritance disabled, this option reenables it.

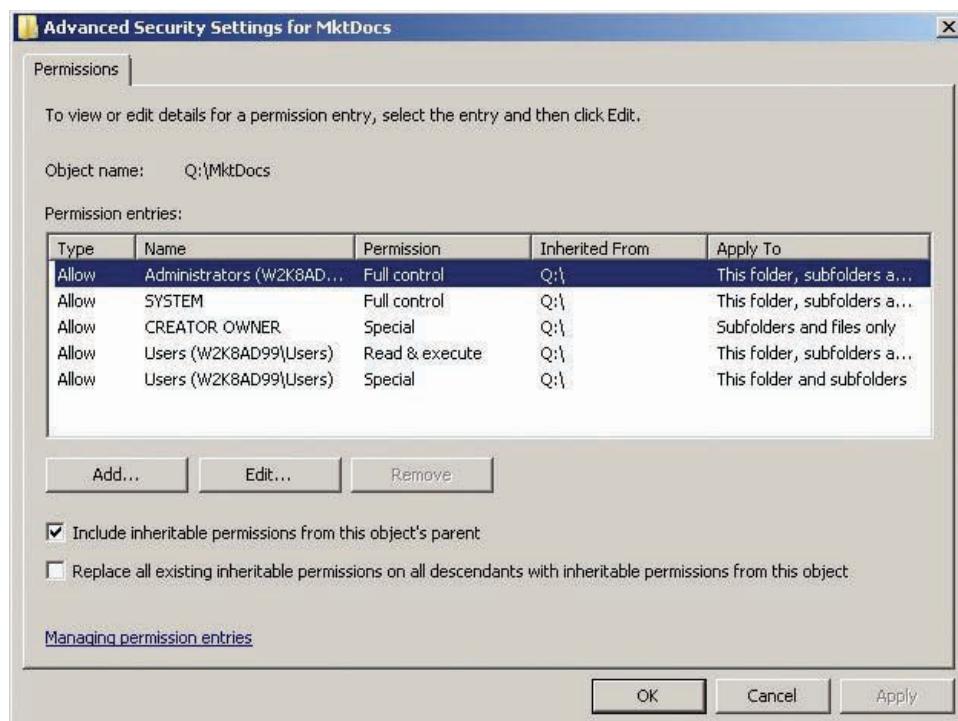


Figure 6-11 The Advanced Security Settings dialog box



Activity 6-8: Examining Default Settings for Volume Permissions

Time Required: 10 minutes

Objective: Examine default permission settings on a volume.

Description: You want a solid understanding of which permissions are inherited by files and folders created on a new volume.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and right-click the **QData** volume and click **Properties**. Click the **Security** tab.
3. Click each ACE in the volume's DACL. You might need to scroll the Permission for Users list box to see the special permissions entry.

4. Click the **Advanced** button. Notice that the Administrators group and SYSTEM special identity are granted Full control. Double-click the **CREATOR OWNER** entry. This special identity is given Full control, but only over subfolders and files. This entry ensures that any user who creates a file or folder is granted Full control permission for that object. A user must have at least the Write standard permission to create files and folders. Click **Cancel**.
5. Double-click the **Users** entry with Special in the Permission column. This entry and the Users entry above it allow users to create folders and files, but only in subfolders. This permission prevents users from creating files in the root of the volume. Click **Cancel**.
6. Double-click the **Everyone** entry. This set of permissions allows the Everyone special identity to view a list of files and folders in the root of the volume (but not open the files or folders). The Apply to setting “This folder only” prevents child objects from inheriting these permissions. Click **Cancel** three times.
7. Create a folder in the root of the QData volume named **TestPerm**.
8. Open the TestPerm folder’s Properties dialog box, and click the **Security** tab. Note that the folder inherited all ACEs except the Everyone entry. Click **Edit**. Click each ACE in the Group or user names list box. Permissions for the entries are grayed out, meaning you can’t change them because they are inherited. Click **Cancel** twice.
9. Create a text file in the TestPerm folder named **Permfile1.txt**.
10. Open the Permfile1.txt file’s Properties dialog box, and click the **Security** tab. Note that the file inherits the TestPerm folder’s permissions except the CREATOR OWNER special identity, which you see only in the DACL of folders. Close any open windows.

6



Activity 6-9: Experimenting with NTFS Permissions

Time Required: 20 minutes

Objective: Experiment with NTFS permissions.

Description: You’re somewhat confused about NTFS permissions, so you decide to create a test folder and some test files to use in a variety of NTFS permission experiments.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and navigate to the **TestPerm** folder you created on the QData volume.
3. First, you want to be able to view file extensions in Windows Explorer so that you can create batch files easily. Click **Organize** on the toolbar, and then click **Folder and Search Options**. Click the **View** tab. Click to clear the **Hide extensions for known file types** check box, and then click **OK**.
4. Create a text file called **TestBatch.bat**. When asked whether you want to change the file extension, click **Yes**.
5. Right-click **TestBatch.bat** and click **Edit**. Type **@ Echo This is a test batch file** and press **Enter**. On the next line, type **@Pause**. Save the file, and then exit Notepad. To test your batch file, double-click it. A command prompt window opens, and you should see “This is a test batch file. Press any key to continue . . . ” Press the **spacebar** or **Enter** to close the command prompt window.
6. Open the Properties dialog box for **TestBatch.bat**, click the **Security** tab, and then click **Advanced**. Click **Edit**. Click to clear the **Include inheritable permissions from this object’s parent** check box to disable inheritance. In the message box that opens, click **Copy** to copy the current permissions, and then click **OK**. Notice that the three permissions entries now indicate “<not inherited>” in the **Inherited From** column. Click **OK**.
7. Click **Edit**. Click **Users** in the Group or user names list box. In the Permissions for Users list box, click to clear the **Read & execute** check box in the Allow column and leave the **Read** check box selected. Click **OK** twice.

8. Log off and log on as **testuser1** with **Password01**. Browse to the **TestPerm** folder on the QData volume. Double-click the **TestBatch.bat** file. Read the error message, and then click **OK**.
9. Right-click the **TestBatch.bat** file and click **Edit**. Notice that you can still open this file because you have Read permission, but you can't run the batch file because you no longer have Read & execute permission. Close the file, and exit Notepad.
10. Right-click **TestPerm** and point to **New**. Strangely, the right-click New menu and the File, New menu choice offer only Folder as an option to create a new file. However, you can create a file in Notepad and save it in this folder.
11. Click **Start**, type **notepad** in the Start Search text box, and press **Enter**. Type your name in the file and click **File, Save As** from the menu. In the Save As dialog box, click the **Browse Folders** button, click **Computer** under Favorite Links, and then double-click the **QData** volume and the **TestPerm** folder. In the File name text box, type **Permfile2.txt**, and click **Save**. Exit Notepad.
12. Open the Properties dialog box for **Permfile2.txt**, and click the **Security** tab. Click the **Test User1** entry. Test User1 has been assigned Full control of the file because of the CREATOR OWNER Full control permission on the parent folder. Click **Advanced**. Click the **Owner** tab, which shows that Test User1 is the file owner.
13. Click the **Permissions** tab, and then click **Edit**. Disable permission inheritance and copy the existing permissions. (Refer back to Step 6, if necessary.) Click **OK** until you get back to the Security tab of **Permfile2**'s Properties dialog box.
14. Click **Edit**. Click the **Test User1** entry, and then click **Remove**. Click the **Users** entry, and then click **Remove**. Click **OK** twice.
15. Double-click **Permfile2.txt**. You should get an “Access is denied” message because you no longer have permission to open this file. Click **OK** and exit Notepad. Although you no longer have access to this file, you are still the file owner and, therefore, can assign yourself permissions.
16. Open the Properties dialog box for **Permfile2.txt**, click the **Security** tab, and then click **Edit**. Click **Add**. Type **testuser1**, click **Check Names**, and then click **OK**. Click **Full control** in the Allow column in the Permissions for Test User1 list box. Click **OK** twice. Verify that you can open, change, and save **Permfile2.txt**.
17. Close all open windows, and log off.



Activity 6-10: Creating a Common Folder for a Group

Time Required: 20 minutes

Objective: Create a folder for the Marketing-G group and assign permissions for users in that group.

Description: The Marketing Department has asked you to create a folder that all users in the department can access. Users should have full control of their own files but be able to just read and modify other users' files.

1. Log on to your server as Administrator, if necessary.
2. Open Active Directory Users and Computers. Click the **Marketing** OU, and create a domain local group named **MktgDocs-DL** that you'll use for permission assignments.
3. Right-click the **Marketing-G** group and click **Add to a group**. Type **MktgDocs-DL**, click **Check Names**, and then click **OK**. When you get a message that the operation was successful, click **OK**. Close Active Directory Users and Computers.



The actions in Step 3 follow the AGDL part of the AGDLP guideline for permission assignment you learned about in Chapter 5.

NOTE

4. Open Windows Explorer, and click to open the **QData** volume.

5. Create a folder named **Marketing**. Open its Properties dialog box, and click the **Security** tab.
6. Disable permission inheritance on the Marketing folder. When asked whether you want to copy or remove existing permissions, click **Remove**. Notice that one entry remains in the Permissions list: The Administrators group is given Full control permission for “This folder only” to prevent error messages when the Administrator attempts to access the folder.
7. Click **Edit**. In the Apply to list box, click **This folder, subfolders and files**. Because you’re working with this folder and subfolders as the Administrator account, making this change prevents “Access is denied” messages on files and subfolders. Normally, company policy dictates whether the Administrators group should have access to all folders and files.
8. Click **OK** until you get to the Security tab for the Marketing folder.
9. Click **Edit**. Click **Add**, type **MktgDocs-DL**, and then click **OK**. The default permissions assigned to a new ACE are Read & execute, List folder contents, and Read. Click the **Write** check box in the Allow column, and then click **OK**.
10. Click **Advanced**, and then click **Edit**. Click **Add**, type **Creator Owner**, and then click **OK**. Click the **Full control** check box in the Allow column. In the Apply to list box, click **Subfolders and files only**. Click **OK** until the Properties dialog box for the Marketing folder is closed.
11. To test your permissions, log off your server and log on as **advuser1** with **Password01**. This user is a member of the Marketing-G group. Change the password when prompted to **Password02**.
12. Browse to the **Marketing** folder, and create a text file named **AdvUser1.txt**. Open the file and type **AdvUser1**. Save the file, and exit Notepad.
13. Log off and log on as **advuser2** with **Password01**. Change the password to **Password02** when prompted.
14. Browse to the **Marketing** folder and open **AdvUser1.txt**. Type **AdvUser2** at the end of the file. Save the file, and exit Notepad. Clearly, you can read and make changes to the file. Try to delete the file. You should get the “Destination Folder Access Denied” message. Click **Continue**. You’re prompted to enter a username and password with permission to delete the file. Click **Cancel**.
15. Log off and log on as **advuser1** with **Password02**. Delete the **AdvUser1.txt** file to verify that the advuser1 user can delete the file, but other users can’t. Create another text file named **AdvUser1.txt** to use in a subsequent activity. Close any open windows, and log off.



A solid grasp of how to use NTFS permissions is essential for an administrator to build an accessible yet secure file-sharing system. However, in a network environment, you’re unlikely to have users log on to servers interactively to access files. Instead, you need to configure file sharing, covered in the following section.

Windows File Sharing

The File Services role is required to share folders. You can install this role by using Server Manager, or you can simply share a folder to have the role installed automatically. Folders in Windows Server 2008 can be shared only by members of the Administrators or Server Operators groups.

Sharing files on the network, as you have seen in previous activities, isn’t difficult in a Windows environment. Nonetheless, you should be familiar with some techniques and options before forging ahead with setting up a file-sharing server. You can use the following methods to configure folder sharing in Windows Server 2008:

- **File Sharing Wizard**—To start this wizard, right-click a folder and click Share. The File Sharing Wizard (see Figure 6-12) simplifies sharing for novices by using friendlier terms for permissions and by setting NTFS permissions to accommodate the selected share permissions. In Figure 6-12, the permissions you see—Reader, Contributor, and Co-owner or

Owner—correspond to the Read, Change, and Full Control share permissions, respectively. This wizard is enabled by default but can be disabled in the Folder and Search Options dialog box in Windows Explorer. In addition, this wizard is disabled on folders where permission inheritance is disabled.



Figure 6-12 The File Sharing Wizard

- *Advanced Sharing dialog box*—To open this dialog box, click Advanced Sharing in the Sharing tab of a folder’s Properties dialog box. (When the File Sharing Wizard is disabled, you can right-click a folder and click Share.) There are quite a few options in this dialog box (see Figure 6-13):

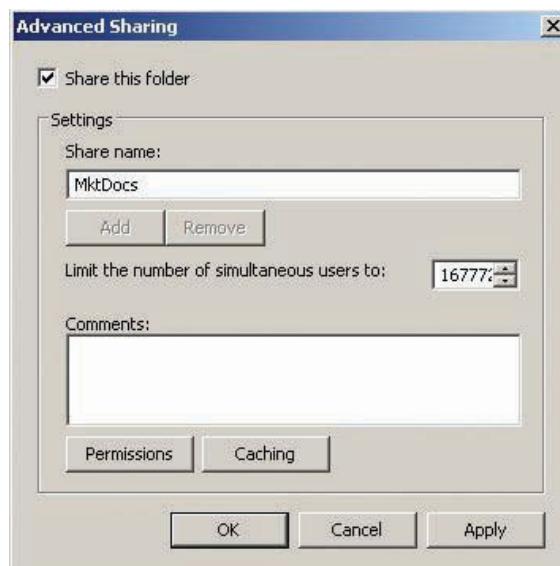


Figure 6-13 The Advanced Sharing dialog box

- Share this folder: Sharing can be enabled or disabled for the folder by clicking this check box.

- Share name: The share name is the name users see in the Network folder of Windows Explorer when browsing the server. To put it another way, the share name is the name you use to access the folder with the UNC path (`\server\share name`). You can add or remove share names. A single folder can have multiple share names and different permissions, simultaneous users, and caching settings for each share name.
- Limit the number of simultaneous users to: In Windows Server 2008, the default limit is 16,777,216, which is, practically speaking, unlimited. In Windows Vista, the maximum number of users who can access a share is 10.
- Comments: You can enter a description of the share's contents and settings in this text box.
- Permissions: Click this button to open the Permissions dialog box shown previously in Figure 6-8. In Windows Server 2008, folders using advanced sharing are configured with the Everyone special identity having Read permission by default.
- Caching: This option controls how offline files are configured. Offline files enable users to disconnect from the network and still have the shared files they were working with available on their computers. When a user reconnects to the network, the offline and network copies of the file are synchronized.
- *Shared Folders snap-in*—You use this component of the Computer Management MMC to monitor, change, and create shares on the local computer or a remote computer. To create a new share, right-click the Shares node under the Shared Folders snap-in and click New Share. The Create a Shared Folder Wizard walks you through selecting the folder to share or creating a new folder to share, naming the share, configuring offline files, and setting permissions.
- *Share and Storage Management*—This snap-in is the most advanced method for creating shares. Like the Shared Folders snap-in, you use a wizard to create shares. You can select the folder to share or create a new share, configure NTFS permissions, choose sharing protocols, configure offline files, and publish the share in DFS.



Activity 6-11: Sharing a Folder with the File Sharing Wizard

Time Required: 15 minutes

Objective: Create a test folder and then share it by using the File Sharing Wizard.

Description: You understand that there are several ways to create shared folders. You decide to try the File Sharing Wizard to see how it sets permissions automatically.

1. Log on to your server as Administrator, if necessary.
2. Open Active Directory Users and Computers. Click the **TestOU** OU. Create a domain local group named **TestSharing-DL** to use for permission assignments. Add the global group **TestGroupG** to TestSharing-DL. Close Active Directory Users and Computers.
3. Open Windows Explorer, and click to open the **QData** volume. Create a folder named **TestShare1**.
4. Open the TestShare1 folder's Properties dialog box, and click the **Security** tab. Make a note of the permissions assigned on this folder. Close the Properties dialog box.
5. Right-click **TestShare1** in the left pane and click **Share** to start the File Sharing Wizard.
6. Click the list arrow next to the Add button and click **Find** in the list. Type **TestSharing-DL**, click **Check Names**, and then click **OK**. In the Permission Level column for the TestSharing-DL entry, click the list arrow and click **Contributor**.
7. Click **Share**. Notice that in the last window of the wizard, you can e-mail links to the shared folder or copy the links to the Clipboard. You can also click the **Show me all the network shares on this computer** link to open the Network browse window for your server. Click **Done**.

8. Right-click **TestShare1** and click **Properties**. Click the **Sharing** tab, and then click **Advanced Sharing**.
9. Click **Permissions**. Notice that the TestSharing-DL group was assigned the Change permission, which corresponds to Contributor in the File Sharing Wizard. The Administrator account has Full Control permission to the share. Click **Cancel** twice.
10. In the TestShare1 folder's Properties dialog box, click the **Security** tab. Scroll through the ACEs in the DACL. Notice that TestSharing-DL and Administrator ACEs were added to the DACL with NTFS permissions to match the share permission. However, all other ACEs were maintained. In the real world, this may or may not be what you intended.
11. Close all open windows.



Activity 6-12: Sharing a Folder with Advanced File Sharing

Time Required: 15 minutes

Objective: Share the Marketing folder created earlier.

Description: Now that you have a solid understanding of sharing folders and NTFS permissions, you decide to share the Marketing folder you created earlier, and then test network access to the folder from a client workstation.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and click to open the **QData** volume. Right-click the **Marketing** folder and click **Share**. The File Sharing Wizard doesn't start, however, because you disabled permission inheritance on this folder earlier. The File Sharing Wizard is disabled on folders where inheritance is disabled. Notice that the Share button is disabled, too.
3. Click **Advanced Sharing**. Click to select the **Share this folder** check box. Leave the share name as is, and then click the **Permissions** button. By default, the share permission is Allow Read for Everyone.
4. Because you don't want the Everyone special identity to have Read permission, click **Remove**. Click **Add**, type **MktgDocs-DL**, click **Check Names**, and then click **OK**.
5. You want all users to be able to create files and have full control over files they create (recall Activity 6-10), so click the **Full Control** check box in the Allow column. Even though users will have Full Control over files they create, NTFS permissions restrict them to Read, Read & execute, and Write on all other files. Click **OK** twice, and then click **Close**.
6. Log on to the domain from your Vista computer as **advuser2** with **Password02**. Click **Start**, type **\serverXX\Marketing** in the Start Search text box, and press **Enter**.
7. Open the **AdvUser1.txt** file created in Activity 6-10. Make some changes to the file and save it. You should be successful because advuser2 has Write permission. Now try to delete the file. You shouldn't be successful because advuser1 owns the file, and advuser2 doesn't have Delete permission. Remember, all members of the Marketing-G group were granted Full Control share permission, but NTFS permissions are more restrictive, allowing Full control only over files the user owns. When applying both share and NTFS permissions, the more restrictive permission of the two is applied.
8. Create a file named **AdvUser2.txt**, and then try to delete it. You should be successful.
9. Close all open windows, and log off the Vista computer.



Activity 6-13: Restricting Access to Subfolders of Shares

Time Required: 15 minutes

Objective: Restrict access to a subfolder of a share.

Description: The Sales Department wants a subfolder of the Marketing share to store sensitive documents that should be available only to the Sales-G group because some Marketing

and Advertising users tend to leak information before it should be discussed outside the company. You could create a new share, but the Sales Department users prefer a subfolder of the existing share.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and click to open the **QData** volume and then the **Marketing** folder. Create a subfolder of the Marketing folder named **SalesConf**.
3. Open the Properties dialog box of the SalesConf folder, and click the **Security** tab. Remove the **MktgDocs-DL** group from the DACL. (*Hint:* You need to disable inheritance first; be sure to copy existing permissions.)
4. Add the **Sales-G** group to the DACL, and give the group **Read & execute** and **Write** permissions. Click **OK** until you close the SalesConf folder's Properties dialog box. *Note:* These steps violate the AGDLP best practice because you didn't use a domain local group to assign permissions. AGDLP is not a hard-and-fast rule, however, but a best practice recommendation. For simplicity's sake, it isn't used in this step.
5. Log on to your Vista computer as **advuser1**. Open Windows Explorer, and click to open the **Marketing** share. Try to open the SalesConf folder. You get an "Access is denied" message. Click **OK**.
6. Log off, and then log on to your Vista computer as **salesperson1** using **Password02**. Open Windows Explorer, and click to open the **Marketing** share. Verify that you can open the SalesConf folder and create a file named **SalesPerson1**.
7. Log off your Vista computer.



In this activity, you restricted access to a folder by simply including in the DACL groups that are allowed access. Although the entire Marketing Department was granted access to the Marketing share, the fact that only the Sales-G group was in the SalesConf DACL effectively blocked all other Marketing Department users from accessing the share's subfolder. Using a Deny permission might have worked, too, but it wasn't necessary in this example. The Deny permission should be used cautiously and only for exceptions. For example, if all members of a group except a few should have access to a resource, users can be added to a group and the group can be added to the DACL with a Deny permission, as you see in Activity 6-14.



Activity 6-14: Restricting Access with Deny Permissions

Time Required: 15 minutes

Objective: Restrict a single user's access to a folder.

Description: A new employee has just been hired in the Sales Department. Company policy states that all employees must be with the company for a 120-day probationary period before being allowed access to confidential material. This new employee should have access to all nonconfidential material and, therefore, be a member of the global Sales-G group. Your solution is to create a global group called DenySales-G and add new users to this group. You then add this group to the DACL of any confidential folders and assign the Deny Full Control permission. After the user is past the probationary period, you can remove this user account from the DenySales-G group. By using a group instead of the user account to deny access, you don't need to hunt down all the confidential folders and remove the user account from their DACLs.

1. Log on to your server as Administrator, if necessary.
2. Open Active Directory Users and Computers. Browse to the **Sales** OU under the Marketing OU.
3. Create a new global group named **DenySales-G**. Use the **_Sales** Template account (created in Chapter 5) to create a user with the full name **New Sales1** and logon name **newsales1**. Assign the password **Password01** and click to clear the **User must change password at next logon** and **Account is disabled** check boxes.

4. Add **newsales1** to the DenySales-G group. Close Active Directory Users and Computers.
5. Open Windows Explorer, and click the **SalesConf** folder under the Marketing folder. Open the Properties dialog box for the SalesConf folder, and click the **Security** tab. Add DenySales-G to the DACL, and then assign the **Deny Full control** permission.
6. Log on to the domain from the Vista computer as **newsales1** with **Password01**.
7. Open the **Marketing** share on \\serverXX\Marketing. Create a text file named **NewSales1.txt** in the Marketing share to verify that you have access to the share.
8. Try to open the **SalesConf** folder. You get an “Access is denied” message. Click **OK**.
9. Close any open windows, and log off the Vista computer.

Default and Administrative Shares

Every Windows OS since Windows NT (excluding Windows 9x and Windows Me) includes **administrative shares**, which are hidden shares available only to members of the Administrators group. On computers that aren’t domain controllers, these shares are as follows:

- *Admin\$*—This share provides network access to the Windows folder on the boot volume (usually C:\Windows).
- *Drive\$*—The *drive* represents the drive letter of a disk volume (for example, C\$). The root of each disk volume (except removable disks, such as DVDs and floppy disks) is shared and accessible by using the drive letter followed by a dollar sign.
- *IPC\$*—IPC means interprocess communications. This share is less an administrative share than it is a system share. The IPC\$ share is used for temporary connections between clients and servers to provide communication between network programs.

Domain controllers have all the previous hidden administrative shares as well as the following default shares:

- *NETLOGON*—Used for storing default user profiles as well as user logon scripts for pre-Windows 2000 clients.
- *Sysvol*—Used by Active Directory for replication between DCs. Also contains group policy files that are downloaded and applied to Windows 2000 and later clients.

Windows creates administrative shares automatically, and permissions on the shares can’t be changed. An administrator can disable sharing on the Admin\$ share or a volume administrative share, but the share is re-created the next time the system starts or when the Server service is restarted. The IPC\$ share can’t be disabled.



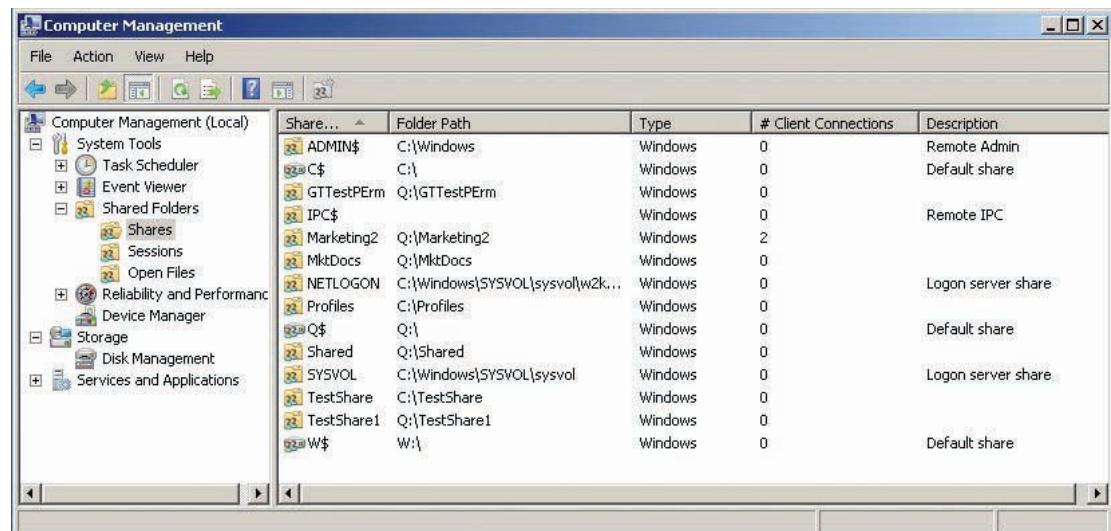
You can prevent Windows from re-creating disabled administrative shares by editing the Registry.

NOTE

The dollar sign at the end of a hidden share name prevents the share from being displayed in a network browse list. To access a hidden share, you must use the UNC path. For example, entering \\serverXX\C\$ opens the root of the C drive on serverXX. You can create your own hidden shares by simply placing a \$ at the end of the share name. Sometimes administrators use hidden shares to prevent users from attempting to access shares for which they don’t have permission.

Managing Shares with the Shared Folders Snap-in

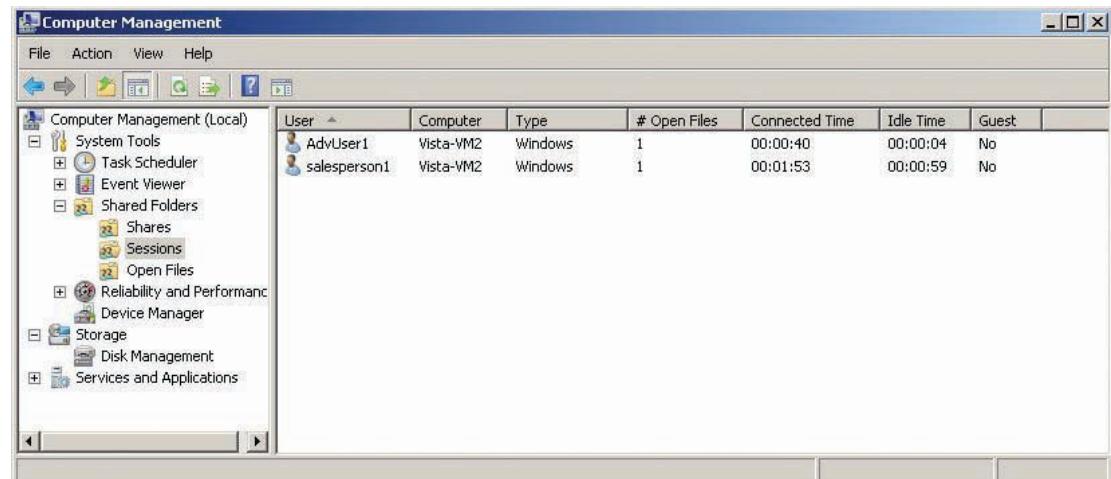
You use the Shared Folders snap-in to create, delete, and monitor shares; view open files; and monitor and manage user connections or sessions. To open this snap-in, add it to an MMC or open the Computer Management MMC. Figure 6-14 shows the following subnodes in the Shared Folders snap-in:



Share...	Folder Path	Type	# Client Connections	Description
ADMIN\$	C:\Windows	Windows	0	Remote Admin
C\$	C:\	Windows	0	Default share
GTTTestPErm	Q:\GTTTestPErm	Windows	0	
IPC\$		Windows	0	
Marketing2	Q:\Marketing2	Windows	2	
MktDocs	Q:\MktDocs	Windows	0	
NETLOGON	C:\Windows\SYSVOL\sysvol\w2k...	Windows	0	Logon server share
Profiles	C:\Profiles	Windows	0	
Q\$	Q:\	Windows	0	Default share
Shared	Q:\Shared	Windows	0	
SYSVOL	C:\Windows\SYSVOL\sysvol	Windows	0	Logon server share
TestShare	C:\TestShare	Windows	0	
TestShare1	Q:\TestShare1	Windows	0	
W\$	W:\	Windows	0	Default share

Figure 6-14 The Shared Folders snap-in

- **Shares**—In the Shares node, you can view all shares, their path on the local file system, and how many clients are currently connected to each share. You can also open the folder on the local file system, stop sharing a folder, and create new shares.
- **Sessions**—The Sessions node lists users who currently have a network connection to the server, from which client computer they’re connected, how many files they have open, and how long they have been connected (see Figure 6-15). Administrators can select a user and close the session.



User	Computer	Type	# Open Files	Connected Time	Idle Time	Guest
AdvUser1	Vista-VM2	Windows	1	00:00:40	00:00:04	No
salesperson1	Vista-VM2	Windows	1	00:01:53	00:00:59	No

Figure 6-15 The Sessions node

- **Open Files**—The Open Files node lists files that network users have open and which user has opened the file (see Figure 6-16).

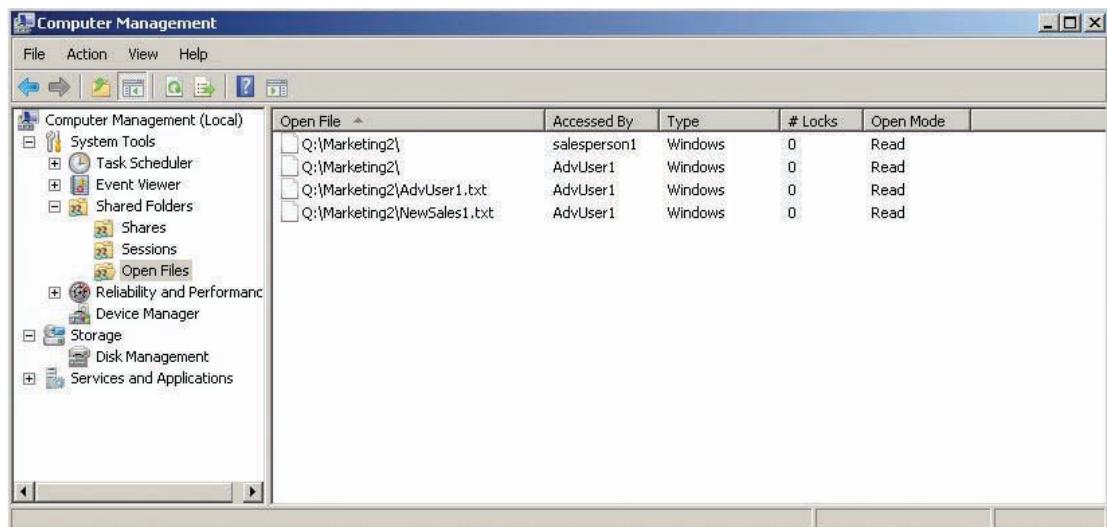


Figure 6-16 The Open Files node

The Shared Folders snap-in is useful for monitoring how much a server's shares are being used and by whom. You can also use this tool to see whether any files are being accessed over the network before shutting down the server or otherwise interrupting server access. You can also check the Idle Time column in the Sessions node to see whether a user is actively using shares on the server (a short idle time) or simply has a share open but hasn't accessed any files for a while (a longer idle time).

You can view and change a share's properties by double-clicking it in the Shares node. You can't change the share's name or the folder location, but you can change the user limit, offline settings, share permissions, and NTFS permissions. In addition, you can publish a share in Active Directory or change the publish options of a published share. In Chapter 3, you used the Shared Folders snap-in to create and publish a share.



Activity 6-15: Publishing and Monitoring Access to a Share

Time Required: 15 minutes

Objective: Monitor access to shared folders.

Description: After creating the Marketing share, you want users to be able to find it in Active Directory, so you decide to publish it. In addition, you want to see how the Sessions and Open Files nodes in the Shared Folders snap-in work.

1. Log on to your server as Administrator, if necessary.
2. Open the Computer Management MMC, click to expand the **Shared Folders** snap-in, and then click the **Shares** node.
3. In the right pane, right-click the **Marketing** share and click **Properties**. Click the **Publish** tab. Click the **Publish this share in Active Directory** check box, and type **Marketing documents** in the Description text box.
4. Click the **Edit** button. In the Edit Keywords dialog box, type **marketing** and click **Add**, type **advertising** and click **Add**, and then type **sales** and click **Add**. Click **OK**. Users can now find this share by using these keywords. Click **OK** to close the Properties dialog box, and leave the Computer Management window open.
5. Log on to the domain from your Vista computer as **advuser1** with **Password02**. Click **Start**, **Network**.

6. Click the **Search Active Directory** toolbar icon. Click the **Find** list arrow, and click **Shared Folders**. Type **advertising** in the Keywords text box, and then click **Find Now**. The Marketing share is listed in the search results. Right-click the **Marketing** share and click **Explore**.
7. Open the **AdvUser1.txt** file you created earlier.
8. On your server, refresh the Computer Management window (by pressing **F5** or clicking the **Refresh** toolbar icon). You should see the # Client Connections column for the Marketing share change to 1.
9. Click the **Sessions** node in the Shared Folders snap-in. You should see that AdvUser1 has a connection with a non-zero value in the # Open Files column.
10. Click the **Open Files** node in the Shared Folders snap-in. You should see Q:\Marketing listed. When a folder is opened in Windows, it's counted as an open file. You might also see the AdvUser1.txt file listed. However, Windows doesn't display the open file for more than a few seconds.
11. Right-click one of the files listed in Open Files and click **Close Open File**. Click **Yes**. Note that this action doesn't affect the Explorer window on your Vista computer, and it doesn't close Notepad if the open file is in Notepad. However, this action does close the connection between the client computer and the file.
12. Close all open windows on your Vista computer and server, and log off Vista.



Accessing File Shares from Client Computers

The file sharing discussion so far has focused on how to create and manage shared resources. However, for shared resources to be useful, users must know how to access them. You have already seen some different access methods in this chapter's activities. The following methods of accessing shared folders are among the most common:

- **UNC path**—The UNC path, which you've seen in examples and activities, uses the syntax `\server\share[\subfolder][\file]`. The parameters in brackets are optional. In fact, the *share* parameter is optional if all you want to do is list shared resources on a server. Using `\server` by itself in an Explorer window lists all shared folders and printers (except hidden shares) on that server. The disadvantage of this method is that the user must know the server name, and in a network with dozens or hundreds of servers, that might be asking a lot.
- **Active Directory search**—The Active Directory search, as you have seen, is easy and allows you to search by keyword or simply list all shared folders in the directory. With this method, users don't need to know the hosting server's name. However, shares aren't published to Active Directory automatically, so this method might not find all shared folders on the network.
- **Browsing the network**—You can open the Network folder from the Start menu and see a list of all computers found on the network (see Figure 6-17). You can then browse each computer to find the share you want. This method has the advantage of not requiring you to know the server's name. However, in Windows Vista, you must enable the network discovery feature (covered in Chapter 8) for your computer to see other computers and for your computer to be seen by other computers. Plus, in a large network, you might be browsing for quite a while to find the right computer.
- **Mapping a drive**—Administrators often set up a logon script for users in which a drive letter is mapped to a network folder where users can store documents. Users can also map a drive letter to shared folders that they access often. Users tend to be more comfortable using drive letters to access files in a Windows environment because all their local resources (hard drives, DVD drives, flash drives) are accessed in this manner. Drive letters can be mapped only to the root of the share, as in `\server\share`, not to a subfolder of the share, as in `\server\share\folder1`.

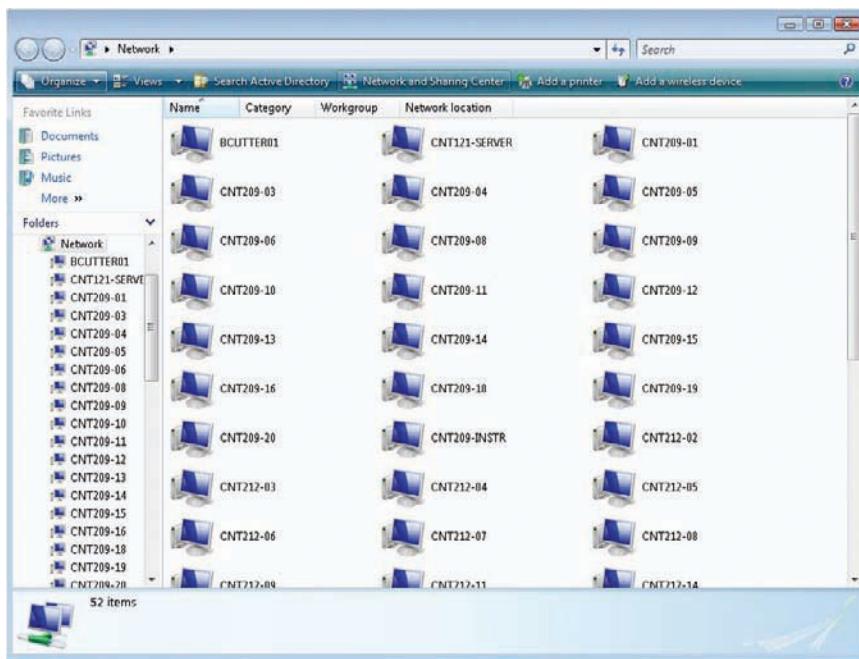


Figure 6-17 Browsing the network

Activity 6-16: Mapping a Drive

Time Required: 15 minutes

Objective: Map a drive letter to a shared folder.

Description: A user in the Sales Department accesses the Marketing share frequently but forgets how to use the UNC path. You decide to show this user several ways to map a drive letter to the share.

1. Log on to the domain from your Vista computer as **salesperson1** with **Password02**.
2. Click **Start**, type **\serverXX** in the Start Search text box, and press **Enter**.
3. Right-click the **Marketing** share and click **Map Network Drive** to open the Map Network Drive dialog box.
4. Click the **Drive** list arrow, and click **M:**. By default, the **Reconnect at logon** box check box is selected, which is what you usually want in this situation. This option means that the M drive always connects to this share when the user logs on. For this activity, click to clear **Reconnect at logon**, as shown in Figure 6-18. You can also use a different username to access this share, if necessary.



Figure 6-18 The Map Network Drive dialog box

5. Click **Finish**. A Windows Explorer window opens, showing the contents of the Marketing share. Close this window.
6. Click **Start, Computer**. Notice that the M drive is listed along with your local drive letters. Right-click the **M** drive and click **Disconnect**.
7. Click **Map network drive** on the toolbar. Click the **M:** drive again, and in the Folder text box, type **\serverXX\marketing**, and then click **Finish**.
8. Disconnect the M drive again. Click **Start, Network**.
9. Click the **Search Active Directory** toolbar icon. Click the **Find** list arrow, and click **Shared Folders**. Type **marketing** in the Name text box, and then click **Find Now**. The Marketing share is listed in the search results. Right-click the **Marketing** share and click **Map Network Drive**. Click **Cancel** because you don't want to map the drive at this time.
10. Close all open windows. Click **Start**, type **cmd** in the Start Search text box, and press **Enter**.
11. At the command prompt, type **net use M: \\serverXX\marketing** and press **Enter**. You should get the message "The command completed successfully." Type **net use** and press **Enter**. You see the M drive listed and the UNC path to which it connects. Leave the command prompt window open.
12. Click **Start, Computer**, and verify that the M drive is indeed there. Go back to the command prompt. Type **net use M: /delete** and press **Enter** to disconnect the M drive. Network administrators put these types of commands in logon scripts to map drives for users.
13. Close all open windows, and log off Vista.

 6

Windows Storage Management

Storage needs in today's networks are growing at a pace that challenges network administrators. Instead of simply needing disk management for a single server, businesses are struggling to develop a comprehensive storage solution for an entire organization. The File Services role, along with its many role services and related features, offers the tools administrators need to provide this type of solution.

At its simplest, the File Services role includes file sharing and the Share and Storage Management snap-in that improves on the Shared Folders snap-in. When you install the File Services role (or when it's installed automatically when you share a folder), the File Server role service is installed, which provides these functions. However, several other role services can be installed, as you can see in Figure 6-19:

- *File Server*—As discussed, the File Server role service is installed automatically when a folder is shared on a server. The Share and Storage Management snap-in is also installed and is available from Server Manager or Administrative Tools.
- *Distributed File System*—DFS allows grouping shared folders from one or more file servers into a single hierarchical folder structure, so users don't have to know the file server where a share is located. DFS includes robust replication technology for shared folder fault tolerance.
- *File Server Resource Manager (FSRM)*—A suite of tools that enables administrators to generate storage reports, define quotas for both volumes and folders, and screen files. Administrators use file screening to control the types of files users can save to a server.
- *Services for Network File System*—Network File System (NFS) is the native file-sharing protocol in UNIX and Linux. This role service makes file sharing between Windows and other OSs that use NFS more convenient.
- *Windows Search Service*—Makes it possible for users to perform fast file searches from client workstations on files stored on the server.

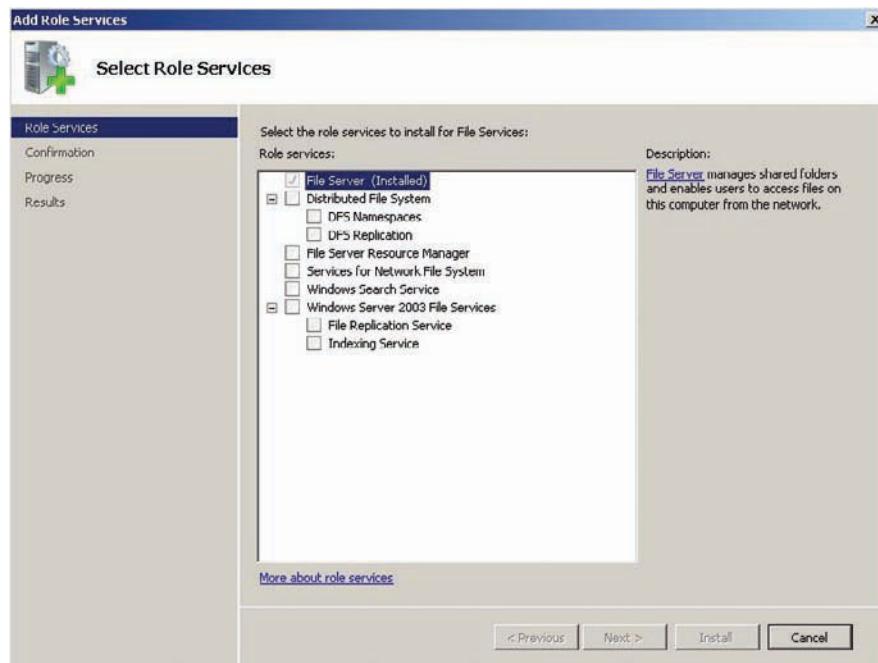


Figure 6-19 Role services in the File Services role

- *Windows Server 2003 File Services*—Adds services that are backward-compatible with Windows Server 2003, such as File Replication Service (FRS) and Indexing Service. FRS provides file synchronization compatibility with DFS. Indexing Service speeds file searching from computers that aren't compatible with Windows Search Service.

The File Services role, along with its role services, is installed in Server Manager. Select the Roles node in the left pane and click Add Roles in the right pane to start the Add Roles Wizard. If the File Services role is already installed, scroll down in Server Manager until you find it, and then click the Add Role Services link to add specific role services. A complete examination of the File Services role is beyond the scope of this book, but you examine the Share and Storage Management snap-in, DFS, and FSRM in the following sections.

Share and Storage Management

The Share and Storage Management snap-in (see Figure 6-20) includes all the functions of the Shared Folders snap-in plus the capability to provision storage, share files by using NFS, publish shares to DFS, and manage volumes. With the provision storage feature, you can create new volumes on local disks or on storage space in a storage area network (SAN). A SAN is a specialized network that connects servers to shared storage devices over high-speed links.

The Shares tab in Share and Storage Management shows information about each share, including the share name, protocol, and local path. In Figure 6-20, Server Message Block (SMB), the Windows file-sharing protocol, is listed as the protocol for all shares. If NFS is installed, and any folders are shared by using it, NFS is listed in the Protocol column. In addition, the Quota and File Screening columns display the status of these features, if they have been enabled with FSRM. A green check mark in the Shadow Copies column indicates that shadow copies are enabled for the volume where the share is located.

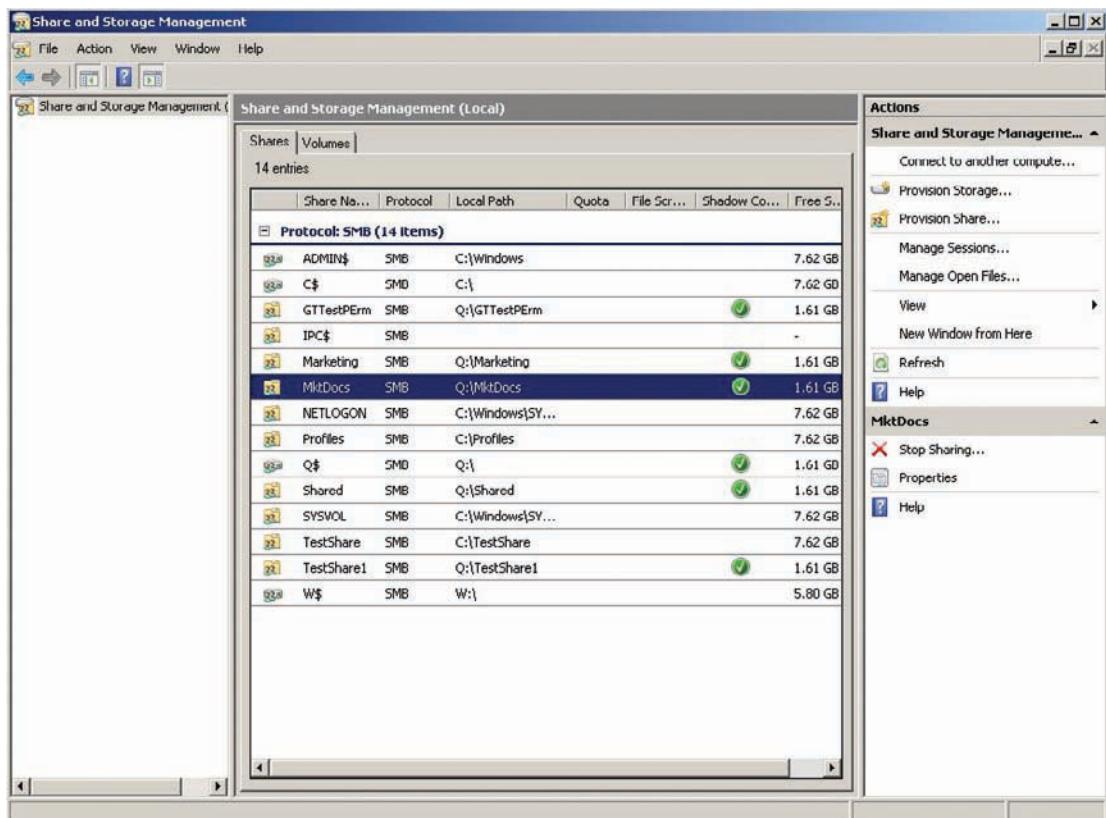


Figure 6-20 The Share and Storage Management snap-in

Activity 6-17: Using Share and Storage Management



Time Required: 15 minutes

Objective: Explore the features of the Share and Storage Management snap-in.

Description: After sharing some folders, you realize that a new MMC has been added to the Administrative Tools folder: Share and Storage Management. You decide to become familiar with this new tool.

1. Log on to your server as Administrator, if necessary.
2. Click the **Server Manager** icon on the Quick Launch toolbar. In the left pane of Server Manager, click to expand the **Roles** node and then the **File Services** node. Click the **Share and Storage Management** snap-in.
3. Click the **Shares** tab in the middle pane, if necessary. Review the information displayed here.
4. Click the **Volumes** tab, which lists all disk volumes installed on the server. You can right-click any volume to select options to extend, format, or delete the volume or view its properties.
5. Right-click the **QData** volume and click **Extend**. In the New capacity text box, type **2.5**, and then click **OK** to extend the QData volume's size to 2.5 GB. Volumes can be extended in Share and Storage Management as long as unallocated space is available adjacent to them. Disk Management must be used to extend a volume to another disk or another place on the same disk.
6. In the Actions pane, click **Provision Share** to start the Provision a Shared Folder Wizard. Click **Browse**. Click the **q\$** folder, and then click **Make New Folder**. Type **NewShare**, click **OK**, and then click **Next**.

7. In the next window, you're given the option to change NTFS permissions. You don't need to change permissions, so click **Next**. In the Share Protocols window, you can select the protocol to use for sharing the folder. A folder can be shared by using SMB or NFS or both. NFS isn't installed, so leave the default setting of SMB, and click **Next**.
8. In the SMB Settings window, you can set user limits, enable access-based enumeration, and configure offline settings. Access-based enumeration, when enabled, prevents users from seeing shared folders they aren't allowed to access in a network browse list. Click **Next**.
9. In the SMB Permissions window, you can set share permissions. Click **Next**.
10. In the DFS Namespace Publishing window, you can choose to display the share in a DFS hierarchy. You won't be including this share in DFS, so just click **Next**.
11. In the next window, you can review your settings before finalizing the share. However, because you're not creating the share at this time, click **Cancel**, and then click **Yes**.
12. In the right pane of Server Manager, click **Provision Storage** to start the Provision Storage Wizard, which steps you through the process of creating a new volume. It's similar to the process you used with the Disk Management snap-in. However, if your network includes a SAN, you can provision storage from available space on it. Click **Cancel**, and then click **Yes**. Close any open windows.

Share and Storage Management is a handy tool for managing shared folders and performing basic local disk management tasks. More advanced disk management tasks require the Disk Management snap-in, available in the Computer Management MMC or as a node under Share and Storage Management in Server Manager. With Disk Management, you can perform the following tasks:

- *Bring new disks online*—New disks installed in Windows Server 2008 are set to the offline state and must be brought online. You can also set an online disk to the offline state for removal or maintenance.
- *Initialize new disks*—After a new disk is brought online, it must be initialized to be used on the server.
- *Import foreign disks*—A disk from another system is considered foreign and must be imported to be used on a Windows server.
- *Create, format, and delete volumes*—After a disk is initialized, volumes must be created and formatted with a file system before they can be used. You can also delete an existing volume.
- *Extend and shrink volumes*—Volumes can be extended to include unallocated space on the same disk or on another disk. New in Windows Server 2008, volumes can be made smaller, perhaps to accommodate a new volume on the same disk.
- *Convert disks from basic to dynamic*—Basic disks support traditional partitions (primary and extended) and don't support advanced volume types, such as RAID. Dynamic disks support RAID volumes and an unlimited number of volumes.
- *Create RAID volumes*—RAID offers high performance and fault-tolerant volume configurations. Windows supports RAID 0 (disk striping), RAID 1 (disk mirroring), and RAID 5 (disk striping with parity).

Distributed File System

Distributed File System (DFS) makes shared files more accessible and reliable by grouping shared folders from multiple servers into a single folder hierarchy and using replication for fault tolerance. A DFS hierarchy is referred to as a namespace. When you install the Distributed File System role service, you can create a namespace that suits the shares in the hierarchy. The DFS Management MMC is installed in Administrative Tools and Server Manager when the role service is installed (see Figure 6-21).

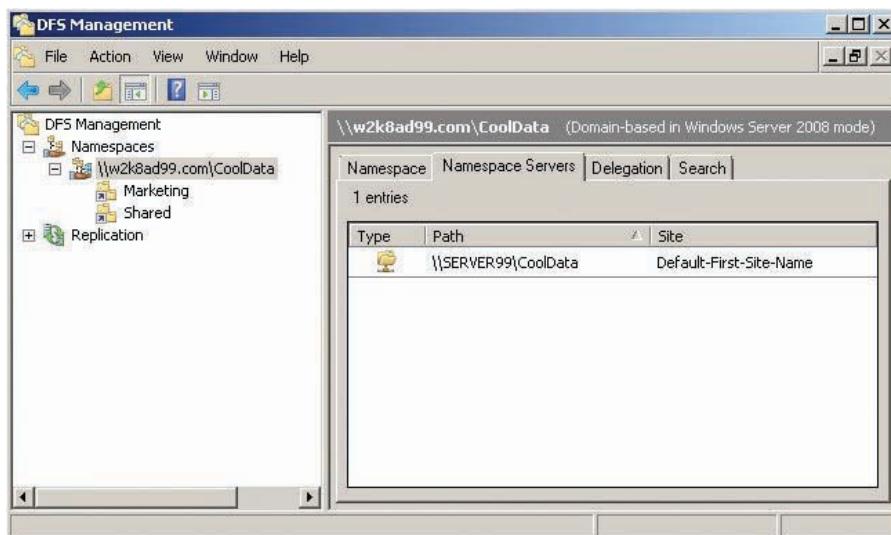


Figure 6-21 The DFS Management MMC

In Figure 6-21, the namespace is called CoolData, and under it is the list of shares consolidated under this namespace. The shares can be hosted on one or more servers. Users can access all shares under the namespace by using the UNC path syntax `\domain\namespace` or `\server\namespace`. In this case, users can access the Marketing and Shared shares with the UNC path `\server99\CoolData` or `\w2k8ad99.com\CoolData`. In addition, a drive letter can be mapped to the namespace. From the user's standpoint, CoolData is a share, and the Marketing and Shared folders just appear to be folders under the share. Figure 6-22 shows what accessing the CoolData namespace looks like from the user's perspective.

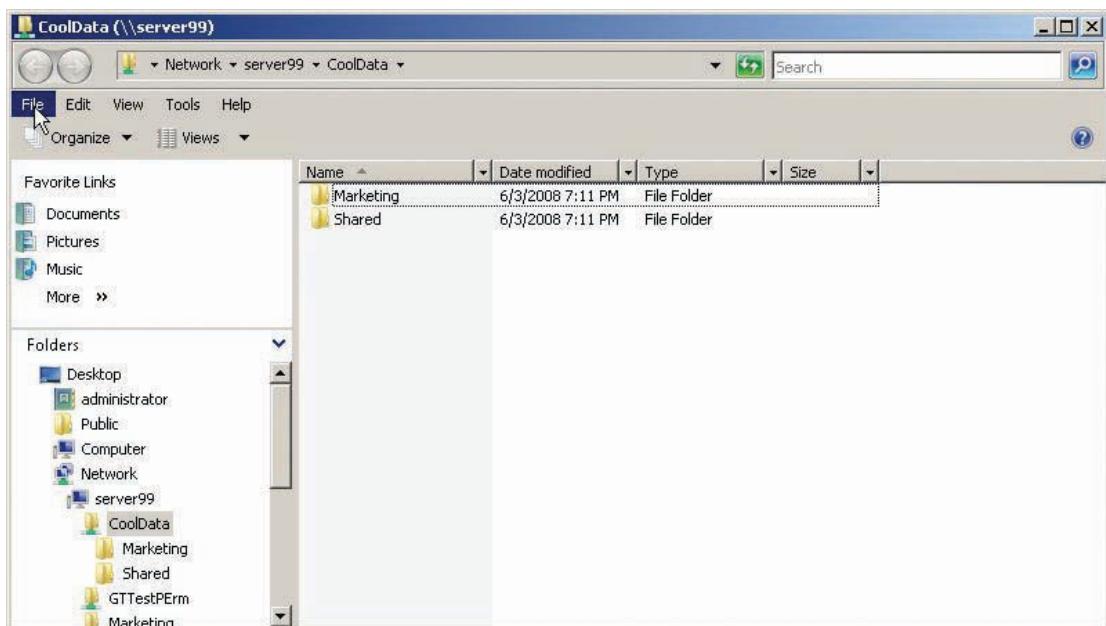


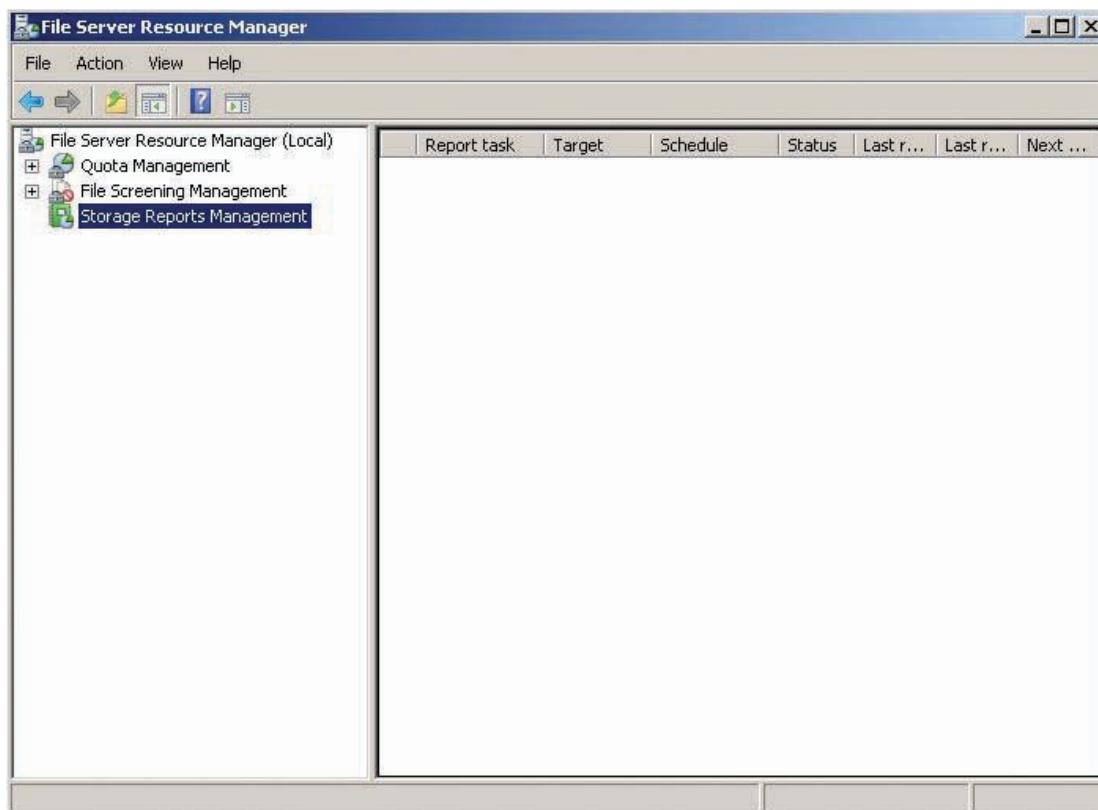
Figure 6-22 Accessing a DFS namespace

Aside from making file shares easier to access, particularly in large networks with dozens or hundreds of shares, DFS provides fault tolerance. You can replicate an entire namespace, along with the shares it hosts, to one or more servers, or replicate a share to another share on another server. Both procedures increase fault tolerance in case a server hosting a share or namespace

fails. An added benefit of replicating all or part of a namespace is that DFS load-balances the servers involved in replication, making file sharing more reliable and faster. A DFS namespace can be domain based or stand-alone. Fault tolerance and load balancing are available only on a domain-based namespace.

File Server Resource Manager

File Server Resource Manager (FSRM) is a suite of services and management tools for monitoring storage space, managing quotas, controlling the types of files that users can store on a server, and creating storage reports. When this role service is installed, the File Server Resource Manager MMC is installed in Administrative Tools and Server Manager and contains three tools (see Figure 6-23):



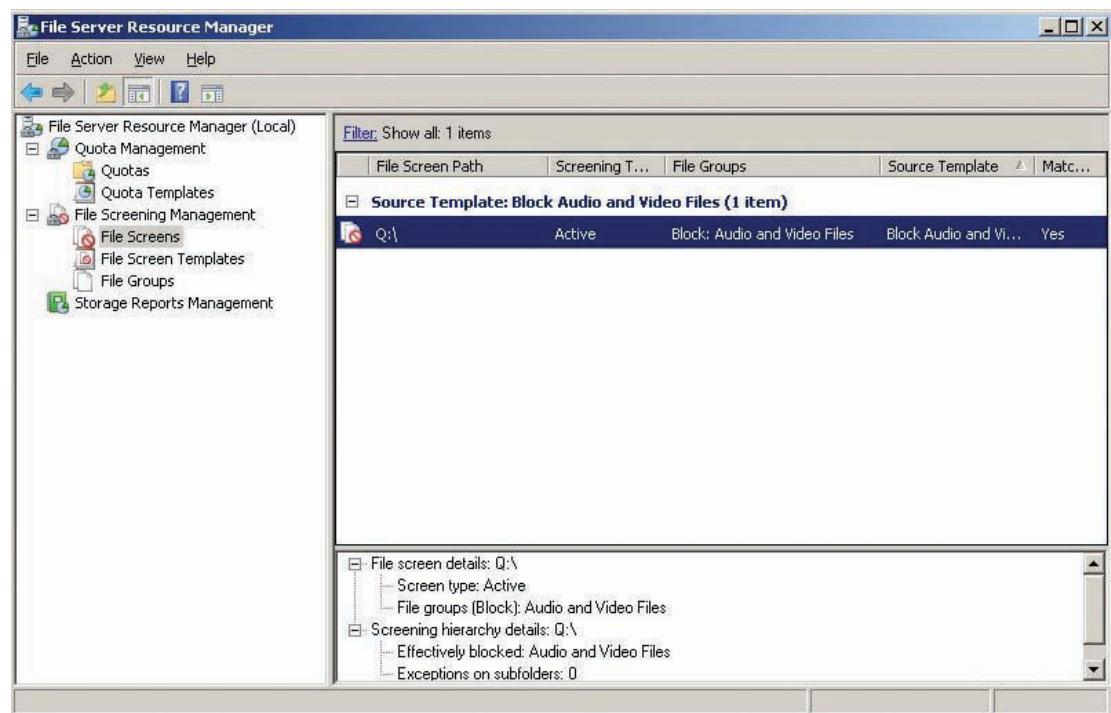


Figure 6-24 The File Screening Management node

- *Storage Reports Management*—You can define usage thresholds on volumes and folders, and any use above these thresholds generates reports on several possible storage parameters, shown in Figure 6-25. You can save reports in a variety of formats, including HTML and text.

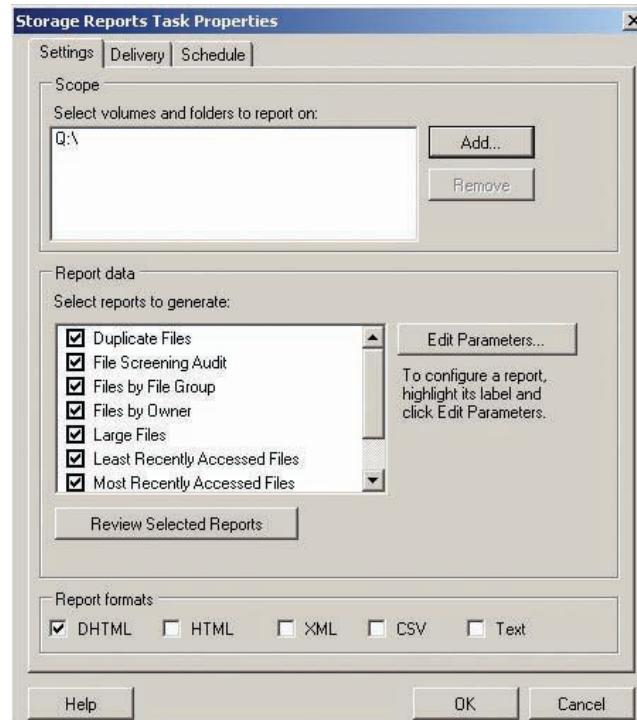


Figure 6-25 The Storage Reports Task Properties dialog box

Windows storage management is a big topic, and this introduction has only scratched the surface. You can find detailed coverage of features and tools in the File Services role in *MCTS Guide to Configuring Microsoft Windows Server 2008 Network Infrastructure* (Course Technology, 2008, 1-4239-0236-X).

Windows Printing

The capability to share printers on the network was one of the main reasons networks flourished during the 1980s and 1990s. Printers were expensive, and users were creating electronic documents with word processors, desktop publishers, and spreadsheets that needed to be printed. Networking computers together made it possible for everyone in the company to use a \$3000 laser printer without having to carry documents on a floppy disk to the lone computer to which the printer was attached. Today, basic printers cost less, but feature-rich color laser printers are still too expensive to put on everybody's desks. In addition, by networking printers, administrators have a way to monitor and control use and know when a printer is low on toner or paper. Windows Server 2008 offers advanced features for managing shared printers and making printing easy and convenient for users.



Printing is not an objective of the 70-640 exam but is covered in the 70-642 exam in detail. This chapter discusses only basic printer and print server management.

NOTE

To understand how to work with and share printers in a Windows environment, first you need to understand the terminology for defining the components of a shared printer:

- *Print device*—The physical printer containing paper and ink or toner to which print jobs are sent. There are two basic types of print devices:
 - Local print device: A printer connected to an I/O port on a computer, usually with a parallel or USB cable.
 - Network print device: A printer attached directly to the network through a NIC.
- *Printer*—The icon in the Printers folder that represents print devices. Windows programs print to a printer, which uses a printer driver to format the print job and send it to the print device or print server. A printer can be a local printer, which prints directly to a local or network print device, or a network printer, which prints to a print server.
- *Print server*—A Windows computer that's sharing a printer. It accepts print jobs from computers on the network and sends jobs to the printer to be printed on the print device.
- *Print queue*—A storage location for print jobs awaiting printing. In Windows Server 2008, the print queue is implemented as a directory (by default, C:\Windows\System32\Spool\Printers) where files that make up each print job are stored until they're sent to the print device or print server.

This section focuses on the print server—specifically, configuring and managing print servers in Windows Server 2008.

Configuring a Print Server

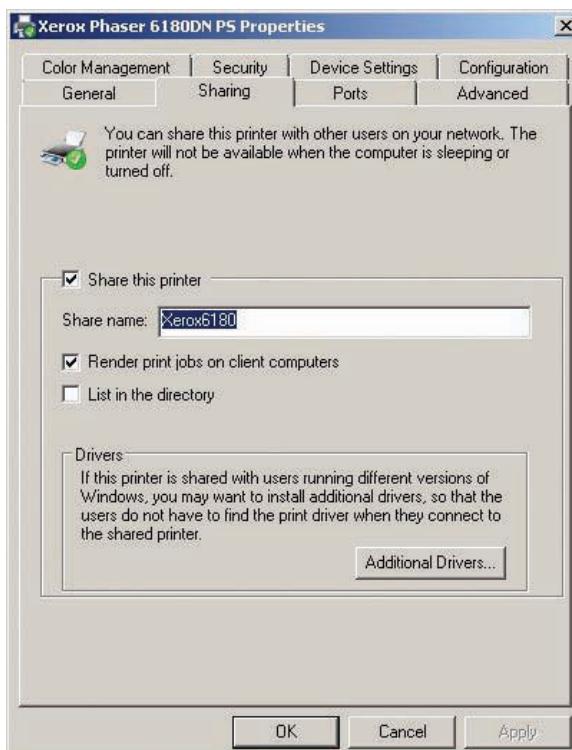
A print server configured in Windows Server 2008 can perform a host of printing functions that aren't possible when users' computers print directly to a print device:

- *Access control*—Using permissions, administrators can control who can print to a printer and who can manage print jobs and printers.
- *Printer pooling*—A single printer represents two or more print devices. Users can print to a single printer, and the print server sends the job to the print device that's least busy.
- *Printer priority*—Two or more printers can represent a single print device. In this case, printers can be assigned different priorities so that jobs sent to the higher priority printer are sent to the print device first.

- *Print job management*—Administrators can pause, cancel, restart, reorder, and change preferences on print jobs waiting in the print queue.
- *Availability control*—Administrators can configure print servers so that print jobs are accepted only during certain hours of the day.

To configure a Windows Server 2008 system as a print server, you just need to share a printer. After a printer is installed, right-click it and click Sharing. The Sharing tab of a print server's Properties dialog box (see Figure 6-26) contains the following options:

- *Share this printer*—When this check box is selected, the print server is shared. By default, the Everyone special identity is assigned Print permissions to shared printers.
- *Share name*—By default, it's the name of the print server in the Printers folder. You can enter a shorter share name or one that's easier to remember.
- *Render print jobs on client computers*—When this check box is selected (the default setting), client computers process the print job and send it to the print server in a format that's ready to go directly to the print device. If this option isn't selected, more processing occurs on the print server.
- *List in the directory*—When this check box is selected, the print server is displayed in Active Directory and can be found by Active Directory searches. By default, this option isn't selected.
- *Additional Drivers*—When a client connects to a shared printer, the printer driver is downloaded to the client from the server automatically when possible. You can click this button to install different printer drivers on the server to support different Windows versions.



6

Figure 6-26 The Sharing tab for a print server

The Advanced tab of a print server's Properties dialog box has more options for controlling the print server, from when it's available to default settings on the print device (see Figure 6-27):

- *Always available/Available from*—Choose the Available from option to set the hours the print server accepts print jobs. Jobs that users submit outside the available hours wait in the local print queue until the print server is available.

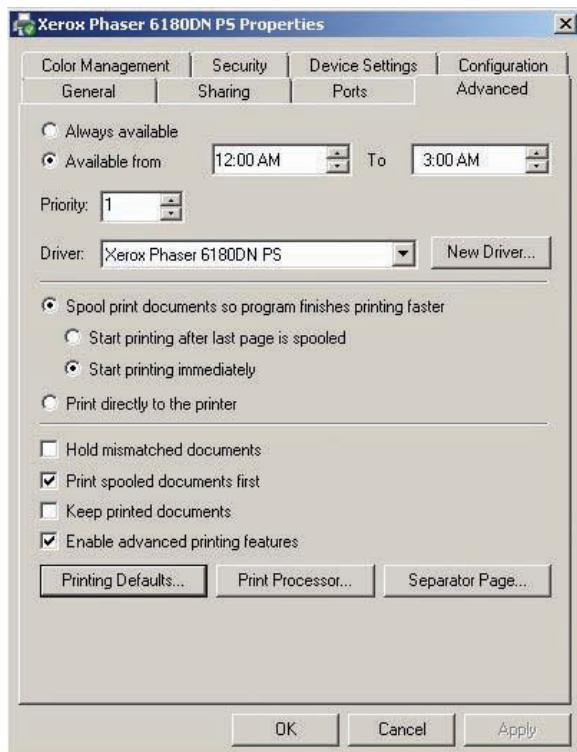


Figure 6-27 The Advanced tab for a print server

- **Priority**—Two or more printers can be configured to send jobs to the same print device, and each printer can have a different priority set. Print jobs sent to the highest priority printer are printed first. For example, you could set up two printers that print to a color laser print device. One printer is available only to managers, and the other is available to staff. Jobs sent to the manager printer, with a priority of 10, print before jobs sent to the staff printer, with a priority of 1.
- **Driver**—This field specifies the print driver in use. To change the driver, click the New Driver button.
- **Spooling options**—Print jobs that are spooled are written as files to the print queue before being sent to the print device. You can specify whether jobs should start printing as soon as a page is received or whether the entire job should be written to the queue before printing starts. The default setting is Start printing immediately. You can turn off spooling by selecting the “Print directly to the printer” option, but this option isn’t recommended, as some applications have to wait until printing is finished before they can be resumed.
- **Hold mismatched documents**—If a print job at the head of the queue requires a different paper type than what’s loaded in the print device, the print server normally stops all printing until the problem is solved. Setting this option (which is disabled by default) holds these print jobs and lets other jobs in the queue print. After the correct paper is loaded, the held document can print.
- **Print spooled documents first**—When this option is set, jobs already in the queue can start printing even if a job with higher priority starts spooling. This setting, which is enabled by default, minimizes printer idle time.
- **Keep printed documents**—Normally, print job files are deleted from the print queue after they have printed. This option, disabled by default, keeps files in the queue so that they can be reprinted if necessary. Setting this option might be a good choice with print jobs that are difficult to reproduce.

- *Enable advanced printing features*—This option, which is selected by default, enables you to use advanced printing options, such as page order and multiple pages per sheet (if supported by the driver). Turning the option off can solve some compatibility issues.
- *Printing Defaults*—You can select default settings for paper handling (one-sided, two-sided), paper sources, paper size, paper type, orientation (landscape or portrait), color or black and white, and so forth.
- *Print Processor*—Click this button to set the default print processor and data type. The existing defaults are normally okay, unless your network has older non-Windows clients.
- *Separator Page*—Click this button and then click Browse to select a separator page that's printed before each print job. Three separator pages are available in C:\Windows\System32: Pcl.sep for PCL printers, Sysprint.sep for PostScript printers, and Sysprtj.sep for PostScript printers with Japanese fonts.



Activity 6-18: Installing and Sharing a Printer

6

Time Required: 10 minutes

Objective: Install and share a printer.

Description: Most employees in the company have been printing directly to a network-attached printer. You have learned that a print server can offer some benefits, so you decide to install the printer and share it on your Windows Server 2008 server.



This activity requires a network-attached printer and its IP address. Your instructor will provide this address.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, type **printers** in the Start Search text box, and then press **Enter**.
3. Click **Add a printer**, and then click **Add a local printer**. Even though the printer is attached to the network, it's considered a local printer because you'll create an IP printer port for it.
4. In the next window, click **Create a new port**. In the Type of port list box, click **Standard TCP/IP Port**, and then click **Next**.
5. In the Hostname or IP address text box, type the network-attached printer's IP address (supplied by your instructor). The port name is filled in automatically, but you can change it, if you like. Click **Next**.
6. If necessary, select the printer manufacturer and model, and then click **Next**. Leave the printer name as is, or enter a different name, if you want. Click **Next**.
7. In the Printer Sharing window, click the **Share this printer so that others on your network can find and use it** option button. Type **SharedPrinter1** in the Share name text box. (Normally, you give a printer a more descriptive name.) Click **Next**.
8. Click **Print a test page**, unless told otherwise by your instructor. If you printed a test page, click **Close**, and then click **Finish**.
9. Right-click the printer you installed and click **Properties**.
10. Click the **Sharing** tab. Click to select the **List in the directory** check box, and then click **Apply**. Your printer is then published to Active Directory so that users can find it. The printer is listed under your domain controller if you enable the User, Contacts, Groups, and Computers as containers option in the View menu of Active Directory Users and Computers.
11. Click the **Ports** tab. You can add a port or change a port's configuration, such as changing the IP address of a TCP/IP port. If you have two or more identical printers, you can click the **Enable printer pooling** option and select additional ports for this printer.

- Click the **Security** tab. Printers don't have share permissions; they have permissions only in the Security tab, and they work similarly to NTFS permissions. Click the ACEs in the Group or user names list box, and review the permissions for each one. Click **Cancel**, and close any open windows.

Printer Permissions Access to printers is controlled much like access to folders and files. However, there's no need to be concerned with permission inheritance on printers. Printers have three standard permissions and six special permissions:

- *Print*—Allows users to connect to a printer and send print jobs to it. By default, the Everyone special identity is assigned the Print permission.
- *Manage printers*—Includes everything in the Print permission plus administering all aspects of the printer: pause and restart the printer, share the printer, change permissions, and change printer properties. By default, the Administrators, Server Operators, and Print Operators groups are assigned this permission along with the Print and Manage documents permissions.
- *Manage documents*—Allows users to manage all jobs in the print queue. By default, the Administrators, Server Operators, and Print Operators groups and the Creator Owner special identity are assigned this permission. Because Creator Owner is assigned this permission, users can manage their own print jobs (pause, cancel, restart, and change properties).

The special permissions include the three standard permissions as well as Read, Change, and Take ownership permissions.



Activity 6-19: Connecting to a Shared Printer

Time Required: 10 minutes

Objective: Connect to a shared printer from a client workstation.

Description: After installing the printer and configuring sharing, you need to set up client workstations to connect to the shared printer.

- Log on to the domain from your Vista computer as **salesperson1** with **Password02**.
- Click **Start**, type **\serverXX** in the Start Search text box, and then press **Enter**. Right-click **SharedPrinter1** and click **Connect**. Windows displays a message that it's connecting to the printer.
- Click **Start**, type **printers** in the Start Search text box, and then press **Enter**. The printer you installed should be in the Printers folder you opened. Right-click the printer and click **Print Test Page**. Each student's test page can be identified by the computer name (your domain controller's name) printed on the test page. Click **Close**.
- On your server, open the **Printers** folder in Control Panel, and double-click the printer you installed. The print queue shows any jobs awaiting printing. (At this point, there aren't any.) Figure 6-28 shows a print queue with two jobs awaiting printing.

Document Name	Status	Owner	Pages	Size	Submitted	Port
Untitled		salesperson1	2	752 KB	8:28:15 PM 6/2/2008	
Untitled		salesperson1	2	752 KB	8:29:02 PM 6/2/2008	

2 document(s) in queue

Figure 6-28 A print queue

5. Click **Printer, Pause Printing** from the menu to prevent jobs in the queue from printing.
6. On your Vista computer, print a test page to the printer.
7. On your server, you see the print job in the print queue window. Right-click the print job and review the actions you can take. Leave the print queue window open.
8. Click **Start, Computer**. Navigate to the **C:\Windows\System32\Spool\printers** folder. This folder stores the jobs you see in the print queue. Two files representing the print job are displayed. Close the Explorer window.
9. On your Vista computer, open the print queue for the printer. You see the job the same way that you see it on the server. Right-click the print job and click **Cancel**. Click **Yes** to confirm. Recall that you can manage your own print jobs because of the Creator Owner's Manage documents permission.
10. On your server in the print queue window, click **Printer, Properties** from the menu. Click the **Security** tab, click **Creator Owner** in the list of ACEs, and then click **Remove**. Click **OK**.
11. On your Vista computer, print another test page to the printer. Right-click the print job and click **Cancel**. Click **Yes** to confirm. You get an "Access denied" message in the status bar of the print queue window.
12. On your server, right-click the print job and click **Cancel**. Click **Yes** to confirm. Click **Printer, Pause Printing** from the menu to unpause the printer.
13. Close all open windows on your Vista computer and server.



Print Management from the Print Services Role You can create printer shares and manage the print server and print queue without installing the Print Services role. However, this role includes many advanced options for managing a print server as well as additional ways to share printers. When you install the Print Services role, you must install the Print Server role service. It provides the Print Management snap-in, which can be used to manage multiple printers and print servers. You can also migrate printers to and from other Windows print servers.

You have the option to install two other role services, too: LPD Service and Internet Printing. The Line Printer Daemon (LPD) Service role service allows UNIX/Linux computers using the Line Printer Remote (LPR) service to print to Windows shared printers. Internet Printing creates a Web site that allows managing print jobs through a Web browser and enables clients with Internet Printing Protocol (IPP) installed to connect to printers and send print jobs to shared printers via the Internet.

After the Print Services role is installed, the Print Management MMC is available in Server Manager and Administrative Tools. You use Print Management to view status information and manage all printers and print servers on the network. By default, local print servers are available in the console, and other print servers can be added to the console. Some tasks you can perform with Print Management include the following:

- *Install a new printer*—Add new printers to any server on the network, not just the local server.
- *Share a printer*—Share an installed printer or change a shared printer's properties and permissions.
- *Migrate printers*—Export printers from one server and import them to another. This feature makes it easy to consolidate print servers or move printers from a server that's been taken out of service.
- *Deploy printers by using group policies*—Printer connections can be set up for users or computers by using group policies, which makes it unnecessary to set up printers on separate client workstations manually.
- *List or remove printers from Active Directory*—Publish printers in Active Directory or remove published printers.
- *Display printers based on a filter*—On a network with dozens or hundreds of printers, you can configure filters to display printers that meet certain criteria. Filters enable you to view in a single window, for example, all printers that currently have jobs waiting or all printers that are out of paper or toner. You can also set up notifications so that an e-mail is sent when criteria are met.

Chapter Summary

- File systems define the method and format that an OS uses to store, locate, and retrieve files from storage media. Windows supports two file systems for storing files on hard disks: FAT and NTFS. NTFS is the file system used on most Windows servers today.
- The FAT file system consists of two variations: FAT16 and FAT32. FAT16 is limited to 2 GB partitions, and FAT32 supports up to 2 TB partitions. FAT16 and FAT32 lack encryption, file compression, and file and folder security. Older versions of Windows, such as Windows 9x, can access only FAT partitions.
- NTFS has been the file system of choice on Windows systems since Windows 2000. Features include file and folder security, disk quotas, mount points, shadow copies, file compression, and EFS. File and folder security enables administrators to limit access to files by certain users or groups of users. Disk quotas limit how much space a user can occupy on a volume. Mount points allow accessing a volume as a folder in another volume's directory structure. With shadow copies, users can access previous versions of shared files or restore deleted files from shares. EFS provides encrypted file storage.
- Files can be accessed interactively (locally) or across the network (remotely). Share permissions are applied only to network access, and NTFS permissions are applied to interactive and network access. When both share and NTFS permissions are applied to a file access, the most restrictive permission of the two is enforced.
- There are three share permissions: Read, Change, and Full Control. NTFS permissions have 6 standard permissions and 13 special permissions. Special permissions can be used to fine-tune file security and control permission inheritance.
- Files can be shared by using the File Sharing Wizard, the Advanced Sharing dialog box, the Shared Folders snap-in, and the Share and Storage Management snap-in. Sharing properties include the share name, maximum connections, permissions, and offline files (caching).
- Windows includes administrative shares automatically, which are hidden and accessible only by members of the Administrators group. Administrative shares are used to access the root of volumes, the C:\Windows folder, and interprocess communication. Domain controllers have two additional default shares: NETLOGON and Sysvol. NETLOGON is available to all users for the logon process, and Sysvol is used for replication.
- Windows storage management is necessary to manage the growing storage needs of today's networks. The File Services role adds tools to manage all aspects of storage; Disk Management is the tool for managing a server's disk system. The File Services role has these role services available: File Server, Distributed File System, File Server Resource Manager, Services for Network File System, Windows Search Service, and Windows Server 2003 File Services.
- Windows printing consists of these components: print device, printer, print server, and print queue. Using a print server helps manage user access to printers with permissions, pooling, prioritization, job management, and availability control. Three standard permissions are available to control access to printers: Print, Manage printers, and Manage documents.
- The Print Services role provides printer sharing, the Print Management snap-in, and optionally the LPD Service and Internet Printing role services. Administrators use Print Management to install new printers, share printers, migrate printers, deploy printers with group policies, and list printers in Active Directory.

Key Terms

administrative shares Hidden shares created by Windows that are available only to members of the Administrators group; they include the root of each volume, the %systemroot% folder, and IPC\$. Hidden shares' names end with a dollar sign.

disk quotas An option on NTFS volumes that enables administrators to limit how much disk space a user can occupy with his or her files.

Distributed File System (DFS) A feature that makes shared files more accessible by grouping shared folders from multiple servers into a single folder hierarchy.

file system Defines the method and format an OS uses to store, locate, and retrieve files from electronic storage media.

NTFS permissions Permissions set on folders or files on an NTFS-formatted volume. NTFS permissions protect both network and interactive file access.

shadow copies A feature on the Windows file system that allows users to access previous versions of files in shared folders and restore files that have been deleted or corrupted.

share permissions Permissions applied to shared folders that protect files accessed across the network. Share permissions are the only method for protecting files on FAT volumes.

volume mount points A feature that enables users to access a volume as a folder in another volume instead of by using a drive letter.

Review Questions

1. Which of the following file systems is supported by Windows Server 2008? (Choose all that apply.)
 - a. FAT
 - b. EXT2
 - c. NTFS
 - d. Reiser
2. Which of the following is true about the FAT32 file system? (Choose all that apply.)
 - a. Supports a maximum partition size of 2 GB
 - b. Supports a maximum file size of 4 GB
 - c. Was not available until Windows 98
 - d. Does not support file permissions
3. An image file of a full DVD can be stored on a FAT32 volume. True or False?
4. Which of the following is true about NTFS?
 - a. It's supported by Windows 98 and later.
 - b. Users can access older versions of a file.
 - c. Compressed files can be encrypted.
 - d. Volumes are accessible only by a drive letter.
5. Which of the following isn't true about disk quotas?
 - a. Users can be prevented from saving files on a volume.
 - b. An event can be generated when a user exceeds the quota limit.
 - c. Quotas can be overridden for groups.
 - d. Quotas can be set without denying disk space to users.
6. Mount points can be created only on an NTFS volume. True or False?
7. Terry stores all her files in the Documents folder on her C drive. She finds that the C drive is getting low on disk space, so she has a new disk installed. She wants to continue using her Documents folder as the location for organizing all her files, and most of her applications use this folder as the default location for opening and saving files. What is the best course of action for Terry to continue working as usual?
 - a. Create a folder named Documents on the new volume, and tell her to copy all her files to the new volume.
 - b. Create a shortcut in her Documents folder that points to a folder on the new volume.

- c. Create a new folder in the Documents folder, and mount the new volume in the folder.
 - d. Redirect Terry's Documents folder to a file server.
8. You have been getting quite a few calls with requests to restore files from a backup because the file was accidentally deleted from a share or because the user needed a previous version of a file that was overwritten. Restoring the files has become a burden, and sometimes you need to repeat the process several times until you find the version the user needs. What can you do to give users a way to access the files they need and reduce your administrative burden?
- a. Adjust permissions on the shares so that users can't delete files except their own. Tell users to back up their own files to local backup media.
 - b. Enable shadow copies for each share.
 - c. Enable shadow copies on the volumes where the shares are hosted.
 - d. Give each user a backup program and an external hard drive.
9. Which of the following is true about file compression? (Choose all that apply.)
- a. Files moved to a new location on the same volume always retain their compression attribute.
 - b. Files copied to a new location on the same volume always retain their compression attribute.
 - c. Files copied to a new location on the same volume inherit the compression attribute from the parent container.
 - d. Files moved to a new location on the same volume inherit the compression attribute from the parent container.
10. Shadow copies always keep 64 previous versions of a file. True or False?
11. Which of the following is true about EFS? (Choose all that apply.)
- a. Unencrypted files that are moved or copied to a folder with the encryption attribute set are always encrypted.
 - b. By default, encrypted files can be opened only by the user account that encrypted the file.
 - c. Any user can be added to an encrypted file's access list.
 - d. Encrypted files moved to a FAT volume become inaccessible.
12. Several users use the same computer. One user, Jim, has encrypted a file because it contains sensitive information and needs Bill to have access to the encrypted file, too. When Jim tries to add Bill to the list of users who can access the file, Bill isn't listed as a user that can be added. How can Bill be added to the list of users allowed to access the encrypted file?
13. Which of the following is true about share and NTFS permissions?
- a. NTFS permissions are applied only to interactive file access.
 - b. Share permissions take precedence over NTFS permissions.
 - c. Share permissions are applied to network and interactive file access.
 - d. NTFS permissions are applied to network access.
14. A user needs to create files and make changes to file contents. Aside from the Read permission, what other permission should the user be granted without allowing more access than is necessary?
- a. Write
 - b. Full control
 - c. Modify
 - d. Create

15. The Tsmith user account has been granted the Read share permission. Tsmith is a member of the Sales group, which has been granted the Change share permission. On the shared folder's Security tab, Sales has been granted Full control, and the Domain Users group has been granted Read permission. Which of the following can Tsmith do in the share when accessing it from the network? (Choose all that apply.)
- Change permissions on all files.
 - Delete all files.
 - Take ownership of all files.
 - Create files.
16. You're the administrator of a file server. Tom, who is on vacation, had created a file that Mary needs access to, but neither her account nor the Administrator account has permission to access the file. What is the best way to allow Mary to access the file?
17. Which of the following can be used to create shares? (Choose all that apply.)
- Advanced Sharing
 - Disk Management
 - File Sharing Wizard
 - Share and Storage Management
18. What is the maximum number of users who can simultaneously access a share created on a Vista computer?
- None (You can't create shares on a Vista computer.)
 - Unlimited
 - 16,777,216
 - 10
19. You need to prevent members of a group from accessing a subfolder of a folder to which the group does have access. What is the best way to do this? (Choose two answers. Each correct answer represents part of the solution.)
- Disable permission inheritance on the subfolder, and copy existing permissions.
 - Add each member of the group to the subfolder's DACL, and assign a Deny permission to each member.
 - Create a new group, and add members of the existing group to this new group. Add the new group to the subfolder's DACL with a Deny permission.
 - Remove the group from the subfolder's DACL.
20. You need to create a share containing confidential information that only a select group of people should know about. You don't want this share to appear in users' network browse lists. What can you do that involves the least administrative effort and disruption?
- Disable network discovery on all computers.
 - Disable network discovery on the computers of users who you don't want to see the share.
 - Put a \$ character at the end of the share name.
 - Put a @ character at the beginning of the share name.
21. What command can you put in a batch file to allow users to access the Public share on the ServPub1 server, using the drive letter P?
- net share P: \\ServPub1\Public
 - net use P: \\ServPub1\Public
 - share \\ServPub1\Public P:
 - share P: \\ServPub1\Public

22. Over the years, your network has grown from 2 servers to 15 servers. Most of these servers have shared folders on them. Users are having difficulty remembering which share is on which server as well as the server names. You want to make access to the share simpler. What is the best solution to this problem?
 - a. Install the Windows Search Service role service.
 - b. Install the File Server Resource Manager role service.
 - c. Install the Distributed File System role service.
 - d. Install the Services for Network File System role service.
23. A folder can be shared only with a single name and single set of share permissions. True or False?
24. You're seeing heavy use on one of your shared printers, and users often have to wait in line to get their print jobs. What printing feature can you use to best alleviate the problem?
 - a. Printer prioritization
 - b. Change availability hours
 - c. Change spooling options
 - d. Printer pooling
25. You have installed a shared printer with the default permissions and want users to be able to manage their own documents in the print queue. What do you need to do?
 - a. Do nothing.
 - b. Assign the Everyone special identity the Manage documents permission.
 - c. Assign the Everyone special identity the Manage printers permission.
 - d. Add Domain Users to the Printer Operators group.

Case Projects



Case Project 6-1: Creating Shared Folders

You have created the OU structure and necessary groups for all users in coolgadgets.com. Now you need to create shared folders for your users. To keep the coolgadgets.com folder structure separate from the one in chapter activities, first create a volume from free disk space on Disk1 (or the disk identified by your instructor), and name it CoolVol1. Create the necessary folders for each Cool Gadgets department, and share these folders. In addition, create a shared Public folder. (If necessary, delete any existing shares that might conflict with the shares you're going to create.) Here are the requirements for these shared folders:

Department folders:

- All users in the department can open all files and, if necessary, run scripts or executable files.
- All users in the department can create new folders and files.
- Users can delete and change permissions only on files they create.
- The Administrators group has full control over all department folders.
- Each department folder should have a subfolder, and any file placed in this subfolder is encrypted.
- All shares should be published to Active Directory.

Public folder:

- All users in the domain can open all files in this folder and, if necessary, run scripts or executable files.

- All users in the Executive OU can create, delete, and change permissions on all files and subfolders.
- This share should be published to Active Directory.

Document your permission settings by creating a table for each folder and listing the ACEs, or take screen shots of the folders' Properties dialog boxes. (Ask your instructor which documentation method to use.)

Case Project 6-2: Running Out of Disk Space

Several months after creating your shared folder structure, you find that disk space is low. You have been told that users should be limited to 1 GB each on CoolVol1. The exception is users in the Executive OU, who have a limit of 2 GB each. Configure your volume to address these requirements, and document your actions.

Case Project 6-3: Configuring Storage Requirements

You have been informed that although disk space use is under control, users are using shared folders for inappropriate types of files. You have been asked to prevent users from storing audio, video, and image files (except JPG files) on CoolVol1. Configure the volume to meet these requirements, and document your actions.

Case Project 6-4: Easing Access to Shares

Users are complaining they have too many share names to remember, and you know new servers with additional shares will be added soon, so the problem only stands to get worse. Configure your server so that all shares can be accessed as folders in the UNC path \\serverXX\CoolShares or \\w2k8adXX.com\CoolShares. Make sure that adding shares on other servers when needed will be easy and that the shared folders will be fault tolerant.



This page intentionally left blank

Configuring Group Policy

After reading this chapter and completing the exercises, you will be able to:

- Describe the architecture and processing of GPOs
- Configure group policy settings
- Work with security templates
- Manage and monitor group policies
- Configure group policy preferences

Group Policy is a powerful tool for network administrators to manage domain controllers, member servers, member computers, and users. It allows administrators to manage most aspects of computer and user environments centrally through Active Directory, eliminating the need, in most cases, to visit individual computers or user desktops.

This chapter covers the architecture of group policies so that you understand what a Group Policy Object (GPO) is and how and where GPOs can be applied to your Active Directory structure. In addition, you learn about the myriad security settings and user and computer environment settings that can be configured through group policies. You also examine how to apply standard security settings throughout your network and audit computers that aren't in compliance with designated standards. Finally, you take a look at group policy preferences, a new feature in Windows Server 2008.

An administrator's solid understanding of how to get the most out of group policies can relieve some of the burden of user and computer management. Even more important, proper design and application of group policies result in a more secure network.

Group Policy Architecture

The processes of centrally maintaining lists of computer and user settings, replicating these settings to all domain controllers, and applying these settings to users and computers are complex. The architecture of group policy is equally complex, at least when you're trying to envision the architecture as a whole. When broken down into its constituent parts, as this section does, the architecture is easier to grasp. Group policy architecture and functioning involve the following components:

- **GPOs**—A GPO is an object containing policy settings that affect user and computer operating environments and security. GPOs can be local (stored on individual computers) or Active Directory objects linked to sites, domains, and OUs.
- **Replication**—Replication of Active Directory-based GPOs ensures that all domain controllers have a current copy of each GPO. Changes to GPOs can be made on any DC and are replicated to all other DCs.
- **Scope and inheritance**—The scope of a group policy defines which users and computers are affected by its settings. The scope can be a single computer, in the case of a local GPO, or an OU, a domain, or a site. Like permissions, policy settings applied to users and computers are inherited from parent containers, and like permission inheritance, an administrator can override the default behavior of group policy inheritance.
- **Creating and linking**—GPOs are created in the Group Policy Management Console and can then be linked to one or more Active Directory containers. Multiple GPOs can be linked to the same container.

Group Policy Objects (GPOs)

A GPO, the primary component of group policies, contains policy settings for managing many aspects of domain controllers, member servers, member computers, and users. There are two main types of GPOs: local GPOs and domain GPOs (discussed later in this section).

Local GPOs Local GPOs are stored on local computers and can be edited by the Group Policy Object Editor snap-in (see Figure 7-1). To use this tool, you can add the Group Policy Editor snap-in to a custom MMC or simply type gpedit.msc in the Start Search text box, which opens a preconfigured MMC called Local Group Policy Editor. To edit policies in the Security Settings node of the local GPO, you can use the Local Security Policy MMC (accessed via Administrative Tools in Windows Vista or XP). Local GPOs on workgroup computers are edited manually with one of those tools. The policy settings on domain member computers can be affected by domain GPOs linked to the site, domain, or OU in Active Directory. Settings in local GPOs that are inherited from domain GPOs can't be changed on the local computer; only settings that are undefined or not configured by domain GPOs can be edited locally.

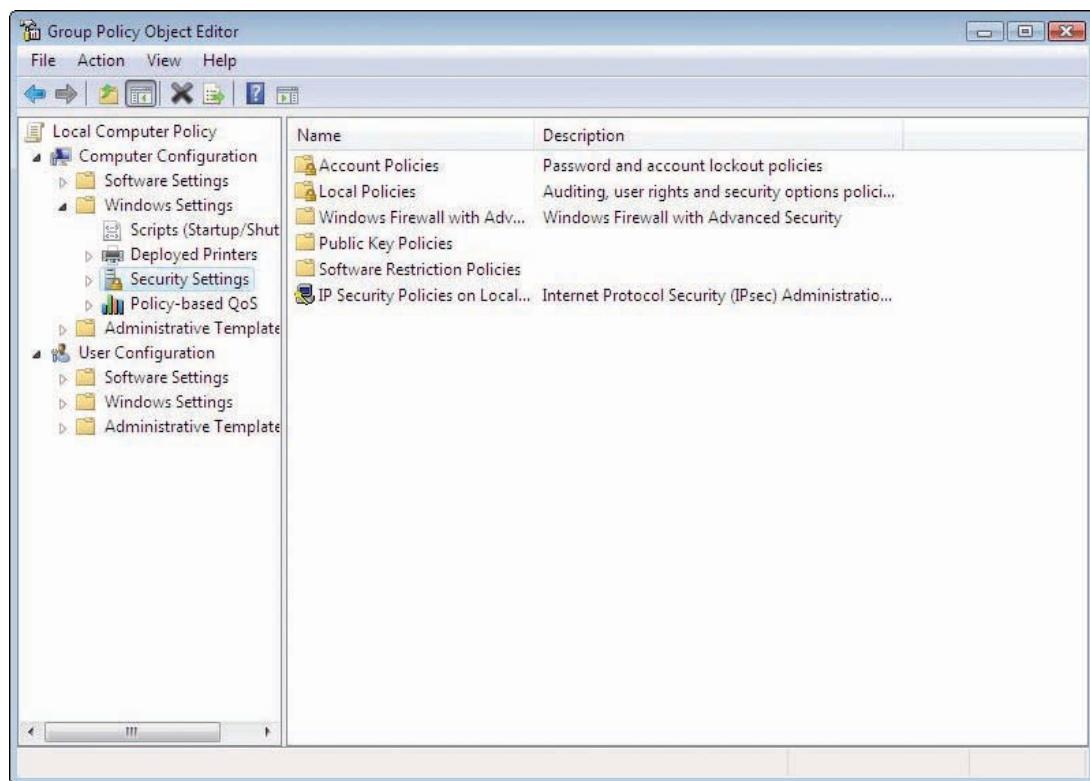


Figure 7-1 The Group Policy Object Editor

Windows XP and 2000 computers have a single GPO that affects all users of the computer. It's the GPO you see when you run Gpedit.msc and is referred to as the Local Computer Policy object. Windows Vista and Server 2008 include the Local Computer Policy object containing Computer Configuration and User Configuration nodes. The policies defined in this GPO, when configured on non-domain computers, apply to all users who log on to the computer. For example, a computer used in a public environment, such as a kiosk, might have policies that severely restrict what users can do on the computer. If the administrator needs to perform these restricted activities, the policies need to be changed first. In addition to the Local Computer Policy, Windows Vista and Server 2008 include more GPOs, discussed in the next section.

New Local GPOs in Windows Vista and Server 2008 The new GPOs in Windows Vista and Server 2008, described in the following list, allow setting different policies depending on who logs on to the computer:

- *Local Administrators GPO*—Members of the local Administrators group are affected by settings in this GPO. The default membership includes the local Administrator account and the Domain Admins global group when the computer is a domain member. This GPO doesn't contain a Computer Configuration node, so policies are limited to user-related settings.
- *Local Non-Administrators GPO*—All users of the computer who aren't members of the local Administrators group are affected by settings in this GPO, including domain users when the computer is a domain member. Like the Local Administrators GPO, this GPO consists of only a User Configuration node.
- *User-specific GPO*—You can configure a GPO that applies to a local user account. This GPO also contains only a User Configuration node and affects only users who log on to the local computer with an account defined in the local SAM database.

To access these GPOs, first add the Group Policy Object Editor snap-in to an MMC. Instead of accepting the default Local Computer Policy when asked to select a GPO, click Browse to open the dialog box shown in Figure 7-2, and select one. Local GPOs are intended to be configured on non-domain computers because domain GPOs take precedence over local GPOs, and administration is centralized by using domain GPOs. In fact, configuring the domain-based group policy “Turn off Local Group Policy objects processing” is a good idea to ensure that all policies are controlled from the domain.

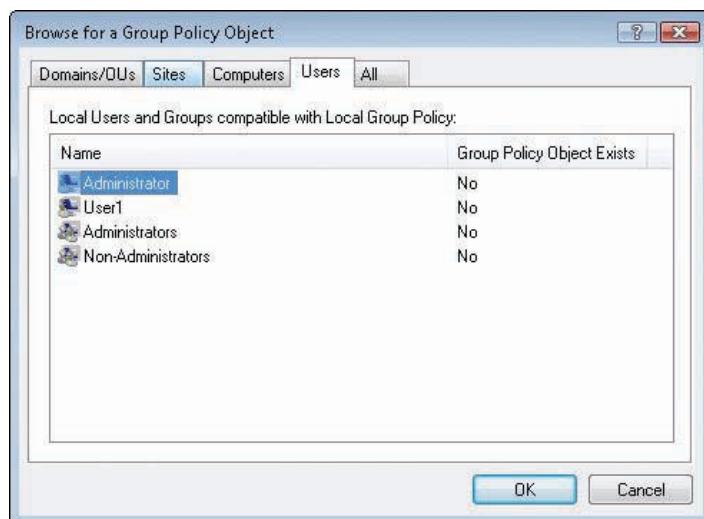


Figure 7-2 Accessing additional local GPOs in Vista

Three of the four local GPOs can contain settings that affect a single user logging on to a Windows Server 2008 or Vista computer. The Local Computer Policy object is processed first for all users and is the only local GPO that affects the computer configuration. The Local Administrators or Local Non-Administrators GPO is processed next, if configured, and the user-specific GPO is processed last, if configured. Any conflicting settings are resolved in that same order. In other words, the last configured policy setting that's applied takes precedence.



Activity 7-1: Working with Vista Local GPOs

Time Required: 15 minutes

Objective: Configure Vista local GPOs.

Description: You want to become familiar with some of the new local GPOs in Windows, so you log on to your Vista computer with the *local* Administrator account, configure some local GPOs, and create a new local user account. Then you see how local GPOs in Vista can affect different users.

1. Log on to your Vista computer with the *local* Administrator account.
2. Click **Start**. Control Panel is an option on the Start menu, but you're going to remove it. Type **gpedit.msc** in the Start Search text box and press **Enter** to open the Group Policy Object Editor for the Local Computer Policy.
3. Click to expand the **User Configuration** node, if necessary, and then the **Administrative Templates** folder. Click the **Control Panel** node.
4. In the right pane, double-click **Prohibit access to the Control Panel**. In the Properties dialog box, click **Enabled**, and then click **OK**. Close the Group Policy Object Editor.
5. Click **Start**. Notice that Control Panel is no longer on the Start menu. Type **mmc** in the Start Search text box and press **Enter**.

6. Click **File, Add/Remove Snap-in** from the MMC menu. In the Available snap-ins list box, click **Group Policy Object Editor**, and then click **Add**.
7. In the Select Group Policy Object dialog box, click **Browse**. In the Browse for a Group Policy Object dialog box, click the **Users** tab. Click **Administrators** in the Name list box, and then click **OK**. Click **Finish** and then **OK**.
8. Click to expand **Local Computer\Administrators Policy**. Click to expand **User Configuration** and **Administrative Templates**, and then click the **Control Panel** node.
9. In the right pane, double-click **Prohibit access to the Control Panel**. In the Properties dialog box, click **Disabled**, and then click **OK**.
10. Click **Start**. The Control Panel should be displayed on the Start menu. Type **compmgmt.msc** in the Start Search text box and press **Enter**. The Computer Management MMC opens.
11. Click to expand the **Local Users and Groups** snap-in, and then click the **Users** folder. Right-click the middle pane and click **New User**.
12. In the New User dialog box, type **TestGPO** in the User name text box and **Password01** in the Password and Confirm password text boxes.
13. Click to clear the **User must change password at next logon** check box. Click **Create**, and then click **Close**. Close Computer Management.
14. Log off Vista and log back on as **TestGPO** with **Password01**. You have to enter the user-name as **VistaXX\TestGPO** so that Vista knows you're logging on to the local computer.
15. Click **Start**. Notice that Control Panel isn't on the Start menu. Type **Control Panel** in the Start Search text box and press **Enter**. You get an error message stating that the operation was canceled because of restrictions on the computer. Click **OK**.
16. Log off the Vista computer and log back on to the domain from your Vista computer as **advuser1**.
17. Click **Start**. Control Panel isn't displayed on the Start menu, which demonstrates that the Local Computer Policy affects domain users as well as local users. The only local GPO that doesn't affect domain users is the user-specific GPO, which can be configured for users only in the local SAM database.
18. Log off and log back on to the Vista computer as Administrator. Open the Group Policy Object Editor (referring to Step 2 if you need help). Change the Prohibit access to the Control Panel policy back to **Not configured**.
19. Close all open windows.



Domain GPOs Domain GPOs are stored in Active Directory on domain controllers. They can be linked to a site, a domain, or an OU and affect users and computers whose accounts are stored in these containers. A domain GPO is represented by an Active Directory object, but it's composed of two separate parts: a group policy template (GPT) and a group policy container (GPC). The GPT and GPC have different functions and hold very different information, but they do have these things in common:

- *Naming structure*—Each GPO is assigned a globally unique identifier (GUID), a 128-bit value represented by 32 hexadecimal digits that Windows uses to ensure unique object IDs. The GPT and GPC associated with a GPO are stored in a folder with the same name as the GPO's GUID. This naming structure makes associating each GPO with its GPT and GPC easier.
- *Folder structure*—Each GPT and GPC has two subfolders: Machine and User. The Machine folder stores information related to the Computer Configuration node of a GPO, and the User folder stores information about the User Configuration node.

One reason administrators must understand the structure of GPOs is so that they know where to look when problems arise, particularly with replication of GPOs (covered later in this

chapter in “Group Policy Replication”). To that end, you examine GPT and GPC group policy components more closely in the following section.

Group Policy Templates A **Group Policy Template (GPT)** isn’t stored in Active Directory but in a folder in the Sysvol share on a domain controller. It contains all the policy settings that make up a GPO as well as related files, such as scripts. Every GPO has a GPT associated with it. The local path to GPT folders on a domain controller is %systemroot%\SYSVOL\sysvol\domain\Policies; %systemroot% represents the drive letter and folder name where the Windows OS is stored, usually C:\Windows, and *domain* is the domain name. Each GPT is actually a series of folders and files, but the root folder has the name of the GPO’s GUID. Figure 7-3 shows the Policies folder with three GPT folders.

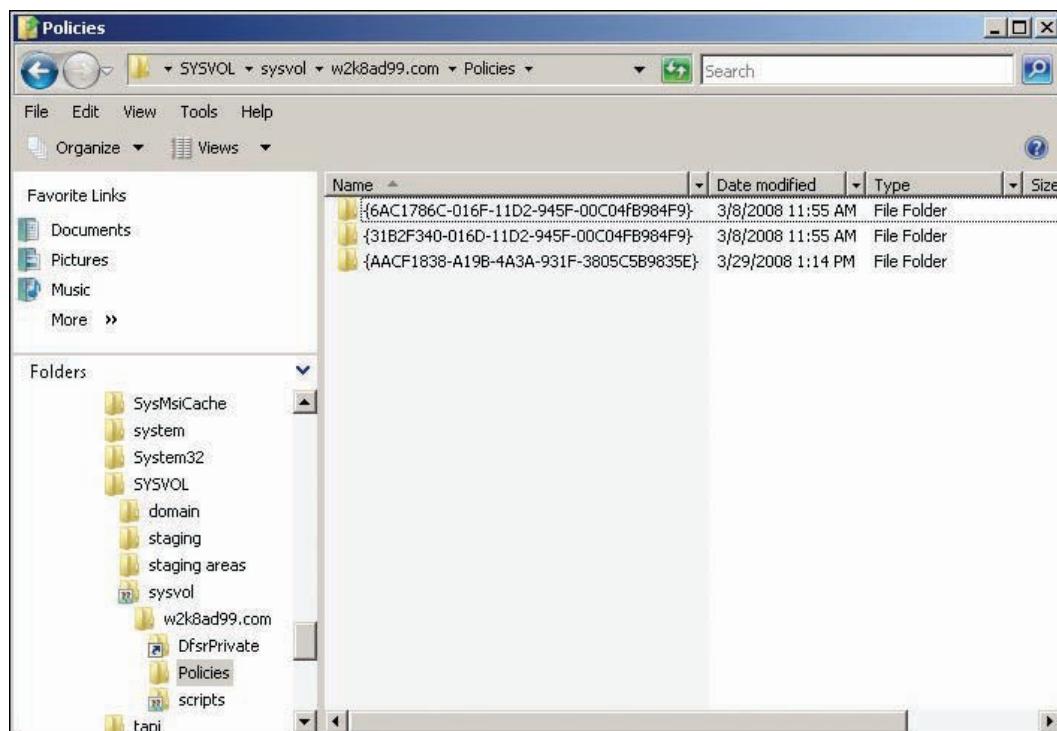


Figure 7-3 The Policies folder with three GPTs

The names of policy folders look random, but two folders have the same name on every domain controller. The folder starting with 6AC1 is the GPT for the Default Domain Controllers Policy, and the folder starting with 31B2 is the GPT for the Default Domain Policy. The third folder is the GPT for the GPO linked to the TestOU folder you created in Chapter 3.

When a new GPO is created, a number of files and subfolders are created under the root folder. The number of files and subfolders in each GPT folder vary depending on which policies have been configured, but each GPT has at least these three items:

- **GPT.ini**—This file contains the version number used to determine when a GPO has been modified. Every time a GPO changes, the version number is updated. When GPO replication occurs, DCs use this version number to determine whether the local copy of the GPO is up to date.
- **Machine**—This folder contains subfolders that store policy settings related to the Computer Configuration node.
- **User**—This folder contains subfolders that store policy settings related to the User Configuration node.

A GPO with few policy settings defined or configured has only a few additional subfolders and files under the root folder. For example, you have made only a few changes to the Default Domain Controllers Policy, which is in the folder starting with 6AC1. If you browse the Machine and User subfolders, you'll likely find only one additional file, GptTmpl.inf. This file contains settings configured in the Security Settings node under Computer Configuration.



Activity 7-2: Browsing GPTs

Time Required: 15 minutes

Objective: Browse subfolders and files in a GPT folder.

Description: You want to get a better idea of how group policies are structured, so you decide to explore the folders where the GPT component of GPOs is located.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and navigate to **C:\Windows\SYSVOL\sysvol\W2K8ADXX.com\Policies**, where you should see a list of folders similar to Figure 7-3, shown previously.
3. In the left pane, click the folder starting with **6AC1**, which is the Default Domain Controllers Policy GPT. Double-click the **GPT.ini** file to open it in Notepad. Notice the version number, which changes each time the GPO is modified. Exit Notepad.
4. Under the GPT folder, click to expand the **MACHINE\Microsoft\Windows NT\SecEdit** folder. Double-click the **GptTmpl.inf** file to open it in Notepad. Knowing the details of what's in this or other GPT files isn't important; you just need to know that they exist and how to find them. You'll probably recognize some information, however. Find the line starting with "SeInteractiveLogonRight," and you'll see Domain Users in this line. In Activity 3-10, you added the Domain Users group to the Allow log on locally right, which is the setting this line pertains to. Exit Notepad.
5. Browse to the third GPT folder (the one that doesn't start with 6AC1 or 31B2), which is associated with the GPO (TestOUGPO) you created and linked to TestOU in Activity 3-10. Double-click the **GPT.ini** file and make a note of the version number; you'll compare it to the GPC version number in the next activity.
6. Click the **User** folder, which contains the **Registry.pol** file, used to store policy settings that affect the Registry of the computer to which the policy is applied. Double-click **Registry.pol**. Windows asks how you want to open the file. Click the **Select a program from a list of installed programs** option, and then click **OK**.
7. In the list of programs, click **Notepad**. Make sure the **Always use the selected program to open this kind of file** check box is selected, and then click **OK**. This file contains the key and value of Registry entries. In this case, the key is related to Windows Explorer, and the value is **NoControlPanel**, which is the policy you set in Activity 3-10. Exit Notepad.
8. Close all open windows, but stay logged on for the next activity.



Group Policy Containers A **Group Policy Container (GPC)** is an Active Directory object stored in the System\Policies folder and can be viewed in Active Directory Users and Computers with the Advanced Features option enabled. The GPC stores GPO properties and status information but no actual policy settings. Like a GPT, the folder name of each GPT is the same as the GPO's GUID.

A GPC is composed of a considerable number of attributes that you can view in the Attribute Editor tab of the GPC's Properties dialog box, as shown in Figure 7-4. Although deciphering the purpose of each attribute isn't always easy, some information the GPC provides includes the following:

- *Name of the GPO*—The displayName attribute tells you the name of the GPO the GPC is associated with.
- *File path to GPT*—The gPCFileSysPath attribute specifies the UNC path to the related GPT folder.

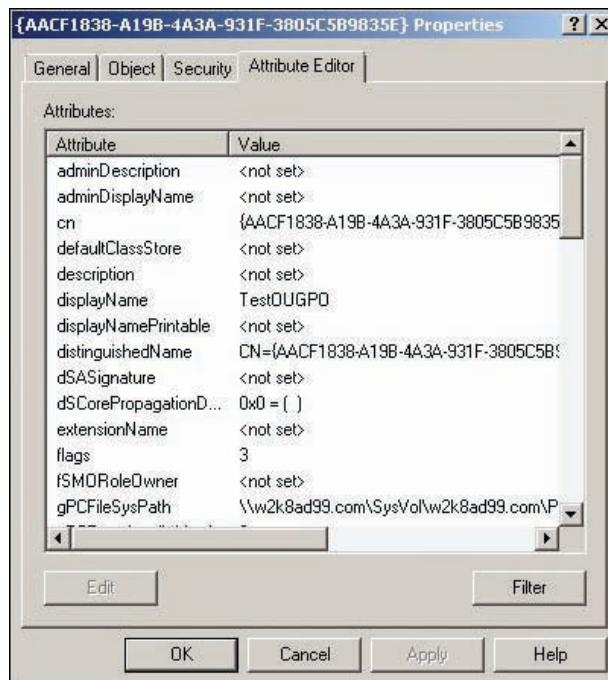


Figure 7-4 Viewing GPC attributes

- **Version**—The versionNumber attribute should have the same version number as the GPT.ini file in the GPT folder.
- **Status**—The flags attribute contains a value that indicates the GPO’s status. In Figure 7-4, it has the value 3, which indicates that the GPO is disabled. A value of 0 means the GPO is enabled.

The GPC might seem less interesting than the GPT, but it’s just as important. This Active Directory object links the GPO to Active Directory, which is critical for GPO replication to all domain controllers.



Activity 7-3: Viewing the Properties of a GPC

Time Required: 15 minutes

Objective: View the properties of a GPC.

Description: You want to get a better idea of how group policies are structured. Now that you have a handle on the purpose and location of GPTs, you want to explore the other component of GPOs, the GPC.

1. Log on to your server as Administrator, if necessary.
2. Open Active Directory Users and Computers. To verify that the Advanced Features option is enabled, click **View** on the menu bar, and click **Advanced Features** if it’s not already selected with a check mark.
3. Click the **System** folder and then double-click the **Policies** folder to see the list of GPC folders, shown in Figure 7-5.
4. In the right pane, right-click the GPC folder associated with TestOUGPO and click **Properties**. In Figure 7-5, it’s the folder starting with AACF; your folder name will likely start with different characters.
5. In the Properties dialog box, click the **Attribute Editor** tab. Scroll down to view some attributes of the GPC. Although you can edit attributes here, it isn’t recommended unless you’re sure of the results.

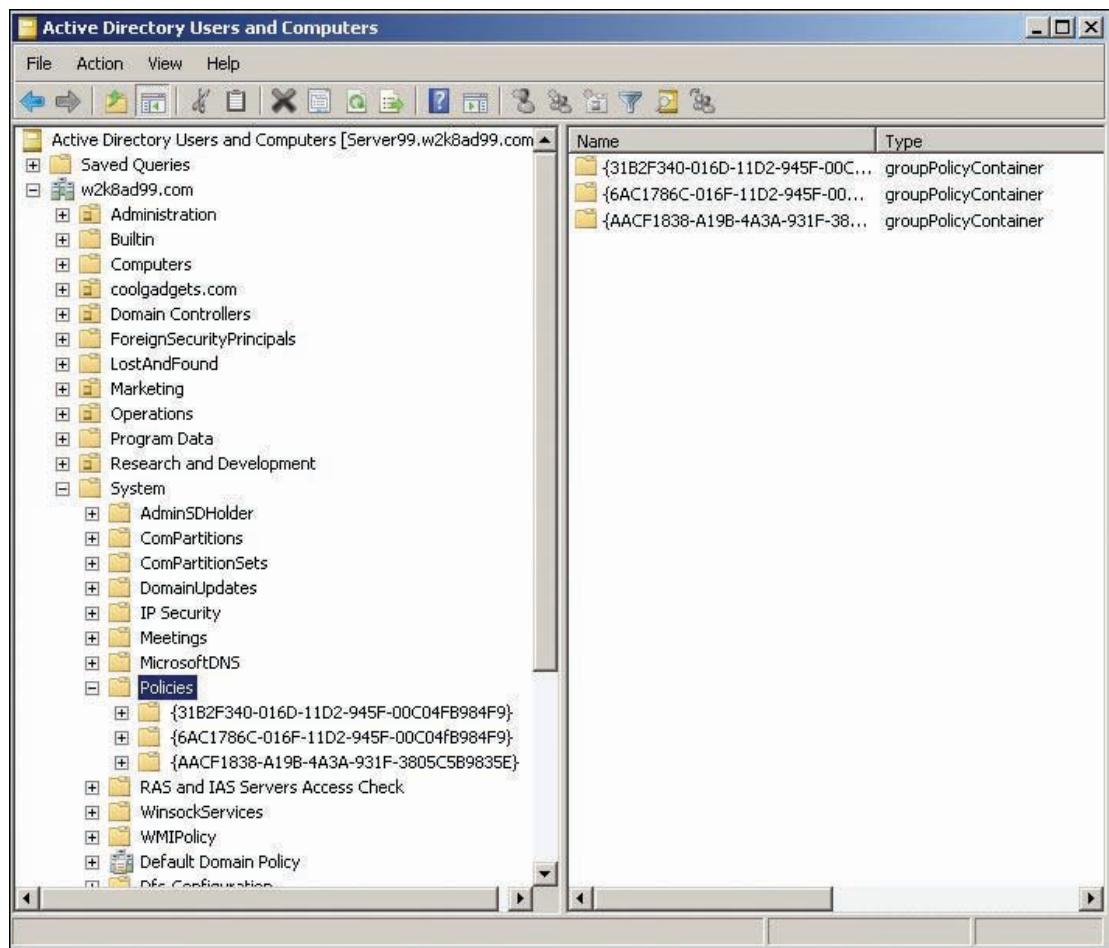


Figure 7-5 The GPC folders in Active Directory Users and Computers

6. Find the **versionNumber** attribute. It should have the same value you noted for the GPT.ini file in Activity 7-2.
7. Find the **flags** attribute. Its value should be 0, indicating that the GPO is enabled. Click **Cancel**.
8. Click **Start**, point to **Administrative Tools**, and click **Group Policy Management** (the same tool you used in Chapter 3).
9. In the left pane of Group Policy Management, click to expand **TestOU**. Click **TestOUGPO**, and in the right pane, click the **Details** tab (see Figure 7-6).
10. Click the **GPO Status** list arrow, click **All settings disabled**, and then click **OK**.
11. Open Active Directory Users and Computers. Click the GPC folder associated with **TestOUGPO**, and then open its Properties dialog box. Click the **Attribute Editor** tab, and then view the value of the **flags** attribute. It's 3, indicating that the GPO is disabled.
12. Click the **flags** attribute and click the **Edit** button. Type **0**, and then click **OK** twice.
13. In Group Policy Management, click **TestOUGPO**, and then click the **Details** tab in the right pane, if necessary. Click the **Refresh** toolbar icon or click **Action, Refresh** from the menu. The GPO status should change to Enabled.
14. Close all open windows, and stay logged on for the next activity.

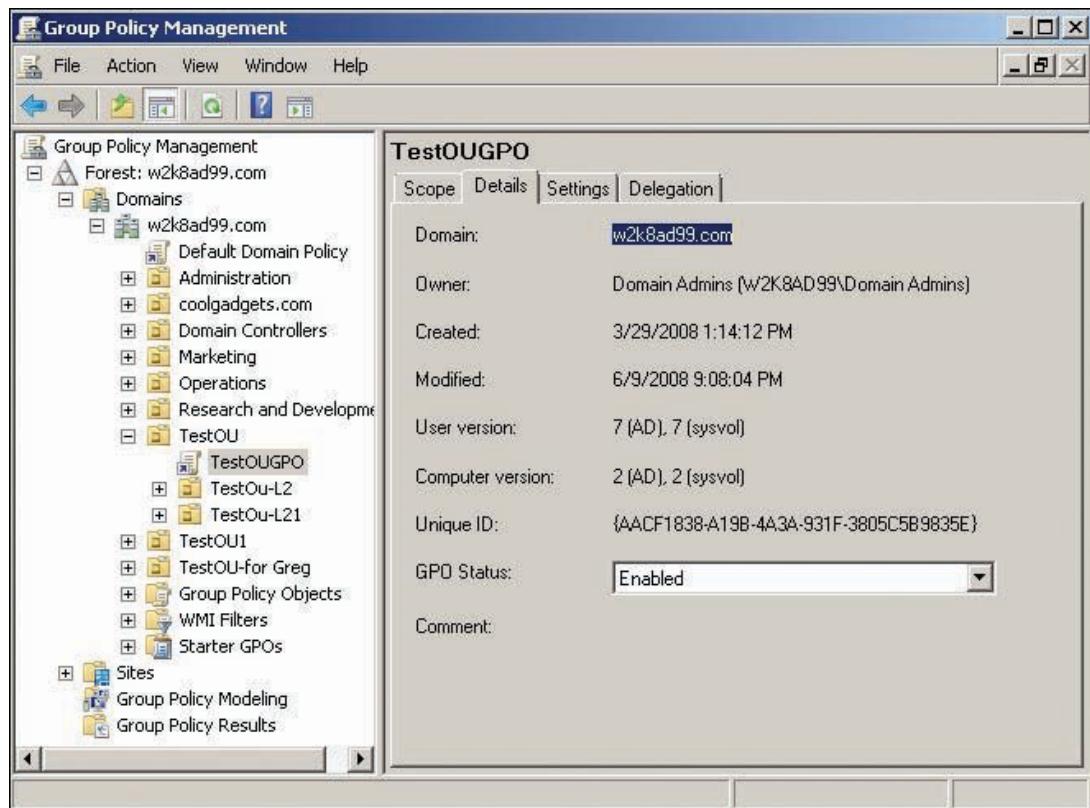


Figure 7-6 The Details tab of a GPO

Group Policy Replication

Because the two components of a GPO are stored in different places on a domain controller, different methods are required to replicate GPOs to all domain controllers. GPCs, which are Active Directory objects, are replicated during normal Active Directory replication. GPTs, located in the Sysvol share, are replicated by using one of these methods:

- *File Replication Service (FRS)*—FRS is used when you have a mix of Windows Server 2008, Windows Server 2003, and Windows 2000 domain controllers.
- *Distributed File System Replication (DFSR)*—DFSR is used when all DCs are running Windows Server 2008.

Of these two replication methods, DFSR is the more efficient and reliable. It's efficient because it uses an algorithm called remote differential compression (RDC) in which only data blocks that have changed are compressed and transferred across the network. DFSR is more reliable because of improvements in handling unexpected service shutdown that could corrupt data and because it uses a multimaster replication scheme.

Because the GPC and GPT use different replication methods, they can become out of sync. As mentioned, GPCs are replicated when Active Directory replication occurs. Between DCs in the same site, this interval is about 15 seconds after a change occurs. Between DCs in different sites, the interval is usually much longer—minutes or even hours. DFSR of the Sysvol share (and, therefore, the GPT) occurs immediately after a change is made. Strange and unpredictable results could occur when a client computer attempts to apply a GPO when the GPC and GPT aren't synchronized. However, starting with Windows XP, the client computer checks the version number of both components before applying GPO settings.

As long as replication services are running correctly, the most likely problem with GPO replication is a delay in clients receiving changes in policy settings. This problem usually occurs when

multiple sites are involved. Replication problems can be diagnosed with Gpoutil.exe, which verifies the version and status of GPOs on all DCs and reports any discrepancies. This tool is part of the Windows Resource Kit and can be downloaded from the Microsoft Download Center.

Creating and Linking GPOs

Chapter 3 introduced you to the Default Domain Policy and Default Domain Controllers Policy, but undoubtedly you'll need to create your own GPOs and link them to Active Directory containers. In fact, if changes are necessary for domain policies or domain controller policies, creating new GPOs and linking them to containers is recommended instead of editing the default GPOs.

The primary tools for managing, creating, and editing GPOs are Group Policy Management Console (GPMC, also called the Group Policy Management MMC) and Group Policy Management Editor (GPME), both of which you used in Chapter 3. The purpose of using these tools is to carry out changes to the security and/or working environment for users or computers. There are several ways to go about this task:

- Edit an existing GPO that's linked to an Active Directory container.
- Link an existing GPO to an Active Directory container.
- Create a new GPO for an Active Directory container.
- Create a new GPO in the Group Policy Objects folder, which isn't linked to an Active Directory object.
- Create a new GPO by using a Starter GPO.



If you edit an existing GPO that's already linked to an Active Directory container, keep in mind that changes in policy settings take effect as soon as clients download them. In other words, there's no Save option in the GPME; changes are saved automatically. Client computers download GPOs at restart, and user policies are downloaded at the next logon. Therefore, the best practice is usually creating GPOs in the Group Policy Objects folder, and then linking them to the target Active Directory container after all changes have been made. When you're changing several policy settings at once or are unsure of the effect policy changes will have, you should test policies before enabling them by using the following method:

1. Set up at least one test computer per OS used in the organization.
2. Join test computers to the domain and place their accounts in a test OU.
3. Create one or more test user accounts in the test OU.
4. Create the new GPO in the Group Policy Objects folder and set the policies you want.
5. Link the GPO to the test OU.
6. Restart and log on to the test computers with the test user accounts to observe the policy effects.
7. Make changes to the GPO, if necessary, and repeat Step 6 until the policy has the desired effect.
8. Unlink the policy from the test OU, and link it to the target Active Directory container.

Editing an Existing GPO To edit an existing GPO, right-click it in the GPMC and click Edit, which opens the GPO in the GPME. In the GPMC, all GPOs are stored in the Group Policy Objects folder, and you can also find GPOs linked to an Active Directory container displayed as shortcut objects in the container to which they're linked. Checking whether and where a GPO is linked is a good idea before editing. To do this, select the GPO in the left pane of the GPMC and view the Scope tab in the right pane (see Figure 7-7). All Active Directory objects the GPO is linked to are listed for the selected location. In this figure, the domain is selected as the location, and you can also select Entire forest or All sites in the Display links in this location list box.

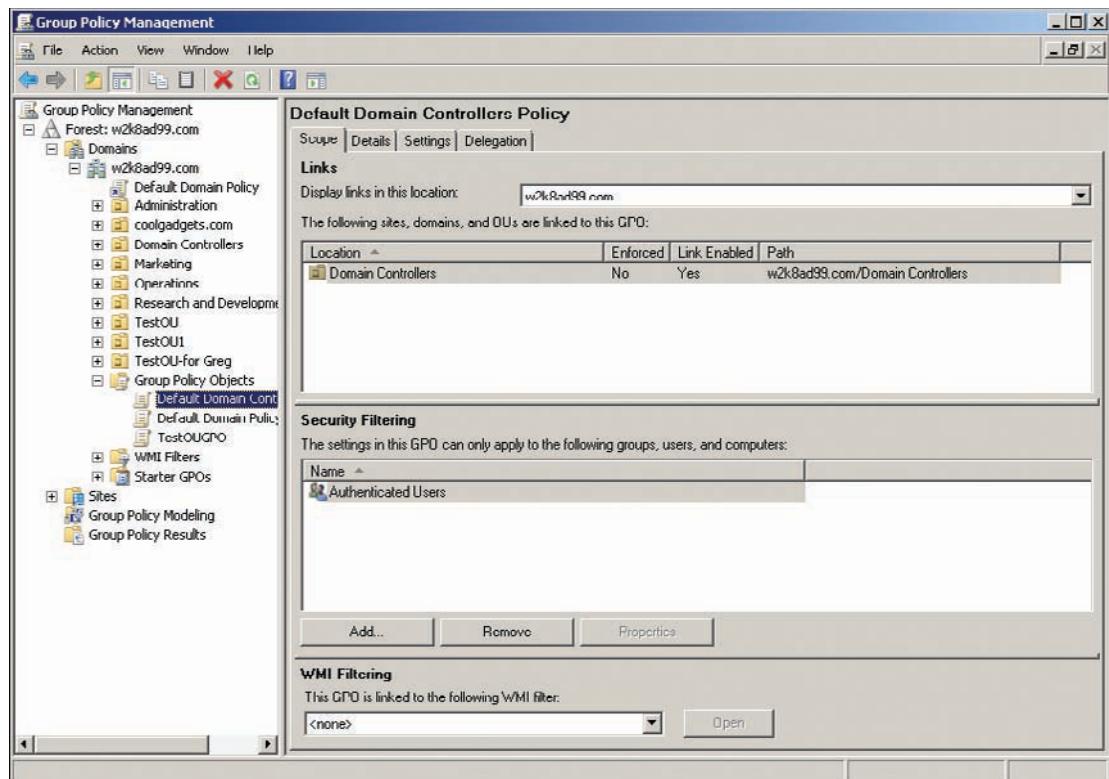


Figure 7-7 The Scope tab in GPMC

As mentioned, editing the two default GPOs is not advisable. One reason is that you can't test the GPO adequately because it's already linked to the domain or the Domain Controllers OU. Another reason is that you might want to revert to the default settings, and you could have difficulty remembering what was changed. The recommended method for making changes to domain policies is creating a new GPO and linking it to the domain. Remember: You can have multiple GPOs linked to the same container. The steps for making policy changes that affect the whole domain are as follows, assuming you already have the test computers, users, and OU set up as described previously:

1. Create the new GPO in the Group Policy Objects folder and set the policies you want.
2. Link the GPO to the test OU, making sure to unlink any GPOs that are linked there from previous tests.
3. Test your policies by following Steps 6 to 8 in the previous list.
4. Make changes to the GPO, if necessary, and repeat testing until the policy has the effect you want.
5. Unlink the policy from the test OU, and link it to the domain.

You might wonder how this procedure tests domainwide settings. Because a GPO can be linked to multiple containers, you could have linked the Default Domain Policy to the test OU as well. However, by default, policy settings are inherited by child objects, so settings in the Default Domain Policy affect objects in all Active Directory containers in the domain, including containers with another GPO linked. If you have two or more GPOs linked to the domain, as in Figure 7-8, GPOs are applied to objects in reverse of the specified link order. In this example, the NewGPO policy is applied, and then the Default Domain Policy is applied. If any settings conflict, the last setting applied takes precedence. GPO processing and inheritance are discussed later in the chapter in "Group Policy Scope and Inheritance."

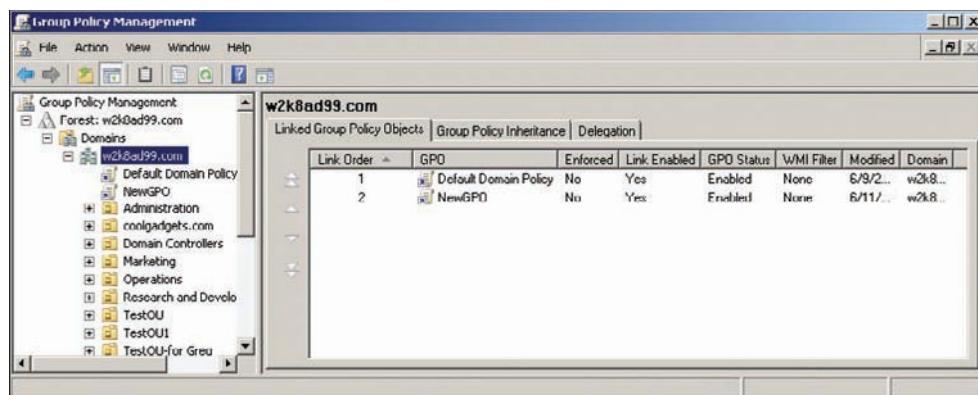


Figure 7-8 Multiple GPOs linked to a container

Creating a New GPO There are two ways to create a new GPO with the GPMC. You can right-click the container you’re linking the GPO to and select “Create a GPO in this domain, and Link it here,” or you can right-click the Group Policy Objects folder and click New. The latter method is preferable for the reasons stated earlier. After creating a GPO, you can edit it and link it to an Active Directory container, if necessary. Because several GPOs can be linked to the same container, the best practice is to create GPOs that set policies narrowly focused on a category of settings, and then name the GPO accordingly. For example, if you need to configure policy settings related to the Network node under Computer Configuration, create a GPO named CompNetwork. If this policy will apply only to a certain container, you could include the container name in the GPO name—for example, TestOU-CompNetwork. Creating and naming GPOs in this manner makes it easier to identify the GPO that sets a particular policy and to troubleshoot GPO processing problems.



Activity 7-4: Creating, Linking, and Unlinking GPOs

Time Required: 15 minutes

ACTIVITY

Objective: Create, link, and unlink GPOs.

Description: You want to be sure you know how to create and test GPOs, so you create a test OU and a GPO linked to it.

1. Log on to your server as Administrator, if necessary.
2. Open Active Directory Users and Computers, and create an OU named **TestGP1** under the domain node.
3. Open GPMC. Right-click **TestGP1** and click **Create a GPO in this domain, and Link it here**. In the New GPO dialog box, type **TestGP1GPO** in the Name text box, and then click **OK**.
4. If necessary, click **TestGP1**. In the right pane, notice that TestGP1GPO is listed as Enabled. Any changes you make to the GPO take effect on any client that updates its policies.
5. Right-click **TestGP1GPO** and click **Delete**. Click **OK**. This action deletes only the link to the GPO, not the GPO itself.
6. Click the **Group Policy Objects** folder to see all your GPOs, including the default GPOs.
7. Right-click **TestGP1GPO** and point to **GPO Status**. You can enable or disable a GPO or just disable the Computer Configuration or User Configuration settings.
8. Right-click the **TestGP1** OU and click **Link an Existing GPO**. In the Select GPO dialog box, click **TestGP1GPO**, and then click **OK**.
9. To link the same GPO to another container, right-click **TestOU** and click **Link an Existing GPO**. In the Select GPO dialog box, click **TestGP1GPO**, and then click **OK**.
10. Click **TestOU**. Notice that both TestOUGPO and TestGP1GPO are linked to TestOU. If both GPOs had the same policy setting configured but with different values, the value of the policy setting in TestOUGPO would take precedence because it would be applied last.

11. Click **TestGP1GPO** in the right pane and click the up arrow to the left of the Link Order column. TestGP1GPO now has link order 1 and TestOUGPO has link order 2, so TestGP1GPO takes precedence if any settings conflict.
12. Right-click **TestGP1GPO** and click **Delete**. Click **OK** in the message box asking you to confirm the deletion. Next, right-click **TestOUGPO** and click **Delete**, and then click **OK** in the message box. No policies should be linked to TestOU now.
13. Click to expand **TestGP1**. Right-click **TestOUGPO** and click **Delete**, and then click **OK** in the message box. Only TestGP1GPO should be linked to TestGP1 at this point.
14. Leave GPMC and Active Directory Users and Computers open for the next activity.



Activity 7-5: Configuring and Testing a GPO

Time Required: 20 minutes

Objective: Configure and test a GPO.

Description: Now that you have a new GPO and an OU to test it on, you move the computer account representing your client Vista computer to the new OU and test some computer settings in the GPO.

1. Log on to your server as Administrator and open Active Directory Users and Computers, if necessary.
2. Click the **Computers** folder, and drag your computer account to the TestGP1 OU. If necessary, click **Yes** in the warning message about moving Active Directory objects.
3. Open GPMC, if necessary. Click the **TestGP1** OU. Right-click **TestGP1GPO** and click **Edit** to open it in Group Policy Management Editor.
4. In GPME, click to expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **User Rights Assignment**.
5. In the right pane, double-click **Allow log on locally** to open its Properties dialog box. Notice that the policy setting is Not defined. Click the **Define these policy settings** check box, and then click **Add User or Group**. In the Add User or Group dialog box, click **Browse**. Type **Administrators** in the Enter the object names to select text box, and click **Check Names**. Click **OK** three times.
6. On your Vista computer, log on to the domain as Administrator. Click **Start**, point to **Administrative Tools**, and click **Local Security Policy**. The Local Security Policy MMC contains only the security settings for the local computer and is the section of the policy that was modified in Step 5.
7. Click to expand **Local Policies** and then click **User Rights Assignment**. Notice in Figure 7-9 that the icon next to the Allow log on locally policy looks like two towers and a scroll instead of the torn-paper icon next to the other policies. This icon indicates that the policy is defined by a domain GPO.

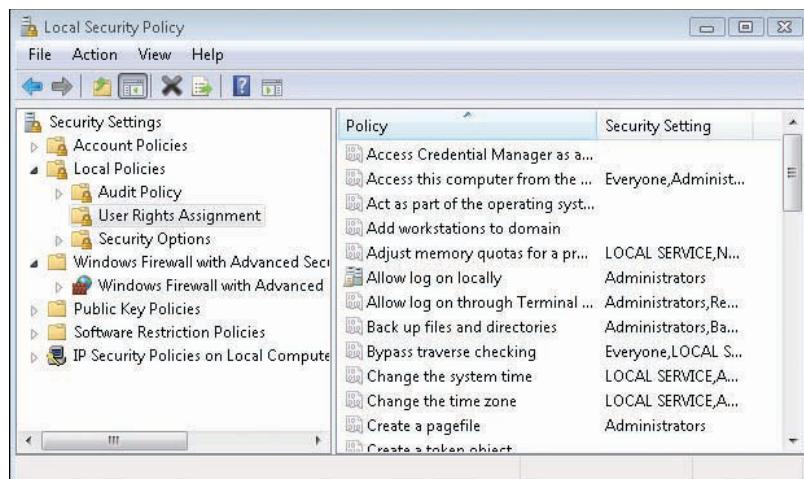


Figure 7-9 The Local Security Policy MMC

8. If your Allow log on locally policy doesn't have the domain GPO icon, the policy hasn't been updated yet on your Vista computer. If so, do the following: Close the Local Security Policy MMC, open a command prompt window, type **gpupdate**, and press **Enter**. Gpupdate.exe immediately updates group policies on the local computer. When it's finished, open the Local Security Policy MMC and navigate back to User Rights Assignment.



In this chapter's activities, if Gpupdate.exe doesn't seem to update policies on the local computer, try using **gpupdate /force**, which reapplies all policy settings, even those that haven't changed.

9. In the right pane, double-click **Allow log on locally**. In the list box of users and groups, click **Administrators**. Neither the Add User or Group nor the Remove button is active because no users, not even administrators, can override domain policies on the local computer. Click **Cancel**.
10. Log off the Vista computer, and then try to log back on as **testuser1**. Because you have restricted local logon to Administrators only, you should get the following message: "You cannot log on because the logon method you are using is not allowed on this computer. Please see your network administrator for more information." The logon method referred to in the message is interactive logon or local logon. Click **OK**.
11. On your server, change the **Allow log on locally** policy on the TestGP1GPO to **Not defined**. Close GPME.
12. On your Vista computer, try again to log on as **testuser1**. You'll probably get the same message about not being able to log on because the policy hasn't been updated yet. Click **OK**. Restart the computer by clicking the red button at the lower right of the logon window and clicking **Restart**. Recall that computer policies are updated every 90 minutes or when the computer restarts.
13. Log on to Vista as **testuser1**. Only an administrator can run the Local Security Policy MMC, but there is a workaround with the Runas command. Click **Start**, type **runas /user:administrator mmc** in the Start Search text box, and press **Enter**. When prompted for the password, type **Password01**.
14. Click **File, Add/Remove Snap-in** from the MMC menu. In the Available snap-ins list box, click **Group Policy Object Editor**, and then click the **Add** button. Click **Finish**, and then click **OK**.
15. In the Group Policy Object Editor, navigate to the **User Rights Assignment** node. In the right pane, double-click **Allow log on locally** to view the list of users and groups assigned this permission. Notice that this right is now assigned from a local GPO rather than a domain GPO, so you can make changes if needed. Click **OK**.
16. Close all open windows and log off the Vista computer. When prompted to save your console settings, click **No**. Close all open windows on your server, but stay logged on for the next activity.



Using Starter GPOs A **Starter GPO** is a GPO template, for lack of a better word, not to be confused with the GPTs discussed earlier. An administrator creates a Starter GPO to be used as a baseline for new GPOs, much like the user account templates discussed in Chapter 5.

When you create a GPO, the New GPO Wizard includes an option to use a Starter GPO. Starter GPOs are stored in the Starter GPOs folder in GPMC. Recall the best practice discussed earlier of creating new GPOs that focus on a narrow category of settings. Starter GPOs can be used to specify a baseline of settings for certain settings categories and then modified when the Starter GPO is used to create the new GPO.

To use a Starter GPO to create a new GPO, select one in the Source Starter GPO list box in the New GPO Wizard (see Figure 7-10), or right-click a Starter GPO in the Starter GPOs folder and click **New GPO From Starter GPO**. To create a Starter GPO, right-click the Starter GPOs folder and click **New**. After creating a Starter GPO, you can edit it just like any GPO. However, Starter GPOs don't contain all the nodes of a regular GPO; only the Administrative Templates folder in both Computer Configuration and User Configuration is included.

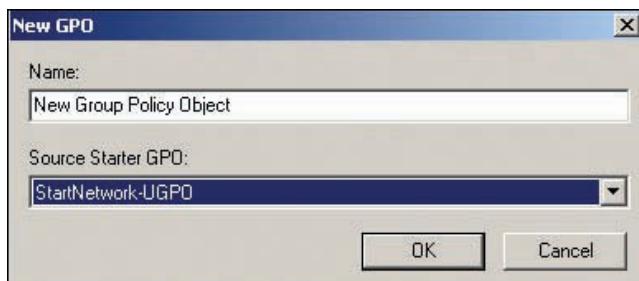


Figure 7-10 Create a new GPO with a Starter GPO



Activity 7-6: Creating and Using Starter GPOs

Time Required: 20 minutes

Objective: Create Starter GPOs to be used to create new GPOs.

Description: Now that you’re more comfortable working with GPOs, you want to start building a library of Starter GPOs for creating new GPOs. You create two: one in the Computer Configuration node for configuring printers and one in the User Configuration node for configuring Start menu options.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC. Right-click the **Starter GPOs** folder and click **New**.
3. In the New Starter GPO dialog box, type **StartPrintersC** in the Name text box. (“Start” stands for Starter GPO, “Printers” refers to the Printers node, and “C” refers to the Computer Configuration node of the GPO.) In the Comment text box, type **Starter GPO for the Printers node of Computer Configuration**, and then click **OK**.
4. Right-click the **StartPrintersC** GPO you created and click **Edit**. In the Group Policy Starter GPO Editor, click to expand **Computer Configuration**, **Policies**, and **Administrative Templates**, and then click the **Printers** node. In the right pane, double-click **Automatically publish new printers in Active Directory**. In the Properties dialog box, click **Enabled**, and then click **Apply**. Click the **Explain** tab and read the explanation of this policy setting. Click **OK**.
5. Double-click **Always render print jobs on the server**. In the Properties dialog box, click **Enabled**, and then click **Apply**. Click the **Explain** tab and read the explanation of this policy setting. Click **OK**.
6. Close the Group Policy Starter GPO Editor. In GPMC, right-click the **Group Policy Objects** folder and click **New**. In the New GPO dialog box, type **PrintConfigGPO** in the Name text box, click **StartPrintersC** in the Source Starter GPO list box, and then click **OK**.
7. Right-click **PrintConfigGPO** in the Group Policy Objects folder and click **Edit**. In GPME, expand **Computer Configuration**, and navigate to the **Printers** node under Administrative Templates to verify that your Starter GPO settings are there. Now you can link this new GPO to a container with computer accounts that have print servers installed, and the printer policies will be in effect on these servers. Close GPME.
8. To see the other method of using Starter GPOs to create new GPOs, click the **Starter GPOs** folder in GPMC. Right-click **StartPrintersC** and click **New GPO From Starter GPO**. The New GPO Wizard starts. Click **Cancel**.
9. Create another Starter GPO named **StartStMenuU**, which will be used as a baseline for Start menu options in a later activity.
10. Right-click the **StartStMenuU** GPO and click **Edit**. In GPME, click to expand **User Configuration**, **Policies**, and **Administrative Templates**, and then click **Start Menu and Taskbar**.

11. Configure the following policies as shown:

- Lock the Taskbar: **Enabled**
- Remove Games link from Start Menu: **Enabled**
- Remove Network icon from Start Menu: **Enabled**

12. Close all open windows, and stay logged on for the next activity.

Starter GPOs can be useful for making sure your policies are consistent throughout the domain by defining baseline settings for group policy setting categories. You can change the baseline settings as needed in the GPO created from the Starter GPO. However, after a new GPO is created from a Starter GPO, any changes to the Starter GPO aren't propagated to the new GPO.

Starter GPOs can also be shared with other administrators by placing them in cabinet files (CAB files). If you click the Starter GPOs folder in GPMC (see Figure 7-11), all Starter GPOs are listed in the right pane. You can use the Save as Cabinet and Load Cabinet buttons to save a Starter GPO as a CAB file and load a Starter GPO from a CAB file.

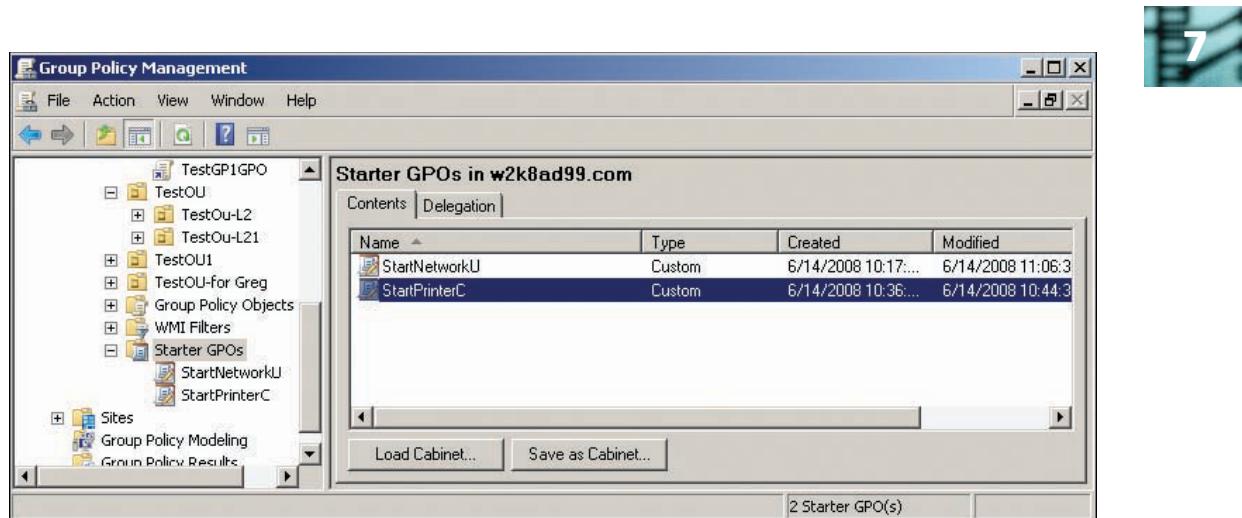


Figure 7-11 Starter GPOs can be shared as CAB files

Group Policy Scope and Inheritance

The scope of a group policy defines which objects in Active Directory are affected by settings in the policy. As stated, GPOs can be linked to sites, domains, and OUs and are applied to objects (users or computers) in this order. When conflicts exist, the last policy setting applied takes precedence. When OUs are nested, the GPO applied to the OU nested the deepest takes precedence over all other GPOs. When a policy setting isn't configured, its status is Not defined or Not configured. When a GPO is applied to an object, only the configured settings have any effect on that object. If two GPOs are applied to an object, and a certain setting is configured on one GPO but not the other, the configured setting is applied. For example, Table 7-1 shows an Active Directory structure similar to what you have been using in this book's activities (shown later in Figure 7-12). In particular, note that Marketing is a parent OU of the Advertising OU.

Table 7-1 GPO inheritance and precedence: Example 1

GPO	Linked to	Policy	Setting
Default Domain Policy	Domain	Lock the Taskbar	Disabled
StMenuMktGPO	Marketing OU	Lock the Taskbar	Enabled
StMenuAdvGPO	Advertising OU	Lock the Taskbar	Not configured

In Table 7-1, the Lock the Taskbar policy is in the GPO's User Configuration node. The policy is Enabled for users in the Marketing OU and any of Marketing's child OUs. The policy is also enabled for users in the Advertising OU (a child of Marketing) because it's not configured in the GPO linked to the Advertising OU. The policy is disabled for all other users in the domain who aren't in the scope of the Marketing OU GPO because of the Default Domain Policy's setting.

Every computer also has one or more local policies, but policies defined in GPOs in Active Directory take precedence over all local policies. So taken together, policies are applied in this order:

1. Local policies
2. Site-linked GPOs
3. Domain-linked GPOs
4. OU-linked GPOs

The last policy applied takes precedence over policies applied earlier, so OU-linked GPOs have the strongest precedence when conflicting policies exist.

Understanding Site-Linked GPOs GPOs linked to a site object affect all users and computers physically located at the site. Because sites are based on IP address, GPO processing determines from where a user is logging on and from what computer based on that computer's IP address. So users who log on to computers at different sites might have different policies applied to their accounts. In addition, mobile computers can have different policies applied depending on the site where the computer connects to the network. Keep in mind that if a site contains computers and domain controllers from multiple domains, a site-linked GPO affects objects from multiple domains. For simplicity, when you have only one site and one domain, domain GPOs should be used rather than site-linked GPOs. As you might imagine, using site-linked GPOs can be confusing for users, particularly with a lot of user mobility between sites, so site-linked GPOs should be used with caution and only when there are valid reasons for different sites to have different policies.

Understanding Domain-Linked GPOs GPOs set at the domain level should contain settings that you want to apply to all objects in the domain. The Default Domain Policy is configured and linked to the domain object by default and mostly defines user account policies. Account policies can be defined only at the domain level. Typically, they're configured by using the Default Domain Policy but can use a different GPO, as long as it's linked to the domain object.

Active Directory folders, such as Computers and Users, are not OUs and, therefore, can't have a GPO linked to them. Only domain-linked GPOs and site-linked GPOs affect objects in these folders. If you need to manage objects in these folders with group policies, moving the objects to OUs is recommended instead of configuring domain or site GPOs to manage them.

It might be tempting to define most group policy settings at the domain level and define exceptions at the OU level, but in a large Active Directory structure, that strategy could become unwieldy. Best practices suggest setting account policies and a few critical security policies at the domain level and setting the remaining policies on GPOs linked to OUs.



Domains and their child domains aren't subject to GPO inheritance. In other words, GPO settings applied to the coolgadgets.com domain are *not* inherited by objects in the US.coolgadgets.com domain.

NOTE

Understanding OU-Linked GPOs Most fine-tuning of group policies, particularly user policies, should be done at the OU level. Because OU-linked policies are applied last, they take precedence over site and domain policies (with the exception of account policies, which can be applied only at the domain level). Because the majority of policies are defined at the OU level, proper OU design is paramount in your overall Active Directory design. Users and computers with similar policy requirements should be located in the same OU when possible.

Because OUs can be nested, so can the GPOs applied to them. When possible, your OU structure should be designed so that policies defined in GPOs linked to the top-level OU apply to all objects in that OU. GPOs applied to nested OUs should be used for exceptions to policies set at the higher level OU or when certain computers or users require more restrictive policies. For example, all full-time employees in the Engineering Department need complete access to Control Panel, but part-time employees should be restricted from using it. You can configure a policy allowing Control Panel access in a GPO linked to the Engineering OU. Then you create an OU under the Engineering OU that contains part-time employees' accounts and link a GPO to it that restricts use of Control Panel.

Changing Default GPO Inheritance Behavior

By default, GPO inheritance is enabled and settings linked to a parent object are applied to all child objects. Therefore, settings in a GPO linked to the domain object are inherited by all OUs and their child objects in the domain. Settings in a GPO linked to the site are inherited by all objects in that site. To see where policies are inherited from, select a container in the left pane of GPMC and click the Group Policy Inheritance tab in the right pane. There are several ways to affect GPO inheritance:

- Blocking inheritance
- Enforcing inheritance
- GPO filtering
- Loopback policy processing



Blocking GPO Inheritance Although the default inheritance behavior is suitable for most situations, as with NTFS permission inheritance, sometimes you need an exception to the default. One method is blocking GPO inheritance, which prevents GPOs linked to parent containers from affecting child containers. To block GPO inheritance, in GPMC, right-click the child domain or OU and click Block Inheritance. You can block inheritance on a domain or an OU. On a domain object, this setting blocks GPO inheritance from a site, and on an OU, it blocks inheritance from parent OUs (if any), the domain, and the site. If inheritance blocking is enabled, the OU or domain object is displayed with a blue exclamation point. Inheritance blocking should be used sparingly; if you find that you need to block GPO inheritance frequently, it's an indication that your OU design is probably flawed and should be reexamined.

What happens if you have a nested OU and want to block GPO inheritance from its parent OU, but you still want domain- and site-linked GPOs to apply? This is where GPO enforcement comes in.

Enforcing GPO Inheritance When GPO inheritance is enforced by setting the Enforced option, the GPO's settings are applied to all child objects, even if a GPO with conflicting settings is linked to a container at a deeper level. In other words, a GPO that's enforced has the strongest precedence of all GPOs in its scope. If multiple GPOs are enforced, the GPO that's highest in the Active Directory hierarchy has the strongest precedence. For example, if a GPO linked to an OU and a GPO linked to a domain are both set to be enforced, the GPO linked to the domain has stronger precedence.

Take a look at some examples of how blocking and enforcing GPO inheritance affect the application of policies. Table 7-2 is similar to Table 7-1, except the Advertising OU has the Block Inheritance option set. Figure 7-12 shows the relevant part of the Active Directory structure in GPMC.

Table 7-2 GPO inheritance and precedence: Example 2

GPO	Linked to	Policy	Setting
Default Domain Policy	Domain	Lock the Taskbar	Disabled
StMenuMktGPO	Marketing OU	Lock the Taskbar	Enabled
StMenuAdvGPO	Advertising OU (Block Inheritance)	Lock the Taskbar	Not configured



Figure 7-12 Relevant Active Directory structure

In Table 7-2, users in the Advertising OU aren't affected by GPOs linked to the Marketing OU or the domain because inheritance is blocked. The Lock the Taskbar policy isn't configured on the Advertising OU, so settings in local GPOs apply. If the policy isn't set in local GPOs, the setting remains unchanged from its current state (whatever that might be). Table 7-3 uses the same example, but with the Enforced option set on the Default Domain Policy.

Table 7-3 GPO inheritance and precedence: Example 3

GPO	Linked to	Policy	Setting
Default Domain Policy (Enforced)	Domain	Lock the Taskbar	Disabled
StMenuMktGPO	Marketing OU	Lock the Taskbar	Enabled
StMenuAdvGPO	Advertising OU (Block Inheritance)	Lock the Taskbar	Not configured

With the configuration shown in Table 7-3, the Lock the Taskbar policy is disabled for all users in the domain because the Enforced option set on the Default Domain Policy takes precedence over all other settings, including the Block Inheritance option on the Advertising OU. The next example in Table 7-4 illustrates the effect of the Enforced option set on two GPOs.

Table 7-4 GPO inheritance and precedence: Example 4

GPO	Linked to	Policy	Setting
Default Domain Policy (Enforced)	Domain	Lock the Taskbar	Disabled
StMenuMktGPO (Enforced)	Marketing OU	Lock the Taskbar	Enabled
StMenuAdvGPO	Advertising OU	Lock the Taskbar	Not configured

When two GPOs have the Enforced option set, the GPO linked to the container highest in the Active Directory hierarchy takes precedence. Therefore, as in the previous example, the Lock the Taskbar policy is disabled for all users in the domain.



Remember that the Block Inheritance option is set on an OU or domain, and the Enforced option is set on a GPO.



Activity 7-7: Demonstrating GPO Inheritance Blocking

Time Required: 20 minutes

Objective: Enable the Block Inheritance option on an OU.

Description: You want to set some policies for personnel in the Marketing Department. However, your salespeople need not be subject to these policies, so you must block inheritance on the Sales OU.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, and click the **Group Policy Objects** folder. Create a GPO in this folder named **StMenuMktGPO**, using the StartStMenuU Starter GPO you created earlier. (Refer to Activity 7-6, if you need a reminder of how to create a GPO from a Starter GPO.)
3. In the left pane, right-click **StMenuMktGPO** and click **Edit**. In GPME, click to expand **User Configuration**, and then navigate to the **Start Menu and Taskbar** node.
4. Set the following policies in the Start Menu and Taskbar node:
 - Remove Music icon from Start Menu: **Enabled**
 - Remove Pictures icon from Start Menu: **Enabled**
5. Close GPME. In GPMC, link the **StMenuMktGPO** GPO to the **Marketing** OU. (Refer to Activity 7-4 for a reminder of how to link GPOs to containers.)
6. Click to expand the **Marketing** OU, if necessary, and then click the **Sales** OU. In the right pane, click the **Group Policy Inheritance** tab. Notice that Sales is inheriting policies from both StMenuMktGPO and Default Domain Policy, and StMenuMktGPO has a higher precedence than Default Domain Policy. Leave GPMC open.
7. Log on to the domain from your Vista computer as **salesperson1** with **Password02**.
8. Right-click the taskbar. The taskbar should be locked, and the Lock the Taskbar option should be disabled. Click **Start** to verify that the Games, Network, Music, and Pictures links are no longer in the right pane of the Start menu. Remain logged on to your Vista computer.
9. On your server, in the left pane of GPMC, right-click the **Sales** OU under the Marketing OU and click **Block Inheritance**. Notice that the list of GPOs in the Group Policy Inheritance tab is empty.
10. On your Vista computer, open a command prompt window. Type **gpupdate** and press **Enter**. After Gpupdate.exe updates group policies, close the command prompt window. (You can also log off and back on again to update user policies.)
11. Right-click the taskbar. The Lock the Taskbar option is no longer disabled. Click **Start**. The links for Games, Network, Music, and Pictures should have been restored.
12. Leave GPMC open, and stay logged on to your server and Vista computer for the next activity.



Activity 7-8: Demonstrating GPO Enforcement

Time Required: 20 minutes

Objective: Enable the Enforced option on a GPO.

Description: You have decided that the Start menu policies you configured in your Starter GPO should be applied to all users in the domain. You create a GPO based on the Starter GPO, link the new GPO to the domain object, and enforce that GPO. (Refer to Figure 7-12 for the relevant Active Directory structure.)

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, if necessary, and click the **Group Policy Objects** folder. Create a GPO in this folder named **StMenuDomainGPO**, using the StartStMenuU Starter GPO you created earlier.

3. Link **StMenuDomainGPO** to the domain object. In the left pane, click the domain object. In the right pane, click the **Linked Group Policy Objects** tab, if necessary. The GPO with link order 1 has the stronger precedence—in this case, the Default Domain Policy.
4. In the right pane, click **StMenuDomainGPO**. To change the link order, click the up arrow to the left of the Link Order column. Click the down arrow so that StMenuDomainGPO again has link order 2.
5. Right-click **StMenuDomainGPO** and click **Enforced**. Click **OK**. Notice the padlock icon next to StMenuDomainGPO indicating that GPO inheritance is enforced.
6. Click the **Sales** OU. In the right pane, click the **Group Policy Inheritance** tab, if necessary. Even though the Sales OU has the Block Inheritance option set, it's forced to inherit settings from StMenuDomainGPO.
7. On your Vista computer, log on as **salesperson1**, if necessary, and open a command prompt window. Type **gpupdate** and press **Enter**.
8. Verify that the two settings from the Starter GPO are now in effect: The taskbar should be locked, and the Network link is no longer on the Start menu. Log off Vista.
9. On your server, right-click **StMenuDomainGPO** under the domain object and click **Delete**. Click **OK**. This action unlinks the GPO from the domain but doesn't delete the GPO. Repeat for **StMenuMktGPO**.
10. Right-click the **Sales** OU and click **Block Inheritance**.
11. Close all open windows, and stay logged on to your server for the next activity.

Activity 7-8 has quite a bit going on with group policy processing, so examine the final settings to review. Table 7-5 lists the relevant GPOs, OUs, and policy settings from Activity 7-8. Both Default Domain Policy and StMenuDomainGPO are linked to the domain. StMenuDomainGPO is enforced so that the two enabled policies apply to all users in the domain. The Sales OU blocks inheritance so that objects in this OU aren't affected by Default Domain Policy or StMenuMktGPO. However, objects in the Sales OU are affected by the two enabled policies in StMenuDomainGPO because this GPO has the Enforced option set, which takes precedence over the Block Inheritance option.

Table 7-5 Blocking and enforcing GPO inheritance

GPO	Linked to	Policy	Setting
Default Domain Policy	Domain	Lock the Taskbar	Not configured
		Remove Music icon from Start Menu	Not configured
		Remove Network icon from Start Menu	Not configured
		Remove Pictures icon from Start Menu	Not configured
StMenuDomainGPO (Enforced)	Domain	Lock the Taskbar	Enabled
		Remove Music icon from Start Menu	Not configured
		Remove Network icon from Start Menu	Enabled
		Remove Pictures icon from Start Menu	Not configured
StMenuMktGPO	Marketing OU	Lock the Taskbar	Enabled
		Remove Music icon from Start Menu	Enabled
		Remove Network icon from Start Menu	Enabled
		Remove Pictures icon from Start Menu	Enabled
None	Sales OU (Block Inheritance)		

GPO Filtering You have seen how to exclude all objects in an OU from inheriting GPO settings, but what if you want to exclude only some objects in the OU? This is where GPO filtering

comes into play. There are two types of **GPO filtering**: security filtering and Windows Management Instrumentation (WMI) filtering.

Security filtering uses permissions to restrict objects from accessing a GPO. Like any object in Active Directory, a GPO has a DACL in which lists of security principals are granted permission to access the GPO. User and computer accounts must have the Read and Apply Group Policy permissions for a GPO to apply to them. By default, the Authenticated Users special identity is granted these permissions to every GPO; Authenticated Users applies to both logged-on users and computers. You can see a GPO's DACL in Active Directory Users and Computers in the System\Policies folder and in the Delegation tab in GPMC, but for basic GPO filtering, you can use the simpler GPMC interface. To view the current security filtering settings, click a GPO in the Group Policy Objects folder in GPMC and click the Scope tab on the right (see Figure 7-13).

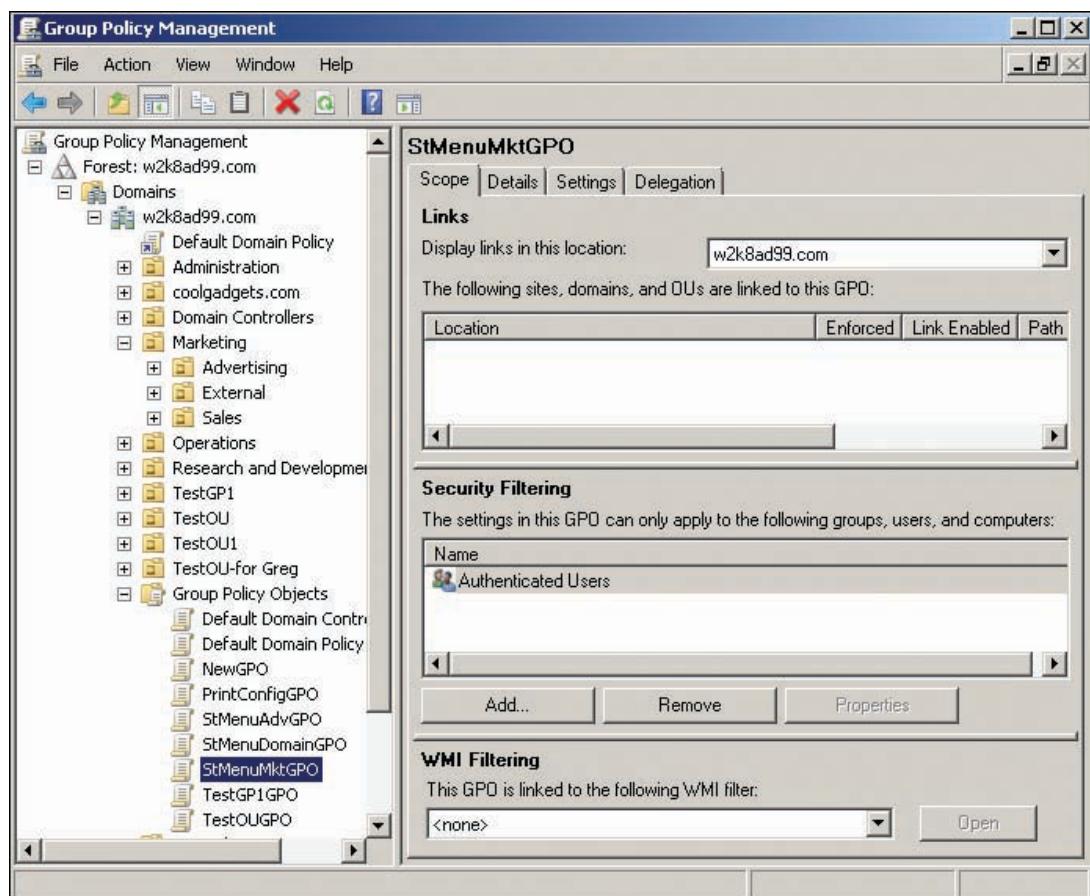


Figure 7-13 Viewing security filtering settings

You use the Security Filtering dialog box in GPMC to add or remove security principals from the GPO access list. For example, if you want a GPO to apply to all users in a domain or OU except a few, follow these steps:

1. Create a security group in Active Directory Users and Computers.
2. Add all the users who should be subject to the GPO as members of the new group.
3. In GPMC, click the GPO in the Group Policy Objects folder and click the Scope tab in the right pane.
4. Use the Security Filtering dialog box to add the new group to this GPO.
5. Use the Security Filtering dialog box to remove the Authenticated Users special identity from this GPO.

Remember that computer accounts are also affected by GPOs. So if the GPO you're filtering contains computer settings, you must add a group containing the computer accounts that should be subject to the GPO's policies.

Another way to use security filtering is to edit the GPO's DACL directly. This method is often easier when the GPO must be applied to many users and/or computers with just a few exceptions. In GPMC, click the GPO in the Group Policy Objects folder, and click the Delegation tab in the right pane to see the complete list of ACEs for the GPO, as in Figure 7-14. You can add security principals to the DACL or click the Advanced button to open the Advanced Security Settings dialog box you have used with other Active Directory objects.

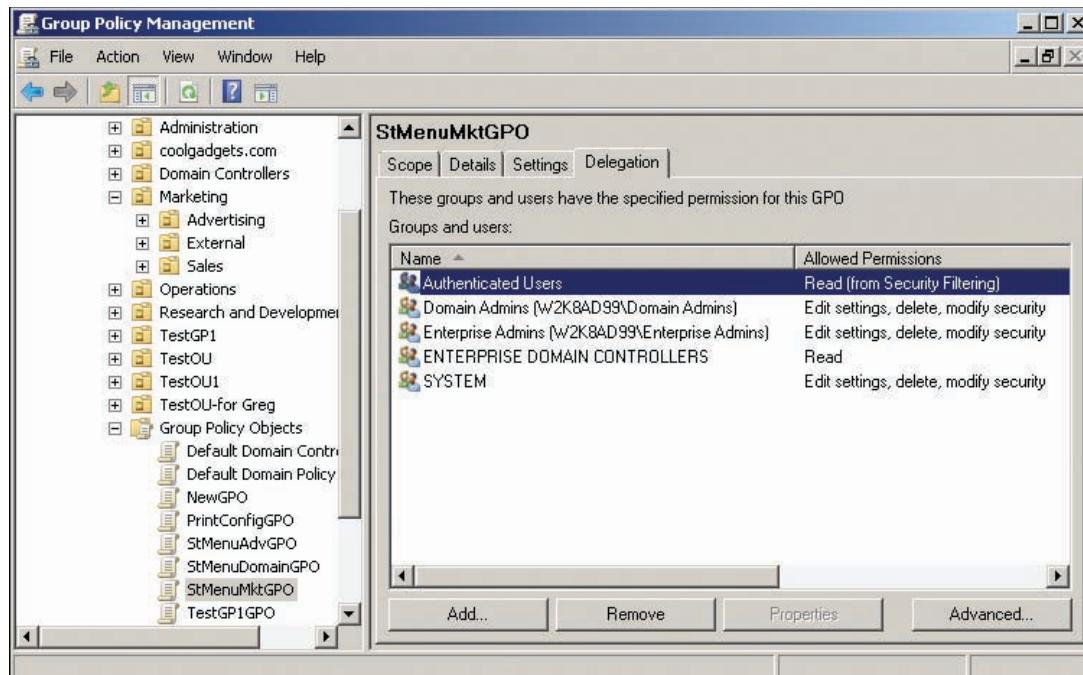


Figure 7-14 The Delegation tab for a GPO

By using the Advanced Security Settings dialog box, you can assign Deny permissions as well as Allow permissions. Assigning the Deny Read permission, for example, enables you to create exceptions to normal GPO processing. You can add a single user or computer account or a group to the DACL and prevent these security principals from being affected by the GPO.

For example, you have a GPO configuring some Internet Explorer settings in the Computer Configuration node that restricts access to advanced features. You have more than 500 computer accounts in different OUs, so you want to link the GPO to the domain so that it affects all computers in the domain. However, you have a dozen or so power users whose computers you want to exempt from these policies. You can create a group, add the power users' computers as members, add the group to the GPO's DACL, and then configure Deny Read permission.

The second type of filtering is WMI filtering. Windows Management Instrumentation (WMI) is a Windows technology for gathering management information about computers, such as the hardware platform, the OS version, available disk space, and so on. WMI filtering uses queries to select a group of computers based on certain attributes, and then applies or doesn't apply policies based on the query's results. You need to have a solid understanding of the complex WMI query language before you can create WMI filters. Here's an example of using one to select only computers running Windows XP Professional:

```
Root\CimV2; Select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP Professional"
```



You can learn more about WMI and WMI filtering by searching on the Microsoft TechNet Web site at <http://technet2.microsoft.com>.

NOTE



Activity 7-9: Using GPO Security Filtering

Time Required: 20 minutes

Objective: Change the default security filtering on a GPO and examine the results.

Description: You're unsure how GPO security filtering works, so you decide to test some settings with a test OU and test GPO.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC. Click to expand the **Group Policy Objects** folder, and then click **TestOUGPO**. In the right pane, click the **Scope** tab.
3. In the Security Filtering dialog box in the right pane, click the **Add** button. Type **Test User1**, click **Check Names**, and then click **OK**.
4. In the Name list box, click **Authenticated Users** and click the **Remove** button. Click **OK** to confirm that you want to remove the delegation privilege. TestUser1 is now the only security principal with Read and Apply Group Policy permissions for TestOUGPO.
5. Click the **Settings** tab, and then click the **show all** link. The Prohibit access to the Control Panel policy should be set to Enabled.
6. Link **TestOUGPO** to **TestOU**.
7. On your Vista computer, log on to the domain as **testuser1**.
8. Check the Start menu to see whether the link to Control Panel is there. (It should not be.) Right-click the desktop and click **Personalize**. You should see a message that the operation was canceled because of restrictions on the computer.
9. Log off and log on as **testuser2**. You should see the link to Control Panel in the Start menu.
10. On your server, change the security filtering for TestOUGPO to add **Authenticated Users** back and remove **Test User1**.
11. With TestOUGPO selected in the left pane of GPMC, click the **Delegation** tab in the right pane, and then click the **Advanced** button.
12. In the Advanced Security Settings dialog box for TestOUGPO, click **Add**. Type **Test User1**, click **Check Names**, and then click **OK**.
13. If necessary, click **Test User1** in the list box at the top, click the **Read** check box in the Deny column, and then click **OK**. Click **Yes** to confirm that you want to set a Deny permission. The current permissions on the GPO allow Authenticated Users members, except TestUser1, to access the GPO.
14. On your Vista computer, you should still be logged on as testuser2. Open a command prompt window, type **gpupdate**, and press **Enter** to update group policies.
15. After the policy update is finished, check the Start menu to verify that Control Panel is no longer available to testuser2.
16. Log off your Vista computer and log on as **testuser1**. Verify that Control Panel is available to testuser1.
17. Log off the Vista computer.
18. On your server, remove **Test User1** from TestOUGPO's DACL, and then unlink **TestOUGPO** from **TestOU**. Close any open windows, and stay logged on for the next activity.



Loopback Policy Processing By default, users are affected by policies in the User Configuration node, and computers are affected by policies in the Computer Configuration node.

Furthermore, users are affected by GPOs within whose scope they fall, and the same goes for computers.

Normally, the policies that affect user settings follow users to whichever computer they log on to. However, you might want user policy settings to be based on the GPO within whose scope the computer object falls. For example, you have an OU named ConfRoomComputers containing all computer accounts of computers in conference rooms. Perhaps you want standardized desktop settings, such as wallpaper, screen savers, Start menu, and so forth, so that these computers have a consistent look for visitors. All the settings mentioned are in the User Configuration node, however, so they can't apply to computer accounts. You don't want all users in the organization to have these settings when they log on to other computers in the company. The solution is to enable the "User group policy loopback processing mode" policy in the Computer Configuration node of a GPO. After this policy is enabled, settings in the User Configuration node of the GPO apply to all users who log on to the computer. To use loopback processing in the conference room computers example, you would take the following steps:

1. Create a new GPO (or edit an existing one), and enable the "User group policy loopback processing mode" policy in the Computer Configuration\Policies\Administrative Templates\System\Group Policy node.
2. In the User Configuration node of the GPO, edit policies to set the wallpaper, screen saver, and Start menu options you want.
3. Link the GPO to the ConfRoomComputers OU.

When users log on to a computer in a conference room, they're now subject to the User Configuration policies you set in the GPO linked to the ConfRoomComputers OU. When users log on to any other computer, they're subject to whatever policies normally affect their user accounts.

Group Policy Settings

As you learned in Chapter 3, GPOs have a Computer Configuration node, affecting all computer accounts in a GPO's scope, and a User Configuration node, affecting all user accounts in a GPO's scope. Most policies in these two nodes affect different aspects of the working environment, but a few policies are the same. If the same policy is configured in both nodes and the settings conflict (for example, one disables a policy and the other enables it), the setting in Computer Configuration takes precedence.

Both nodes have a Policies folder and a Preferences folder (discussed later in the chapter). Under the Policies folder are these three folders: Software Settings, Windows Settings, and Administrative Templates.

Chapter 3 covered the types of policies in these folders briefly, but now you examine them more closely. The Software Settings and Windows Settings folders include items called extensions because they extend the functionality of Group Policy beyond what was available in Windows 2000. The Administrative Templates folder contains categorized folders or nodes with settings that affect users' or computers' working environments, mainly by changing Registry settings.

Policy settings can be managed or unmanaged. A managed policy setting is applied to a user or computer when the object is in the scope of the GPO containing the setting. When the object is no longer in the GPO's scope or the policy is set to Not configured, however, the setting on the user or computer reverts to its original state. You have seen this behavior in earlier activities, when the Prohibit access to the Control Panel policy affected the user only as long as the user was in the GPO's scope. An unmanaged policy setting is persistent, meaning it remains even after the computer or user object falls out of the GPO's scope. The policies that are preloaded in Active Directory are managed policies, but you can customize Group Policy by adding your own policies, which are unmanaged.

Policies in the Computer Configuration Node

The Computer Configuration node applies policies to computers regardless of who logs on to the computer. Most important, this node contains most of the security-related settings in the Account Policies, User Rights Assignment, Audit Policy, and Security Options nodes. Computer

Configuration policies are uploaded to a computer when the OS starts and are updated every 90 minutes thereafter. Although many policies take effect when the GPO is updated, some might require a computer restart. The next sections cover some important policies in the Computer Configuration node of a GPO.

Computer Configuration: Software Settings

The Software Settings node contains the Software Installation extension, which can be configured to install software packages remotely on computers, regardless of who logs on to the computer. Applications are deployed with the Windows Installer service, which uses installation packages called MSI files. An MSI file is a collection of files packaged into a single file with an .msi extension and contains the instructions Windows Installer needs to install the application correctly.

In the Computer Configuration node, software packages are assigned to target computers, meaning installation of the software is mandatory, and assigned packages are installed the next time the computer starts. To assign a software package to a computer, you must create a shared folder on a server that gives the computer the Read & execute permission. Typically, you do this by assigning the necessary permissions to the Authenticated Users special identity. If you're deploying several applications through Group Policy, you can create a separate folder in the share for each package. After creating the share and copying the installation package to it, you can create your deployment policy by using the Software Installation extension.



The User Configuration node also has a Software Installation extension with additional deployment options for users, as you see later in this chapter.

NOTE



Activity 7-10: Deploying Software to a Computer

Time Required: 20 minutes

Objective: Create a software installation policy and deploy a software package to a computer.
Description: All computers in the Operations Department will benefit from a utility that's available as a free download from the Microsoft Web site. You decide to deploy the utility by using group policies. You want to test your policy first, so you link it to the TestGP1 OU where your Vista computer account is.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer, and click the **QData** volume. Create a new folder called **SoftDeploy** in this volume.
3. Right-click **SoftDeploy** and click **Share**. In the File Sharing Wizard, type **Authenticated Users** in the text box at the top, and then click **Add**. The default permission of Reader is sufficient. Leave Administrator in the permissions list at the bottom. Click **Share**, and then click **Done**.
4. In Windows Explorer, click to expand the **SoftDeploy** folder, and create a subfolder named **SyncToy**. (**SyncToy** is the name of the utility you're deploying.) Close all open windows on your server.
5. Log on to the domain from your Vista computer as Administrator.
6. Start Internet Explorer and go to www.microsoft.com/download. In the Search text box, type **synctoy** and click **Go**.
7. Click the **SyncToy v1.4** link, and then click the **Download** button. In the File Download - Security Warning dialog box, click **Save**. By default, the file is saved in the Downloads folder in the Administrator's profile. Click **Save**.

8. Click **Open Folder**. Right-click the **Setup** file and click **Copy**.
9. Click **Start**, type **\serverXX\SoftDeploy\SyncToy** in the Start Search text box, and press **Enter**.
10. Right-click the resulting Explorer window and click **Paste**. Close all open windows on your Vista computer.
11. On your server, open GPMC. Click the **Group Policy Objects** folder, and create a GPO in it named **SwInstComp**. Right-click **SwInstComp** and click **Edit**. In the GPME, click to expand **Computer Configuration**, **Policies**, **Software Settings**, and **Software Installation**.
12. Right-click the **Software Installation** extension, point to **New**, and click **Package**. In the Open dialog box, type **\serverXX\SoftDeploy\SyncToy** and press **Enter**. Click the **Setup.msi** file, and then click **Open**.
13. In the Deploy Software dialog box, click **OK**. The Advanced option allows you to set additional options for package deployment, but for now, stick with the default deployment options. Click **Software Installation** in the left pane of GPME. The name of the application is listed in the right pane. Close GPME.
14. In GPMC, link the **SwInstComp** GPO to the **TestGP1** OU (where your Vista computer account is).
15. Restart your Vista computer. Log on to the domain as **testuser1**.
16. Click **Start**, **All Programs**. SyncToy should be listed near the top of the list of programs. (If you don't see SyncToy, verify that your Vista computer account is in the TestGP1 OU and the SwInstComp GPO is linked to TestGP1. If necessary, restart your computer again, as it can take a while for group policies to take effect.)
17. Click the **SyncToy** item in All Programs to start the installation, if you want. Depending on the MSI file, some applications self-install, but others simply provide a link that installs the package the first time it's clicked. Installing SyncToy isn't necessary, but it's a handy utility for synchronizing files between a computer and a removable drive, such as a thumb drive.
18. Close all open windows on your Vista computer and server.

Advanced Application Deployment Options To access additional options for deploying applications, click the Advanced option button in the Deploy Software dialog box. This action opens the Properties dialog box shown in Figure 7-15, which contains several tabs with options for changing how the application is deployed:

- *Deployment tab*—You can select whether a package is published or assigned. In the Computer Configuration node of a GPO, software packages can only be assigned, so the Published option is disabled, as shown in Figure 7-15. The deployment type you select determines what's available in the Deployment options section, including when and how an application is deployed. For example, an application can be installed at user logon or when a document used by the application is opened. Another deployment option uninstalls the application automatically if the user or computer falls out of the GPO's scope.
- *Upgrades tab*—A package upgrade can be deployed by specifying which existing packages are to be upgraded by the new package.
- *Categories tab*—You use this tab to associate a published package with a category. Control Panel's Programs applet (Add/Remove Programs in Windows XP) lists available applications under the specified categories. This option is used only for packages published in the User Configuration node.
- *Modifications tab*—You can use this tab to customize a package installation by using a transform file (.mst extension). Select the transform files for customizing the installation of the MSI file.

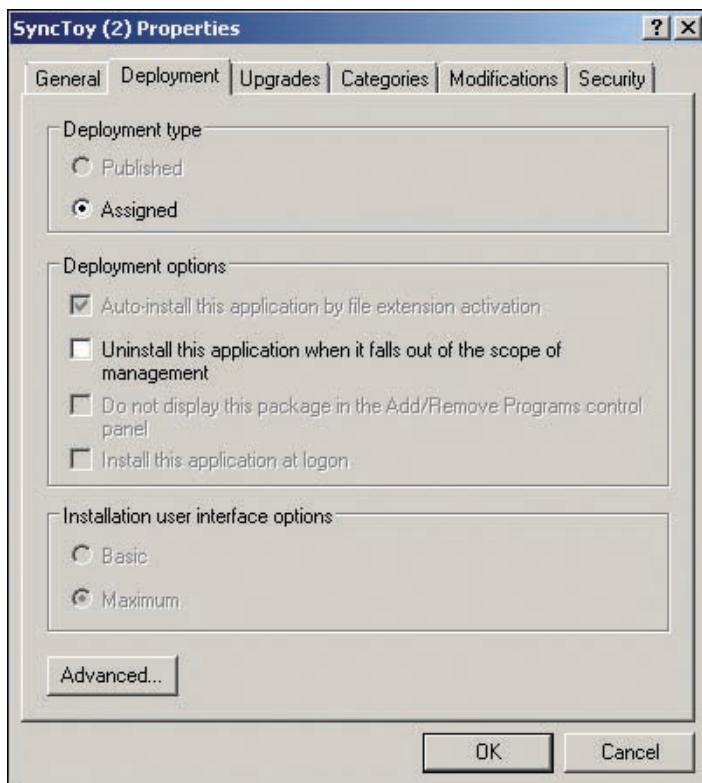


Figure 7-15 Configuring advanced deployment options

After a package is deployed to a computer, by default it's not installed again. However, if changes have been made to the original package, right-click the package in the Software Installation extension and click All Tasks, and then click Redeploy application. This action reinstalls the package on the target computers. To remove a deployed package, right-click the package and click All Tasks, and then click Remove. You have the option to uninstall the software immediately or simply prevent new installations yet allow users to use already deployed packages.

Computer Configuration: Windows Settings

The Windows Settings folder contains four subnodes:

- *Scripts (Startup/Shutdown)*—You can create scripts in a variety of scripting languages, including VBScript, JScript, and batch files. Startup scripts run when the computer starts, and shutdown scripts run before the computer shuts down. Scripts must be placed in the Scripts folder under the GPO's GPT folder in the Sysvol share.
- *Deployed Printers*—Printers can be deployed to computers by simply specifying the UNC path to a shared printer. The next time a computer in the GPO's scope starts, the printer is installed. This policy is new in Windows Server 2008.
- *Security Settings*—This node consists of a number of subnodes and is discussed in more detail in the next sections.
- *Policy-based QoS*—QoS policies, new in Server 2008, enable administrators to manage the use of network bandwidth on a per-computer or per-user basis and prioritize network packets based on the type of data the packet carries.

Security Settings Subnode: Account Policies There are well over 100 policies under Security Settings. Some of the most important are under Account Policies and Local Policies because they contain baseline security options for your computers. The Account Policies subnode contains settings that affect user authentication and logon. A GPO with settings configured in

Account Policies must be linked to the domain for these policies to have any effect. If a GPO linked to an OU has settings configured in Account Policies, they are essentially ignored so that all account policies are in GPOs linked to the domain. The Default Domain Policy is configured with default account policies settings, and many administrators keep all account policies in this GPO. Account Policies contains three subnodes:

- *Password Policy*—Contains the following policies that control password properties:
 - Enforce password history: Contains a value between 0 and 24 (the default), which indicates how many passwords Windows remembers before a user can reuse a password. A value of 0 means Windows doesn't keep a password history. To keep users from changing their password many times in succession to skirt this policy, you should set the Minimum password age policy.
 - Maximum password age: A value between 0 and 999 indicates how many days a user can use a password before having to change it. If a user doesn't change his or her password within the required number of days, the password expires and the user can't log on until the password is changed. A value of 0 means the password never expires. The default is 42 days.
 - Minimum password age: A value between 0 and 998 indicates how many days must elapse before a user can make successive password changes. A value of 0 means users can change their passwords as often as they want. The default is 1.
 - Minimum password length: A value between 0 and 14 indicates the minimum number of characters a user's password must be. A 0 means blank passwords are allowed. The default is 7.
 - Password must meet complexity requirements: If enabled (the default setting), a user's password must meet certain requirements: at least six characters (or meeting the Minimum password length policy, whichever is longer); doesn't contain more than two consecutive characters found in the user's account name or full name; and must contain characters from three of these categories—uppercase letters, lowercase letters, numbers, and special characters (\$, @, !, #, and so on).
 - Store passwords using reversible encryption: If enabled, passwords are stored with a method that's essentially plaintext and not secure. This policy should be set only if a critical application requires access to user passwords for authentication purposes. The default is disabled.
- *Account Lockout Policy*—Contains the following policies that control user account lockout:
 - Account lockout duration: Contains a value between 0 and 99999 that indicates how many minutes a user's account is locked and, therefore, unable to be used for logon if the “Account lockout threshold” setting is exceeded. The account is unlocked automatically after this number of minutes passes. A value of 0 means the account remains locked until an administrator unlocks it. The default is Not defined because this setting has meaning only when the Account lockout threshold is defined and is not zero. After the Account lockout threshold is defined with a nonzero value, the suggested setting is 30.
 - Account lockout threshold: Contains a value between 0 and 999 that determines how many times a user's password can be entered incorrectly before the account is locked out. The default is 0.
 - Reset account lockout counter after: Contains a value between 1 and 99999 that indicates the number of minutes that must elapse between failed logon attempts before the failed logon attempt counter is reset to 0. The default is Not defined because this setting has meaning only when the Account lockout threshold is defined and is not zero. When Account lockout threshold is defined with a nonzero value, the suggested setting is 30.

- **Kerberos Policy**—Administrators can use this suite of policies to fine-tune parameters for Kerberos, the default authentication protocol in a Windows domain. The policies deal with the length of time Kerberos authentication tickets are active. Shortening the active time increases security but increases authentication overhead, too. In most cases, the default values shouldn't be changed.

Security Settings Subnode: Local Policies Local Policies is so named because all settings in its subnodes pertain to security options applied to computers and what users can and can't do on the local computer to which they log on. Because these policies affect computers, they are usually defined in GPOs linked to OUs containing computer accounts, such as the Default Domain Controllers Policy. There are three subnodes of Local Policies:

- **Audit Policy**—An administrator can audit events occurring on a computer, including logon and logoff, file and folder access, Active Directory access, and system and process events (see Figure 7-16). Auditing can be enabled for successful events, failed events, or both. For example, you can audit a user's successful access to a file or attempted accesses that fail or both. Auditing file and folder access should be used sparingly and for only short periods because of the system overhead it creates. By default, no audit policies are defined on either default GPO. However, in Windows Server 2008, certain events, such as logons and directory service access, are audited by default. Events created by auditing are listed in the Security log, which you can view with Event Viewer.

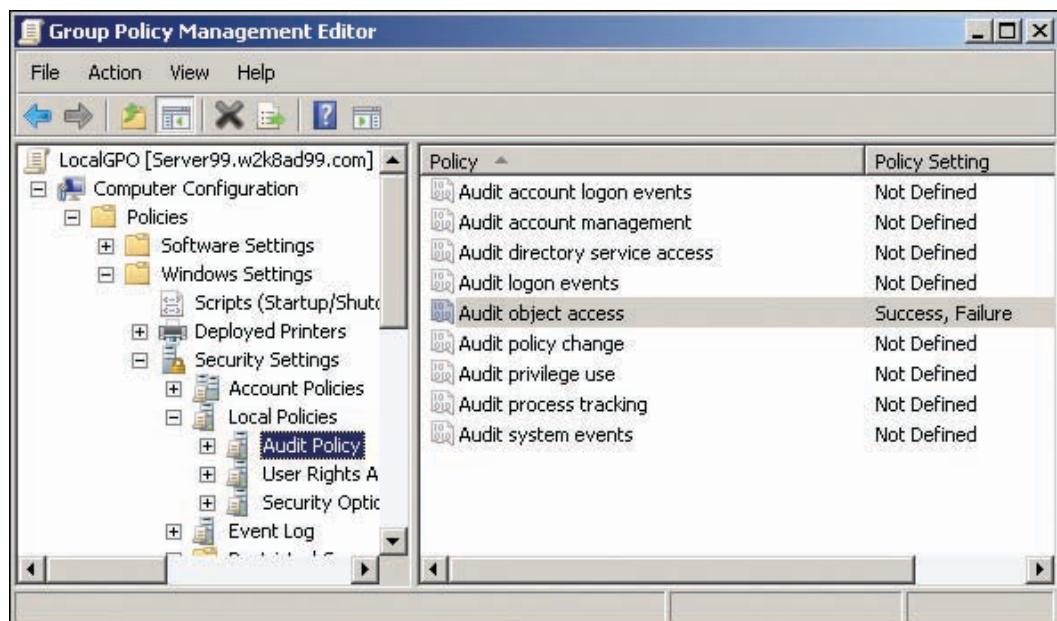


Figure 7-16 Policies in the Audit Policy subnode

- **User Rights Assignment**—User rights define the actions that users can take on a computer, such as shutting down the system, logging on locally, and changing the system time. More than 40 user rights policies can be assigned (see Figure 7-17). For each policy, you can add users or groups. The Default Domain Controllers Policy defines a number of User Rights Assignment policies.

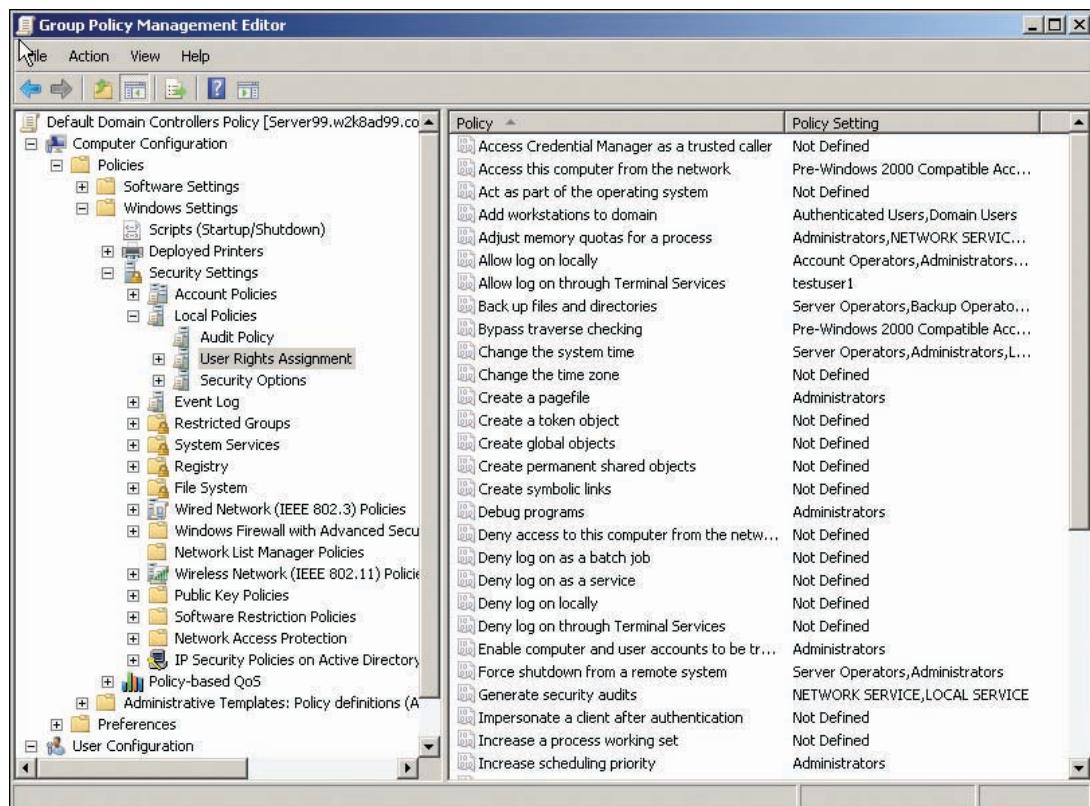


Figure 7-17 Policies in the User Rights Assignment subnode

- **Security Options**—Almost 80 settings can be found in this subnode. Available policies are organized into 16 categories, such as Interactive logon, Network access, and User Account Control. Only a handful of the policies are defined in Default Domain Policy and Default Domain Controllers Policy. The majority of these policies are configured with a simple Enable or Disable setting. An example is Interactive logon: Do not display last user name. If this policy is enabled, the account name of the last user to log on isn't displayed in the logon window.

Auditing Object Access Auditing, particularly auditing access to file system objects, requires additional explanation. There are two steps for auditing objects:

- Enable the Audit object access policy for success, failure, or both.
- Enable auditing on target objects for success, failure, or both.

Auditing object access involves considerable overhead because objects must be monitored and events must be written to the Security log when access occurs. A single object access, such as opening a file, can create several log entries. For this reason, auditing objects should typically be done for brief periods or when an object is accessed infrequently. In highly secure environments, auditing access to sensitive data on an ongoing basis can be useful. Because auditing writes events to the Security log, it makes little sense to enable auditing unless the logs are checked regularly.

As mentioned, Windows Server 2008 logs successful logon events and certain other events by default, even though auditing isn't enabled by default. If you check the Security log, you'll see quite a few events logged there, most pertaining to computer accounts logging on and off. Windows Server 2008 adds subcategories in each category of audit events shown in Figure 7-16 for more control over the types of events that are audited. Unfortunately, the subcategories can't be managed with GPME; you must use the Auditpol.exe command-line tool. By default, some subcategories are enabled, such as logon and logoff events, and these subcategories take precedence over policies set in GPOs.

To clear all audit policy subcategories so that auditing is controlled only by Group Policy, type auditpol /clear at a command prompt. This command stops all auditing on the computer where you run it, unless auditing is enabled in the local policy or a GPO in the computer's scope. For more information on Auditpol.exe, see <http://support.microsoft.com/kb/921469/>.



Activity 7-11: Deploying a Shutdown Script to a Computer

Time Required: 15 minutes

Objective: Create and deploy a shutdown script.

Description: You have several applications that create temporary files with a .temp extension that are slowly eating away disk space on domain member computers. You write a shutdown script that deletes all files with a .temp extension, and you want to deploy this script to all computers in the domain by using group policies. First, you test the script and its deployment on your test OU.

1. Log on to your server as Administrator, if necessary.
2. Start Notepad, and in a new text document, type **del /F /S c:*.*.temp**. The /F option forces deletion of read-only files, and the /S option deletes the file in the current directory and all subdirectories. (Note: Most temporary files created by Windows use the .tmp extension. However, Starter GPO files have a .tmplx extension, and the del *.tmp command would delete these files, too.)
3. Click **File**, **Save As** from the menu. Choose the desktop as the location for saving your file. In the Save as type list box, click **All Files (*.*)**. Type **deltemp.bat** in the File name text box, and click **Save**. Exit Notepad.
4. Right-click **deltemp.bat** on your desktop and click **Copy**.
5. Open GPMC. Click the **Group Policy Objects** folder and create a GPO named **ScriptsGPO**.
6. Right-click **ScriptsGPO** and click **Edit**. In GPME, click to expand **Computer Configuration**, **Policies**, and **Windows Settings**, and then click **Scripts**. Double-click **Shutdown** in the right pane. In the Shutdown Properties dialog box, click **Show Files**. In the resulting Explorer window, right-click the right pane and click **Paste**. Note the path where the script is stored—a folder in the Sysvol share on your DC. Close the Explorer window.
7. In the Shutdown Properties dialog box, click **Add**. In the Add a Script dialog box, click **Browse**. Click **deltemp.bat**, and then click **Open**. Click **OK** twice.
8. Close GPME. Link **ScriptsGPO** to the **TestGP1** OU.
9. Log on to your Vista computer as **testuser1**. Create a text file on your desktop named **Test.temp**. (Note: You might have to disable the option in Windows Explorer for hiding extensions for known file types; otherwise, your file might be named Test.temp.txt. To do so, in Windows Explorer, click Organize on the toolbar, and click Folder and Search Options. Click the View tab, and click to clear the Hide extensions for known file types check box.)
10. Open a command prompt window, type **gpupdate**, and press **Enter**. After Gpupdate.exe is finished, restart your computer. (If you don't run Gpupdate, you have to restart the computer to load the policy, and then shut it down again to make the shutdown script run.)
11. Log on as **testuser1** again, and verify that Test.temp has been deleted.
12. On your server, unlink **ScriptsGPO** from **TestGP1**.



Activity 7-12: Working with Password Policies

Time Required: 15 minutes

Objective: Change and test password policies.

Description: You want to change some account policies, particularly password policies, from their default settings. You know you should create a new GPO, edit the account policies as needed, and link the GPO to the domain so that it has higher precedence than the Default

Domain Policy. This way, you can revert to the default account policies easily by unlinking the new GPO.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, and click the **Group Policy Objects** folder. Create a GPO in this folder named **AccountGPO**.
3. Right-click **AccountGPO** and click **Edit**. In GPME, click to expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Account Policies**, and then click **Password Policy**. In the right pane, double-click **Enforce password history**. Click the **Define this policy setting** check box, leave the Passwords remembered value at 0, and then click **OK**.



To see a detailed description of any policy, double-click the policy, and click the Explain tab in its Properties dialog box.

4. In the right pane of GPME, double-click **Minimum password age**. Click the **Define this policy setting** check box, set the value to **0** days so that passwords can be changed immediately, and then click **OK**. Windows provides a suggested value for Maximum password age because this policy must be defined if Minimum password age is defined. Click **OK** to accept the suggested value.
5. Before you test this policy, see how things work with the current policy in place. The default value for the policy you changed is 24, which means you shouldn't be able to change your password to the same value. Press **Ctrl+Alt+Del**, and then click **Change a password**. In the Old password text box, type your current password. In the New password and Confirm password text boxes, type your current password. Click the arrow next to the Confirm password text box. You get a message stating that Windows is unable to update the password. Click **OK**, and then click **Cancel** twice.
6. In GPMC, link **AccountGPO** to the domain. AccountGPO is added with link order 2, but you want its settings to take precedence, so change the link order to **1**.
7. Open a command prompt window, type **gpupdate**, and press **Enter**. When Gpupdate.exe is finished, try to change your password again, still using the same password for both the old and new passwords. You should be successful.
8. Leave GPME open if you're going on to the next activity.



Activity 7-13: Working with Account Lockout Policy

Time Required: 15 minutes

Objective: Change and test account policies.

Description: As a continuation from the previous activity, you change settings in Account Lockout Policy and test your changes.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, if necessary. Right-click **AccountGPO** and click **Edit**. In GPME, click to expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Account Policies**, and then click **Account Lockout Policy**. Double-click **Account lockout threshold**. Click the **Define this policy setting** check box, change the invalid logon attempts value to **2**, and then click **OK**.
3. The Suggested Value Changes dialog box suggests values for the Account lockout duration and Reset account lockout counter after settings. Click **OK** to accept these settings.
4. Open a command prompt window, type **gpupdate**, and press **Enter**. (Password policies that affect domain users are stored on domain controllers, not member computers, so the policy must be updated on the domain controller.)

5. On your Vista computer, attempt to log on twice as **testuser1** with an incorrect password. Attempt to log on a third time with the correct password. You should get a message stating that the account is currently locked out.
6. On your server, open Active Directory Users and Computers. Open the Properties dialog box for **Test User1**, located in TestOU, and click the **Account** tab. Under the Logon Hours button is a message stating that the account is locked out. Click the **Unlock account** check box. The account unlocks automatically after the number of minutes in the “Account lockout duration” setting expires, if it’s not unlocked manually. Click **OK**.
7. Attempt to log on from your Vista computer again. You should be successful.
8. Before you go on to the next activity, return policies in Account Lockout Policy to their default settings. On your server, open GPMC, if necessary. Expand the domain node, if necessary, so that you can see the two policies linked to it. Right-click **AccountGPO** and click **Delete**. Click **OK** to confirm the deletion. That’s it! No need to remember which policies to undo; by using a second GPO linked to the domain, you can simply link it or unlink it, depending on your policy requirements.



Activity 7-14: Disable Default Auditing

Time Required: 15 minutes

Objective: Disable default event auditing on a domain controller.

Description: Your event logs have become much too large because of Windows Server 2008’s default logging. You want to turn off default logging by using the Auditpol command.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Local Security Policy**.
3. Click to expand **Local Policies**, and then click **Audit Policy**. Verify that all audit policies are set to No auditing, the default setting in Windows Server 2008 and Vista. Not defined is the default setting in the Default Domain Policy and Default Domain Controllers Policy. Close the Local Security Policy MMC.
4. Click **Start**, point to **Administrative Tools**, and click **Event Viewer**. Click to expand **Windows Logs** in the left pane, and then click the **Security** log. Scroll through the events displayed in the right pane. You’ll probably see quite a few events pertaining to logon, logoff, and directory service access.
5. Right-click the **Security** log in the left pane and click **Clear Log**. Click **Clear**. One new event is created, which indicates the event log was cleared. This event is always logged.
6. On your Vista computer, log off, if necessary, and then log on as **testuser1**.
7. On your server, right-click the **Security** log and click **Refresh**. You should see several events created by the logon from the Vista computer.
8. Open a command prompt window, type **auditpol /get /category:*** | **more**, and press **Enter**. Press the **spacebar** to page through the resulting display. This command displays all the sub-categories of audit policies and their current settings.
9. Type **auditpol /clear** and press **Enter**. When prompted, type **y** and press **Enter**. Type **auditpol /get /category:*** | **more** and press **Enter**. Press the **spacebar** to page through the resulting display. Notice that all audit policies have been set to No auditing. This setting comes from the local policy because no audit policies are set in Active Directory.
10. In Event Viewer, clear the **Security** log again. On your Vista computer, log off and log on again as **testuser1**. Refresh the **Security** log again to verify that no new events were created (aside from the event of clearing the log).
11. Close all open windows, and log off Vista.



Activity 7-15: Working with Audit Policies

Time Required: 15 minutes

Objective: Enable and test auditing of object access.

Description: You have a share containing very sensitive files. Access to these files is not frequent, and only a few users access them. Because of the files' sensitive nature, you want to know who is accessing them (include those who shouldn't be attempting access) and when. You enable auditing object access and auditing the sensitive files.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, and click the **Group Policy Objects** folder. Create a GPO in this folder named **LocalGPO**.
3. Right-click **LocalGPO** and click **Edit**. In GPME, expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **Audit Policy**. In the right pane, double-click **Audit object access**. In the Properties dialog box, click the **Define these policy settings** check box. Click **Success** and **Failure**, and then click **OK**. Close GPME.
4. In GPMC, link **LocalGPO** to the **Domain Controllers** OU. Close GPMC. Open a command prompt window, and type **gpupdate** and press **Enter**. Then type **auditpol /get /category:*** **| more** and press **Enter**. Page through the output, noting that all subcategories under Object Access are set to Success and Failure. Close the command prompt window.
5. Open Windows Explorer, and navigate to **Q:\Shared**. (This folder should be shared from activities completed in Chapter 6.) Delete all files and folders in the Shared folder.
6. Create a file in the Shared folder called **Confidential.txt**. Right-click **Confidential.txt** and click **Properties**. Click the **Security** tab, and then click the **Advanced** button.
7. In the Advanced Security Settings for Confidential.txt dialog box, click the **Auditing** tab, and then click the **Edit** button. Click **Add**. Type **Domain Users**, click **Check Names**, and then click **OK**.
8. In the Auditing Entry for Confidential.txt dialog box, click the **Successful** and **Failed** check boxes for the Full control permission. Click **OK** until you get back to the Windows Explorer window.
9. Open **Confidential.txt** in Notepad, and then close it and exit Notepad. Open Event Viewer. Right-click the **Security** log and click **Refresh**. You'll probably find a number of events listed. Unfortunately, when object access auditing is enabled, many events are audited, as indicated by the list of subcategories you saw under Object Access in Step 4. You can use the Auditpol command to turn auditing off for specific subcategories.
10. Open GPMC. Right-click **LocalGPO** and click **Edit**. In GPME, navigate to the **Audit Policy** node. In the right pane, double-click **Audit object access**. In the Properties dialog box, click to clear the **Define these policy settings** check box, and then click **OK**. Close GPME.
11. In GPMC, unlink **LocalGPO** from the **Domain Controllers** OU. Close all open windows, and stay logged on for the next activity.



Activity 7-16: Reviewing Additional Local Policies

Time Required: 20 minutes

Objective: Review several User Rights Assignment and Security Options settings.

Description: You have some experience using group policies to set User Rights Assignment and Security Options policies, but you haven't taken the time to see everything that's available in these nodes. You open GPME and explore these two nodes.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, and then navigate to and right-click **LocalGPO** and click **Edit** to open it in GPME.

3. Click to expand **Computer Configuration, Policies, Windows Settings, Security Settings, and Local Policies**, and then click **User Rights Assignment**. Browse the list of policies and double-click any that look interesting or that aren't self-explanatory. Click the **Explain** tab and read the detailed description. Suggested policies to view in detail include Add workstations to domain, Back up files and directories, Bypass traverse checking, Deny log on locally, Load and unload device drivers, and Take ownership of files or other objects.
4. Browse the **Security Options** node in a similar manner. Suggested policies to view in detail include Accounts: Administrator account status, Accounts: Rename administrator account, Accounts: Limit local account use of blank passwords to console logon only, Audit: Force audit policy subcategory settings, Devices: Prevent users from installing printer drivers, Interactive logon: Do not display last user name, Interactive logon: Message text for users attempting to log on, Interactive logon: Prompt user to change password before expiration, Network access: Shares that can be accessed anonymously, Network security: Force logoff when logon hours expire, Shutdown: Clear virtual memory pagefile, User Account Control: Behavior of the elevation prompt for standard users, and User Account Control: Run all administrators in Admin Approval Mode.
5. Close all open windows, and stay logged on for the next activity.



Fine-Grained Password Policies Account policies set with Group Policy apply to all users in the domain, and GPOs containing account policy settings are useful only when linked to the domain. This lack of flexibility in account policies, particularly password policies, has always been considered a weakness of Group Policy. Windows Server 2008 provides a solution called **fine-grained password policies**, although this method takes more effort than simply using the Group Policy Management Editor. Fine-grained password policies can be defined only on Windows Server 2008 domain controllers, and the domain functional level must be Windows Server 2008. These policies can define all the settings in the Password Policy and Account Lockout Policy nodes but do not include settings for the Kerberos Policy node.

Fine-grained password policies are created by defining a Password Settings Object (PSO) in the Password Settings Container (PSC). In Active Directory Users and Computers, the PSC is in the System folder and contains no PSOs by default. After the PSO is defined with the appropriate settings, it can be linked to one or more users or global groups in the same domain as the PSO. (PSOs can't be linked to OUs.) Two tools are available to create a PSO: ADSI Edit and LDIFDE. This section discusses using ADSI Edit. The general steps for creating a fine-grained password policy with ADSI Edit are as follows:

1. Open ADSI Edit.
2. Create a new object of type msDS-PasswordSettings in the PSC.
3. Fill in all the required values for your new PSO.
4. Link the PSO to users and/or global groups.

Before Windows Server 2008 and the capability to create fine-grained password policies, the only way an organization could impose more stringent (or less stringent) password policies on certain users in a domain was to create another domain and move the users there. With fine-grained password policies, an administrator can create baseline password and account lockout policies for the domain, and then create one or more PSOs for groups of users who should have different policies. For example, you might have three categories of users in an organization: the typical user who requires a moderately strong password policy, the part-time user who has little access to the network and needs a less stringent policy, and the secure user who has access to sensitive data and needs a very strong policy. The typical user's policy can come from group policies, and the other two user categories can have PSOs defined and linked to global groups containing these users as members.



Activity 7-17: Creating a Fine-Grained Password Policy

Time Required: 20 minutes

Objective: Create a fine-grained password policy linked to a group.

Description: You have a group of users in the Sales Department who would benefit from a less stringent password policy than what's defined for the domain. You have discovered that Windows Server 2008 has fine-grained password policies that can be applied to a user or group. You create a policy and link it to the group.

1. Log on to your server as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **ADSI Edit**.
3. In the left pane, right-click **ADSI Edit** and click **Connect to**. In the Connection Settings dialog box, type **w2k8adXX.com** in the Name text box, and then click **OK**. This step is necessary because you're using ADSI Edit for the first time; it won't be necessary the next time you use ADSI Edit.
4. Double-click the domain node. Double-click **DC=w2k8adXX, DC=com** and then **CN=System**. Right-click **CN=Password Settings Container**, point to **New**, and click **Object**. Click **msDS-PasswordSettings** in the Select a class list box, if necessary. This object class creates a PSO. Click **Next**.
5. In the Value text box for the **cn** attribute, type **Sales-PSO**, the name of the PSO, and then click **Next**.
6. In the Value text box for the **msDS-PasswordSettingsPrecedence** attribute, type **5**. This attribute is used for PSO precedence; if more than one PSO is linked to the same user, the lowest value takes precedence. Click **Next**.
7. Continue entering values for attributes as shown in the following list, clicking **Next** after each one:
 - **msDS-PasswordReversibleEncryptionEnabled**: **FALSE**
 - **msDS-PasswordHistoryLength**: **0**
 - **msDS-PasswordComplexityEnabled**: **FALSE**
 - **msDS-MinimumPasswordLength**: **4**
 - **msDS-MinimumPasswordAge**: **(None)**
 - **msDS-MaximumPasswordAge**: **(Never)**
 - **msDS-LockoutThreshold**: **0**
 - **msDS-LockoutObservationWindow**: **(None)**
 - **msDS-LockoutDuration**: **(None)**
8. Click **Finish**. Close ADSI Edit and open Active Directory Users and Computers.
9. Navigate to **System, Password Settings Container**. Right-click **Sales-PSO** and click **Properties**. Click the **Attribute Editor** tab.
10. Double-click the **msDS-PSOAppliesTo** attribute. Click **Add Windows Account**. Type **Sales-G**, click **Check Names**, and then click **OK** three times.
11. In Active Directory Users and Computers, navigate to and expand the **Marketing** OU and then click the **Advertising** OU. Right-click **Advertising User3** and click **Reset Password**. Type **pass1** in the New password and Confirm password text boxes, and then click **OK**. Windows doesn't allow that password because it doesn't meet length or complexity requirements. Advertising User3 is subject to the password policy defined in the Default Domain Policy (minimum length of 7 characters and must meet complexity requirements). Click **OK**.
12. Click the **Sales** OU. Right-click **Sales Person3** and click **Reset Password**. Type **pass1** in the New password and Confirm password text boxes, and then click **OK**. The password change is successful because Sales Person3 is now subject to the new PSO you created and linked to the global group Sales-G. Click **OK**.
13. Close all open windows, and stay logged on for the next activity.

Additional Security Settings Subnodes Beyond Account Policies and Local Policies, there are 13 more subnodes under Security Settings:

- *Event Log*—Control parameters of the main logs in Event Viewer on target computers.
- *Restricted Groups*—Control group membership for both domain groups and local SAM groups. After the policy is applied, existing members of the target group are deleted and replaced with the membership specified in the policy.
- *System Services*—Manage the startup mode and security settings of services on the target computers.
- *Registry*—Set NTFS permissions on Registry keys on the target computer.
- *File System*—Set NTFS permissions and control auditing and inheritance on files and folders on the target computers.
- *Wired Network (IEEE 802.3) Policies*—For Vista computers, controls a variety of authentication parameters on computers with wired connections to the network.
- *Windows Firewall with Advanced Security*—Controls firewall settings on Windows Vista and Server 2008 computers.
- *Network List Manager Policies*—Controls aspects of the networks (public, private, domain, and so on) identified by Windows Vista and Windows Server 2008.
- *Wireless Network (IEEE 802.11) Policies*—Controls how wireless clients can connect to wireless networks, including network type (ad hoc or infrastructure), service set identifier (SSID), authentication, and encryption protocols. Policies can be created for Vista and XP computers.
- *Public Key Policies*—Controls parameters associated with Public Key Infrastructure, including EFS and certificate handling.
- *Software Restriction Policies*—Controls which software can run on a computer.
- *Network Access Protection*—Controls the NAP environment for target computers, including enforcement services, user interface, and servers used for health registration certificates.
- *IP Security Policies on Active Directory*—Control IPSec policies on target computers. IPSec is a network protocol that provides secure, encrypted communication between computers.



Computer Configuration: Administrative Templates

The settings in Administrative Templates affect the HKEY_LOCAL_MACHINE section of the computer's Registry. Hundreds of settings are defined in this node, and many more can be added through customization. The Administrative Templates folder uses policy definition files, called **administrative template files**, in the XML format, which makes creating your own policies fairly easy if you need to control a setting not provided by default. These text files, referred to as ADMX files because of their .admx extension, specify Registry entries that should be controlled and the type of data the entries take. Many software vendors provide administrative template files for controlling their applications' settings through group policies. For example, Microsoft offers administrative template files for the Microsoft Office suite.

Windows versions before Vista and Server 2008 used .adm files. This format can still be used on the same system as ADMX files, but you can create and edit ADMX files only on Vista or Server 2008 computers. ADMX files also have an .adml extension, which provides a language-specific user interface in Group Policy Management Editor. On a Server 2008 or Vista computer, you can find all ADMX and ADML files under %systemroot%\PolicyDefinitions and open them in Notepad or another text editor.

The Administrative Templates folder, where many aspects of the computer working environment are controlled, contains the following folders and nodes, most of which have additional subnodes:

- *Control Panel*—This folder has only a few policies in Computer Configuration. Settings in Regional and Language Options allow administrators to set and restrict the language in the Control Panel user interface. The User Accounts policy configures a default user logon picture for all users on the target computers.

- *Network*—A host of network settings can be controlled on the target computers, including but not limited to Background Intelligent Transfer Service (BITS) parameters, DNS client settings, Microsoft Peer-to-Peer Networking Services (discussed in Chapter 8), network connection settings, and offline files configuration.
- *Printers*—Policies in this folder control how computers interact with network printers, including automatic printer publishing in Active Directory, automatic printer pruning, and Internet printing parameters.
- *System*—This folder contains more than 30 subnodes. Some computer functions that can be controlled in this node include disk quotas, group policy, system logon, power management, and user profiles.
- *Windows Components*—This folder contains more than 50 subnodes with policies for configuring the CD/DVD autoplay feature, Internet Explorer, and Windows Update, among others. Some settings in this folder have an identical counterpart in the User Configuration node. When a conflict exists, the setting in Computer Configuration takes precedence.



An additional node under Administrative Templates called All Settings displays all Administrative Template settings and can be sorted in alphabetical order. You can select View, Filter Options from the GPME menu to list policies by certain criteria or keywords, too.

Policies in the User Configuration Node

Policies set under the User Configuration node follow a user wherever he or she logs on. As mentioned, this node has the same top-level folders as Computer Configuration: Software Settings, Windows Settings, and Administrative Templates. Many of the policy categories are the same, but there are important differences in the actual policies. Notably, because most security settings and account policies apply to computers rather than users, the User Configuration node has far fewer security settings. User Configuration policies tend to focus on the user working environment: Windows features the user can and can't access, the desktop look and feel, user profile settings, and so forth. The following sections describing policies available in the User Configuration node use an approach similar to the earlier “Policies in the Computer Configuration Node.”

User Configuration: Software Settings

The Software Installation extension performs the same function as in Computer Configuration—deploying software to remote destinations—but has important differences in options and execution. A software package can only be assigned to a computer, but there are two options for deploying software to users:

- *Published*—A published application isn't installed automatically; instead, a link to install the application is in Control Panel's Programs and Features (Vista and Server 2008) or Add/Remove Programs (Windows XP). Administrators can assign a category to each published application so that if many packages are published, they're listed under the assigned category in Control Panel. Published applications can also be configured to install when the user opens a file type associated with the application.
- *Assigned*—Applications assigned to users are advertised as a link on the Start menu and installed the first time the user opens a file type associated with the application or clicks the link in the Start menu.

An advanced deployment is also possible and has options similar to those in the Computer Configuration node.

User Configuration: Windows Settings

Windows Settings contains seven subnodes, four of which have the same name as in the Computer Configuration node:

- *Remote Installation Services*—Controls the options that are available to users during remote OS installation using RIS.
- *Scripts (Logon/Logoff)*—Identical to the Scripts (Startup/Shutdown) policy, except scripts specified here can be run only by users in the GPO's scope. If both a startup and logon script are to run, the startup script runs first. If both a shutdown and logoff script are to run, the logoff script runs first.
- *Security Settings*—This subnode contains two folders: Public Key Policies, which defines parameters for using certificate services, and Software Restriction Policies, which controls the applications a user can run.
- *Folder Redirection*—Controls which folders in a user's profile are redirected to a location outside the user's profile folder. Redirecting users' profile folders to a network share is recommended when roaming profiles are used to reduce logon and logoff delays and reduce the bandwidth needed to upload and download profile data.
- *Policy-based QoS*—The same function as in the Computer Configuration node but applied to users.
- *Deployed Printers*—The same function as in the Computer Configuration node but applied to users.
- *Internet Explorer Maintenance*—Enables administrators to customize aspects of IE, including a browser title, a logo, and toolbars. Home pages and Favorites URLs can also be specified, and administrators can configure connection, security, and program settings.

7

Next, you examine a few of these nodes in more detail: Software Restrictions (under the Security Settings subnode), Folder Redirection, and Internet Explorer Maintenance.

Security Settings Subnode: Software Restriction Policies Software restriction policies are designed to prevent users from running certain applications or to allow users to run only certain applications. Aside from preventing users from using programs at work that don't contribute to their productivity, software restriction policies can add a layer of security to your network by preventing malware from running.

Software Restriction Policies is found in both the Computer Configuration and User Configuration nodes. By default, it's empty, but you can create a policy by right-clicking the folder and clicking New Software Restriction Policies. When a new policy is created, Software Restrictions Policies contains two folders and three policies (see Figure 7-18).

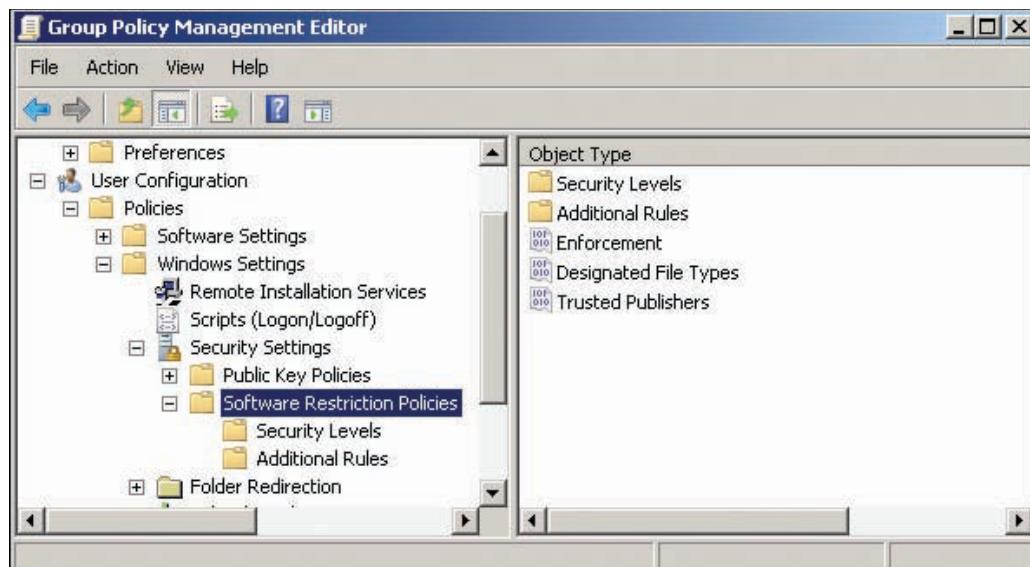


Figure 7-18 The Software Restriction Policies folder

The Security Levels folder contains three rules explained in the following list, one of which you select as the default rule for the policy. You can then create exceptions to the default rule.

- **Disallowed**—No software can run, regardless of the user’s security access.
- **Basic User**—All software can run with access rights of a normal user, regardless of the user’s actual rights on the system. This rule prevents users with administrative access from running programs that could cause harm with that level of access.
- **Unrestricted**—This is the default setting on a new policy. All programs can run according to the user’s actual access rights. This setting, with no additional rules defined, is the same as having no software restriction policy assigned.

The Additional Rules folder is where you create exceptions to the default rule by identifying applications or application locations that are allowed or disallowed. There are four ways to identify applications designated as exceptions to the default rule:

- **Hash**—A digital fingerprint of the application file is created, based on the file’s attributes, to uniquely identify it.
- **Certificate**—Some software publishers provide a digital certificate to uniquely identify an application.
- **Path**—The path on the local system or a UNC path to the application file.
- **Network zone**—An Internet zone that defines the Web sites from which applications can run.

For each additional rule you create, you can specify whether applications meeting the rule criteria should be disallowed, run as a basic user, or unrestricted. When you create a new software restriction policy, two path rules are created automatically to define unrestricted locations programs can run from: one specifying the default Program Files directory and one specifying the Windows directory. Three policies can be configured in the Software Restriction Policies folder:

- **Enforcement**—Specifies how restrictions should be enforced. You can exempt members of the Administrators group, and you can exempt library files, such as DLLs.
- **Designated File Types**—Specifies which file types are to be considered executable files. You can add your own file types or remove certain types from the list.
- **Trusted Publishers**—Specifies trusted publisher policy options, such as who can manage the list of trusted publishers (users or administrators) and certificate verification parameters.



Activity 7-18: Creating a Software Restriction Policy

Time Required: 20 minutes

Objective: Create a software restriction policy and test it.

Description: You want to begin locking down some computers in your company by restricting which programs users can run. You want to use settings in the Software Restriction Policies folder, so you decide to create a simple policy to test this feature.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC. Click to expand the **Group Policy Objects** folder, and then right-click **TestOUGPO** and click **Edit**. In GPME, expand **User Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Software Restriction Policies**. Right-click **Software Restriction Policies** and click **New Software Restriction Policies**.
3. Click the **Security Levels** folder to see the three default rules in the right pane. The Unrestricted rule has a small check mark indicating that it’s currently selected as the default. Double-click **Disallowed** to open this rule’s Properties dialog box, and click **Set as Default**. Click **Yes**, and then click **OK**.
4. Click the **Additional Rules** folder. As mentioned, two path rules were created automatically that refer to a Registry key specifying the Windows directory and the Program Files directory.

They can be deleted or you can leave them as is (recommended). Double-click the path rule listed first to open the dialog box shown in Figure 7-19. Both rules are set to Unrestricted. Click **Cancel**.

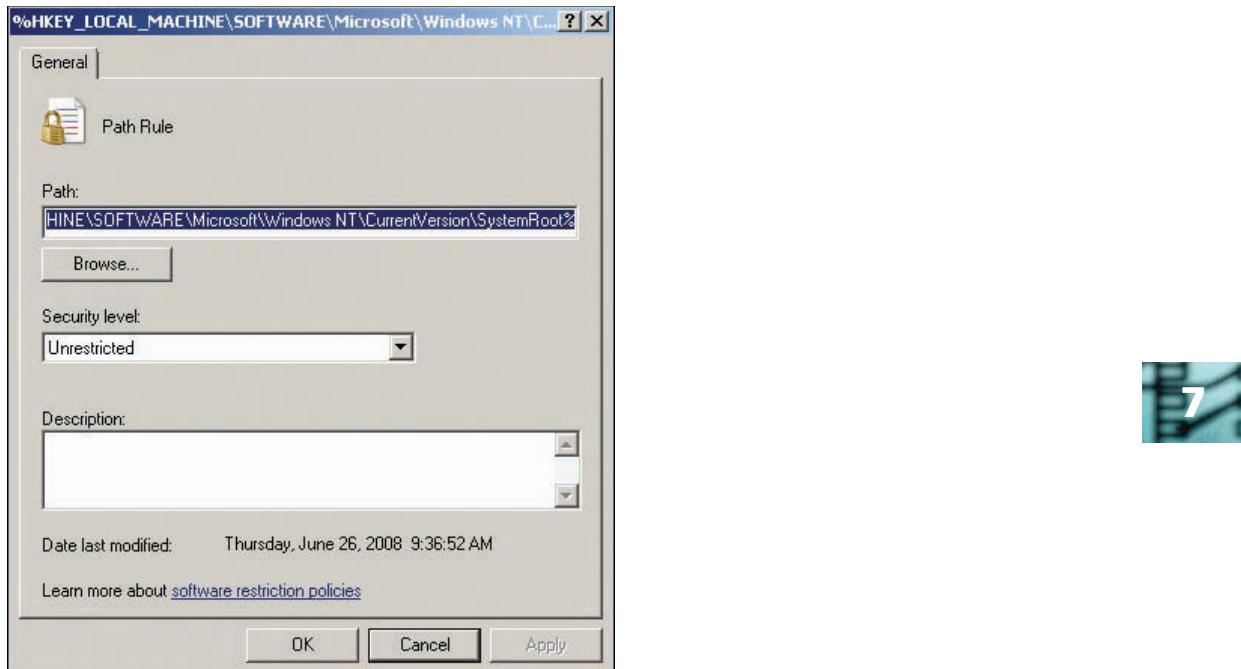


Figure 7-19 Viewing a path rule

5. Click **Software Restriction Policies**. Double-click **Enforcement** in the right pane. In the Properties dialog box, click **All users except local administrators**, and then click **OK**.
6. Double-click **Designated File Types** in the right pane. In the Properties dialog box, scroll through the list of file types that are considered executable files, and then click **Cancel**. Close GPME.
7. In GPMC, link **TestOUGPO** to **TestOU**.
8. Log on to the domain from your Vista computer as Administrator. Open a command prompt window, type **gpupdate**, and press **Enter**. Close the command prompt window.
9. Open the C drive in Windows Explorer, and create a file named **test.bat** in the root of the C drive. Open test.bat in Notepad, and type the command **dir /s**. Save the file and exit Notepad. This simple batch file will run the Dir command and list files in subdirectories.
10. To be sure your batch file works, open a command prompt window, type **C:\test.bat**, and press **Enter**. You exempted local administrators from the policy, so the Administrator account can still run this program.
11. Log off your Vista computer (if necessary), and then log on again as **testuser1**.
12. Start Notepad to verify that you can run programs located in the C:\Windows directory. Exit Notepad.
13. Open a command prompt window, type **c:\test.bat**, and press **Enter**. You should get a message stating that the program is blocked by group policy.
14. Log off your Vista computer. On your server, unlink **TestOUGPO** from **TestOU**. Right-click **TestOUGPO** and click **Edit** to open GPME. Navigate to the **Software Restriction Policies** node, and then right-click it and click **Delete Software Restriction Policies**. Click **Yes**. Close all open windows.

The Folder Redirection Subnode **Folder redirection** allows an administrator to set policies that redirect one or more folders in a user's profile directory. Folder redirection is useful

when you want users to store their documents on a server for easy backup, but you don't want to change the way users access their document folders. It's also quite useful when roaming profiles are in use because it decreases the network bandwidth needed to upload and download a user's roaming profile. To redirect a folder, right-click it in the Folder Redirection node and click Properties to open the dialog box shown in Figure 7-20.

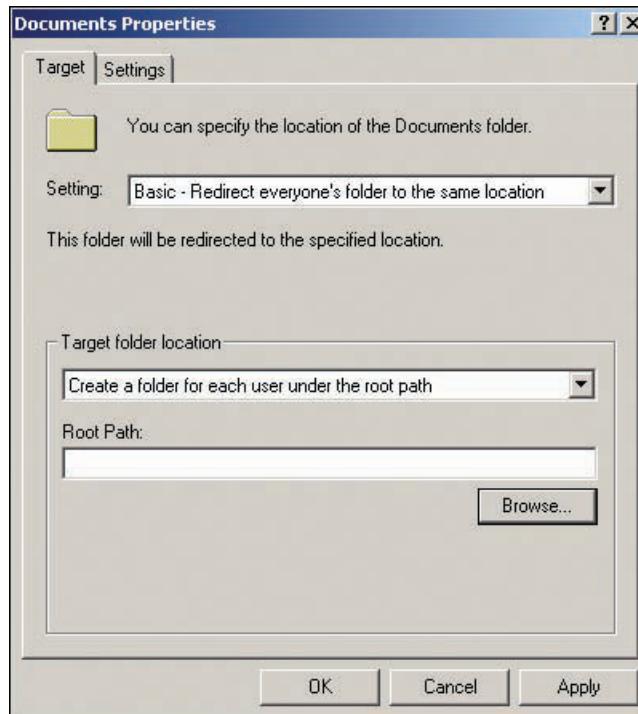


Figure 7-20 Configuring folder redirection

In the Target tab of a folder's Properties dialog box, you can select Basic redirection, which redirects the selected folder for all users in the GPO's scope to one location, or Advanced redirection, which enables you to specify different locations for different groups of users. In the Settings tab, you can specify options for redirection, including whether the folder should remain redirected or revert to its original location if the policy is removed.



Activity 7-19: Creating a Folder Redirection Policy

Time Required: 15 minutes

Objective: Redirect the Documents folder.

Description: You're considering using roaming profiles and know that the bandwidth this feature consumes can be excessive. You decide to test folder redirection so that you can decrease the bandwidth required when you use roaming profiles.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC, and click the **Group Policy Objects** folder. Right-click **TestOUGPO** and click **Edit**. Expand **User Configuration**, **Policies**, **Windows Settings**, and **Folder Redirection**. Right-click the **Documents** folder and click **Properties**.
3. In the **Documents Properties** dialog box, click the **Target** tab, if necessary, and then click **Basic** in the Setting drop-down list. Click the **Target folder location** list arrow to view the available options, and then, if necessary, click **Create a folder for each user under the root path** in the list. In the **Root Path** text box, type **\serverXX\Shared**.

4. Click the **Settings** tab, and review the available options. Click to clear the **Grant the user exclusive rights to Documents** check box. Click **Redirect the folder back to the local user-profile location when policy is removed**, click **OK**, and then click **Yes**.
5. In GPMC, link **TestOUGPO** to **TestOU**.
6. Folder redirection, although applied to users, sometimes requires a computer restart when it's first applied. Restart your Vista computer and log on to the domain from your Vista computer as **testuser1**.
7. Click **Start, Documents**. Create a text file in Documents named **TestRedirect**.
8. Click **Start**, type **\serverXX\Shared** in the Search text box, and press **Enter**. You should see a folder named **testuser1** in the share. Double-click the **testuser1** folder and double-click the **Documents** folder. The **TestRedirect** file you created in your **Documents** folder should be there. Log off your Vista computer. (If the **Documents** folder is not being redirected, try logging off and logging back on again. Sometimes you need to log on twice before the policy takes effect. If this method doesn't work, run **Gpupdate.exe**.)
9. On your server, open GPMC, if necessary. Right-click **TestOUGPO** and click **Edit**. Under the **Folder Redirection** node in GPME, right-click **Documents** and click **Properties**. Click the **Target** tab, if necessary, and disable folder redirection by clicking **Not configured** in the Setting list box. Click **OK**, and then close any open windows.



The Internet Explorer Maintenance Subnode Some companies want to customize their users' Internet Explorer browser with the company name or logo, or they might want to force a user's home page to be the corporate Web site. These settings and a host of others can be configured with the Internet Explorer Maintenance policies.



Activity 7-20: Creating an Internet Explorer Policy

Time Required: 10 minutes

Objective: Set a browser title and home page for IE browsers.

Description: You want all your users to have certain IE browser settings, such as the home page and a title bar reflecting the company name, so you configure the Internet Explorer Maintenance policies.



This activity requires access to the Internet to test the policy.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC. Click the **Group Policy Objects** folder, and create a GPO in this folder named **IEGPO**.
3. Right-click **IEGPO** and click **Edit**. In GPME, expand **User Configuration, Policies, Windows Settings**, and **Internet Explorer Maintenance**. Click to select the **Internet Explorer Maintenance** node in the left pane.
4. In the right pane, double-click **Browser User Interface**. In the right pane, double-click **Browser Title**. In the **Browser Title** dialog box, click the **Customize Title Bars** check box. In the **Title Bar Text** text box, type **CoolGadgets.com**, and then click **OK**.
5. Click **URLs** in the left pane of GPME, and then double-click **Important URLs** in the right pane. In the **Important URLs** dialog box, click the **Customize Home page URL** check box, type **http://coolgadgets.tomsho.com** in the **Home page URL** text box, and then click **OK**. Close GPME.
6. In GPMC, link **IEGPO** to your domain.
7. Log on to the domain from your Vista computer as **testuser1**.

8. Open Internet Explorer. You should see “Windows Internet Explorer provided by CoolGadgets.com” in the title bar, and the home page should be a page maintained by the author.
9. Close any open windows, and log off Vista.

User Configuration: Administrative Templates

The settings in Administrative Templates under User Configuration affect the HKEY_CURRENT_USER section of the computer’s Registry. Most of the information discussed previously about Administrative Templates in the Computer Configuration node applies to the User Configuration node. Administrative Templates in User Configuration also contain the Control Panel, Network, System, and Windows Components subnodes as well as the following subnodes:

- *Desktop*—Controls the look of users’ desktops, determines which icons are available, and can limit actions users can take on the desktop.
- *Shared Folders*—Controls whether a user can publish shared folders and DFS root folders.
- *Start Menu and Taskbar*—Controls the look and operation of the Start menu and taskbar.

Hundreds of settings are available in Administrative Templates—far too many to explain in detail in this book. The best way to become acquainted with the myriad settings that can be controlled through Group Policy is to click the Explain tab of policies you want to investigate further.

Using Security Templates

Security templates are text files with an .inf extension that contain information to define policy settings in the Computer Configuration\Policies\Windows Settings\Security Settings node of a local or domain GPO. You can use them to easily create and deploy security settings to a local or domain GPO. Simply right-click the Security Settings node and click Import policy, and then select a security template file to apply. Security templates can also be used to verify the current security settings on a computer against the settings in a template. There are three tools for working with security templates, discussed in the following sections: Security Templates snap-in, Security Configuration and Analysis snap-in, and Secedit.exe.

Security Templates Snap-in

You use the Security Templates snap-in to create and edit security templates. You can create templates for computers with differing security requirements, such as servers with different roles installed or different physical locations. Servers in branch offices that don’t have tight physical security, for example, might require stronger security settings than servers in a secure location. Computers used by employees who have access to sensitive information often require tighter security than computers used by employees with limited access on the network.



Before Windows Server 2008, preconfigured security templates were designed for servers, domain controllers, and workstations with varying needs for security. They are no longer available. However, when Windows Server 2008 is configured as a domain controller, the initial security settings are in %systemroot%\Security\Templates\DC Security.inf.

Figure 7-21 shows the Security Templates snap-in with a new security template named LowSecurityWS. Notice that only a subset of the policies in a GPO are available in the template. When a user creates a new template, it’s stored in the user’s Documents folder in Security\Templates. After the template is created, it can be imported into a local or domain GPO or be used by the Security Configuration and Analysis snap-in. If you configure account policies in your template to import into a GPO, remember that settings in the Account Policy node are used only when linked to a domain or applied to a local GPO.

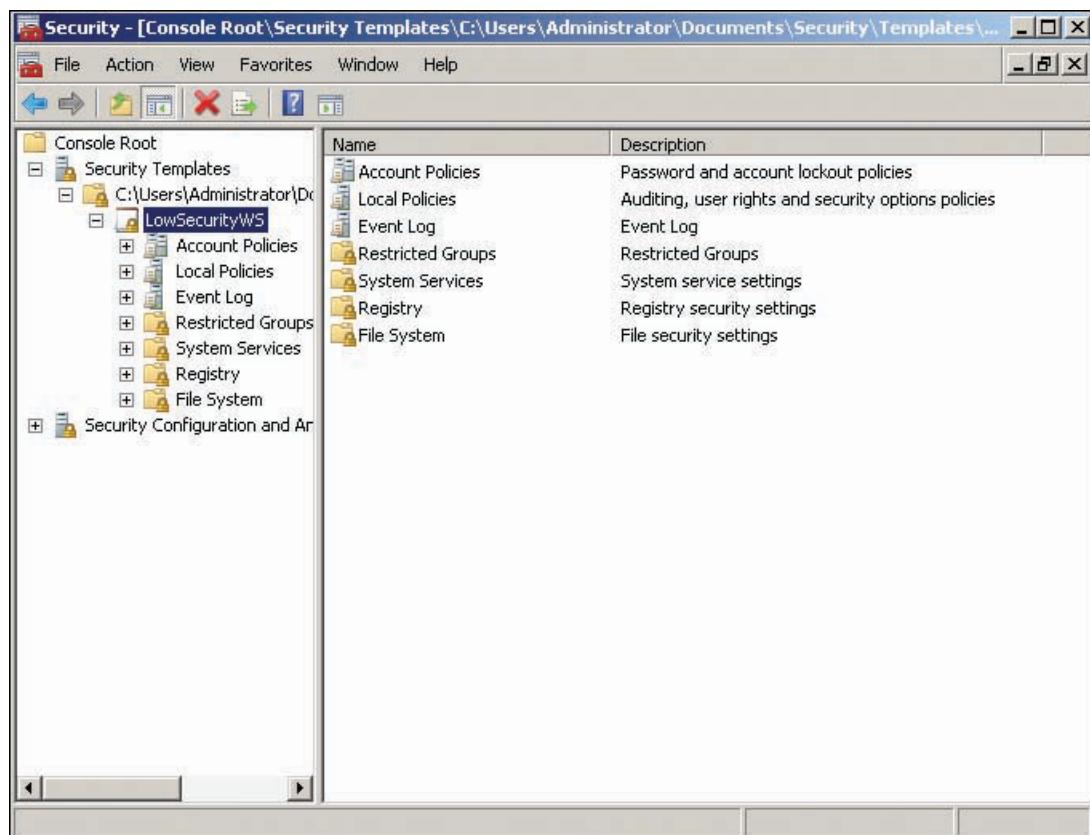


Figure 7-21 The Security Templates snap-in

Security Configuration and Analysis Snap-in

The Security Configuration and Analysis snap-in is useful for checking a computer's existing security settings against the known settings in security template files that have been imported into a security database. You can also use this snap-in to apply a security template to a computer. Windows doesn't supply a preconfigured MMC, so you have to add this snap-in to an MMC. If you'll be working with security templates quite a bit, you can create a custom MMC containing the Security Templates and Security Configuration and Analysis snap-ins.

When you analyze a template against the current security settings on a computer, a report is generated. For each policy setting, there are five possible results:

- An X in a red circle indicates that the template policy and current computer policy don't match.
- A check mark in a green circle indicates that the template policy and computer policy are the same.
- A question mark in a white circle indicates that the policy wasn't defined in the template or the user running the analysis didn't have permission to access the policy.
- An exclamation point in a white circle indicates that the policy doesn't exist on the computer.
- No indicator indicates that the policy wasn't defined in the template.



Activity 7-21: Creating a Security Template

Time Required: 10 minutes

Objective: Create a security template.

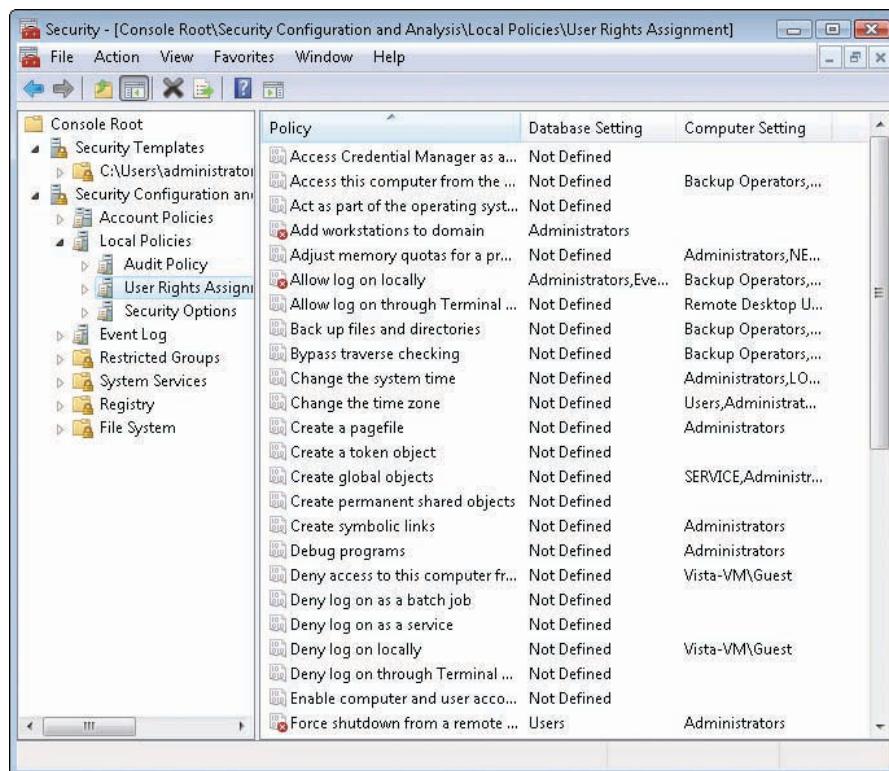
Description: You want to create a set of security baselines for your servers and computers. You start by exporting your Vista computer's current security settings to a new security

template and editing some settings appropriate for computers that don't require a high level of security. Then you analyze the template settings against your Vista computer's current security settings.



You create the security template on the Vista computer in this activity, but you could create all your templates on a server share, and then access them as needed from your workstations to perform a security configuration analysis.

1. Log on to the domain from your Vista computer as Administrator.
2. Open the Local Security Policy MMC from Administrative Tools. Right-click **Security Settings** and click **Export policy**. In the File name text box, type **LowSecurityWS**, and then click **Save**. Close the Local Security Policy MMC.
3. Click **Start**, type **mmc** in the Start Search text box, and press **Enter**. Click **File, Add/Remove Snap-in** from the menu. In the Available snap-ins list box, click **Security Templates** and click **Add**. Click **Security Configuration and Analysis** and click **Add**. Click **OK**.
4. Click **File, Save As** from the menu. In the Save in list box, click **Desktop**. Type **Security** in the File name text box, and then click **Save**.
5. Click to expand **Security Templates**. Click to expand the folder under Security Templates, and then click **LowSecurityWS**. (To create a new template from scratch, you right-click the folder and click **New Template**.)
6. Click to expand **LowSecurityWS** and **Local Policies**, and then click **User Rights Assignment**. In the right pane, double-click **Back up files and directories**. In the Properties dialog box, verify that the **Define these policy settings in the template** check box is selected. Click **Add User or Group**. In the User and group names text box, type **Users**, and then click **OK** twice.
7. Double-click **Change the time zone**. In the Properties dialog box, click **Users**, click the **Remove** button, and then click **OK**.
8. Double-click **Force shutdown from a remote system**. In the Properties dialog box, click **Add User or Group**. In the User and group names text box, type **Users**, and then click **OK** twice.
9. In the left pane, click **Security Options**. In the right pane, double-click **Accounts: Limit local account use of blank passwords to console logon only**. Click **Disabled**, and then click **OK**.
10. Double-click **Interactive logon: Do not require CTRL+ALT+DEL**. Click to select the **Define these policy settings in the template** check box, if necessary. Click **Enabled**, and then click **OK**.
11. Right-click **LowSecurityWS** and click **Save**.
12. Click the **Security Configuration and Analysis** snap-in, then right-click it and click **Open Database**. In the File name text box, type **wslowsec**, and then click **Open**. In the Import Template dialog box, click **LowSecurityWS**, and then click **Open**. Read the message in the right pane.
13. Right-click **Security Configuration and Analysis** and click **Analyze Computer Now**. Click **OK**.
14. Under Security Configuration and Analysis, expand **Local Policies** and then click **User Rights Assignment**. You should see a window similar to Figure 7-22. Each policy has a Database Setting column and a Computer Setting column. (The red and green indicators you see on some policies were explained previously.)
15. Click the **Security Options** node to see the results of the analysis.
16. Close all open windows, but stay logged on to the Vista computer for the next activity. When prompted to save the MMC, click **No**.



The screenshot shows the Windows Security Configuration and Analysis snap-in. The left pane displays a tree view of security policies: Console Root, Security Templates, C:\Users\administrator, Security Configuration and Analysis, Account Policies, Local Policies (selected), Audit Policy, User Rights Assignment (selected), Security Options, Event Log, Restricted Groups, System Services, Registry, and File System. The right pane lists 'Policy' items with their 'Database Setting' and 'Computer Setting'. A large number '7' is visible in the top right corner of the window.

Policy	Database Setting	Computer Setting
Access Credential Manager as a...	Not Defined	
Access this computer from the ...	Not Defined	Backup Operators,...
Act as part of the operating syst...	Not Defined	
Add workstations to domain	Administrators	
Adjust memory quotas for a pr...	Not Defined	Administrators,NE...
Allow log on locally	Administrators,Eve...	Backup Operators,...
Allow log on through Terminal ...	Not Defined	Remote Desktop U...
Back up files and directories	Not Defined	Backup Operators,...
Bypass traverse checking	Not Defined	Backup Operators,...
Change the system time	Not Defined	Administrators,LO...
Change the time zone	Not Defined	Users,Administrat...
Create a pagefile	Not Defined	Administrators
Create a token object	Not Defined	
Create global objects	Not Defined	SERVICE,Administr...
Create permanent shared objects	Not Defined	
Create symbolic links	Not Defined	Administrators
Debug programs	Not Defined	Administrators
Deny access to this computer fr...	Not Defined	Vista-VM\Guest
Deny log on as a batch job	Not Defined	
Deny log on as a service	Not Defined	
Deny log on locally	Not Defined	Vista-VM\Guest
Deny log on through Terminal ...	Not Defined	
Enable computer and user acco...	Not Defined	
Force shutdown from a remote ...	Users	Administrators

Figure 7-22 The Security Configuration and Analysis snap-in

Secedit.exe

Secedit.exe is a command-line program that performs many of the same functions as the Security Configuration and Analysis snap-in. Because it's run from the command line, however, you can use it in scripts and batch files to automate the process of working with security templates. Secedit.exe has options to import or export some of or all the settings between a security database and a template file. It can also compare settings between a security database and a computer's current settings or apply a security database to a computer.



Activity 7-22: Exploring the Secedit.exe Command

Time Required: 10 minutes

Objective: Explore the syntax of the Secedit.exe command.

Description: You want to start working with Secedit.exe so that you can create batch files and scripts to work with security templates more easily. You start by using the command to display the options and syntax.

1. Log on to the domain from your Vista computer as Administrator, if necessary.
2. Open a command prompt window, type **secedit**, and press **Enter** to see a list of options to use with Secedit.exe.
3. Type **secedit /configure | more**. You see a description of the option followed by the correct syntax to use it.
4. Repeat Step 3, substituting **/analyze**, **/import**, **/export**, **/validate**, and **/generaterollback** for **/configure** to see the syntax for these options.
5. Type **cd \users\administrator.w2k8adXX\security\database** and press **Enter** to change to the directory where the Wslowsec database from the previous activity was created. Type **dir** and press **Enter**. You should see the Wslowsec.sdb file.
6. Type **secedit /analyze /db wslowsec.sdb /log seelog.txt** and press **Enter**.

7. Type **Notepad seilog.txt** and press **Enter** to see a text file of the security analysis report. Exit Notepad.
8. Close the command prompt window, and log off Vista.

Group Policy Management and Monitoring

Creating, configuring, and testing group policies are essential parts of managing a Windows network. As you have seen, it's no small job to get your policies working in an optimal fashion and tested properly. Windows includes tools for managing GPOs and monitoring group policies to help make designing and testing easier. The following sections cover these aspects of group policy management and monitoring:

- GPO management with GPMC
- Backing up, restoring, and migrating GPOs
- Group policy results and modeling
- Creating and working with an ADMX central store

GPO Management with GPMC

You have already created and linked GPOs by using GPMC, but several other options are available to fine-tune how you use GPOs. This section discusses GPO delegation, GPO status, and link status.

GPO Delegation The possible permissions for GPO delegation depend on whether you're working with the GPO or the target to which the GPO is linked. Eight possible permissions can be applied to GPOs and the container objects to which they're linked through delegation:

- *Create GPOs*—This permission applies only to the Group Policy Objects folder where you can find all GPOs in the GPMC. When you click the Group Policy Objects folder in GPMC and click the Delegation tab in the right pane, you can view, add, and remove security principals who are allowed to create GPOs in the domain (see Figure 7-23). By default, Domain Admins, Group Policy Creator Owners, and the System special identity have this permission.

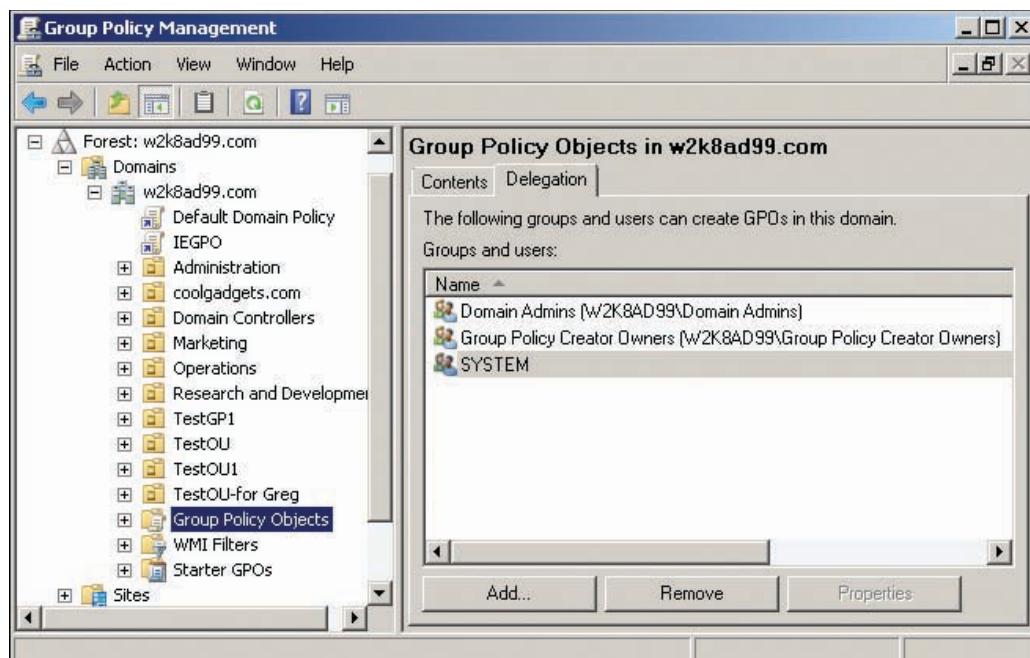


Figure 7-23 Viewing settings in the Delegation tab

- *Link GPOs*—This permission can be set on sites, domains, and OUs and determines who can link or unlink a GPO to or from the container. Administrators, Domain Admins, Enterprise Admins, and the System special identity are granted this permission by default.
- *Perform Group Policy Modeling analyses*—Set on domains and OUs and determines who can run the GPO Modeling Wizard (discussed in “Group Policy Results and Modeling” later in this chapter) on the specified container. The default users are the same as for the Link GPOs permission.
- *Read Group Policy Results data*—Set on domains and OUs and determines who can run the Group Policy Results Wizard (discussed in “Group Policy Results and Modeling” later in this chapter) on users and/or computers. The default users are the same as for the Link GPOs permission.
- *Read*—Set on GPOs, users with this permission can view settings and back up a GPO. By default, the Enterprise Domain Controllers universal group has this permission for all GPOs.
- *Read (from Security Filtering)*—Used in group policy filtering. By default, Authenticated Users has this permission for all GPOs. It includes both the Read and Apply Group Policy permission and is generally set in the Scope tab of a GPO’s Properties dialog box.
- *Edit settings, delete, modify security*—Set on GPOs and determines who can edit, change status on, back up, delete, and change security on a GPO. By default, Domain Admins, Enterprise Admins, and the System special identity are granted this permission.
- *Edit Settings*—Security principals can change existing settings, import settings, and enable or disable a GPO. No users are granted this permission by default.



Managing GPO Status and Link Status After a GPO is created, it can be in one of the following states:

- *Link status: unlinked*—The GPO is in the Group Policy Objects folder but has not been linked to any container objects.
- *Link status: enabled*—The GPO is listed under the container object and the link is enabled. This status is achieved by right-clicking a container, clicking Link an Existing GPO, and choosing a GPO from the Group Policy Objects folder or by right-clicking a container and clicking “Create a GPO in this domain, and Link it here.”
- *Link status: disabled*—The GPO is listed under the container object and the link is disabled. Link status can be toggled between enabled and disabled by right-clicking a GPO linked to a container and clicking Link Enabled.
- *GPO status: Enabled*—The GPO is fully functional. In the Group Policy Objects folder, right-click a GPO, point to GPO Status, and click Enabled.
- *GPO status: User Configuration Settings Disabled*—The User Configuration node is not processed by the group policy client. In the Group Policy Objects folder, right-click a GPO, point to GPO Status, and click User Configuration Settings Disabled.
- *GPO status: Computer Configuration Settings Disabled*—The Computer Configuration node is not processed by the group policy client. In the Group Policy Objects folder, right-click a GPO, point to GPO Status, and click Computer Configuration Settings Disabled.
- *GPO status: All Settings Disabled*—The GPO is disabled. In the Group Policy Objects folder, right-click a GPO, point to GPO Status, and click All Settings Disabled.

GPO Backup and Migration

In a large, complex network, with many different policy needs for users, servers, and workstations, configuring and testing GPOs often take many hours. Thankfully, Windows provides a solution for backing up, restoring, and migrating GPOs in case disaster strikes. GPO backups are also useful if you need to revert to an older version of a GPO, and with GPO migration, you can use your carefully thought-out GPO settings on other systems.

GPO Backup and Restore When you back up a GPO, the policy settings are backed up but so are the security filtering settings, delegation settings, and WMI filter links. What is not backed up are the WMI filter files associated with the WMI links, IPSec policies, and GPO container links. Backing up a GPO is a simple three-step process:

1. In GPMC, right-click the GPO in the Group Policy Objects folder and click Back Up.
2. Select (or create) a folder where the GPO should be stored.
3. Enter a description of the GPO, if needed, and click Back Up.

Multiple GPOs can be stored in the same folder, so you need not create a new folder each time you back up a GPO. The folder where you store GPO backups should be secure and backed up by a regular system backup routine. You can also right-click the Group Policy Objects folder and select options to back up all GPOs and manage backups.

The procedure for restoring a GPO varies, as follows:

- *Restore a previous version*—If the settings of a backed up GPO have been changed and you need to revert to an older version, you right-click the GPO in the Group Policy Objects folder, and click Restore from Backup. All policy and security settings in the current GPO are replaced by the backup GPO's settings.
- *Restore a deleted GPO*—Right-click the Group Policy Objects folder and click Manage Backups to open the Manage Backups dialog box (see Figure 7-24). You can select which GPO you want to restore, view a backed up GPO's settings, or delete a backed up GPO. Multiple versions of backed up GPOs are listed by default, or you can specify seeing only the latest version of each GPO.

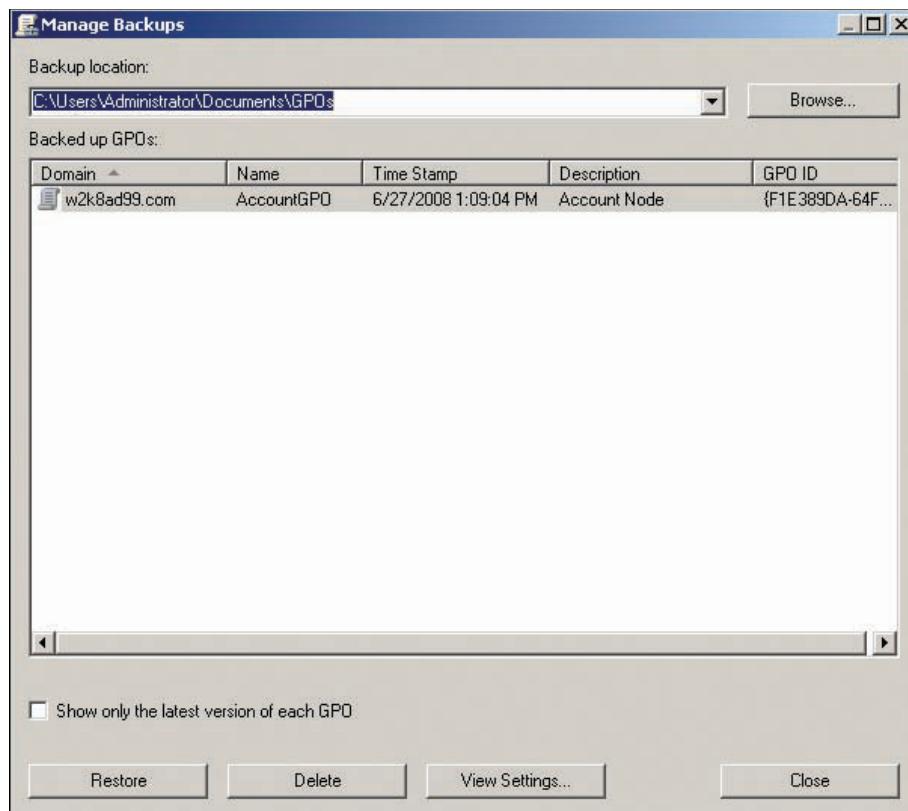
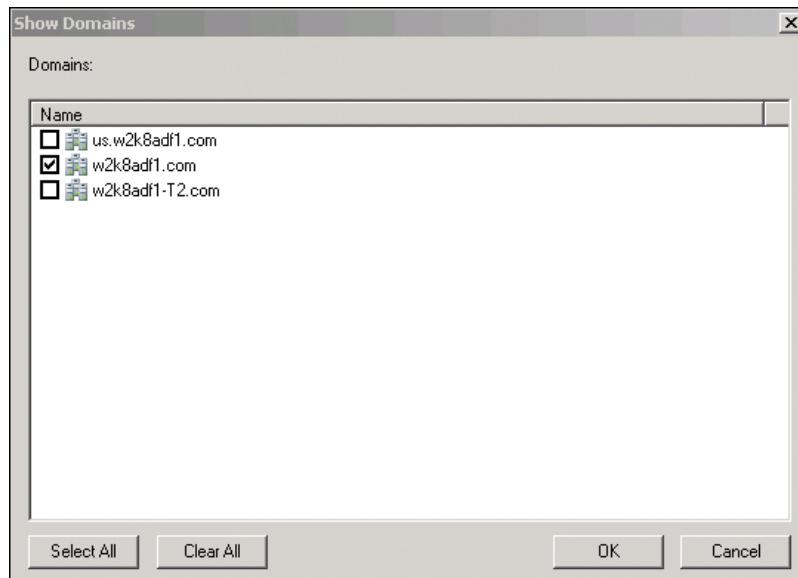


Figure 7-24 Managing GPO backups

- *Import settings*—You can import settings from a backed up GPO to an existing GPO. This is similar to restoring a GPO, except the existing GPO need not be the same GPO as the backed up GPO. As with a GPO restore, all existing settings in the current GPO are deleted.

GPO Migration You might need to migrate GPOs from one domain to another for a variety of reasons. For example, you have a multidomain environment, and two domains have similar policy requirements. After perfecting the GPOs in one domain, you can migrate them to be used in the other domain. Migration is also useful when you have set up a test environment similar to one of your production domains. You can configure and test a GPO in the test environment thoroughly, and then migrate it to the production domain.

GPOs can be migrated across domains in the same or different forests by adding the domain to GPMC. To add a domain in the same forest, right-click the Domains node in the left pane of GPMC and click Show Domains to open the dialog box shown in Figure 7-25. Then select the domains you want to add to GPMC.



7

Figure 7-25 Add a domain from the same forest to GPMC

To add a domain from a different forest, right-click the Group Policy Management node in the left pane of GPMC and click Add Forest. Then enter the name of the domain in the forest that you want to add. Figure 7-26 shows GPMC with multiple domains and multiple forests.

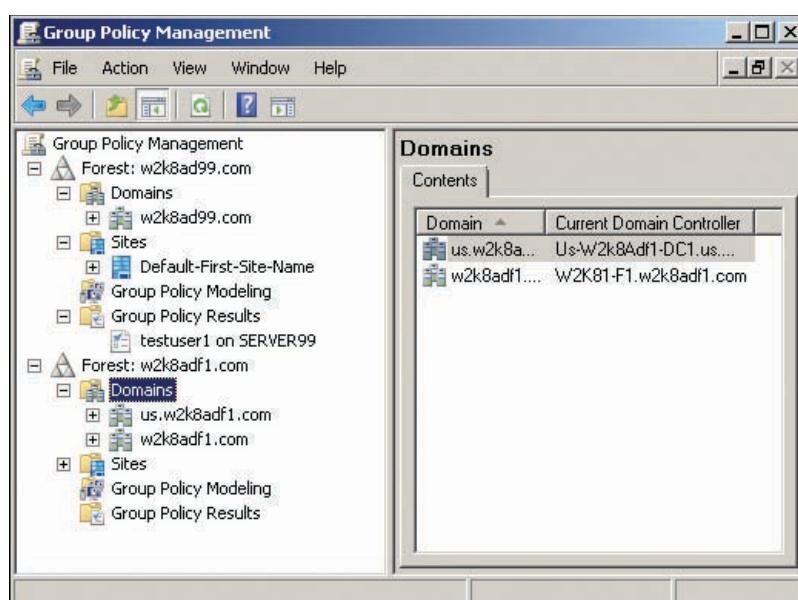


Figure 7-26 GPMC with multiple forests and domains

When you have multiple domains in GPMC, you can simply copy and paste a GPO from the Group Policy Objects folder of the source domain to the Group Policy Objects folder of the target domain. The Cross-Domain Copying Wizard starts when you click Paste in the target folder. The wizard gives you the option to use default permissions or preserve existing permissions on the GPO and translates any security principals or UNC paths in the GPO. Recall that security principals are assigned in policies such as User Rights Assignment and Restricted Groups, and UNC paths are used in policies such as Folder Redirection, Software Installation, and Scripts. This information must be modified or translated during the migration process.

A second method for migrating GPOs uses the backup and import procedure. The biggest difference between these two methods is that the copy-and-paste method creates a new GPO, and the backup and import procedure overwrites settings in an existing GPO in the target domain.

Group Policy Results and Modeling

The Group Policy Results Wizard built into GPMC creates a report to show administrators which policy settings apply to a user, computer, or both. This tool provides the same information as the **Resultant Set of Policy (RSOP)** snap-in but centralizes the tool in GPMC. To create a report, right-click the Group Policy Results node in GPMC and click Group Policy Results Wizard. In the wizard, you choose for which computer and which users you want to display policy settings. Reports can be generated only for users who have logged on to the specified computer. After the wizard finishes, the report has three tabs (shown in Figure 7-27):

- **Summary**—Shows information about objects in the report and which GPOs affect them. You can right-click in this window and click Print or Save Report (which saves it in an HTML or XML file).
- **Settings**—Displays all defined settings and the GPOs the settings came from (the Winning GPO column in Figure 7-27). As with the Summary tab, you can right-click to print or save the report.
- **Policy Events**—Displays all events in Event Viewer that are generated by group policies.

The screenshot shows the Group Policy Management console window. The left pane displays the navigation tree for the 'Group Policy Management' snap-in, including forests, domains, sites, and group policy modeling and results nodes. The right pane is titled 'testuser1 on SERVER99' and contains three tabs: 'Summary', 'Settings' (which is selected), and 'Policy Events'. The 'Settings' tab displays the 'Group Policy Results' report for the user 'testuser1' on the server 'W2K8AD99'. The report header indicates the data was collected on 6/27/2008 at 2:14:58 PM. The report is organized into sections: Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies/Password Policy, Account Policies/Account Lockout Policy, Account Policies/Kerberos Policy, Local Policies/Audit Policy, and Local Policies/User Rights Assignment. Each section lists policies, their settings, and the 'Winning GPO' that applies the setting. For example, under 'Local Policies/User Rights Assignment', the 'Allow log on locally' policy is set to 'Authenticated Users, Domain Users, SERVICE, LOCAL SERVICE, Account Operators, Administrators, Power Users' and is controlled by the 'Default Domain Controllers Policy'.

Figure 7-27 The Group Policy Results report

A command-line program, Gpresult.exe, performs a similar task as the Group Policy Results Wizard in GPMC and the Resultant Set of Policy snap-in. Because it's a command-line program, however, it can be used in batch files, and output can be redirected to text files. To use Gpresult.exe, type gpresult at a command prompt followed by parameters. For example, to create an RSoP report on a computer for testuser1, type the following:

```
gpresults /USER testuser1 /V
```

This command displays a verbose (detailed) report showing the computer policy settings and the GPO they originated from as well as the policy settings that affect testuser1.

Group Policy Modeling is a what-if tool for group policies. Like Group Policy Results, it's a wizard built into GPMC that shows administrators which policy settings would apply to a computer and/or user if moved to a different container. Essentially, the report shows which policy settings will be in effect for a user whose account is placed in a particular OU and whose computer is placed in a particular OU. You can even select user and computer membership in security groups so that GPO filtering is taken into account. Group Policy Modeling produces a report similar to Group Policy Results with Summary and Settings tabs. Instead of a Policy Events tab, the third tab, Query, summarizes the what-if choices that were made to produce the report.



The ADMX Central Store

ADMX files, as discussed, contain the settings in the Administrative Templates folder. The **ADMX central store** is a centralized location for maintaining ADMX files so that when an ADMX file is modified from one domain controller, all DCs receive the updated file. You can also create custom ADMX files that are available to all administrators to use without having to copy the files from one location to another.

The default location of ADMX files is in the %systemroot%\PolicyDefinitions folder on Windows Server 2008 and Vista computers. Without a central store, any ADMX file you customize or create would have to be copied manually to all other systems where group policies are being configured and managed. In a large network with many people working with group policies, ADMX files would get out of sync rapidly without a central store.

To create a central store, simply create a folder named PolicyDefinitions in the %systemroot%\SYSVOL\sysvol\domainname\policies folder (the same location where GPTs are stored). Under the PolicyDefinitions folder, create a language-specific folder that uses the two-character ISO standard for worldwide languages. Variations of some languages use an additional two characters to specify the country. For example, English is en-us for U.S. English or en-GB for Great Britain English. In a network with multiple domain controllers, the central store should be created on the DC that controls the PDC emulator role.

After creating folders for the central store, you just need to copy the ADMX files from their current location to the central store location. If you're managing ADMX files from a computer other than where you created the central store, the process is easy—simply copy the ADMX files to the Sysvol share (\server\Sysvol\Policies\PolicyDefinitions). Because the Sysvol share is replicated, the files and folders in the PolicyDefinitions folder are, too.



Activity 7-23: Creating the ADMX Central Store

Time Required: 10 minutes

Objective: Create the ADMX central store.

Description: You want administrators to be able to work on group policies and customize administrative templates from any Windows Server 2008 or Vista computer. To keep ADMX files from becoming unsynchronized, you need to create a central store.

1. Log on to your server as Administrator, if necessary.
2. Open Windows Explorer and navigate to **C:\Windows**. Click the **Windows** folder in the left pane. Right-click the **PolicyDefinitions** folder in the right pane and click **Copy**.
3. Navigate to **C:\Windows\SYSVOL\sysvol\w2k8adXX.com\policies**.

4. Right-click the **Policies** folder and click **Paste**. By pasting the entire PolicyDefinitions folder, there's no need to create the folder structure.
5. Click the new **PolicyDefinitions** folder to inspect the contents. There should be more than 140 ADMX files and a language-specific folder.
6. To see the contents of an ADMX file, you can open it with Notepad. To associate ADMX files with Notepad, double-click **Desktop.admx**. When asked what you want to do, click **Select a program from a list of installed programs** and click **OK**.
7. In the Open With dialog box, click **Notepad**, click to select the **Always use the selected program to open this kind of file** check box, if necessary, and then click **OK**.
8. Browse through the Desktop.admx file to get an idea of how these files are structured.
9. Close all open windows.

ADMX files are complex. If you want to learn more about them to customize existing ADMX files or create your own Administrative Templates for use in Group Policy, search for “managing ADMX files” on the Microsoft Web site. You’ll find a number of documents, including a step-by-step guide for managing ADMX files.

Group Policy Preferences

The Preferences folder is new in Windows Server 2008. Unlike user or computer policies that can't be changed by users, group policy preferences enable administrators to set up a standardized environment yet still allow users to make changes to configured settings. Both the Computer Configuration and User Configuration nodes have a Preferences folder with two subnodes—Windows Settings and Control Panel Settings—containing a number of settings organized into categories. With group policy preferences, you can perform many useful tasks, including the following:

- Create and modify local users and groups.
- Enable and disable devices on a computer, such as USB ports, floppy drives, and removable media.
- Create drive mappings.
- Manage power options.
- Create and manage files, folders, and shortcuts.
- Create and modify printers.
- Customize application settings.

Many of the tasks you can accomplish with preferences have been managed by complex logon scripts in the past. The Preferences folder should reduce the need for scripts substantially. In addition, new preferences can be created. For example, software vendors can create ADMX files for managing settings in their applications.

As mentioned in Chapter 3, computers need the Group Policy Preferences Client Side Extensions (GPP CSE) package installed to recognize and download settings in the Preferences folder when processing group policies. Because group policy preferences were developed and released after Windows Vista, only Windows Server 2008 has this package installed. Windows Vista, Windows Server 2003 SP1, and Windows XP SP2 are the only OS versions that support the GPP CSE. You can download this package at <http://download.microsoft.com>; search on “client side extensions.”



Activity 7-24: Downloading and Installing the CSE for Vista

Time Required: 10 minutes

Objective: Download and install the CSE for Vista.

Description: You want to begin testing what types of settings you can control with the Preferences folder, but you realize that you must install the CSE package to test preferences on a Vista computer.

1. Log on to the domain from your Vista computer as Administrator.
2. Start Internet Explorer and go to download.microsoft.com. In the Search text box, type **client side extensions Vista** and click **Go**.
3. Click the **Group Policy Preference Client Side Extensions for Windows Vista (KB943729)** link.
4. Click **Continue** to validate your copy of Vista. (You might get a pop-up message asking if you noticed the information bar. If so, click **Close**. Then click the yellow information bar at the top of the Web page, click **Install ActiveX Control**, and click **Install**. This procedure installs the Genuine Windows Validation Component needed to validate your copy of Vista.)
5. Click **Download** and then **Open**. In the Windows Update Standalone Installer dialog box, click **OK**. Click **I Accept** to accept the license terms, and then click **Close**.
6. Close Internet Explorer, and stay logged on to Vista for the next activity.



Activity 7-25: Configuring and Testing Preferences



Time Required: 15 minutes

Objective: Configure preferences and test them on a Vista computer.

Description: You want to be able to give certain domain users administrative capabilities on any Vista computer they log on to, so you create a global group in the domain called **Local_Admns**, and then set a preference to add this group to the local Administrators group on Vista computers.

1. Log on to your server as Administrator, if necessary.
2. Open Active Directory Users and Computers. Click the **Users** folder, and then create a global security group named **Local_Admns** in this folder. Add **Test User1** to this group.
3. Open GPMC, and click the **Group Policy Objects** folder. Right-click the **TestGP1GPO** GPO and click **Edit**. In GPME, click to expand **Computer Configuration**, **Preferences**, and **Control Panel Settings**, and then click **Local Users and Groups**.
4. Right-click **Local Users and Groups**, point to **New**, and click **Local Group**.
5. Make sure **Update** is the selected action. Click the **Group name** list arrow, and click **Administrators (built-in)** in the list.
6. Click **Add**. Click the selection button next to the Name text box. In the Select User, Computer, or Group dialog box, type **Local_Admns**, click **Check Names**, and then click **OK**. Make sure the action is **Add to this group**, and then click **OK** twice.
7. Click to expand **Computer Configuration**, **Preferences**, and **Windows Settings**, and then click **Folders**. Right-click **Folders**, point to **New**, and click **Folder**. In the Action section, click **Create**.
8. In the Path text box, type **C:\TestPrefs**, and then click **OK**. Close GPME.
9. Log on to the domain from your Vista computer as Administrator, if necessary.
10. Open a command prompt window, type **gpupdate**, and press **Enter**. Close the command prompt window.
11. Open Windows Explorer, and navigate to **C:**. You should see a new folder named **TestPrefs** there.
12. Open the Computer Management MMC. Click to expand **Local Users and Groups**, click **Groups**, and then double-click **Administrators** to open the Properties dialog box. You should see **Local_Admns** in the Members text box. Click **OK**.
13. Close all open windows, and log off.

Preferences operate the same way as policies for default inheritance and scope. However, you can target users or computers for each preference based on a set of criteria. This feature is called **item-level targeting**. The Properties dialog box for each preference has a Common tab

(see Figure 7-28) where you can set options that control how the preference is applied. Select Item-level targeting, and then click the Targeting button to define criteria that a computer or user must meet before the preference is applied. Figure 7-29 lists the properties that can be selected to define criteria.

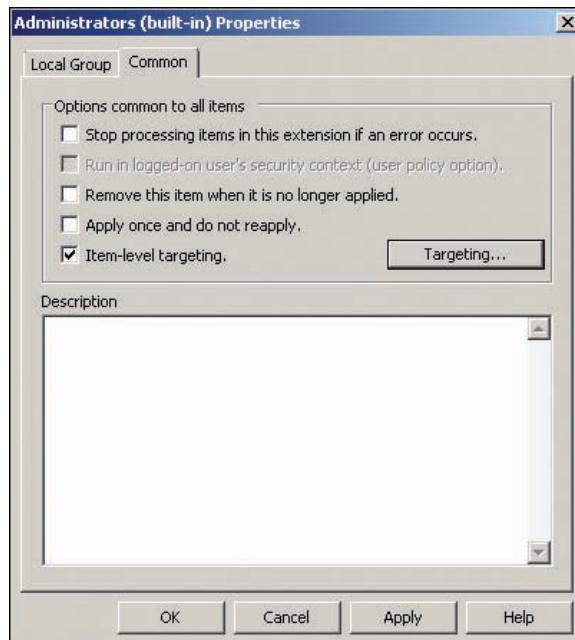


Figure 7-28 Setting preferences in the Common tab

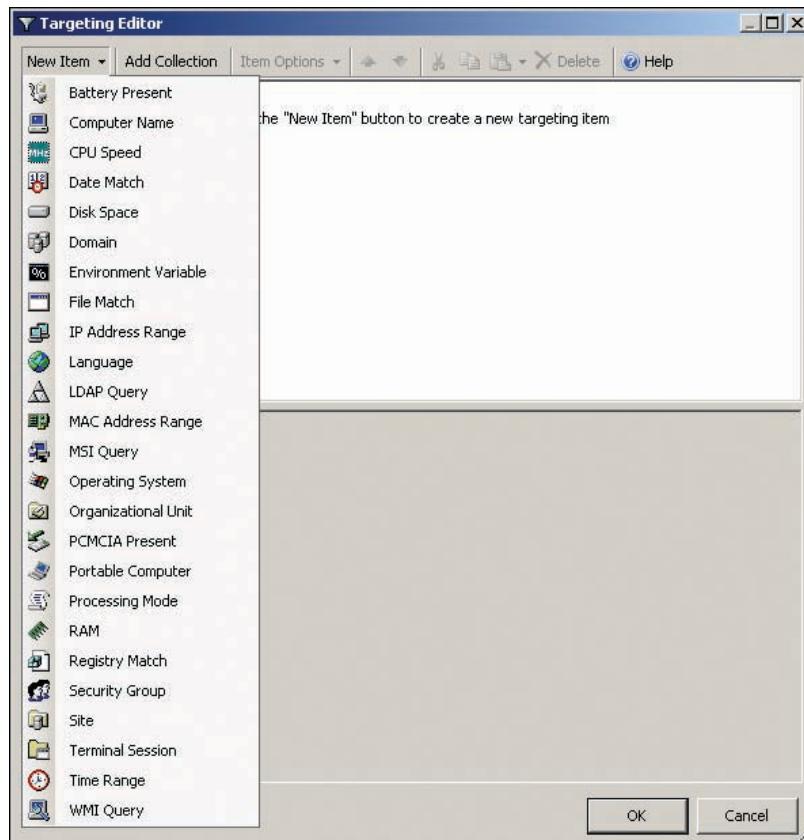


Figure 7-29 The Targeting Editor for preferences



Activity 7-26: Cleaning up GPO Links

Time Required: 5 minutes

Objective: Unlink GPOs from the domain and OUs.

Description: After considerable testing of group policies, you check your domain and OU and unlink any unnecessary GPOs from them.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC. Check each OU and verify that the only GPOs linked to objects are the ones shown in the following list. Any other GPOs linked to the domain or OUs should be unlinked.
 - Domain: Default Domain Policy, IEGPO
 - Domain Controllers: Default Domain Controllers Policy
3. Close GPMC, and log off your server.

As you can see, group policy preferences are a powerful feature for fine-tuning the working environment of domain users and computers. Administrators should spend some time exploring the capabilities available in the Preferences folder and testing item-level targeting situations.



Chapter Summary

- Group policy architecture and function involves these components: GPOs, replication, scope and inheritance, and creating and linking GPOs. GPOs can be local or domain. Windows Vista and Server 2008 have three new local GPOs (stored on the local computer). A domain GPO consists of a Group Policy Template (GPT), stored in the Sysvol share, and a Group Policy Container (GPC), stored in Active Directory.
- GPO replication is handled by Active Directory replication for GPCs and by FRS or DFSR for GPTs. DFSR is used only when all DCs are running Windows Server 2008.
- You use the GPMC to create, link, and manage GPOs and the GPME to edit GPOs. Changes to linked GPOs take effect as soon as the user logs on or the computer restarts, or at the time of the next policy refresh, whichever comes first. GPO changes should be made when the GPO is not linked to a container object.
- Starter GPOs are like template files for GPOs. You can create a new GPO by using a Starter GPO as a baseline. Starter GPOs contain only the Administrative Templates folder in the Computer Configuration and User Configuration nodes.
- GPOs can be linked to sites, domains, and OUs. Policies are applied in this order, and the last policy setting applied takes precedence when conflicts exist. Local policies are applied before domain policies, so when conflicts exist, domain policies take precedence over local policies.
- Default GPO inheritance can be changed by using inheritance blocking, enforcement, GPO filtering, and loopback policy processing.
- The Computer Configuration and User Configuration nodes contain three subnodes: Software Settings, Windows Settings, and Administrative Templates. If settings in these two nodes conflict, computer settings take precedence. Software Settings can be used to assign or publish software packages remotely to users and assign software packages remotely to computers.
- The Security Settings node in Computer Configuration contains the Account Policies subnode with settings that affect all domain users. The Account Policies subnode contains Password Policy, Account Lockout Policy, and Kerberos Policy subnodes.
- The Local Policies subnode in the Security Settings node contains Audit Policy, User Rights Assignment, and Security Options. To audit object access, you must enable the object access audit policy and then enable auditing on the target object.
- Fine-grained password policies, new in Windows Server 2008, make it possible for administrators to define different password policies for select groups of users. ADSI Edit and LDIFDE are the two tools for creating fine-grained password policies.

- Administrative Templates can control hundreds of settings on computers and for users. Administrative Templates in Windows Server 2008 and Vista use ADMX files to define the policies that affect settings in the HKLM and HKCU sections of the Registry.
- Security templates are used to transfer security settings easily from one GPO or computer to another and can be used to analyze a computer's current settings against a security database created from one or more security templates.
- Group policy management involves managing GPO delegation and GPO status as well as GPO backup and migration. Group policy monitoring involves group policy results and group policy modeling. The ADMX central store can be created to ensure that ADMX files are synchronized among all computers where group policies are managed.
- Group policy preferences, new in Windows Server 2008, enable administrators to set up user and computer environments with preferred settings, but these settings can be changed, unlike policy settings.

Key Terms

administrative template files XML format text files that define policies in the Administrative Templates folder in a GPO. You can create custom ADMX files to create your own policies.

ADMX central store A centralized location for maintaining ADMX files so that when an ADMX file is modified from one domain controller, all DCs receive the updated file.

domain GPOs Group Policy Objects stored in Active Directory on domain controllers. They can be linked to a site, a domain, or an OU and affect users and computers whose accounts are stored in these containers.

fine-grained password policies A new feature in Server 2008, used to set different password and account lockout policies for targeted users and groups. These policies are created by defining a Password Settings Object (PSO) in the Password Settings Container (PSC).

folder redirection A feature that enables administrators to set policies that redirect folders in a user's profile directory, usually to a location on a server.

GPO filtering A method to alter the normal scope of a GPO and exclude certain objects from being affected by its settings. GPO filtering methods include security filtering, which uses GPO permissions, and WMI filtering, which uses Windows Management Instrumentation queries to select objects.

Group Policy Container (GPC) A GPO component that's an Active Directory object stored in the System\Policies folder. The GPC stores GPO properties and status information but no actual policy settings.

Group Policy Template (GPT) A GPO component that's stored as a set of files in the Sysvol share. It contains all the policy settings that make up a GPO as well as related files, such as scripts.

item-level targeting A feature of group policy preferences that enables administrators to target users or computers for each preference based on a set of criteria.

local GPOs A Group Policy Object that's stored on local computers and can be edited by the Group Policy Object Editor snap-in.

Resultant Set of Policy (RSOP) A report showing which policy settings apply to a user, computer, or both and where these policy settings originated. RSOP reports can be created using the RSOP snap-in, the Group Policy Results Wizard in GMPC, and the Gpresult.exe command-line program.

security templates Text files with an .inf extension that contain information to define policy settings in the Computer Configuration\Policies\Windows Settings\Security Settings node of a local or domain GPO.

Starter GPO A GPO template that can be used as a baseline for creating new GPOs, much like user account templates.

Review Questions

1. Which of the following is a GPO on a Vista computer? (Choose all that apply.)
 - a. Local Administrators
 - b. Local Default User
 - c. Local Default Domain
 - d. Local Non-Administrators
2. Where is a GPT stored?
 - a. In a folder named the same as the GPO in the Sysvol share
 - b. In a folder named the same as the GUID of the GPO in Active Directory
 - c. In a folder named the same as the GUID of the GPO in the Sysvol share
 - d. In a folder named the same as the GPO in Active Directory
3. A user-specific local GPO takes precedence over a site-linked GPO. True or False?
4. You're having replication problems with your GPOs and suspect that the version numbers have somehow gotten out of sync between the GPT and the GPC. What can you do to verify the version numbers on a GPO?
 - a. Check the versionNumber attribute of the GPC and open the GPT.ini file.
 - b. Check the versionNumber attribute of the GPT and open the GPC.ini file.
 - c. Right-click the GPO in GPMC, click Properties, and view the version in the General tab.
 - d. Right-click the GPO in GPME, click Properties, and view the version in the General tab.
5. All your domain controllers are running Windows Server 2008. You're noticing problems with GPT replication. What should you check?
 - a. Verify that Active Directory replication is working correctly.
 - b. Verify that FRS is operating correctly.
 - c. Verify that DFSR is operating correctly.
 - d. Check the GPOReplication flag for the GPT in the Attribute Editor.
6. The ideal way to create a GPO on a production system is to right-click the OU to which it will be linked and click "Create a GPO in this domain, and Link it here." True or False?
7. You have created a GPO that defines settings only in the Local Policies node. You want the settings to apply to all computers in the domain and take precedence over any other GPOs. Which of the following is the best approach?
 - a. Link the new GPO to the domain, and unlink the Default Domain Policy. Right-click the domain object and click Enforced.
 - b. Link the new GPO to each OU containing computer accounts, and make sure it has link order 1.
 - c. Link the new GPO to the domain, and then right-click the new GPO and click Enforced.
 - d. Link the new GPO to the domain, make sure it has the highest link order, and then right-click the domain object and click Block Inheritance.
8. Which of the following represents the correct order in which GPOs are applied to an object that falls within the GPO's scope?
 - a. Site, domain, OU, local GPOs
 - b. Local GPOs, domain, site, OU
 - c. Domain, site, OU, local GPOs
 - d. Local GPOs, site, domain, OU



9. Your network consists of three sites and two domains, with some computers from both domains located at each site. Each site has certain security settings that should apply to all computers from both domains when they're located at the site. What's the best way to ensure that the correct security settings will be applied to the computers at each site?
 - a. Create three OUs in each domain, one for each site. In both domains, place the computer accounts in the OU corresponding to the site where the computer is located. Apply a GPO with the appropriate security settings to each OU in both domains.
 - b. Create three GPOs, one for each site, with the appropriate security settings. Apply the GPOs to the corresponding site, and enforce the GPO.
 - c. Create three GPOs, one for each site. Apply the GPOs to the domain object in both domains. Create three groups, one for each site, and place the computer accounts in the appropriate groups. Use GPO filtering to make sure the policy configured for each site affects only the corresponding group of computers.
 - d. On each computer in each site, configure the local GPO in GPOE with the appropriate security settings. In GPOE, right-click the Computer Configuration node and click Block Inheritance.
10. Objects in an OU with the Block Inheritance option set are affected by a domain-linked GPO with the Enforced option set. True or False?
11. You have created a GPO named RestrictU and linked it to the Operations OU (containing 30 users) with link order 3. RestrictU sets several policies in the User Configuration node. After a few days, you realize the Operations OU has three users who should be exempt from the restrictions in this GPO. You need to make sure these three users are exempt from RestrictU's settings, but all other policy settings are still in effect for them. What's the best way to proceed?
 - a. Move the three users to a new OU. Create a GPO with settings appropriate for the three users, and link it to the new OU.
 - b. Create an OU under Operations, and move the three users to this new OU. Create a GPO, and link it to this new OU. Configure the new OU to block inheritance of the RestrictU GPO.
 - c. Create a global group and add the three users as members. Configure GPO security filtering so that the global group is denied access to the GPO.
 - d. Set the Enforced option on RestrictU with an Enforce filter that excludes the three user accounts.
12. You have a new sales forecasting application that you want to make available to all users in the Sales OU. You want them to be able to find this application on the Start menu of any computer they log on to. What's the best way to do this?
 - a. Create a new GPO, and configure a Software Installation policy in the User Configuration node to assign the application. Link the GPO to the Sales OU.
 - b. Create a new GPO, and configure a Software Installation policy in the User Configuration node to publish the application. Link the GPO to the Sales OU.
 - c. Create a new GPO, and configure a Software Installation policy in the Computer Configuration node to assign the application. Link the GPO to the Sales OU.
 - d. Create a new GPO, and configure a Software Installation policy in the Computer Configuration node to publish the application. Link the GPO to the Sales OU.
13. You have been getting phone calls about resetting the password for a group of 10 part-time employees, who work only one or two days per week and have limited access to network resources. Because of domain account policies, they have to change their passwords every 14 days and are required to use complex passwords of at least 10 characters. You think these users have a difficult time keeping up with their passwords because of their infrequent

- working hours. What can you do to reduce phone calls from them without compromising the security of other users' passwords?
- Place these users and their computers in their own OU. Create a new GPO with less restrictive password settings, and link it to the new OU.
 - Remove these users' computers from the domain and set a local GPO with less restrictive password settings on each of their computers.
 - Place these users and their computers in their own OU. In GPMC, create a new PSO in the Group Policy Objects folder, and link it to the OU.
 - Add the part-time users to a global group. Use ADSI Edit to create a new PSO, and link the PSO to the global group.
14. You have been working with ADMX files to modify existing Administrative Templates and to create new templates. You work on different domain controllers, depending on your location. Despite a concerted effort, your ADMX files are getting out of sync. How can you solve this problem?
- Remove group policy management tools from all but one domain controller so that policies can be managed from only one computer.
 - Create an ADMX store in the Sysvol share, and copy the ADMX files to the ADMX store.
 - Create an ADMX store in Active Directory, and move all your ADMX files to Active Directory.
 - Share the %systemroot%\PolicyDefinitions folder on all your domain controllers, and set up Task Scheduler to copy ADMX files automatically from one system to all other systems.
15. You have set up roaming profiles for all users in your network, but users are complaining that logon and logoff take a long time. You investigate and arrive at a solution that doesn't require users to change the way they work and can be implemented quickly. Which solution did you most likely choose?
- Upgrade your network infrastructure to increase bandwidth.
 - Forbid users from storing files in their profile folders.
 - Set folder redirection policies.
 - Revert back to nonroaming policies.
16. You're concerned that some domain controllers and workstations don't meet security requirements. What should you do to verify security settings on a computer against a list of known settings?
17. None of the computers in an OU seem to be getting computer policies from the GPO linked to the OU, but users in the OU are getting user policies from this GPO. Which of the following is a possible reason that computer policies in the GPO aren't affecting the computers? (Choose all that apply.)
- The GPO link is disabled.
 - The Computer Configuration settings are disabled.
 - The computer accounts have Deny Read permission.
 - The OU has the Block Inheritance option set.
18. You need to move some user and computer accounts in Active Directory, but before you do, you want to know how these accounts will be affected by the new group policies they will be subject to. What can you do?
- Run Secedit.exe.
 - Run Group Policy Modeling.
 - Run Group Policy Results.
 - Run RSoP.



19. You have configured some group policy preferences on a GPO linked to an OU; this GPO has been working fine for months. To test the preferences, you log on to a Vista computer as a user who should be affected by these settings, but the preferences don't appear to take effect. You restart the computer and log on again. Neither the computer nor the user seem to be affected by the preference settings. What's the most likely cause of the problem?
 - a. The User Configuration settings are disabled on the GPO.
 - b. The GPO link is disabled.
 - c. The GPP CSE package isn't installed.
 - d. The user and computer are security filtered.
20. You want to set a group policy preference that affects only computers with a CPU speed of at least 2.0 GHz. What's the best way to do this?
 - a. Configure item-level targeting.
 - b. Move all computers meeting the criteria into a separate OU.
 - c. Configure the group policy client on each computer with this type of CPU.
 - d. You can't set this preference.
21. You don't have policies that force settings for the look of users' computer desktops. Each user's chosen desktop settings are applied from his or her roaming profile to any computer he or she logs on to. You think it's important for users to have this choice, but you'd like a consistent look for computers used for product demonstrations to customers. What's the best way to do this without affecting users when they log on to other computers?
 - a. Configure desktop policies in the Computer Configuration node of a GPO, and link this GPO to the OU containing the demonstration computers.
 - b. Configure loopback policy processing in Computer Configuration. Configure the desktop settings in User Configuration, and link the GPO to the OU containing the demonstration computers.
 - c. Create a new user named Demo. Configure Demo's desktop settings, and use only this user to log on to demonstration computers.
 - d. Create a new GPO with a startup script that configures desktop settings appropriate for demonstration computers when these computers are started. Link the GPO to the OU containing the demonstration computers. Instruct users to restart demonstration computers before using them.
22. You want to create policies in a new GPO that affects only computers with Windows XP installed. You don't want to reorganize your computer accounts to do this, and you want computers that are upgraded to Vista to fall out of the GPO's scope automatically. What can you do?
 - a. For each policy, use selective application to specify Windows XP as the OS.
 - b. Create a new OU, place all computer accounts representing computers with Windows XP installed in this OU, and link the GPO to this OU.
 - c. Create a group called XPComputers. Place all computer accounts representing computers with Windows XP installed in this group, and use this group in a security filter on the GPO. Link the GPO to the domain.
 - d. Configure a WMI filter on the GPO that specifies Windows XP as the OS. Link the GPO to the domain.
23. When a policy setting in Computer Configuration and User Configuration in the same GPO conflict, the Computer Configuration policy setting takes precedence. True or False?
24. You're a consultant for a small company that uses eight Windows Vista computers in a workgroup configuration. The owner asked you to set restrictive policies on users to prevent them from making Control Panel, desktop, and other changes. The owner wants to be

exempt from these policies but shouldn't be a member of the local Administrators group. What should you do?

- a. Configure the Local Computer Policy object, and then configure a user-specific GPO for the owner.
 - b. Configure the Local Computer Policy object, and use GPO filtering to exempt the owner from this policy.
 - c. Install Windows Server 2008 and configure Active Directory. Add the Vista computers to the domain, configure a GPO for the domain, and use filtering to exempt the owner.
 - d. Configure the Local Computer Policy object, and then configure a logon script for the owner that changes the restrictive settings.
25. You want to have a library of GPOs that specify baseline settings for different policy categories, and you can use this library to create new GPOs with baseline settings already configured. What's the best way to accomplish this?

Case Projects



The following case projects work with GPOs for the coolgadgets.com OU structure. When possible, GPOs should be named CG-OU*whereLinked*-C/U. For example, a GPO linked to the coolgadgets.com OU that configures computer settings should be named CG-coolgadgets-C.

Case Project 7-1: Creating a Computer GPO for Cool Gadgets

Create a GPO that meets the following requirements:

- Create a startup script policy that applies to all computers in the domain. The script should create a folder in the root of the C drive with the same name as the computer name. The script should then run the Gpresult.exe program for the Administrator user and the computer scope and send RSoP data output to a file named Gpresult.txt in the directory that was created. (*Hint:* At a command prompt, type gpresult /? for syntax help.)
- Set computer security policies that affect all computers as follows:
 - Deny guests the ability to log on to computers from the network.
 - Do not display the last username that logged on to a computer.
 - Do not allow a system to be shut down unless somebody is logged on.
 - When logon hours expire, users should be logged off the system.
- Set the following additional policies that affect all computer accounts:
 - Change the default group policy refresh interval to 45 minutes for computers, with the random time interval set to 15 minutes.
 - Configure user profiles to be deleted after 90 consecutive days of nonuse.
 - Configure Windows Update so that updates are downloaded and installed automatically every day at 3:00 a.m.

Case Project 7-2: Creating a Software Installation Policy

Create a software installation policy that affects all domain users and places the program XML Notepad, a handy XML editor available on the Microsoft download site, on each user's Start menu.

Case Project 7-3: Analyzing Security Settings

Create a security database with Security Configuration and Analysis, using a template file created by exporting settings from the GPO created in Case Project 7-1. Use this security database to analyze the security settings of your Vista computer. Print the log file and hand it in to your instructor.

Case Project 7-4: Configuring Preferences

Configure user preferences for users in the Engineering OU:

- When an Engineering user logs on to a computer, the user account is added to the local Administrators group on that computer.
- When an Engineering user logs on to a computer, the Administrative Tools folder appears on his or her Start menu.
- Enable the hibernation power mode but only if the computer being used by the user is identified as a portable computer and a battery is present. Set the power scheme to hibernate mode if the lid of the laptop is closed or when the power button is pressed.

Introduction to Windows Networking

After reading this chapter and completing the exercises, you will be able to:

- Describe networks using Windows terminology
- Configure and troubleshoot TCP/IP protocols
- Describe IPv6 addressing

The focus of this book is on Active Directory and the many related roles and services that Windows Server 2008 provides. No matter how well you have designed and configured your Active Directory environment, file system, and group policies, however, their value to users and computers is limited without a smoothly running network.

This chapter covers configuring Windows networking components from the perspective of keeping Windows servers connected and available to network clients. Windows Server 2008 adds several new tools and network enhancements, covered in this chapter, to help with that goal.

A key to understanding any network today is solid knowledge of the TCP/IP protocol and the tools for configuring and troubleshooting it. This chapter covers TCP/IP, IPv4 addressing, and IPv6. Your understanding of IPv4 addressing in particular is critical to understanding how to configure sites in Active Directory.

A main objective of the 70-640 certification exam is configuring the Domain Name System (DNS) infrastructure to support Active Directory. DNS is a protocol in the TCP/IP suite, so understanding Windows networking and TCP/IP prepares you for the extensive coverage of this topic in Chapter 9.

Understanding the Windows Networking Paradigm

Before Windows Server 2008 and Vista, users' view of the network to which their computers were connected was mostly limited to the status of network connections in the Network Connections window and My Network Places. Windows Vista and Windows Server 2008 offer the Network and Sharing Center that visually depicts the networks your computer has a connection to and shows status information for each network. Discovered networks are categorized by security access level (public, private, or domain) so that security settings can be applied according to the network connection. The focus on security makes working with Windows Server 2008 and Vista networks both easier and more complex. Configuring basic network settings without having to worry as much about security makes networking easier for novices, but the more advanced settings of Windows networking involve more complex tools.

In the following sections, you examine the Network and Sharing Center and then learn about the enhancements made in Windows networking since Windows Server 2003 and XP. Before you get started, however, a discussion of the networking terms used in Windows is in order.

Windows Networking Terminology

Most OS vendors use a set of terms to describe networking components and processes, and Microsoft is no different. Some terms are standard for the industry, but others might not be. You learned some of these terms in Chapter 1, but the following list should be helpful in this chapter's discussion on networks:



This list of terms is by no means complete. Entire books are written on network terminology and concepts, such as *Guide to Networking Essentials, Fifth Edition* (Course Technology, 2006, 1-4188-3718-0).

NOTE

- **Network media**—The cables (or airwaves, with wireless networks) through which network signals travel to communicate from one computer or device to another.
- **Network interface card (NIC)**—The hardware that connects a computer to the network media. The NIC is often part of the motherboard but can also be an add-on card. Microsoft usually refers to the NIC as the “network adapter.”
- **NIC driver**—Software that communicates between a NIC and the OS. To function, every NIC must have a driver installed that's specific for its model.
- **Hub or switch**—The device that connects a computer to the rest of the network. In a wired network, one end of the connection medium is plugged into a computer's NIC and the other end into the hub or switch. In a wireless network, this device is called an access point.
- **Router**—A network device that forwards communication packets from one network to another. Routers are the basis for the Internet.
- **Network protocol**—The rules and syntax that computers use to communicate with one another. TCP/IP is the most well-known protocol.

- **Client**—A software component, such as Client for Microsoft Networks, that allows your computer to access files, printers, and other resources on other computers.
- **Service**—A software component that allows your computer to offer network resources to clients. File and Printer Sharing for Microsoft Networks is an example of a service.
- **Network**—A group of computers that share the same network address and communicate with one another through hubs or switches. (Computers communicating through a router are on separate networks.)
- **Internet**—Two or more networks connected through a router make up an internetwork.
- **Network connection**—In Windows, a **network connection** is represented by an icon in the Network Connections window that shows the components needed for the computer to connect to a network. Typically, these components entail a NIC and its driver, one or more network protocols, and configuration parameters. Some connections, such as dial-up, use a modem instead of a NIC.
- **Network discovery**—Microsoft uses the term **network discovery** to describe the process whereby a computer finds other computers on a network and allows other computers to find it. Discovered computers are displayed in a network list, so users can simply double-click a computer to view its available shared resources.

The Network and Sharing Center

The Network and Sharing Center is your window into your computer's network environment. With this tool, you can create network connections, view the status of existing connections, and troubleshoot network problems. In addition, you can enable and disable the discovery of other computers on the network and configure folder sharing. There's a lot going on in the Network and Sharing Center (see Figure 8-1), and you tackle this tool in sections:

- The network map
- Sharing and Discovery
- Tasks

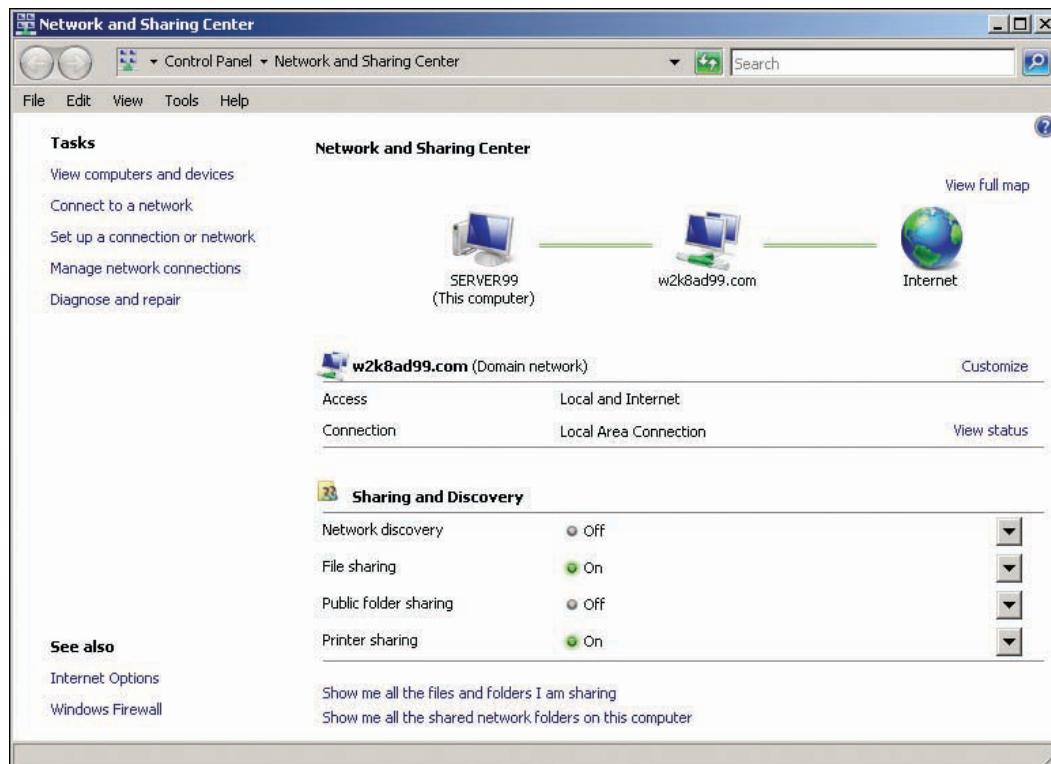


Figure 8-1 The Network and Sharing Center

The Network Map The **network map** displays a graphical view of the network from your computer’s perspective. The basic view, shown as the three icons with lines between them in Figure 8-1, includes your computer, the networks to which your computer is connected, and the Internet. The lines between icons are green if the connection is functioning or black with a red X if no connection is detected. When your computer first connects to a network, you’re prompted to select the type of network you are connecting to: Home, Work, or Public. Based on your choice, Windows designates your network as one of the following location types:

- **Public**—Indicates the computer is connected to a network located in a public place, such as a wireless network in an Internet café, a school, or a library, or directly to the Internet. By default, when a public network is detected, network discovery is turned off, and firewall settings are configured for tighter security.
- **Private**—Indicates the computer is connected to a private workgroup network without a direct connection to the Internet. Network discovery is enabled by default, and firewall settings are configured with somewhat less stringent rules than for a public network. The network type is configured as private when you choose Home or Work when you first set up a network connection.
- **Domain**—When a private network is selected and the computer detects the domain of which it’s a member, a domain network is selected automatically. Network discovery is enabled by default on a domain network. You can’t select a domain network manually, nor can you change it to a different type.



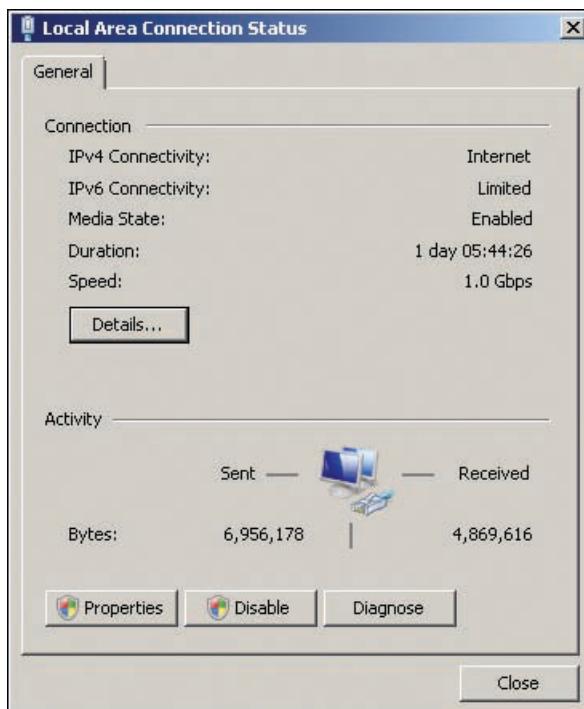
Windows might not detect a domain network properly and show it as private or unknown. If your computer is a member of a Windows domain and currently connected to the domain, but Windows doesn’t detect it as such, try disabling and reenabling the network interface to correct the problem.

If you click the computer icon on the basic map, Windows Explorer opens the same window as when you click Start, Computer. If you click the icon representing the network (w2k8ad99.com in Figure 8-1), a Network window opens (the same window as when you click Start, Network). If network discovery is enabled, you see a list of discovered servers and computers. Your default Web browser opens if you click the Internet icon.

Under the basic map in the Network and Sharing Center, each network your computer is connected to is displayed with Customize and View status options. Click the Customize link to change the network name, select a different icon to represent the network, and, if it’s not a domain network, change the location type to public or private. The network name is generally the domain name or simply “Network,” if no domain name is defined.

Clicking the View status link opens the status dialog box for the network connection (see Figure 8-2), where you can view detailed information about your network connection, view and configure its properties, disable the connection, and diagnose problems.

To see a more detailed network map, click the View full map link at the top right in the Network and Sharing Center. However, network mapping is disabled by default on domain and public networks. Administrators can enable the network map feature on these networks by using group policies. In Group Policy Management Console (GPMC), network map-related policies are in Computer Configuration\Administrative Templates\Network\Link-Layer Topology



8

Figure 8-2 Viewing the network connection status

Discovery. Figure 8-3 shows an example of a more detailed network map. The information box under the gtVista1 computer pops up when you hover over it. Hovering your mouse over any device shows a similar information box. In Figure 8-3, Windows has correctly determined that the gtVista1 computer is connected to a switch, and Server99, Vista-VM, and GT-Vista are connected to a hub.

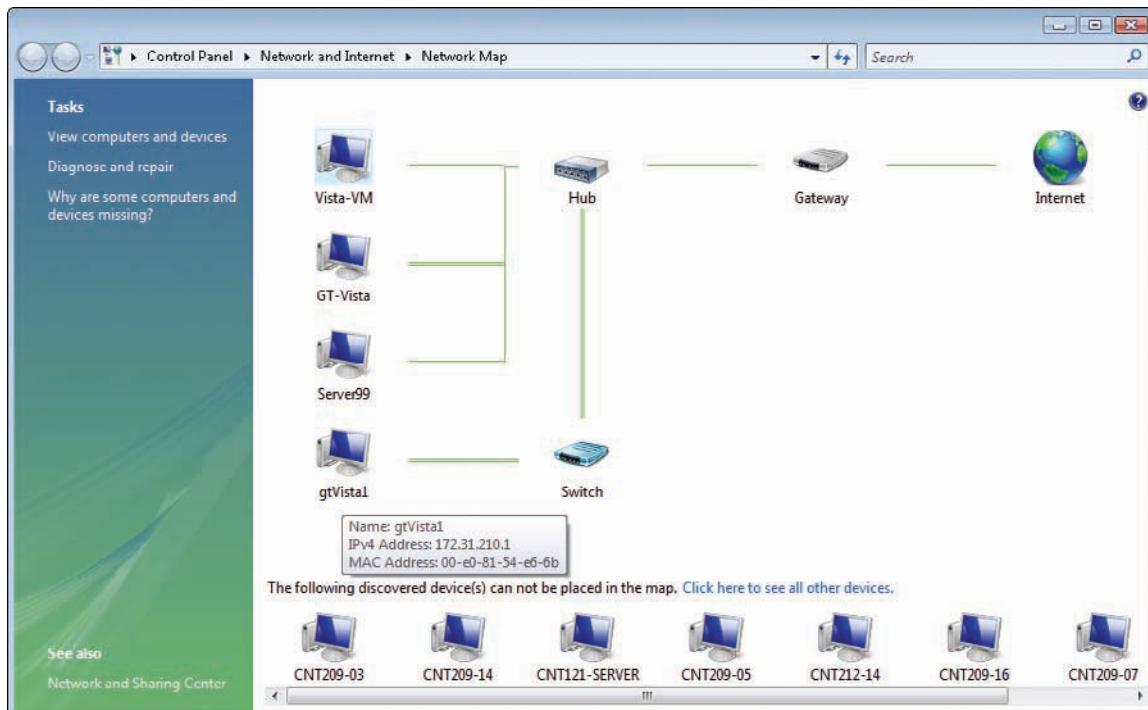


Figure 8-3 A detailed network map

The devices in Figure 8-3 at the bottom of the window can't be placed in the map because they are running Windows Server 2003 or XP and don't have the necessary Link Layer Topology Discovery (LLTD) protocol installed. LLTD, installed by default in Vista and Windows Server 2008, is used to discover computers and place them on the map. Devices can't be placed on a network map for other reasons, too:

- A computer running Vista is connected to a network designated as public.
- LLTD is disabled. Protocols can be enabled and disabled in a network adapter's Properties dialog box.
- Network discovery is turned off.
- Firewall settings on the computer or network are preventing Windows from detecting the computer.
- The NIC drivers don't support LLTD.

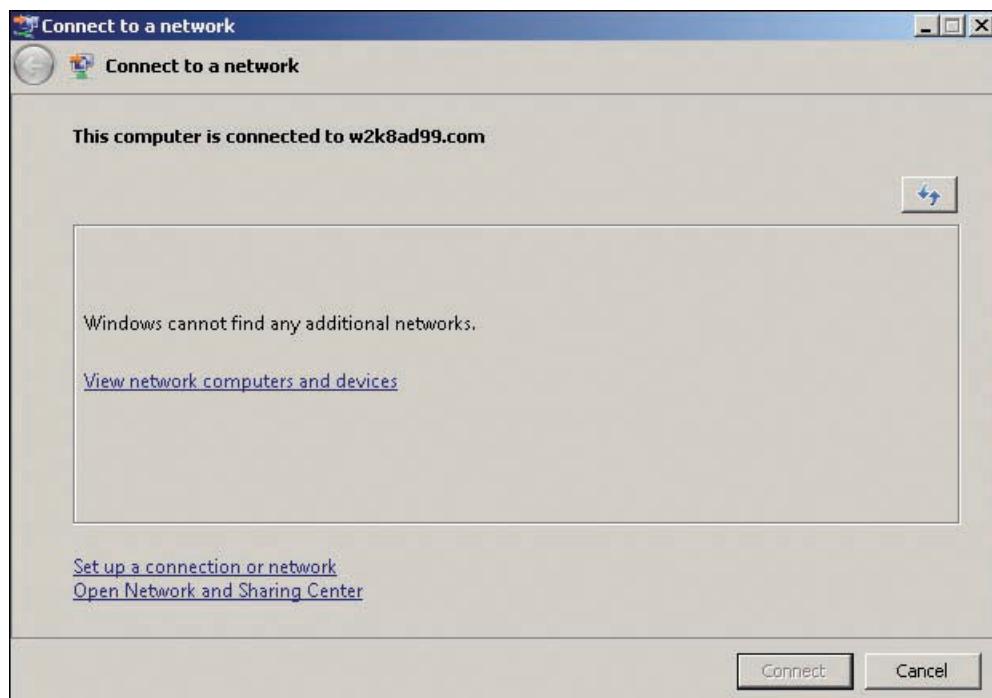
The Sharing and Discovery Section You can enable and disable the following functions in the Sharing and Discovery section of the Network and Sharing Center:

- *Network discovery*—If turned on, this computer can discover and view other computers on the network and be discovered by other computers. When it's enabled, you can open the Network window to view other computers by clicking the network's icon in the basic network map or by clicking Start, Network. If turned off, this computer can't discover other computers and can't be discovered. If you open the Network window with network discovery off, you see a message to that effect. Disabling this setting does not, however, prevent this computer from being accessed by UNC path or from accessing other computers by UNC path. In domain networks, enabling network discovery displays Custom instead of On next to this option in the Sharing and Discovery section, and only domain members are discovered.
- *File sharing*—If turned on, folders can be shared with other users on the network. If turned off, any existing shares (except administrative and default shares) are no longer shared. Sharing a folder enables this option automatically.
- *Public folder sharing*—If turned on, the Public folder can be shared to allow all network users to open files or to open, change, and create files. If turned off, the Public folder isn't accessible to network users, but users logged on interactively can still access the folder. Turning on this option also enables file sharing.
- *Printer sharing*—If turned on through the Network and Sharing Center, all printers attached to the computer are shared with network users. If a printer is shared via its Properties dialog box in the Printers folder in Control Panel, this option is enabled, but other printers are not shared automatically. Turning on this option also enables file sharing.

The two links in the Sharing and Discovery section display information about what's currently being shared. The "Show me all the files and folders I am sharing" link opens the results of a default saved search called Shared By Me, which is stored in the Searches folder in each user's profile. The "Show me all the shared network folders on this computer" link opens the Network window and lists all shares on the current computer. You see the same results if you type \\serverXX in Windows Explorer or the Start Search text box.

The Tasks Section The Tasks section of the Network and Sharing Center has links to perform the following tasks:

- *View computers and devices*—Opens the Network window and lists all the computers discovered. If network discovery is off, no devices are displayed, and you see a message explaining this fact as well as an option to enable network discovery and file sharing. A domain network lists only computers that are members of the domain and have network discovery enabled.
- *Connect to a network*—Opens the Connect to a network window (see Figure 8-4) that lists networks found by Windows, including wireless networks.



8

Figure 8-4 The Connect to a network window

- *Set up a connection or network*—Starts the Set up a connection or network Wizard (see Figure 8-5). This wizard walks you through setting up a connection to the Internet through a wireless, broadband, or dial-up connection or setting up a dial-up or VPN connection to another network, such as your workplace.

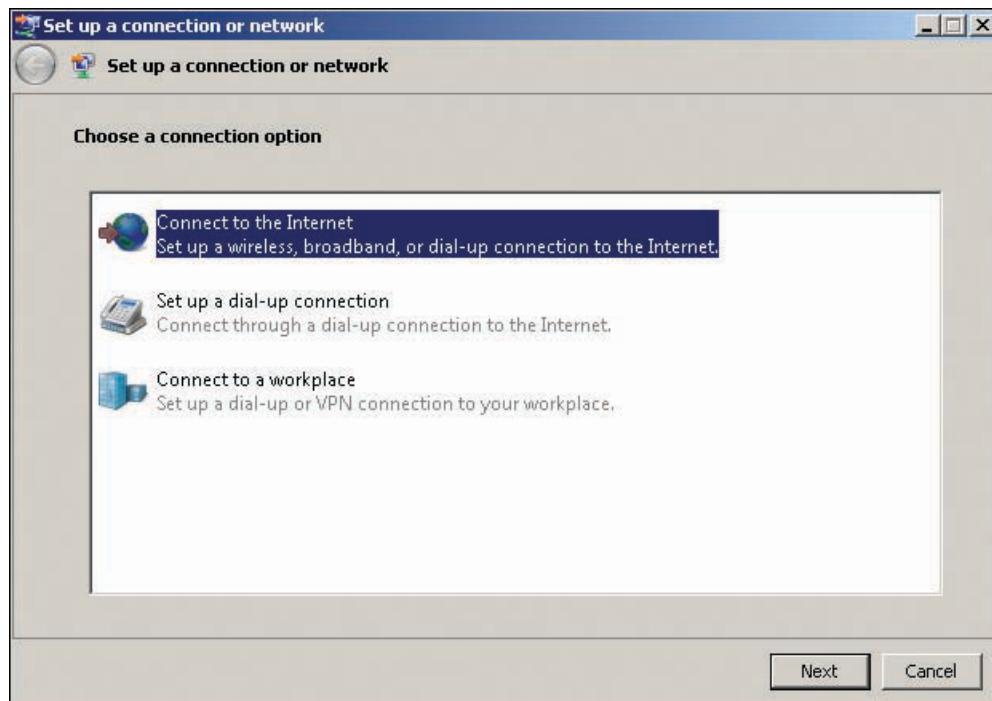


Figure 8-5 The Set up a connection or network Wizard

- *Manage network connections*—Opens the Network Connections window, where you can check connection status and configure existing connections.
- *Diagnose and repair*—Runs the Windows Network Diagnostics program, which attempts to find and solve network connection problems.



Activity 8-1: Working with the Network and Sharing Center

Time Required: 10 minutes

Objective: View and configure features in the Network and Sharing Center.

Description: You're familiar with configuring networking in Windows Server 2003 and Windows XP, but you need to work with the Network and Sharing Center features in Windows Server 2008 and Vista.

1. Log on to your server as Administrator.
2. Click the **network** taskbar icon and click **Network and Sharing Center**.
3. In the Network and Sharing Center, click the **ServerXX (This computer)** icon. Close the Explorer window that opens. Click the **w2k8adXX.com** icon. By default, network discovery is off, so unless it has been enabled, you won't see any computers in the Network window that opens. Close the Network window. Click the **Internet** icon, and then close Internet Explorer.
4. Click the **View full map** link. The network map function is disabled by default. Close the Network Map window.
5. Click the **Customize** link next to **w2k8adXX.com (Domain network)**. You can give your network a customized name, if you want. You can't change the network type when it's a domain network. If your network is listed as public or private, you can change the type here. Click the **Change** button next to Network Icon. You can select an icon appropriate for the network type. Click **Cancel**, and then click **Next**. Click **Close**.
6. Click the **View status** link next to Local Area Connection. In the Local Area Connection Status dialog box, you can view properties related to your network connection. Click **Close**.
7. Under Sharing and Discovery, click the arrow next to Network discovery. Click **Turn on network discovery**, and then click **Apply**. Notice that the status changes to Custom. (If the status of network discovery is already Custom, you can skip this step.)
8. Click the **w2k8adXX.com** icon in the basic network map. You'll probably see only your server in the Network window. If your Vista computer is running and network discovery is on, you see your Vista computer as well. Close the Network window.
9. Click the **Manage network connections** link under Tasks. To make a shortcut to the Network Connections window, drag the Network icon in the address bar to your Quick Launch toolbar. Now you can access this window quickly. Close the Network Connections window and Network and Sharing Center.



Activity 8-2: Using Group Policy to Change Network Settings

Time Required: 15 minutes

Objective: Set group policies to enable network mapping.

Description: You want to be able to view your domain computers with the network map feature. You have found the policy to control this setting, so you decide to create a GPO and apply it to the domain so that all computers have mapping enabled.

1. Log on to your server as Administrator, if necessary.
2. Open GPMC.
3. Click to expand the **Group Policy Objects** folder, and create a GPO in this folder named **NetworkGPO**. Right-click **NetworkGPO** and click **Edit**.

4. In Group Policy Management Editor (GPME), expand **Computer Configuration**, **Policies**, **Administrative Templates**, and **Network**.
5. Click **Link-Layer Topology Discovery**. In the right pane, enable the **Turn on Mapper I/O (LLTDIO) driver** and **Turn on Responder (RSPNDR) driver** policies. For both policies, click to enable the **Allow operation while in domain** option. Close GPME.
6. In GPMC, link **NetworkGPO** to the domain.
7. Open a command prompt window, type **gpupdate**, and press **Enter**. Close the command prompt window when Gpupdate.exe is finished.
8. Open the Network and Sharing Center, and click **View full map**. After a moment, the network map should be displayed. If your Vista computer isn't displayed in the map, start your Vista computer and log on to the domain as Administrator, if necessary. Run **gpupdate** on your Vista computer, and then close the command prompt window. Refresh the network map on your server by clicking the Network Map window and pressing **F5**.
9. Note that enabling the above policies doesn't enable network discovery, only the network map feature. Close all open windows, and stay logged on to your server.



Currently, there's no group policy setting to enable network discovery on computers. However, you can create a script that runs at computer startup or user logon with this command: netsh advfirewall firewall set rule group="network discovery" new enable=yes.



TCP/IP Operation and Configuration

TCP/IP is the default network protocol installed on Windows computers. Beginning with Windows Server 2008 and Vista, two versions are installed: TCP/IPv4 and TCP/IPv6. This section discusses TCP/IPv4, as it's still the dominant protocol used in today's networks. TCP/IPv6 is covered later in this chapter. The differences between TCP/IPv4 and TCP/IPv6 are limited to the IP part of the protocol. Therefore, the discussion of TCP/IP in general applies to both versions; only when IP is covered is the discussion specific to version 4 or 6.

TCP/IP is a suite of protocols, so when it's installed on a computer, a number of protocols, services, and programs are usually installed with it. Some are listed here with a brief description:

- *Domain Name System (DNS)*—DNS resolves domain names to addresses. When a network resource is requested by its name, such as \\serverXX\Shared or http://www.microsoft.com, DNS client software queries a DNS server to resolve the name of the server hosting the resource to its IP address. Windows computers running TCP/IP have the DNS client protocol installed automatically, and a DNS server can be added as a server role in Windows Server 2008 (discussed in Chapter 9). A DNS server is required to run a Windows Server 2008 domain. By default, the DNS client protocol is installed on each computer that installs the TCP/IP suite. The DNS server role can be installed on a Windows Server 2008 server.
- *Dynamic Host Configuration Protocol (DHCP)*—DHCP provides automatic IP address configuration. By default, Windows computers are configured to request their IP address configuration from a DHCP server. The client portion of DHCP is installed by default on all computers that install TCP/IP. The DHCP server role can be installed in Windows Server 2008.
- *Transmission Control Protocol (TCP)*—The component of the TCP/IP suite that provides reliable data transfer between computers. TCP handles flow control, packet sequencing, and data acknowledgements to help ensure that data transfers are completed without error. TCP is used by applications that require reliable transfer of large amounts of data.
- *User Datagram Protocol (UDP)*—A lightweight protocol that performs some functions of TCP but is used by applications that usually transfer a small amount of data and, therefore, don't require the reliability features of TCP.

- *Internet Protocol version 4(IPv4)*—The component of the TCP/IPv4 suite that provides network addressing and routing. IPv4 is currently the most commonly used version of IP.
- *Internet Control Message Protocol (ICMP)*—The protocol the Ping program uses to test whether a computer can communicate with another computer. ICMP is also used by computers and network devices to send status messages to one another.
- *Address Resolution Protocol (ARP)*—Resolves a computer’s IP address to its physical, or Media Access Control (MAC), address. When a computer or router must deliver a packet of data to another computer or router in the same network, ARP can be used to request the destination device’s MAC address.

The TCP/IP suite has several other protocols, but the ones in this list are enough to understand IP address configuration and DNS, the two main networking topics discussed in this book. For a thorough discussion of networking in Windows Server 2008, see *MCTS Guide to Configuring Microsoft Windows Server 2008 Network Infrastructure* (Course Technology, 2008, 1-4239-0236-X).

TCP/IP Communication

Communication between two computers using TCP/IP often begins when one computer (the client) requires access to a resource or service on another computer (the server). When a user initiates the communication, the server’s name is usually used. For example, a user wants to view the home page for *www.coolgadgets.com*. The user opens a Web browser and types “*www.coolgadgets.com*” in the address bar. For communication to proceed, the Web server’s name (*www.coolgadgets.com*) must be resolved to its IP address, which involves a request to a DNS server.

After the client has the Web server’s IP address, it must determine whether it’s on the same network or a different network. The client finds this information by comparing its IP address with the Web server’s IP address (discussed more in the next section). If the client and Web server are on the same network, the client must get the Web server’s MAC address before the request can be sent. If they’re on different networks, the client sends the request to its default gateway, or router. The router forwards the request until it gets to a router connected to the Web server’s network. Understanding the basics of TCP/IP communication helps you better understand IP configuration and addressing, discussed next.

IPv4 Address Configuration

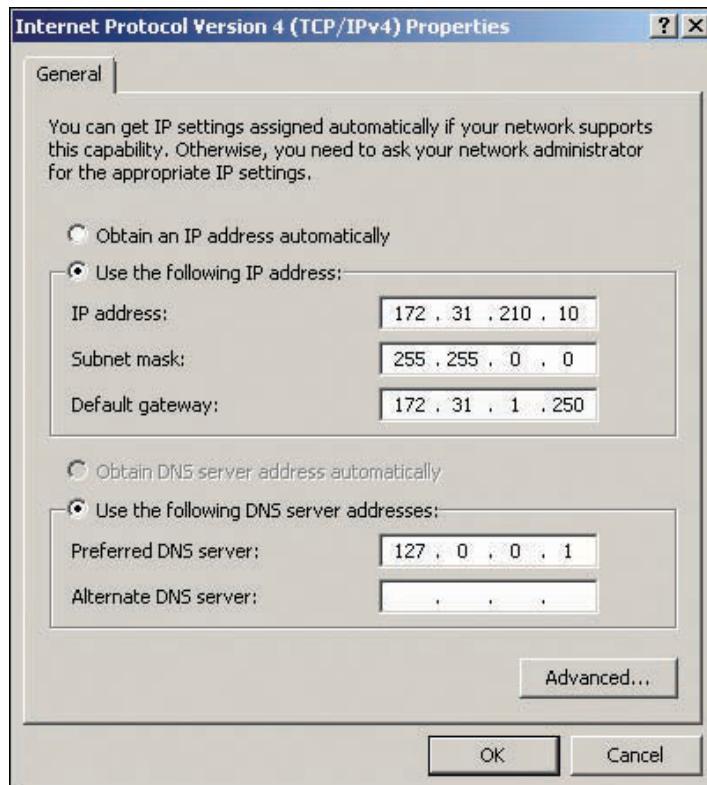
An IP address is a 32-bit number divided into four 8-bit values called octets. Each **octet** can have a value from 0 to 255. IP addresses are written in dotted decimal notation, yielding an address consisting of four decimal numbers, each in the range 0 to 255, separated by a period. For example, in the IP address 10.255.0.100, 10 is the first octet and 100 is the fourth octet.

Every IP address contains a network ID, which specifies the network on which the computer is found, and a host ID, which uniquely identifies the computer on that network. Determining how many bits of the IP address are the network ID and how many are the host ID depends on the **subnet mask**, another 32-bit dotted decimal number that consists of an unbroken series of binary 1 digits followed by an unbroken series of binary 0 digits.

A series of eight binary 1s equals the decimal value 255. For example, a valid subnet mask is 255.255.0.0, which is 16 binary 1s followed by 16 binary 0s. However, 255.0.255.0 is not a valid subnet mask because it doesn’t consist of an unbroken series of 1s followed by an unbroken series of 0s. Each 1 bit specifies that the corresponding bit in the IP address is part of the network ID, and each 0 bit specifies that the corresponding bit in the IP address is part of the host ID. For instance, IP address 10.255.0.100 with subnet mask 255.255.255.0 tells you (and the computer) that 10.255.0 is the network ID and 100 is the host ID. Understand, however, that you must use the network ID and host ID together when communicating with another computer.

When you configure an IP address on a Windows computer in the IP protocol Properties dialog box shown in Figure 8-6, you must include both an IP address and a subnet mask.

By doing so, the computer can determine on which network it is located. When a packet is sent to a destination computer, the computer compares its own network ID to the destination network ID. If they differ, the packet must be sent to a router. In Figure 8-6, the network ID of the IP address is 172.31, and the host ID is 210.10.



8

Figure 8-6 The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box

Assigning IP Address Classes When you enter an IP address in the Properties dialog box shown in Figure 8-6, Windows fills in a subnet mask automatically, which you can change if necessary. Windows bases the suggested subnet mask on the class of the IP address you enter. Three classes of IP addresses can be assigned: class A, class B, or class C. The class to which an IP address belongs is determined by the value of the address's first octet, as shown in Table 8-1.

Table 8-1 IP address classes

Value of first octet	Class
1–127	A
128–191	B
192–223	C



There are also class D and E addresses, which can't be assigned to hosts. Class D addresses, with the first octet in the range 224 to 239, are used for multicast applications. Class E addresses, in the range 240 to 255, are reserved for experimental use.

NOTE

The address class determines the default number of bits used to specify the network ID and, therefore, the default subnet mask for an address. Table 8-2 lists the default number of bits for specifying the network ID in each address class.

Table 8-2 Default subnet mask and number of network ID bits for each address class

Class	Default subnet mask	Number of bits in network ID
A	255.0.0.0	8
B	255.255.0.0	16
C	255.255.255.0	24

In Figure 8-6, when the IP address 172.31.210.10 is entered in the IP address text box, Windows recognizes it as a class B address and assigns a subnet mask of 255.255.0.0 by default.

IP Address Assignment Rules When you assign a computer an IP address, there are some rules to remember:

- Every IP address configuration must have a subnet mask.
- All hosts on the same physical network must share the same network ID in their IP addresses.
- All host IDs on the same network must be unique.
- You can't assign an IP address in which all the host ID bits are 0. This type of IP address is reserved as the network ID. For example, IP address 172.31.0.0 with subnet mask 255.255.0.0 is reserved to identify network 172.31.
- You can't assign an IP address in which all the host ID bits are 1. This type of IP address is reserved as the network broadcast address. For example, IP address 172.31.255.255 with subnet mask 255.255.0.0 has all host ID bits set to 1 and is reserved as the broadcast address for the 172.31 network.
- Computers assigned different network IDs can communicate only by sending network packets to a router, which forwards the packets to the correct network.

Subnetting If IP addresses have a default subnet mask assigned based on the value of the IP address's first octet, why do you even need to specify the subnet mask? The reason is the default subnet mask doesn't always suit the needs of today's networks. Address classes and default subnet masks were designed when TCP/IP was in its infancy, and computer networks and the Internet were almost unheard of. They met the needs of the few government agencies and universities using TCP/IP in the late 1970s and 1980s.

After computer networks were being installed in every business, and users wanted access to the new information source called the Internet, the address class system clearly needed some flexibility—hence, subnet masks that could be configured irrespective of the address class. This use of subnet masks became known as Classless Interdomain Routing (CIDR). For example, assigning the IP address 172.31.210.10 with a subnet mask of 255.255.255.0 is perfectly acceptable. In this case, the network ID is 172.31.210 and the host ID is 10. Why would you want to assign a subnet mask different from the default, however? Aren't the default subnet masks good enough? In some cases, they are, but not in others.



Another way of specifying an IP address and its subnet mask is CIDR notation. CIDR notation uses the format A.B.C.D/n; n is the number of 1 bits in the subnet mask or, expressed another way, the number of bits in the IP address representing the network ID. The n is referred to as the IP prefix or just prefix. For example, 172.31.210.10 with a 255.255.255.0 subnet mask is expressed as 172.31.210.10/24 in CIDR notation.

Take, for instance, the address 172.31.0.0 with the default subnet mask 255.255.0.0. As Table 8-2 showed, this subnet mask allows for a 16-bit host ID. With these 16 bits, you can assign more than 65,000 host addresses, starting with 172.31.0.1 and ending with 172.31.255.254. (Remember that you can't assign an address with all 0 bits or all 1 bits in the host ID, so you have to exclude 172.31.0.0 and 172.31.255.255 from the possible IP addresses you can assign to a host.) The exact calculation for the number of hosts is $2^n - 2$; n is the number of bits in the host ID. Being able to assign this many addresses might seem like an advantage if you have a large network. However, having such a large address space assigned to a single network has two distinct disadvantages: If you're actually using the number of computers the address space affords (in this case, more than 65,000), communication efficiency suffers, and if you aren't using the addresses, precious address space is wasted.

All computers and devices that share the same network ID in their IP address are said to be in the same broadcast domain. A broadcast domain defines which devices must receive a packet that's broadcast by any other device. A broadcast is a packet addressed to all computers on the network. TCP/IP communication relies heavily on broadcast packets to perform a variety of functions. For example, DHCP and ARP use broadcasts to perform their tasks. Every time a computer receives a broadcast packet, the NIC generates an interrupt, causing the CPU to stop what it's doing to read the packet. If the broadcast isn't relevant to the computer, the packet is usually discarded. Now imagine 65,000 computers on the same broadcast domain; at any moment, probably several thousand are sending broadcast packets. The amount of traffic generated and the additional CPU utilization would likely bring the network to a screeching halt. Preventing this problem is where subnetting comes in.

If you do have 65,000 computers in your organization, instead of creating one large network with the network address 172.31.0.0/16, you can divide this enormous network into many smaller networks. For example, you can use 172.31.0.0/24, 172.31.1.0/24, and so forth up to 172.31.255.0/24. This strategy makes 256 smaller networks with a maximum of $2^8 - 2$, or 254, devices per network. (With 24 network bits, there are 8 bits in the host ID because an IP address has 32 bits total.) If a computer on one network needs to communicate with a computer on another network, the packets are sent to a router that locates the network and forwards the data. Now the maximum size of your broadcast domain is only 254 computers, which is more manageable.

Another reason to subnet is to conserve IP addresses. Companies that maintain Internet-connected devices need public Internet addresses, which must be unique in the world—meaning a public address can be assigned to only one device on the Internet. In the past, if a company had four Web servers and two routers that needed public addresses, the only recourse an ISP had was to assign a class C network address consisting of 254 possible host addresses, thereby wasting 248 addresses. By subnetting a network, the ISP can assign an address such as 198.60.123.0/29 that uses only addresses 198.60.123.0 through 198.60.123.7, which satisfies the company's needs and still makes addresses 198.60.123.8 through 198.60.123.254 available for other customers.

This section has by no means been a thorough discussion of subnetting, but it should provide the information you need to understand IP address configuration and the importance of grouping computers by subnets when designing Active Directory sites.



For an online tutorial on subnetting, try www.learntosubnet.com.

Configuring Multiple IP Addresses Windows OSs allow assigning multiple IP addresses to a single network connection in the Advanced TCP/IP Settings dialog box shown in Figure 8-7. As long as the address isn't assigned via DHCP, you can click the Add button and enter a new IP address and subnet mask. Multiple IP addresses can be useful in these situations:

- The computer is hosting a service that must be accessed by using different addresses. For example, a Web server can host multiple Web sites, each assigned a different IP address and domain name.

- The computer is connected to a physical network that hosts multiple IP networks. This situation can occur if your network addressing scheme is transitioning from one network ID to another, and you need a server to be available to both the old and the new IP addresses until the transition is completed. It can also occur when you have multiple groups of computers (or hosts and virtual machines) connected to the same physical network but with different network addresses. If all the computers need access to server resources, the servers can be configured with IP addresses to serve all the IP networks.

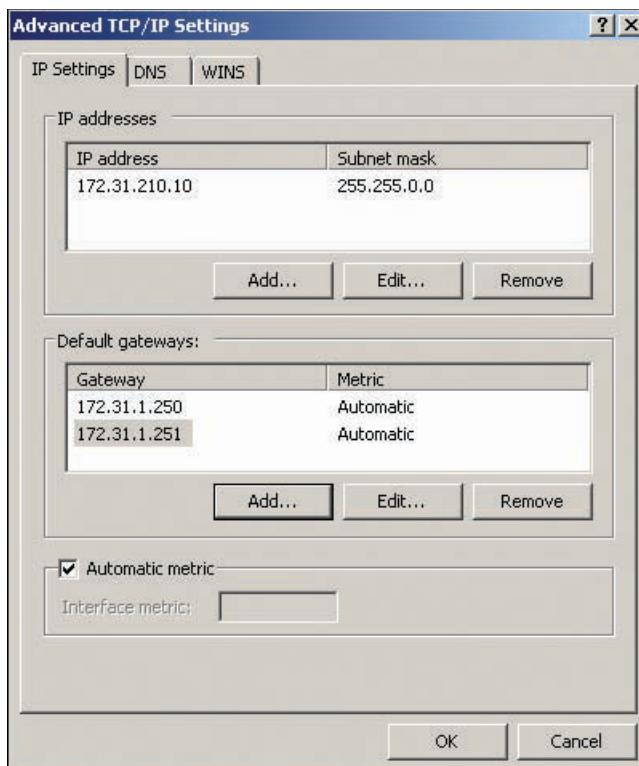


Figure 8-7 The Advanced TCP/IP Settings dialog box



When multiple IP addresses are assigned to a Windows computer that uses a Windows DNS server supporting dynamic DNS (the default DNS server configuration), the DNS server has a host entry for each IP address assigned to the computer.

Configuring the Default Gateway Almost all IP address configurations require a default gateway address. The default gateway, which is usually a router or a computer configured to act as a router, tells the computer where packets destined for another network should be sent. By definition, the default gateway's address must have the same network ID as the host's network ID.

You can configure multiple default gateways in the Advanced TCP/IP Settings dialog box, and then Windows attempts to select the gateway with the best metric automatically. The **metric** is a value assigned to the gateway based on the speed of the interface used to access the gateway. Multiple gateways provide fault tolerance to a computer, so if the primary default gateway is no longer responding, Windows switches to another gateway. By using a new feature in Windows Server 2008 and Vista called fail-back, Windows attempts periodically to communicate with the original default gateway. If the original gateway comes back online, Windows switches back to it.

Using Multihomed Servers A multihomed server has two or more NICs, each attached to a different IP network. Each NIC is assigned a network connection and requires its own

IP address for the network to which it's connected. This type of configuration can be used in the following situations:

- A server is accessed by internal clients (clients on the network) and external clients (clients on the Internet or an extranet). For example, you have a server for services such as file and print sharing, DHCP, and DNS that also acts as a public Web server.
- A server provides resources for computers on multiple subnets of the network. Interfaces can be configured for each subnet, which provides more throughput than is possible with a single NIC.
- A server is configured as a router or VPN server. Both functions require multiple NICs.

For network connections to a LAN, Windows uses names such as Local Area Connection, Local Area Connection 2, and so forth, which aren't very descriptive. Renaming each network connection to describe the network it connects to is recommended. For example, if a server is connected to internal and external networks, you might name one connection LAN-Internal and the other LAN-External. If the server is connected to two internal networks, you could use the network address in the names, such as LAN-172.31 and LAN-172.16. To rename a connection, right-click it in the Network Connections window and click Rename.

When a server is multihomed, it's usually connected to two physical as well as logical networks. Each physical network likely has a router. Simply configuring a default gateway for each interface might be tempting. However, Windows always chooses only one default gateway for sending packets to remote networks. For example, a server could receive a packet through an interface connected to the internal network and send the reply to the default gateway on the external network. You probably don't want this to happen. To solve this problem, you can use the Route command, explained in the next section.

Using the Route Command Windows computers maintain a routing table that dictates where a packet should be sent, based on the packet's destination address. The Route command-line program enables you to display and alter the routing table's contents. Figure 8-8 shows partial results of the Route Print command, which displays the contents of the routing table.

IPv4 Route Table					
Active Routes:					
Network Destination	Netmask	Gateway	Interface	Metric	
0.0.0.0	0.0.0.0	172.31.1.250	172.31.210.10	11	
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306	
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306	
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306	
172.31.0.0	255.255.0.0	On-link	172.31.210.10	266	
172.31.210.10	255.255.255.255	On-link	172.31.210.10	266	
172.31.255.255	255.255.255.255	On-link	172.31.210.10	266	
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306	
224.0.0.0	240.0.0.0	On-link	172.31.210.10	266	
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306	
255.255.255.255	255.255.255.255	On-link	172.31.210.10	266	
Persistent Routes:					
Network Address	Netmask	Gateway Address	Metric		
0.0.0.0	0.0.0.0	172.31.1.250	1		

Figure 8-8 Results of the Route Print command

The results of the Route Print command are displayed in five columns. The first column, Network Destination, is a network number against which an IP packet's destination address is compared. The Netmask column displays the subnet mask associated with the network destination. The Gateway column is the address of the router where packets with a destination address matching the network destination should be forwarded. The Interface column is the address of the NIC the packet should be sent through to reach the gateway. The Metric column is the value assigned to the route. If the routing table contains two or more entries that can reach the same destination, the one with the lowest metric is chosen.

In Figure 8-8, notice the network destination of 0.0.0.0 with a netmask of 0.0.0.0. This entry indicates the default route or default gateway. A packet with a destination address that doesn't match any entries in the routing table is forwarded to the gateway address in the default route entry, in this case 172.31.1.250. A gateway specified as On-link simply means the network destination is a network connected directly to one of the computer's interfaces. All Network Destination entries beginning with 127 indicate the computer's loopback address, which means "this computer." The Network Destination entries starting with 224 are multicast addresses, and entries starting with 255 are broadcast addresses. All packets with a multicast or broadcast destination address are sent to the local network, not to a router.

The Route command can be used to change the routing table. For instance, a multihomed computer might have two or more possibilities for a default gateway. Best practices dictate configuring only one interface with a default gateway. However, suppose you have a server connected to two networks: 192.168.1.0/24 and 172.16.208.0/24. The 192.168.1.0 network connects to the Internet, and the 172.16.208.0 network is part of the internal network and is also connected to networks 172.16.200.0/24 through 172.16.207.0/24. In addition, the 192.168.1.0 network has no possible way to get to the 172.16 networks. If your default gateway is configured on the 192.168.1.0 network (as it should, because it's connected to the Internet), when your server replies to a packet from the 172.16.200.0 to 172.16.207.0 networks, it sends the reply to the 192.168.1.0 interface because that's where the default gateway is. Remember that, by default, the routing table contains entries only for networks the computer is directly connected to plus the default route. So the server doesn't have an entry for the 172.16 networks, except 172.16.208.0. Any packets sent to these networks go to the default gateway, which can't deliver them to the destination network. To solve this problem, you can add routes to the routing table by using the following command:

```
Route add 172.16.200.0 mask 255.255.255.0 172.16.208.250
```

This command creates a routing table entry for the 172.16.200.0 network with the subnet mask 255.255.255.0 and the gateway 172.16.208.250, which is the router on your server's network. You could make eight entries, one for each remote network, or a single entry, as shown:

```
Route add 172.16.200.0 mask 255.255.248.0 172.16.208.250
```

This entry consolidates networks 172.16.200.0 through 172.16.207.0 into a single entry by using a modified subnet mask, a technique called supernetting.



You can find a good article on supernetting at http://articles.techrepublic.com.com/5100-10878_11-5034906.html.

IP Configuration Command-Line Tools

Several other command-line tools are available to help you troubleshoot, display, and configure IP addresses and related TCP/IP settings on a Windows computer. This section examines the following tools:

- Ping
- Ipconfig
- Arp
- Tracert
- Nslookup

A number of additional network configuration and troubleshooting tools are available, but they are used most commonly to verify correct IP configuration settings and connectivity.

The Ping Command You have used Ping to test connectivity between two computers. Ping sends an ICMP Echo Request packet to the destination IP address specified in the command.

If the destination computer receives the ICMP Echo Request, it replies with an ICMP Echo Reply packet. When the computer receives the reply packet, the Ping program displays a message similar to this one:

```
Reply from 192.168.100.201 bytes=32 time=<1ms TTL=128
```

In this output, the IP address is the address of the computer that sent the reply. The bytes=32 parameter specifies how many data bytes are in the ICMP message. You can change the number of data bytes with options in the Ping command. The time=<1ms parameter indicates that the reply took less than a millisecond from the time the ICMP Echo Request was sent. The TTL=128 indicates the message's time to live, which specifies how many routers a packet can go through before the packet should be expired and discarded. At each router, the TTL is decremented. If the TTL reaches 0, the router sends the source computer a message indicating that the TTL expired before reaching its destination.

To see the options available with the Ping command, type Ping /? at a command prompt. Some of the options are as follows:

- -t—Sends ICMP Echo Request packets continually until you press Ctrl+C to stop. By default, Ping sends four packets.
- -a—Tries to resolve the IP address to a hostname. If the name can be resolved, it's printed in the first line of the Ping output.
- -n *count*—The *count* parameter is the number of Echo Request packets to send.
- -l *size*—The *size* parameter is the number of data bytes to send in each Echo Request packet. The default is 32 bytes.
- -i *TTL*—*TTL* is the number of routers the packet can go through on the way to the destination before the packet should be expired.



The Ipconfig Command As you've learned in previous chapters, Ipconfig is usually used to display a computer's IP address settings but can perform other tasks, depending on the options specified:

- No options—Displays the basic IP configuration, including the IP address, subnet mask, and default gateway.
- /all—Displays extended IP configuration information, such as the computer name, domain name, network adapter description, physical (MAC) address, whether DHCP is used, and DNS address.
- /release—Releases its IP address back to the DHCP server if DHCP is used. If the address is released, the computer is assigned the invalid address of 0.0.0.0.
- /renew—Renews the IP address configuration lease.
- /displaydns—Windows caches the most recent DNS lookup request results, and this option displays the contents of the local DNS cache. If a computer recently did a DNS lookup for *www.yahoo.com*, for example, it keeps that information in local memory so that the next time the address is needed, a DNS query is unnecessary.
- /flushdns—Deletes cached DNS information from memory. This option can be useful if a computer's IP address or hostname was changed recently, and the cache contains obsolete information.
- /registerdns—Requests new DHCP leases and registers these names again with a DNS server.

The Arp Command The Arp command displays or makes changes to the Address Resolution Protocol (ARP) cache, which contains IP address–MAC address pairs. As discussed, when an IP packet is sent to a destination on the local network, the sending device must have the destination's MAC address. The source computer retrieves the MAC address by sending a broadcast ARP request packet to the local network. The ARP request packet essentially asks “Who has IP address A.B.C.D?” The computer on the local network that's assigned

the IP address sends an ARP reply message containing its MAC address. When a computer learns another computer's MAC address, it keeps the address in its ARP cache temporarily so that it doesn't have to send another ARP request packet to communicate with that computer again. Entries in the ARP cache are kept for only a few minutes to prevent them from becoming obsolete. Some options for the ARP command are as follows:

- -a, -g—Displays the contents of the ARP cache. These options perform the same function.
- -d—Deletes the entire contents of the ARP cache or a single entry specified by IP address. This option can be useful if a computer's NIC has changed recently, and the cache contains obsolete information.
- -s—Adds a permanent entry to the ARP cache by specifying a host's IP address and MAC address. This option should be used only if the address of a frequently accessed computer is unlikely to change. Remember: If the NIC is changed on a computer, its MAC address changes as well.

The Tracert Command Tracert is usually called “trace route” because it displays the route packets take between two computers. Tracert displays the address or DNS name of each router a packet travels through to reach the specified destination. It then sends a series of three ICMP Echo Request packets with a TTL value starting at 1 and increases the value until the destination is reached. Each router a packet encounters along the way to the destination decrements the TTL value by 1. If the TTL value reaches 0, the router sends a TTL-expired message back to the sending computer and drops the packet. When Tracert receives the TTL-expired message, it records the sending router's IP address and the time to receive a reply and displays that information. Next, a new series of three ICMP Echo Request packets are sent with an incremented TTL value. This procedure continues until all routers between the source and destination have been recorded.

Tracert is useful for troubleshooting the routing topology of a complex network and finding the bottleneck between a computer and a destination network. Because Tracert displays the time it took to receive a reply from each router, a router (or the link to this router) showing an inordinately long delay might be where the bottleneck lies.

The Nslookup Command Nslookup is used to test and troubleshoot DNS operation and can be used in command mode or interactive mode. In command mode, you type “nslookup *host*”; *host* is the name of a computer in the local domain or a fully qualified domain name. Nslookup replies with the specified host's IP address. By default, Nslookup uses the DNS server address configured in the IP address settings. Following are some examples of using Nslookup in command mode:

```
nslookup server99
nslookup www.yahoo.com
nslookup www.google.com 172.31.1.200
```

The first two commands query the default DNS server. The last command queries a DNS server at address 172.31.1.200. Because you can specify a different DNS server, you can compare the results of different DNS servers to verify correct DNS operation.

To use interactive mode, just type “nslookup” at the command prompt, and nslookup displays which server it's using to perform lookups. You can type a question mark at the interactive mode prompt to get a list of available options and commands.



Activity 8-3: Configuring a Second IP Address

Time Required: 15 minutes

Objective: Add a second IP address to your server.

Description: You want to test configuring multiple IP addresses on a server.

1. Log on to your server as Administrator, if necessary.
2. Click the **Network Connections** icon on the Quick Launch toolbar.

3. Right-click **Local Area Connection** and click **Properties**. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
4. In the Properties dialog box, click the **Advanced** button to open the Advanced TCP/IP Settings dialog box. Under the IP addresses list box, click **Add**. Type **192.168.100.XX** for the IP address and **255.255.255.0** for the subnet mask. Click **Add**, click **OK** twice, and then click **Close**.
5. Open a command prompt window. Type **ipconfig** and press **Enter**. You should see two IPv4 address and subnet mask entries.
6. Log on to the domain from your Vista computer as Administrator.
7. Open a command prompt window, and type **ping -a 192.168.100.2xx** and press **Enter**. Type **ping -a 192.168.100.XX** and press **Enter**. The -a option tells the Ping command to try to resolve the address to the computer name. In both instances, your server name should have been returned.
8. Type **ping serverXX** and press **Enter**. There's no telling which address will be used in the ping. When you ping the server name, a DNS lookup is performed, and DNS returns a list of all addresses configured for this host. The first one in the list is the address Ping uses. DNS rotates the order in which it lists addresses when more than one entry exists for a hostname.
9. Type **ipconfig /displaydns** to display the local DNS cache. You see both IP address entries for your server.
10. Type **ipconfig /flushdns** to delete the local DNS cache. Try pinging serverXX again. If Ping uses the same address as in Step 9, try flushing the DNS cache again and then pinging again. Eventually, you should get the other IP address in the Ping output because DNS rotates the order in which it sends the addresses.
11. Type **nslookup serverXX** and press **Enter**. Nslookup should display both IP addresses configured for serverXX.
12. Stay logged on to your Vista computer with the command prompt window open for the next activity.



Activity 8-4: Using the Arp Command

Time Required: 10 minutes

Objective: Use the Arp command to display and delete ARP entries.

Description: You want to see how the Arp command-line program works, so you display the ARP cache, and then delete its contents. Next, you use the Ping and Arp commands to see the difference between pinging a computer on a local and a remote network.

1. If necessary, log on to the domain from your Vista computer as Administrator, and open a command prompt window.
2. Type **arp -a** and press **Enter**. You should see a few entries. Those listed as static in the Type column are created automatically by Windows. The dynamic entries are a result of your computer having recently sent an Arp request message for the specified IP address. Note that these Arp messages are sent automatically by your computer whenever it needs to get another computer's MAC address, such as when your Vista computer needs to contact the domain controller when you log on.
3. Type **arp -d** and press **Enter**. Type **arp -a** and press **Enter**. The -d option deletes the ARP cache. After the second command, you might get the message "No ARP Entries Found," or you might see an entry or two if your computer tried to contact another computer in the time between the two Arp commands.
4. Type **arp -d** and press **Enter** to clear any recently acquired entries, and then immediately type **ping serverXX** and press **Enter**. Type **arp -a** and press **Enter** again. You should see an ARP entry for your server.

5. Type **arp -d** and press **Enter**, and then type **ping www.yahoo.com** and press **Enter**. Type **arp -a** and press **Enter**. The ARP cache should have at least two dynamic entries: One is your server's IP address, and the other should be for your default gateway address. Notice that there's no ARP entry for the address of www.yahoo.com. The entry for your server exists because your computer had to do a DNS lookup for www.yahoo.com and, therefore, had to get your server's MAC address because your server is also the DNS server. The entry for your default gateway exists because the Ping packet had to be sent to your router to reach the network where www.yahoo.com is located. Remember, the MAC address is used to deliver a packet to a device only on the local network, whether the device is a computer or a router.
6. Stay logged on to your Vista computer and leave the command prompt window open for the next activity.



Activity 8-5: Using the Tracert Command

Time Required: 10 minutes

Objective: Use the Tracert command.

Description: Internet access has been slow, so you use the Tracert command to try to determine where the bottleneck is. This activity requires Internet access.

1. If necessary, log on to the domain from your Vista computer as Administrator, and open a command prompt window.
2. Type **tracert serverXX** and press **Enter**. Because there are no routers between your Vista computer and your server, you should get only one response line of output. Notice that three times are displayed because Tracert sends three packets for each TTL value it uses. By sending three packets, you can average the times to get a more accurate picture of the response time.
3. Type **tracert www.yahoo.com** and press **Enter**. Some router hops include a name with the router's address, and you can sometimes use this name to get an idea of the router's geographical location or ISP.
4. To speed up Tracert's results, you can tell it not to do router name lookups. Type **tracert -d www.yahoo.com** and press **Enter**. The results are displayed considerably faster, especially if you're several router hops away from www.yahoo.com.
5. Close the command prompt window, and log off Vista.

Managing Protocols

Each network connection in Windows Server 2008 has protocols and services associated with it. Figure 8-9 shows the Properties dialog box for a typical network connection. Beside each installed service or protocol is a check box. If the check box is selected, the service or protocol is bound (meaning it's enabled) to the network connection. If the check box is not selected, the service or protocol isn't bound to the connection. Unbinding an item from a network connection doesn't affect the service or protocol's operation if it's bound to another network connection. The items listed in Figure 8-9 are default services and protocols installed for every local area connection in Windows Server 2008 and Vista. Following is a description of each protocol or service:

- **Client for Microsoft Networks**—This service allows the computer to access Windows shared resources by using Server Message Block (SMB). SMB is the default file and printer sharing protocol in Windows. If this service is disabled on the network connection, the computer can't access shared resources on other computers by using that network connection.
- **QoS Packet Scheduler**—This service allows an application to reserve network bandwidth for high-priority traffic. Typically, the computer uses 100% of available bandwidth if running applications require it. If a video-conferencing application, for example, is running along with file transfers, Internet traffic, and so forth, video-conferencing performance could suffer if it gets only 5% or 10% of the total bandwidth. Using QoS, the video-conferencing application can reserve bandwidth, ensuring that it can operate at a satisfactory

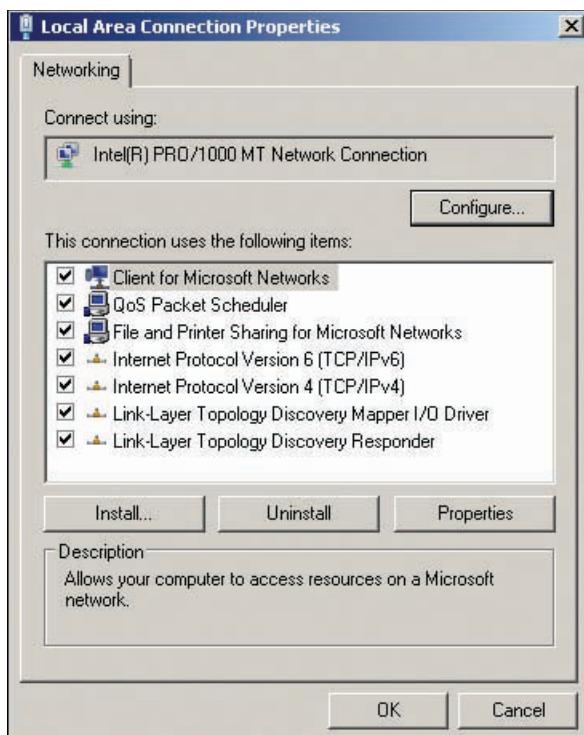


Figure 8-9 The Local Area Connection Properties dialog box

performance level. By default, QoS Packet Scheduler allows reserving up to 20% of the bandwidth. This value can be changed in a computer's local group policy or with a domain GPO in the Computer Configuration\Administrative Templates\Network\QoS Packet Scheduler node.

- *File and Printer Sharing for Microsoft Networks*—This service, the complement to Client for Microsoft Networks, allows a computer to host shared resources that are accessible by computers using Client for Microsoft Networks. Unbinding this service from a network connection effectively prevents client computers from accessing shared folders or printers through that connection. For security reasons, users whose computers have connections to both a private and public network should usually disable File and Printer Sharing for Microsoft Networks on the connection to the public network.
- *Internet Protocol Version 6 (TCP/IPv6)*—IPv6, the eventual successor to IPv4, is installed by default in Windows Server 2008 and Vista, but if your network does not use it, disabling it on your network connections is safe. IPv6 is discussed later in “Internet Protocol Version 6.”
- *Internet Protocol Version 4 (TCP/IPv4)*—IPv4 remains the most widely used protocol on networks. Until IPv6 replaces it as the standard protocol on LANs and the Internet, this protocol should be bound to your network connections.
- *Link-Layer Topology Mapper I/O Driver*—The LLTD protocol is used to build the network map in the Network and Sharing Center. On network connections where you don't want to create a network map, you can unbind this protocol safely.
- *Link-Layer Topology Discovery Responder*—LLTD responds to requests from the LLTD Mapper I/O Driver so that a computer running this protocol can be placed on a network map. This protocol is installed by default in Vista and Windows Server 2008 and can be downloaded and installed on Windows XP computers so that they can appear on a map. On network connections where you don't want the computer to appear on a map, you can unbind this protocol safely.



Activity 8-6: Disabling Services

Time Required: 15 minutes

Objective: Disable the File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks services.

Description: You want to see the effect of disabling networking services on your client and server.

1. Log on to your server as Administrator, if necessary.
2. Click the **Network Connections** icon on the Quick Launch toolbar.
3. Right-click **Local Area Connection** and click **Properties**. Click to clear the **File and Printer Sharing for Microsoft Networks** check box, and then click **OK**.
4. First, log off Vista and restart before you continue with this step. Then log back on to the domain from your Vista computer as Administrator, and open the Network and Sharing Center. Click **View computers and devices** in the Tasks section. Notice that ServerXX is listed. Unbinding File and Printer Sharing doesn't prevent the server from being discovered. Double-click **ServerXX**.
5. After a while (possibly a minute or more), you should get a Network Error message stating that Windows can't access \\serverXX (see Figure 8-10). Click the **Diagnose** button to run Windows Network Diagnostics, which attempts to identify the problem. Windows Network Diagnostics should determine that although the server is online, it's not responding to requests (see Figure 8-11). This tool also suggests that a firewall is blocking the connection. This diagnosis is incorrect, but unbinding the service from the interface has the same effect as a firewall. Click **Cancel**.

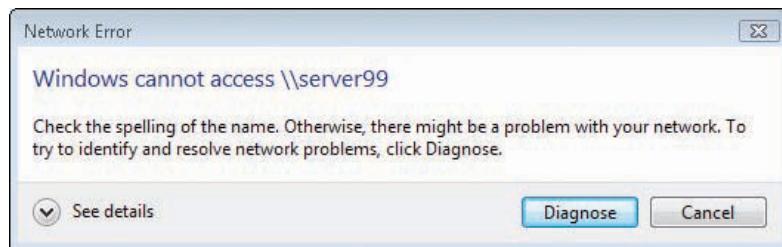


Figure 8-10 A Network Error message



Figure 8-11 A Windows Network Diagnostics message

6. On your server, open the Local Area Connection Properties dialog box, click the **File and Printer Sharing for Microsoft Networks** check box to reenable this service, and then click **OK**.
7. On your Vista computer, try again to access **\ServerXX**. You should see a list of shared folders and printers on ServerXX. If the folders aren't displayed immediately, close the Explorer window and try again. It might take several attempts before the folders appear.
8. Close all open windows on Vista and your server. *Log off Vista and log back on*. You must log off to clear any open connections with your server, which is necessary for the next steps.



If logging off Vista doesn't seem to have cleared open connections, restart your Vista computer.

9. On your Vista computer, open the Network Connections window and then the Local Area Connection Properties dialog box. Click to clear the **Client for Microsoft Networks** check box, and then click **OK**.
10. Click **Start**, type **\ServerXX** in the Start Search text box, and press **Enter**. The Network Error message should be displayed. Click **Diagnose**. Unfortunately, Windows Network Diagnostics is unable to determine the problem. Click **Cancel**.
11. Open the Local Area Connection Properties dialog box. Click to enable the **Client for Microsoft Networks** check box again, and then click **OK**.
12. Try again to access **\ServerXX**. You should see the list of shared folders and printers.
13. Close all open windows and log off Vista.



Network Bindings By default, every installed service and protocol is bound to every network connection. As you have seen, however, you can disable bindings on a network connection. When you have multiple network adapters and, therefore, multiple network connections, you might also need to change the order in which adapters and protocols are bound to network services. For example, you have both IPv4 and IPv6 installed and bound to a network connection, the default configuration in Windows Server 2008 and Vista. When you attempt to access a Windows share on another computer using Client for Microsoft Networks, Windows sends the request by using all protocols bound to Client for Microsoft Networks. However, Windows waits until it receives a response from the highest priority protocol before continuing.

To see why, examine Figure 8-12. Client for Microsoft Networks has both IPv4 and IPv6 bound to it. IPv4 is listed first, so it's the highest priority protocol. Even if a response is received from IPv6 first, Windows waits for a response from IPv4 or until it times out. For now, this is probably what you want because IPv4 is likely your predominant protocol. Suppose your network switches over to IPv6, however, and some of the servers have disabled IPv4. Everything still works, but there might be a noticeable delay because Client for Microsoft Networks times out waiting for a response from IPv4 before it uses the response from IPv6.

Fortunately, you can reorder protocol bindings by simply selecting the protocol whose order you want to change and clicking the up or down arrows you see in the Adapters and Bindings tab in Figure 8-12. Binding order applies to network connections as well. Looking at Figure 8-12 again, two Local Area Connections are configured on this computer. When a service attempts to access a network resource or respond to a resource request, the network connections are prioritized in the order shown. If the connections aren't listed in the order of primary use, you should change the order by clicking the up or down arrow.



NOTE To open the Advanced Settings dialog box for network connections, click Advanced, Advanced Settings from the menu in the Network Connections window. To enable the menu bar on a Vista computer, you must click Organize on the toolbar, point to Layout, and click Menu Bar.

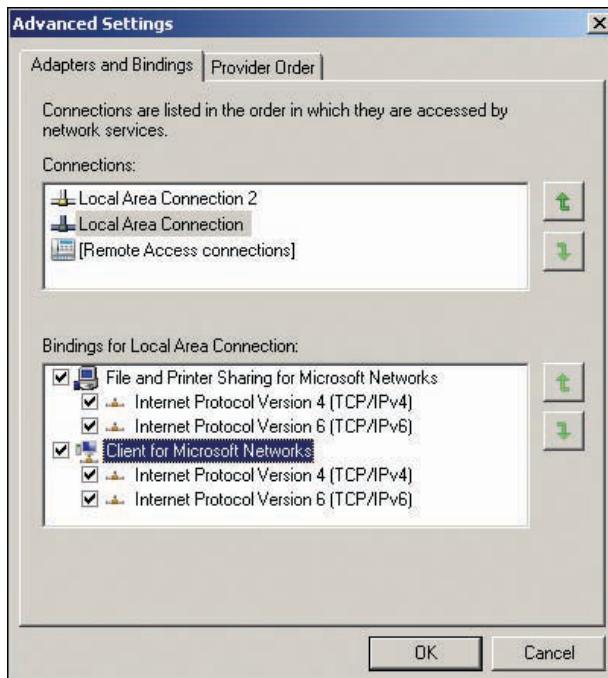


Figure 8-12 The Advanced Settings dialog box for network connections

Network Providers A **network provider** is a software component that allows Windows applications to connect to resources on other computers. Connecting to resources on different OSs might require different procedures and, therefore, different network providers. There are network providers for Windows networks, virtual networks (such as VMware), Novell networks, Linux networks, and so forth, and each one performs actions, such as making and breaking connections, specific to the network type. When a network resource is requested, Windows attempts to access it in the order in which installed network providers are listed (see Figure 8-13). For example, a network resource, such as \\server\share, could be hosted on a Windows server, a

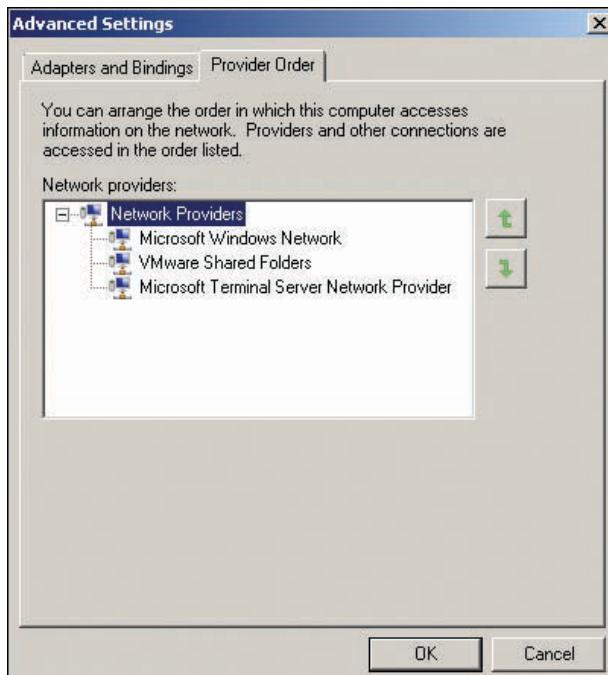


Figure 8-13 The Provider Order tab

Novell server, or another server. To prevent timeout delays, the most frequently used network type should be first in the provider order list.



Activity 8-7: Changing the Binding Order

Time Required: 15 minutes

Objective: Change the binding order for installed protocols.

Description: You will be changing to IPv6 as your primary protocol soon, so you want to see how to set IPv6 as the highest priority protocol. You also need to support the Network File System (NFS) on Linux and UNIX network clients, so you want to install a new provider and see how changing the provider order affects resource access.



To add Services for NFS, you must be running Vista Ultimate Edition or Vista Enterprise Edition.



1. Log on to your server as Administrator, if necessary.
2. Open the Network and Sharing Center, and click the **Manage network connections** link under Tasks.
3. In the Network Connections window, click **Advanced, Advanced Settings** from the menu. Click the **Adapters and Bindings** tab, if necessary.
4. To change the binding order, in the Bindings for Local Area Connection list box, click **Internet Protocol Version 6 (TCP/IPv6)** under File and Printer Sharing for Microsoft Networks, and then click the green up arrow. You don't want this change to remain, so click **Cancel**.
5. Log on to the domain from your Vista computer as Administrator.
6. Next, you're going to install a new provider for NFS. Click **Start, Control Panel**, and click **Programs** and then click **Programs and Features**.
7. Click the **Turn Windows features on or off** link under Tasks. In the Windows Features list box, click to expand **Services for NFS**. Click the **Client for NFS** check box, and then click **OK**. After Client for NFS is installed, close the Programs and Features applet.
8. Open the Network Connections window. By default, Vista hides the menu bar. Click **Organize**, point to **Layout**, and click **Menu Bar**.
9. Click **Advanced, Advanced Settings** from the menu, and then click the **Provider Order** tab. The NFS Network provider should be listed last. Leave this dialog box open.
10. As a test, click **Start**, type **\serverXX\shared** in the Start Search text box, and press **Enter**. Time how long it takes for the Explorer window to open the share.
11. After the share opens, close it. In the Advanced Settings dialog box, click **NFS Network**. Click the up arrow until NFS Network is listed first in the provider order, and then click **OK**.
12. Open the **\serverXX\shared** share again and time how long it takes to open it. Depending on a number of factors, opening the share will probably take longer this time because the NFS Network provider is attempted before the Microsoft Windows Network provider.
13. Change the provider order so that **Microsoft Windows Network** is first in the list and **NFS Network** is last. Close all open windows on your Vista computer and server, but stay logged on to Vista.

Internet Protocol Version 6

A number of improvements have been made in TCP/IP since Windows Server 2003 and XP. For example, Windows Server 2003 and XP use a dual-stack architecture, in which IPv4 and IPv6 use separate implementations of the complementary protocols in the TCP/IP suite such as TCP and UDP. This type of implementation led to a more complex configuration and operation of IPv6 in these OSs.

Windows Server 2008 and Vista use **dual-IP layer architecture**, which means the IP protocol is the only component of the TCP/IP suite that's different in IPv6. IPv4 and IPv6 share the common components of the suite (see Figure 8-14). This architecture results in improved reliability and performance in TCP/IP.

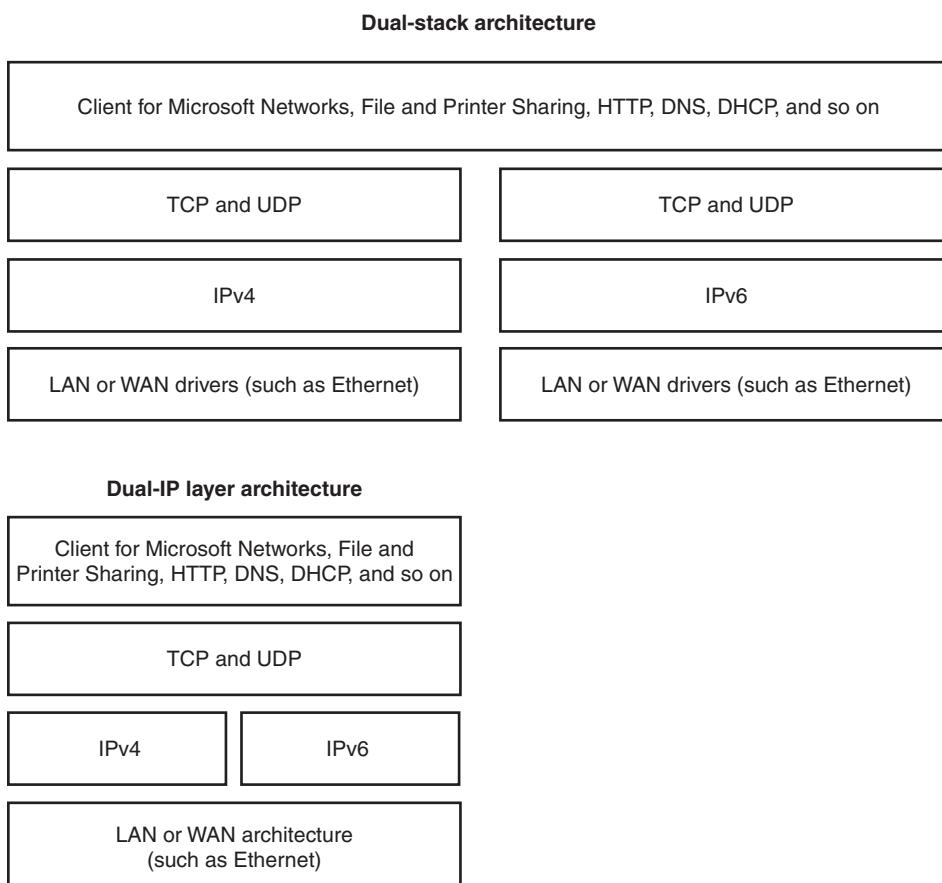


Figure 8-14 Dual-stack versus dual-IP layer architecture

IPv6 Overview

The Internet Engineering Task Force (IETF) developed IPng (IP next generation) in 1994, which was later named IPv6. IPv6 was developed to address IPv4's shortcomings. Some improvements and changes in IPv6 include the following:

- *Larger address space*—Recall that IPv4 addresses are 32 bits, which provide a theoretical four billion addresses. IPv6 addresses are 128 bits, so the number of possible addresses can be expressed as 34 followed by 37 zeros, or 340 trillion trillion trillion. It's probably safe to say that running out of IPv6 addresses is unlikely.
- *Hierarchical address space*—Unlike IPv4, in which numbers in the IP address have little meaning other than the address class and the network and host IDs, IPv6 addresses have a more defined structure. For example, the first part of an address can indicate the ISP.
- *Autoconfiguration*—IPv6 can be self-configuring or autoconfigured from a router running IPv6 or through DHCPv6.
- *Built-in Quality of Service (QoS) support*—IPv6 includes built-in fields in packet headers to support QoS strategies without requiring the installation of additional protocol components, as IPv4 does.
- *Built-in security*—In designing IPv6, security was considered from the beginning, whereas to achieve secure communication in IPv4, add-on protocols are required.

IPv6 Address Structure The good news with IPv6 is that subnetting as done in IPv4 will be a thing of the past. The bad news is that you still need to work with binary numbers, and with 128 bits in the address, there are quite a few new things to learn.

IPv6 addresses are written as eight 16-bit hexadecimal numbers separated by colons. For example, a valid IPv6 address looks like this:

fe80:0:0:0:18ff:0024:8e5a:60

There are a couple of things to note in this address:

- IPv6 addresses often have several 0 values. One or more consecutive 0 values can be written as a double colon (::), so the preceding address can be written as fe80::18ff:0024:8e5a:60. However, you can have only one double colon in an IPv6 address.
- Leading 0s are optional. The value 0024 in the previous example could just as easily have been written as 24, and the value 60 could have been written as 0060.

In Windows, when you view an IPv6 address in the network connection's Status dialog box or after using Ipconfig, you see a percent sign followed by a number at the end of the address. The number following the percent sign is called the global routing prefix, or just prefix. The prefix specifies how many bits of the IPv6 address identify the network, as it does with an IPv4 address. If your computer has IPv6 enabled and is self-configuring, your IPv6 address probably starts with fe80 and ends with /10 or /16. Addresses that start with fe80 are called **link-local addresses** and are self-configuring. Link-local addresses can't be routed and are somewhat equivalent to Automatic Private IP Addressing (APIPA) in IPv4. Link-local addresses can be used for computer-to-computer communication in small networks where no routers are needed, but more often, they are simply one step in the process toward autoconfiguration by a router or DHCPv6 server.



The IPv6 Host ID The host ID of an IPv6 address is typically 64 bits and uses the interface's MAC address to make up the bulk of the address. Because a MAC address is only 48 bits, the other 16 bits come from the value FF-FE inserted after the first 24 bits of the MAC address. In addition, the first two zeros that compose most MAC addresses are replaced with 02. For example, given the MAC address 00-0C-29-7C-F9-C4, the host ID of an IPv6 address is 02-0C-29-FF-FE-7C-F9-C4. This autoconfigured 64-bit host ID is referred to as an Extended Unique Identifier (EUI)-64 interface ID.

By default, Windows Server 2008 and Vista don't use EUI-64 interface IDs when configuring the link-local address. Instead, they create random interface IDs when autoconfiguring an interface address. However, you can configure Windows Server 2008 and Vista to use the EUI-64 interface address by using the following command:

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

You might wonder if there's an equivalent for the IPv4 loopback address of 127.0.0.1. There is, and it's ::1. If you expanded this address, you would have 0:0:0:0:0:0:1.



Activity 8-8: Working with IPv6

Time Required: 15 minutes

Objective: Use Ipconfig and Ping with IPv6, and change the IPv6 interface address.

Description: Your company has plans to move to IPv6. Because you haven't used IPv6 before, you want to become comfortable with using common tools, such as Ipconfig and Ping.

1. Log on to your domain from your Vista computer as Administrator, if necessary.
2. Open a command prompt window.
3. Type **ipconfig** and press **Enter**. Find the output line starting with "Link-local IPv6 Address." Notice that the assigned address starts with fe80:: (assuming your network doesn't have an IPv6-configured router). The fe80 indicates a link-local IPv6 address, and the :: indicates a

string of 0 values—in this case, a string of three consecutive 0 values. The rest of the address (64 bits) has been randomly assigned by Windows.

4. Type **ping ::1** and press **Enter**. Windows replies because you just pinged your own computer. Type **ping -a ::1** and press **Enter**. The -a option tells Windows to display the hostname for the ::1 address, which is the name of your Vista computer.
5. Type **ping -6 serverXX** and press **Enter**. The -6 option tells Ping to use IPv6 addresses. You should receive a reply from your server. Now ping your server by using the IPv6 address the previous ping replied with. You can include the %8 at the end of the address or omit it.
6. Type **getmac** and press **Enter** to display your computer's MAC address. Make a note of this address.
7. Type **netsh interface ipv6 set global randomizeidentifiers=disabled** and press **Enter**.
8. Type **ipconfig** and press **Enter**. Notice that the last 64 bits of the IPv6 address now look like your MAC address, with the addition of FF-FE after the first 24 bits and 02 instead of the first 00 of your MAC address.
9. Close the command prompt window, and log off.

Subnetting with IPv6 Although subnetting as done in IPv4 will be a thing of the past, it doesn't mean subnetting won't be used at all in IPv6 networks. Typically, ISPs allocated IPv4 addresses to businesses in groups specified by a network address and IP prefix. ISPs try to give a business only the number of addresses it requires. However, with IPv6 having such a large address space, most address allocations will have a /48 prefix, even for small home networks. This means the network ID is 48 bits, and the network administrator has 80 bits for assigning subnets and host IDs. Because the host ID is 64 bits, 16 bits are left for creating subnets. This number of bits allows for 65,536 subnets, more than enough for all but the largest organizations. Large conglomerates can get multiple /48 prefix addresses or /47 prefix addresses, which provide more than 130,000 subnets. A typical IPv6 address, then, as assigned by an ISP looks like Figure 8-15.

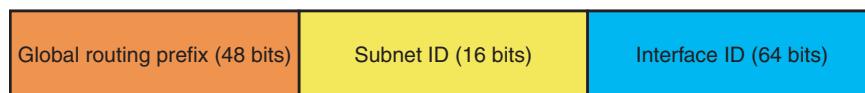


Figure 8-15 Structure of a typical IPv6 address

With 16 bits available to subnet, there are many strategies you can use. A small network that doesn't have multiple subnets can simply leave the subnet ID as all 0s, for example, and an address in this situation might look like this:

2001:DB8:A00:0000:020C:29FF:FE7C:F9C4/64

This address begins with 2001:DB8, which is not random. The IPv6 developers realized that people will be writing about how to work with IPv6, so instead of authors using random values for examples, they reserved 2001:DB8 for use in documentation. The A00 in the address is the last 16 bits of the network prefix and was randomly chosen for this example. The 0s following the A00 are the subnet ID, and the last 64 bits are the computer's interface ID. The /64 just indicates that the network portion of the address is the first 64 bits (network prefix plus subnet ID).

A network that does need to subnet could just take the 16 bits for the subnet ID and start counting. For example, a company could make the first three subnets as follows; the bold part of the address is the subnet ID, and the 64-bit interface ID has been omitted.

- 2001:DB8:A00:0000
- 2001:DB8:A00:0001
- 2001:DB8:A00:0002

Large organizations with multiple locations could take a more structured approach and assign each location a bank of subnets as in the following:

- 2001:DB8:A00:0000—Assigned to New York location
- 2001:DB8:A00:4000—Assigned to London location
- 2001:DB8:A00:8000—Assigned to Shanghai location

With this strategy, each location has 4000 hexadecimal subnet IDs to work with. For example, New York can make subnets 2001:DB8:A00:0000, 2001:DB8:A00:0001, 2001:DB8:A00:0002, and so forth, up to 2001:DB8:A00:3FFF. Put another way, each location can configure up to 16,384 subnets. As you can see, subnetting does still exist in IPv6, but it's a more straightforward process than in IPv4.



For more on IPv6, see <http://technet.microsoft.com/en-us/library/bb878121.aspx>.

Chapter Summary

- Windows Server 2008 and Vista have a new way of visualizing a computer's network connection: the Network and Sharing Center, where you can view the status of network connections and configure their properties. This window is organized into these sections: a network map, Sharing and Discovery, and Tasks.
- The network map is a visual representation of computers and connecting devices in your network. In the Sharing and Discovery section, you can enable and disable functions for network discovery, file sharing, public folder sharing, and printer sharing. The Tasks section has links to perform tasks such as viewing computers, connecting to a network, setting up a network connection, managing a network, and diagnosing network problems.
- TCP/IPv4, the predominant networking protocol in use today, is actually a suite of protocols and services, such as DNS, DHCP, TCP, IPv4, ICMP, and ARP, among others.
- TCP/IP communication usually involves a DNS lookup and an ARP request. ARP is used to get the MAC address for a computer or router to which a packet must be sent. ARP is used only to get the MAC address of devices on the same network as the computer sending the request.
- An IP address is a 32-bit dotted decimal number divided into four octets. Every IP address must have a subnet mask to indicate which part of the IP address is the network ID and which part is the host ID. There are three IP address classes: A, B, and C, each with a default subnet mask.
- Subnetting uses a modified subnet mask to divide a large network into smaller, more manageable networks. An IP network is referred to as a broadcast domain. Subnetting reduces the adverse effect of the many broadcasts in a large broadcast domain. Subnetting also conserves IP addresses by assigning to a company only the number of public IP addresses it requires.
- You can configure multiple IP addresses and default gateways on a network connection. A computer with two or more NICs is called a multihomed server. Multihoming can cause problems with internal routing on a computer, which can be fixed with the Route command.
- Several command-line tools are available for checking status and troubleshooting IP configuration, including Ping, Ipconfig, Arp, Tracert, and Nslookup.

- Several services and protocols are bound to a network connection by default, including Client for Microsoft Networks, QoS Packet Scheduler, File and Printer Sharing for Microsoft Networks, IPv6, IPv4, LLTD Mapper I/O Driver, and LLTD Responder. You can change the binding order of protocols, services, and network providers.
- IPv6 uses a 128-bit address expressed by 8 16-bit hexadecimal numbers separated by a colon. Some reasons for this new IP version are a larger address space, a hierarchical address space, autoconfiguration, built-in QoS, and built-in security.

Key Terms

dual-IP layer architecture The current implementation of IPv6 in Windows Vista and Server 2008. Both IPv4 and IPv6 share the other components of the stack; the dual-stack layer used by Windows XP and Server 2003 duplicates the other TCP/IP layers.

link-local address Similar in function to the IPv4 APIPA addresses, link-local IPv6 addresses begin with fe80, are self-configuring, and can't be routed.

metric A value assigned to the gateway based on the speed of the interface used to access the gateway.

network connection An icon in the Network Connections window that shows the components needed for the computer to connect to a network.

network discovery The process whereby a computer finds other computers on a network and allows other computers to find it.

network map A graphical view of the network from your computer's perspective. It includes your computer, the networks to which your computer is connected, other devices on the network, and the Internet.

network provider A software component that allows Windows applications to connect to resources on other computers.

octet An 8-bit value; a number from 0 to 255 that's one of the four numbers found in a dotted decimal IP address.

subnet mask A 32-bit dotted decimal number consisting of an unbroken series of binary 1s followed by an unbroken series of binary 0s; used with an IP address to determine the network ID.

Review Questions

1. Which of the following is needed if a computer with IP address 172.31.210.10/24 wants to communicate with a computer with IP address 172.31.209.122/24?
 - a. Hub
 - b. Router
 - c. Switch
 - d. a. or c.
2. A computer that wants to share a network resource should have which of the following installed?
 - a. Service
 - b. Client
 - c. Network discovery
 - d. LLTD Responder
3. The LLTD protocol must be installed and enabled for a computer to be discovered and listed in a network browse list. True or False?

4. You're setting up a new network connection and select Work as the location of the network to which you're connecting. Windows detects Windows Server 2008 running Active Directory on the network. Which type of network will be shown in the network map?
- Private
 - Public
 - Domain
 - Work
5. Which of the following is a reason that a computer might not appear in a network map? (Choose all that apply.)
- The computer is on a network designated as private.
 - The computer is running Windows Server 2003.
 - LLTD Responder is disabled.
 - LLTD Mapper I/O Driver is disabled.
6. If you turn on printer sharing in the Network and Sharing Center, all printers on the computer are shared. True or False?
7. You have just typed the commands ipconfig /flushdns and ping server1. Which of the following protocols is used first as a result of these commands?
- TCP
 - DNS
 - ICMP
 - DHCP
8. You have just completed a default installation of Windows Server 2008. You know that the TCP/IP protocol is installed. How does the server get assigned an IP address?
- TCP
 - DNS
 - ARP
 - DHCP
9. You have just typed the commands arp -d, ipconfig /flushdns, and nslookup server1, and your DNS server is on the same network as the computer from which you enter the commands. Which of the following protocols is used first as a result of these commands?
- TCP
 - DNS
 - ARP
 - DHCP
10. The IP address 10.240.0.0/8 is invalid. True or False?
11. Which of the following is a good reason to subnet an IPv4 network? (Choose all that apply.)
- Eliminate the need for ARP requests.
 - Decrease the size of the broadcast domain.
 - Allow broadcasts to reach more computers.
 - Conserve IP addresses.



12. Which of the following IP addresses has 12 bits in the host ID?
 - a. 172.31.21.12/16
 - b. 172.31.89.100/12
 - c. 12.49.127.88/8
 - d. 12.156.109.252/20
13. You have set up an e-mail server that needs to respond to e-mail requests using mail.coolgadgets.com and mail.niftytools.com in the request URL. How can you do this?
 - a. Install two NICs and assign the same IP address to both NICs. Configure DNS to map one MAC address to mail.coolgadgets.com and the other MAC address to mail.niftytools.com.
 - b. Configure two IP addresses on one NIC. Configure DNS to map one IP address to mail.coolgadgets.com and the other IP address to mail.niftytools.com.
 - c. Install two NICs and connect each one to a different network. Set up the router on each network to forward mail packets to the NIC bound to the correct URL.
 - d. Install two NICs and assign different IP addresses to each NIC, but make sure both IP addresses use the same network ID. Configure the NICs to use default gateways on different networks.
14. You have a server with two NICs, each attached to a different IP network. You're having problems communicating with devices on remote networks that send packets to one of the interfaces. The server receives the packets fine, but the server's replies never reach the intended destination network. Replies to packets that come in through the other interface seem to reach their destination without any problems. What can you do that will most likely solve the problem?
 - a. Configure a second default gateway on the interface exhibiting problems.
 - b. Change the default gateway to use the router that's on the network of the interface exhibiting problems.
 - c. Use the Route command to add routes to the networks that aren't receiving replies.
 - d. Replace the NIC that's having problems replying to packets.
15. You have just changed the IP address on a computer named Computer5 in your domain from 172.31.1.10/24 to 172.31.1.110/24. You were communicating with this computer from your workstation fine right before you changed the address. Now when you try the command "ping computer5" from your workstation, you don't get a successful reply. Other computers on the network aren't having a problem communicating with the computer. Which command might help solve the problem?
 - a. arp -d
 - b. ipconfig /flushdns
 - c. tracert computer5
 - d. ping -6 172.31.1.110
16. A user complains that opening NFS shares on his recently installed Linux computer from his Windows computer is taking an inordinately long time. Opening shares on Windows servers doesn't seem to take as long. He'll be using his Linux computer to store and back up files more often than he'll be accessing shares on Windows computers. What is a good course of action to improve the speed of opening Linux shares?
17. You're running the network map feature on your Windows Server 2008 machine. An older computer used by a colleague doesn't appear on the map, however. What could be the problem?
 - a. Your network connection isn't bound to the LLTD Responder protocol.
 - b. Your colleague's network connection isn't bound to the LLTD Mapper I/O Driver protocol.
 - c. Your colleague's computer is running Windows XP.
 - d. Your colleague's computer is running Windows Vista.

18. Which of the following is a benefit of using IPv6 rather than IPv4? (Choose all that apply.)
 - a. You can assign four times the number of addresses in IPv6.
 - b. Subnetting to conserve IP addresses is less of a concern.
 - c. Features to improve communication security and quality are built into IPv6.
 - d. IPv6 addresses are expressed as 16 8-bit numbers separated by colons, which are easier to read than dotted decimal notation.
19. Which of the following is a valid IPv6 address? (Choose all that apply.)
 - a. fe80:0:0:FEED::1
 - b. 2001:DB8:00AB:11:3344
 - c. fe80:DB8::EE::8901
 - d. 2001:DB8:BAD: F00D:0020:3344:0:e4
20. You want all 100 computers in your domain to have network discovery enabled. What's the best way to do this?
 - a. Configure a policy in the Computer Configuration\Policies\Administrative Templates\Network node to enable network discovery and link the GPO to the domain.
 - b. Send an e-mail to all users with detailed instructions on how to enable network discovery.
 - c. Write a script containing the command to enable network discovery and distribute it as a startup script by using a group policy.
 - d. Use Remote Desktop to configure the feature on all computers in the domain.



Case Projects



Case Project 8-1: Creating a List of MAC Addresses

You have been asked to create a list of all MAC addresses and corresponding IP addresses and computer names in your network. Propose at least two methods to accomplish this task. Your network has almost 100 computers in a Windows Server 2008 domain network with statically assigned IP addresses. Using the tools available in Windows Server 2008, implement the procedure you think will work best. Write a short report of your results and submit it to your instructor.

Case Project 8-2: Creating a GPO to Configure Network Settings

Create a GPO and perform any other required tasks that do the following for all computers in the domain:

- Enables network discovery
- Sets the IPv6 address to use the MAC address in its interface ID
- Enables all computers to be placed in a network map
- Sets QoS parameters to allow reserving up to 40% of network bandwidth

Write an explanation of how you accomplished each task and where you would link the GPO, print a report of the GPO settings, and submit both to your instructor. You don't need to actually configure the GPO (unless your instructor requires it), but you can do so to test it, if needed.

Case Project 8-3: IP Addressing Practice

Start your Web browser, and go to www.learntosubnet.com. Under IP Addressing, click View and Print Practice Problems link. Accept the EULA and print the page. Complete the exercises and turn in your work to your instructor.

Case Project 8-4: Using Additional Networking Tools

A number of network tools can help you troubleshoot a network, such as protocol analyzers and scanners. Find, download, and install the following tools on your Vista computer:

- Microsoft Network Monitor: Protocol analyzer and network monitoring tool (formerly available as an option to install in Windows but must be downloaded for Vista and Windows Server 2008)
- Netinfo 6.5: Trial version of a suite of networking tools, including a ping and port scanner

If necessary, use the help that comes with these tools to understand how they work and what you can do with them. Write a brief report explaining how these tools can be useful in understanding and troubleshooting network communication. Use Wireshark to capture all the packets generated by pinging your server from your Vista computer (using “ping serverXX”). Make sure you clear your ARP and DNS caches first. Print the first 10 packets captured.

Configuring DNS for Active Directory

After reading this chapter and completing the exercises, you will be able to:

- Describe the structure of Domain Name System
- Install and use the DNS Server role in Windows Server 2008
- Configure DNS zones
- Configure advanced DNS server settings
- Monitor and troubleshoot DNS

To function properly, Active Directory depends on a service to resolve computer names to addresses and to find computers that offer specific services. In fact, most network systems today would be almost unusable without a name-to-address translation system; without one, users and computers would need to know the address of each computer they communicate with. Because the TCP/IP suite is the default protocol for Windows, Domain Name System (DNS) is the default name resolution protocol for Windows computers. For Windows domain networks, DNS is required for operation. This chapter describes the structure of the worldwide DNS system, but the focus is on installing, configuring, and maintaining DNS in an Active Directory environment.

Introduction to Domain Name System

Domain Name System (DNS) is a distributed hierarchical database composed mainly of computer name and IP address pairs. A distributed database means that no single database contains all data; instead, data is spread out among many different servers. In the worldwide DNS system, data is distributed among thousands of servers throughout the world. A hierarchical database, in this case, means there's a structure to how information is stored and accessed in the database. In other words, unless you're resolving a local domain name for which you have a local server, DNS lookups often require a series of queries to a hierarchy of DNS servers before the name can be resolved.

The Structure of DNS

To better understand the DNS lookup process, reviewing the structure of a computer name on the Internet or in a Windows domain is helpful. Computer names are typically expressed as *host.domain.top-level-domain*; the *top-level-domain* can be com, net, org, us, edu, and so forth. As you learned in Chapter 3, this naming structure is called the fully qualified domain name (FQDN). The DNS naming hierarchy can be described as an inverted tree with the root at the top (named “.”), top-level domains branching out from the root, and domains and subdomains branching off the top-level domains (see Figure 9-1).

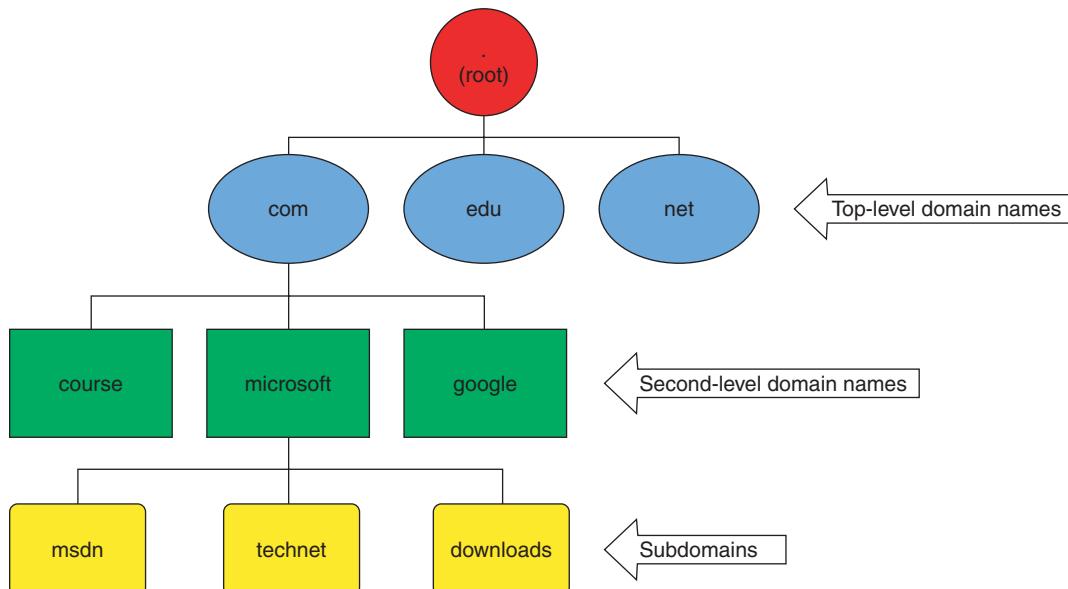


Figure 9-1 A partial view of the DNS naming hierarchy

The entire DNS tree is called the **DNS namespace**. When a domain name is registered, the domain is added to the DNS hierarchy and becomes part of the DNS namespace. Every domain has one or more servers that are authoritative for the domain, meaning the servers contain a

master copy of all DNS records for that domain. A single server can be authoritative for multiple domains.

Each shape in Figure 9-1 has one or more DNS servers managing the names associated with it. For example, the root of the tree has several DNS servers called **root servers**, which keep a database of addresses of other DNS servers managing top-level domain names. These other servers, aptly named, are called **top-level domain (TLD) servers**. Each top-level domain has servers that maintain addresses of other DNS servers. For example, the .com TLD servers maintain a database containing addresses of DNS servers for each domain name ending with .com, such as yahoo.com and microsoft.com. These second-level DNS servers contain hostname/IP address pairs for computers in their networks.

The DNS Database DNS servers maintain a database of information that contains zones. A **zone** is a grouping of DNS information that represents one or more domains and possibly sub-domains. Each zone contains a variety of record types called resource records. A **resource record** contains information about network resources, such as hostnames, other DNS servers, domain controllers, and so forth, and is identified by a letter code. Table 9-1 lists resource record types, the identifying codes, and a description of the resource record.

Table 9-1 DNS resource record types

Record type (code)	Description
Start of Authority (SOA)	Less a resource than an informational record, the SOA identifies the name server that's authoritative for the domain.
Host (A)	The most common resource record; consists of a computer name and IPv4 address.
IPv6 Host (AAAA)	Like an A record, but uses an IPv6 address.
Name Server (NS)	The FQDN of a name server that has authority over the domain. NS records are used by DNS servers to refer queries to another server that's authoritative for the requested domain.
Canonical Name (CNAME)	A record that contains an alias for another record and enables you to refer to the same resource with different names yet maintain only one host record. For example, you could create an A record for a computer named "web" and a CNAME record that points to the A record but allows users to access the host with the name "www."
Mail Exchanger (MX)	Contains the address of an e-mail server for the domain. Because e-mail addresses are typically specified as user@domain.com, the mail server's name is not part of the e-mail address. To deliver a message to the mail server, an MX record query supplies the address of a mail server in the specified domain.
Pointer (PTR)	Used for reverse DNS lookups. Although DNS is mainly used to resolve a name to an address, it can also resolve an address to a name by using a reverse lookup. PTR records can be created automatically on Windows DNS servers.
Service Records (SRV)	Allows DNS clients to request the address of a server that provides a specific service instead of querying the server by name. This type of record is useful when an application doesn't know the name of the server it needs but does know what service is required. For example, in Windows domains, DNS servers contain SRV records with the addresses of domain controllers so that clients can request the logon service to authenticate to the domain.

9

DNS records can be added and changed by using one of two methods:

- *Static updates*—With this method, an administrator must enter DNS record information manually. This method is reasonable with a small network of only a few resources accessed by name, but in a large network, static updates can be an administrative burden.
- *Dynamic updates*—Referred to as **Dynamic DNS (DDNS)**, computers in the domain can register or update their own DNS records, or DHCP can update DNS on the clients' behalf when a computer leases a new IP address. Both the client computer and the DHCP server must be configured to use this feature.

The DNS Lookup Process

- Two different types of DNS lookup can be performed:
- **Iterative query**—When a DNS server receives an **iterative query**, it responds with the best information it has to satisfy the query, such as the IP address of an A record it retrieves from a local zone file or cache. If the DNS server doesn’t have the specific information, it might have the IP address of a name server that *can* satisfy the query; this type of response is called a **referral**. If the server has no information, it sends a negative response that essentially says “I can’t help you.” DNS servers usually query each other by using iterative queries.
 - **Recursive query**—A **recursive query** instructs the DNS server to process the query until it responds with an address that satisfies the query or with an “I don’t know” message. A recursive query might require a DNS server to contact several other DNS servers before it finally sends a response to the client. Queries made by DNS clients are recursive queries.

A typical DNS lookup made by a DNS client can involve both recursive and iterative queries. A sample query demonstrating the hierarchical nature of DNS (see Figure 9-2) is outlined in the following steps:

1. A user types www.microsoft.com in the Web browser’s address bar. The computer running the Web browser, called the DNS client or **resolver**, sends a recursive query to the address of the DNS server in its IP configuration. Typically, this DNS server, called the local DNS server, is maintained on the corporate network or at the ISP.
2. The local DNS server checks its local zone data. If the name isn’t found locally, it sends an iterative query to a DNS root server.
3. The root server sends a referral to the local DNS server with a list of addresses for the TLD servers handling the com top-level domain.
4. The local DNS server sends another iterative query to a com TLD server.
5. The com TLD server responds with a referral to DNS servers responsible for the microsoft.com domain.
6. The local DNS server then sends another iterative query to a microsoft.com DNS server.
7. The microsoft.com DNS server replies with the host record IP address for www.microsoft.com.
8. The local DNS server responds to the client with the IP address for www.microsoft.com.

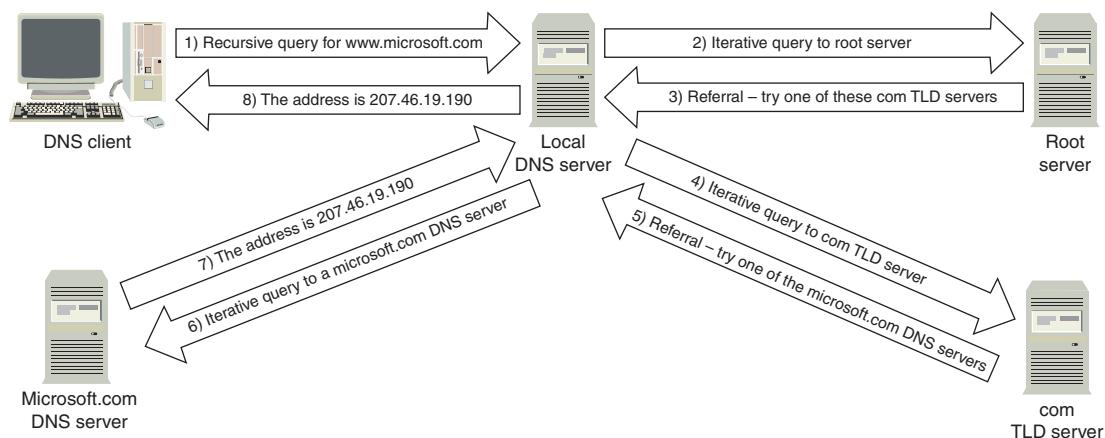


Figure 9-2 A DNS hierarchical lookup

Thankfully, the process depicted in Figure 9-2 doesn’t occur with every DNS lookup. Computers cache information they get from DNS, as you learned in Chapter 8. Furthermore, the local DNS server also caches recent lookups. So the entire process shown in Figure 9-2 occurs only when neither the computer doing the lookup nor the local DNS server has a cached copy of the requested name resolution.

To add one more wrinkle to the DNS lookup process, DNS clients maintain a text file called Hosts that can contain static DNS entries. On Windows, this file is stored in %systemroot%\System32\drivers\etc. By default, it contains two entries on Windows Server 2008 and Vista computers for resolving the local loopback address for both IPv4 and IPv6. The format of the file is simply IP address and hostname separated by one or more spaces. A typical Hosts file in Windows Server 2008 looks like this:

```
127.0.0.1    localhost  
::1          localhost
```

The entries in the Hosts file are cached at system startup and each time the file is changed. Of course, you can add as many entries as you like to the Hosts file. Usually, however, the Hosts file is left as it is because in a dynamic network, static DNS entries are likely to cause more harm than good. Some people use the Hosts file as a sort of Web filter. You can add entries to this file for hosts on domains that create pop-up ads and fill your Web pages with advertisements. For each entry, simply use the address 127.0.0.1. Unless you're running a Web server locally, your browser won't get a response from this address, and the ad will be blocked. You can even download a Hosts file that's already loaded with hundreds of entries for well-known Web advertisers, such as doubleclick.net.

DNS Server Roles

DNS servers can perform one or more of the following roles for a zone:

- *Authoritative server*—As discussed, an **authoritative server** for a domain holds a complete copy of a zone's resource records.
- *Forwarder*—A **forwarder** is a DNS server to which other DNS servers send requests they can't resolve themselves. A forwarder is commonly used when a DNS server on an internal, private network receives a query for a domain on the public Internet. The internal DNS server forwards the request recursively to a DNS server connected to the public Internet. This method prevents the internal DNS server from having to contact root servers and TLD servers directly because the forwarder does that on its behalf.
- *Conditional forwarder*—A **conditional forwarder** is a DNS server to which other DNS servers send requests targeted for a specific domain. For example, computers in the coolgadgets.com domain might send a DNS query for a computer named server1.niftytools.com. The DNS server in the coolgadgets.com domain can be configured with a conditional forwarder that in effect says “If you receive a query for niftytools.com, forward it to the DNS server handling the niftytools.com domain.” Servers that are forwarders or conditional forwarders require no special configuration, but the servers using them as forwarders must be configured to do so.
- *Caching-only server*—A **caching-only DNS server** isn't configured with any zones. Its sole job is to field DNS queries, do recursive lookups to root servers or send requests to forwarders, and then cache the results. After the query results are cached, the caching server can respond to a similar query directly. Caching servers are ideal for branch offices so that local computers' queries are forwarded to an authoritative server at a main office.

DNS Zones

As mentioned, a zone is a database containing resource and information records for a domain. There are three different types of zones:

- *Primary zone*—The **primary zone** contains a read/write master copy of all resource records for the zone. Updates to resource records can be made only on a server configured as a primary zone server, referred to as the primary DNS server. A primary DNS server is considered authoritative for the zone it manages.
- *Secondary zone*—The **secondary zone** contains a read-only copy of all resource records for the zone. Changes can't be made directly on a secondary DNS server, but because it contains an exact copy of the primary zone, it's considered authoritative for the zone.

- **Stub zone**—The **stub zone** contains a read-only copy of only the SOA and NS records for a zone and the necessary A records to resolve NS records. A stub zone forwards queries to a primary DNS server for that zone and is not authoritative for the zone.



Activity 9-1: Installing a New Domain Controller in a Subdomain

Time Required: 1 hour

Objective: Install a new domain controller in a subdomain.

Description: Several activities in this chapter and Chapter 10 can be done only with multiple domain controllers, so using virtual machines is highly recommended. (See Appendix C for more information.) This activity doesn't provide step-by-step instructions; it specifies the parameters you should select for the new domain controller.

1. Install Windows Server 2008 Enterprise Edition on a physical or virtual machine.
2. Assign **Password02** to the Administrator account.
3. Name the new server **Server1XX** (replacing XX with your assigned student number).
4. Assign the IP address **192.168.100.1XX** (replacing XX with your assigned student number), the subnet mask **255.255.255.0**, and the DNS server address **192.168.100.2XX** (the address of your ServerXX). Ask your instructor for the default gateway.
5. In Server Manager, install the Active Directory Domain Services Role. When the installation is finished, run **Dcpromo.exe**.
6. When prompted, install the domain controller in a new domain in an existing forest. Name the domain **subXX.w2k8adXX.com**. (Note: Make sure you read each window of the installation wizard carefully, and verify that you're entering the correct information.)
7. When prompted, click to clear the check box for including DNS as an option.
8. When the installation is finished, log on to this domain controller so that you're ready for the next activity.



Activity 9-2: Installing DNS on the New Domain Controller

Time Required: 20 minutes

Objective: Install DNS on a new domain controller.

Description: You have just installed a new domain controller in a new subdomain, but you realize you need to install DNS now.

1. Make sure you're logged on to Server1XX, and open Server Manager.
2. Click **Roles** in the left pane. In the right pane, click **Add Roles** to start the Add Roles Wizard. In the wizard's welcome window, click **Next**.
3. In the Select Server Roles window, click the **DNS Server** check box, and then click **Next**. In the Introduction to DNS Server window, click **Next**.
4. In the Confirm Installation Selections window, click **Install**. When the installation is finished, click **Close**. Close Server Manager.
5. Click **Start**, point to **Administrative Tools**, and click **DNS** to open DNS Manager.
6. Click to expand **Server1XX**, and then click **Forward Lookup Zones**. Notice that there are no zones. The DNS server on ServerXX holds the information for the new subdomain.
7. Now that Server1XX is a DNS server, you're going to change its IP address configuration so that it uses itself for DNS lookups. Open a command prompt window. Type **netsh interface ipv4 set dnsserver "Local Area Connection" static 127.0.0.1 primary** and press **Enter**. Type **ipconfig /all** and press **Enter** to verify that the DNS server is now 127.0.0.1. Close the command prompt window.
8. Later you create a new zone for the subXX subdomain. For now, close all open windows and log off or shut down Server1XX.



Activity 9-3: Using DNS Manager

Time Required: 15 minutes

Objective: Explore DNS Manager.

Description: You're unfamiliar with DNS, except for installing it recently. Your network is growing, and you need to manage and monitor your DNS database and settings. You start by familiarizing yourself with DNS Manager.

1. Log on to **ServerXX** as Administrator.
2. Click **Start**, point to **Administrative Tools**, and click **DNS** to open DNS Manager.
3. Click to expand **ServerXX**, if necessary, and then click **Forward Lookup Zones**. You should see a window similar to Figure 9-3.

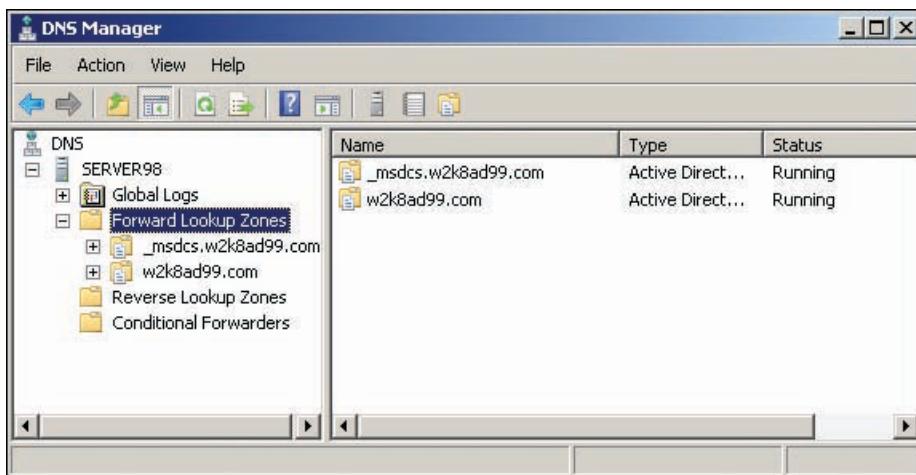


Figure 9-3 DNS Manager

4. Double-click your **W2k8adXX.com** domain to see a number of folders and resource records in the right pane. Look in the **Timestamp** column. Most records have a timestamp, except the SOA record, which is listed as static. All records except the SOA record were created dynamically. The SOA record was created by the DNS installation process, when the zone was created automatically.
5. The first few entries show “(same as parent folder)” in the **Name** column, which means they take on the domain’s name. If DNS gets an A record query for w2k8adXX.com without a hostname, it returns the IP addresses shown for the “(same as parent folder)” A record entries. Double-click the **Start of Authority (SOA)** record. In the SOA Properties dialog box, review the information available in all the tabs. The SOA record is discussed in more detail later in this chapter. Click **Cancel**.
6. You should see two records for serverXX, one for each IP address. (Recall that you added a second IP address to your server’s Local Area Connection interface in Activity 8-3.) Double-click either **ServerXX** A record entry. Figure 9-4 shows the Properties dialog box for an A record. You can’t change the Host or FQDN fields of an A record, but you can change the IP address. If you make a change, you can click the Update associated pointer (PTR) record check box to have the PTR record reflect the address change.
7. Click the **Security** tab. DNS records stored in Active Directory have the same type of permission settings as other Active Directory and NTFS objects, including permission inheritance and special permissions. You can assign permissions to users to allow them to manage DNS records, if necessary. Click **Cancel**.
8. Click to expand the **subXX** folder in the left pane. You should see several folders and a couple of A resource records in the right pane. The A records should contain the IP address of the new domain controller you installed.

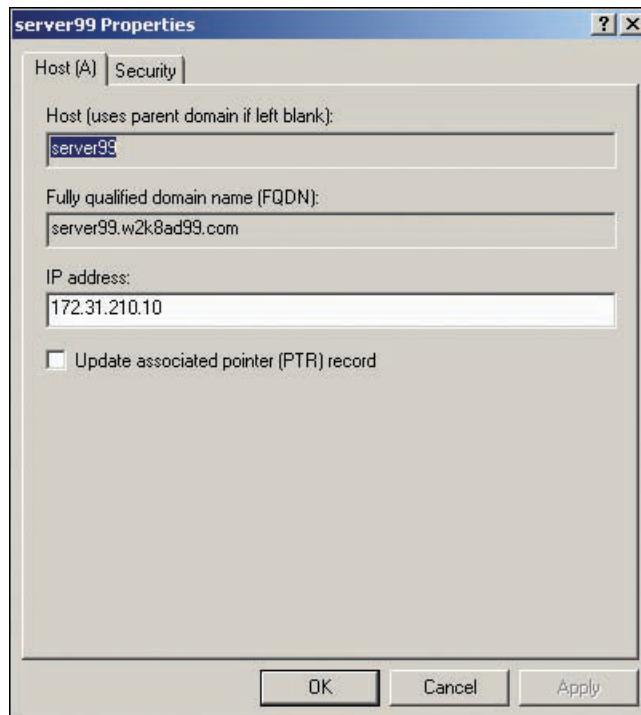


Figure 9-4 The Properties dialog box for an A record

9. Click **View, Advanced** from the menu. The Advanced view option shows additional information in DNS Manager, such as a new folder called Cached Lookups.
10. Click to expand **Cached Lookups** and click to expand the **.(root)** folder. Under the **.(root)** folder are one or more subfolders named for TLDs (com, edu, net, and so on). Click to expand the **com** folder. Domains you have visited with Vista or Windows Server 2008 have a folder containing A, NS, and other resource records. Cached entries don't require queries to external DNS servers.
11. Browse through the folders until you find an A or a CNAME record. (If you can't find one, start your Web browser and go to www.microsoft.com to create a record in the microsoft folder. Close your browser and refresh DNS Manager.) Double-click the **A** or **CNAME** record. In the Properties dialog box, you see a time to live (TTL) value, which tells DNS how long to keep the cached entry. The referring DNS server (an authoritative DNS server for the domain the record came from) sends the TTL value. Click **Cancel**.
12. Click the **com** folder. You should see several NS entries with names in the Data column, such as a.gtld-servers.net, b.gtld-servers.net, and so on, referred to as "generic top-level domain (GTLD) servers." These servers are responsible for com domains throughout the Internet. Double-click **a.gtld-servers.net**. Notice that no IP address is associated with the entry. When your DNS server needs to find the address of a com name server, it must query to find the address of a TLD server first. Click **Cancel**.
13. Right-click **Cached Lookups** and click **Clear Cache** to delete the cache. There are no entries in the cache now, except some folders and an entry for localhost. Clear your local DNS cache by opening a command prompt window, typing **ipconfig /flushdns**, and pressing **Enter**. Close the command prompt window.
14. Start your Web browser, go to any com domain, and then exit your Web browser.
15. Refresh DNS Manager (click **Action, Refresh**). Click to expand the **.(root)** folder, and then click the **com** folder. You should see the list of GTLD servers and a folder for the domain you visited (possibly more than one folder). Click the **net** folder, and then double-click the **GTLD-SERVERS** folder. You see several A records for the GTLD servers listed and perhaps some AAAA entries with IPV6 addresses.

16. Right-click **ServerXX** in the left pane and click **Properties**. Examine the properties of the DNS server. Many of the tabs and properties are discussed later in this chapter. Click **Cancel**.
17. Leave DNS Manager open and stay logged on to your server for the next activity.

Using DNS in Windows Server 2008

Windows domains and Active Directory rely exclusively on DNS for resolving names and locating services. When a workgroup computer attempts to join a domain, it contacts a DNS server to find records that identify a domain controller for the domain. When a member computer or server starts, it contacts a DNS server to find a domain controller that can authenticate it to the domain. When domain controllers replicate with one another and when trusts are created between domains in different forests, DNS is required to resolve names and services to IP addresses.

During Active Directory installation, Windows attempts to find a DNS server and, if it's unsuccessful, asks whether you want to install DNS. When a new forest is created, it's best to have Windows install DNS during Active Directory installation because Windows automatically creates all the initial zone records that Active Directory needs. If DNS is installed later, you have to create the zone database manually.

Installing DNS

You might need to install DNS manually on a domain controller, member server, or stand-alone server. In any case, you start by installing the DNS Server role from Server Manager. If the DNS server is intended to manage domain name services for Active Directory, you should install the DNS Server role on a domain controller so that you gain the benefits of Active Directory integration. If you're installing DNS on a domain controller, Windows detects the installation and informs you that DNS zones will be integrated with Active Directory, as shown in Figure 9-5.

9

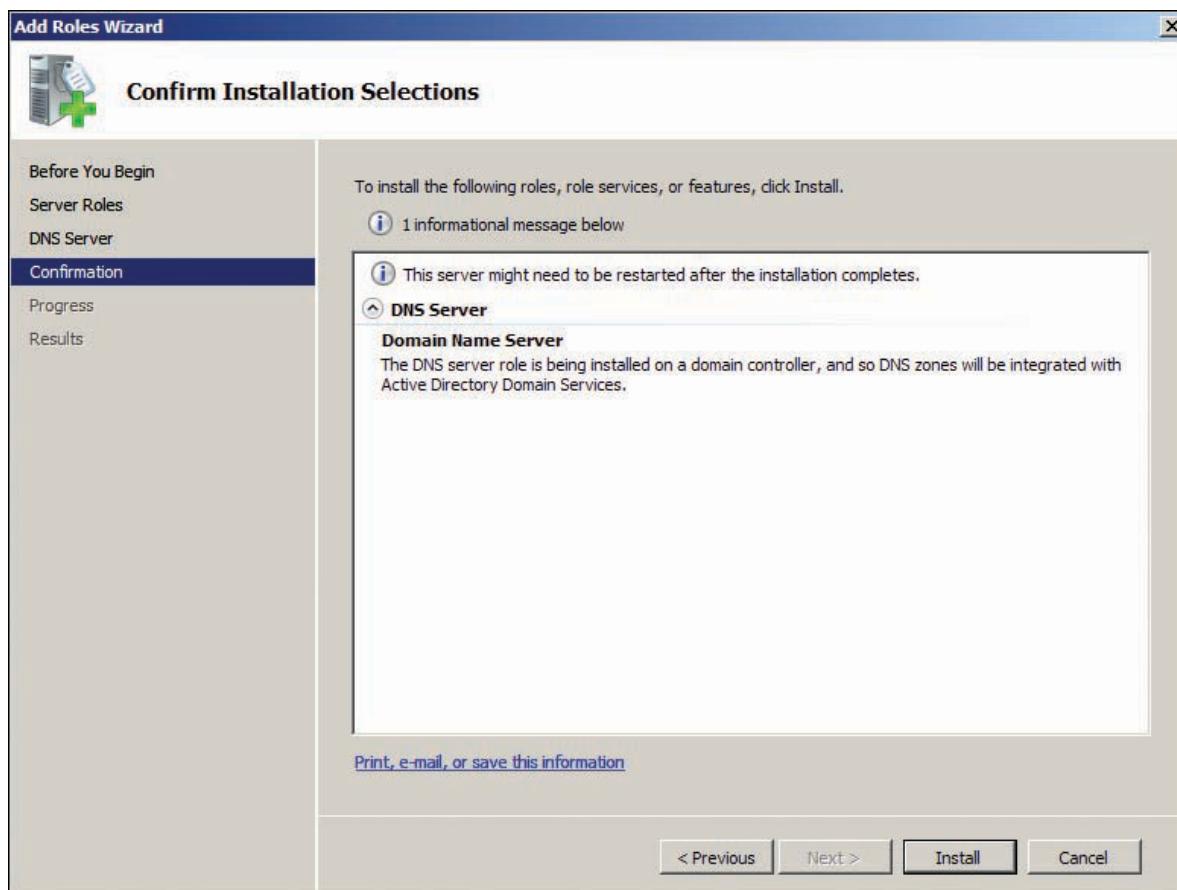


Figure 9-5 Installing DNS on a domain controller

When you install the DNS Server role, there are no choices to make—just a couple of clicks, and you’re finished. When you finish the installation, DNS Manager, shown previously, is available in the Administrative Tools folder and in Server Manager.

Creating DNS Zones

As mentioned, when DNS is installed as part of the Active Directory installation, the DNS zone that’s created is integrated with Active Directory by default and called an **Active Directory-integrated zone**. An Active Directory-integrated zone is not a new zone type; it’s a primary or stub zone with the DNS database stored in an Active Directory partition rather than a text file. Because Active-Directory zones are replicated to other domain controllers automatically, only primary and stub zones can be Active Directory integrated. Therefore, a secondary zone can’t be an Active Directory-integrated zone, but a file-based secondary zone can be created from an Active Directory-integrated zone, as when two DNS servers are in different forests.

If DNS is installed on a domain controller that’s part of an existing domain, zone information is copied to the new domain controller by default when Active Directory replication occurs. No action is necessary on the administrator’s part to create zones; they are replicated from other DCs in the domain.

Although DNS zones are created automatically during Active Directory installation, you might need to create a zone manually in the following situations:

- When you don’t install DNS at the time you install Active Directory
- When you install DNS on a server that’s not a domain controller
- When you create a stub zone
- When you create a secondary zone for a primary zone that’s not Active Directory integrated
- When you create a primary or secondary zone for an Internet domain

If you create a zone manually, you can choose whether it should be Active Directory integrated. A zone that isn’t Active Directory integrated is referred to as a **standard zone**. Figure 9-6 shows the zone type options when you’re creating a new zone.

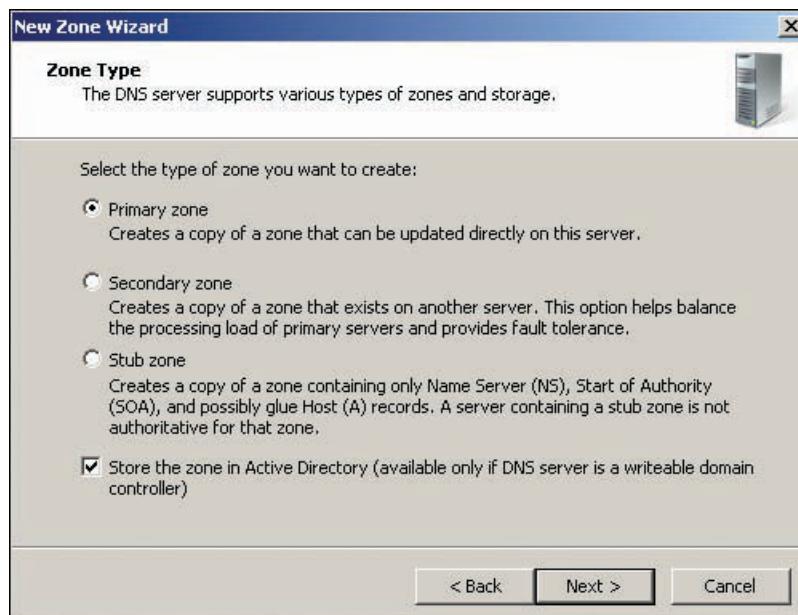


Figure 9-6 Selecting the zone type

Active Directory-Integrated Zones The “Store the zone in Active Directory” check box in Figure 9-6 means you want the zone to be stored in an Active Directory partition. The server where you’re creating the new zone must be a standard domain controller (as opposed to

a read only domain controller). When you're storing the zone in Active Directory, the only valid zone type options are primary and stub zones.

If you're creating a standard zone, the zone database is stored in a text file called *zone-name*.dns; the *zone-name* is generally the domain name. This file is located in the %systemroot%\system32\dns folder on the DNS server. A standard zone can be a primary, secondary, or stub zone.

An Active Directory-integrated zone has a number of advantages over a standard zone:

- *Automatic zone replication*—When DNS is installed on a new domain controller, zones are replicated to the new DNS server automatically. Standard zones require configuring zone transfers manually.
- *Multimaster replication and update*—Multiple domain controllers can be configured as primary DNS servers, and changes can be made on any of these domain controllers. Multimaster replication provides fault tolerance because no single server is relied on to make DNS changes. Changes to DNS are replicated to all other DCs in the domain configured as DNS servers. In contrast, a standard zone has a single primary DNS server (and possibly one or more secondary servers), which is the only server where changes to the database can be made. If the primary server fails, DNS changes can't be made until a primary server is brought online.
- *Secure updates*—DNS can be configured to allow dynamic DNS updates only from DNS clients that have authenticated to Active Directory. This option prevents rogue clients from poisoning the DNS database.
- *Efficient replication*—Replication of Active Directory-integrated zones can target only the DNS record properties that have changed. This option conserves bandwidth, compared with standard zones, which transfer the entire zone database.

9

Zone Replication Scope Active Directory-integrated zones are stored in an Active Directory partition, but there are a few options for which partition the zone is stored in and to which DCs zone information is replicated. After selecting the zone type and specifying that the zone be stored in Active Directory, you're asked to select the zone replication scope (see Figure 9-7) with one of these options:

- *To all DNS servers in this forest*—Stores the zone in the forest-wide DNS application directory partition called ForestDNSZones. This partition is created when DNS is installed on the first DC in the forest.

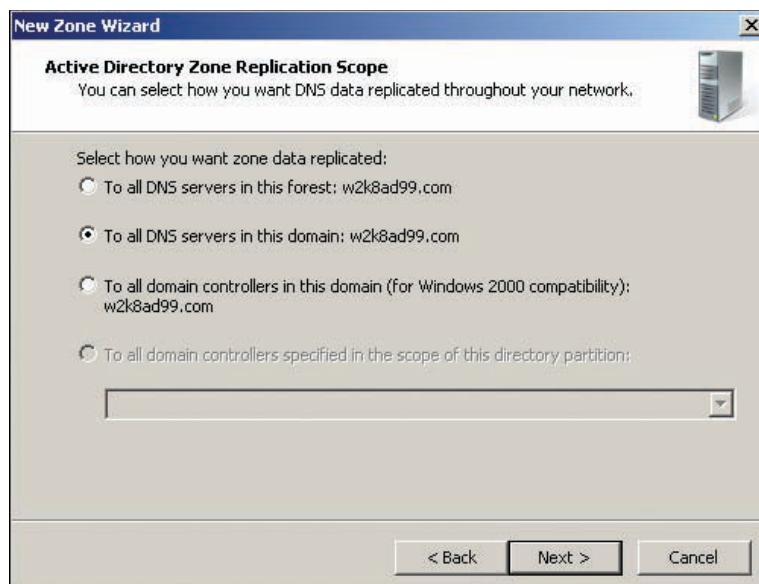


Figure 9-7 Selecting a zone replication scope

- *To all DNS servers in this domain*—Stores the zone in the domain-wide DNS application directory partition called DomainDNSZones. It's the default option for new zones.
- *To all domain controllers in this domain (for Windows 2000 compatibility)*—Stores the zone in the domain partition, which is used to store most Active Directory objects. DNS zone information is replicated to all other DCs in the domain, regardless of whether the DNS Server role is installed. This option is the only one available for Windows 2000 DCs and should be selected if DNS information must be replicated to Windows 2000 DNS servers.
- *To all domain controllers specified in the scope of this directory partition*—A custom DNS application partition must be created before selecting this option, and the partition must use the same name on each DC hosting DNS that should participate in replication. Use this option to limit which DNS servers receive zone data to control replication traffic. Custom DNS application partitions are created by using DnsCmd.exe (included with Windows Server 2008). For more information on using this command-line program, see <http://support.microsoft.com/kb/884116>.

Forward and Reverse Lookup Zones After choosing the zone type and replication scope, the next step is deciding whether the zone should be a forward lookup zone or a reverse lookup zone:

- **FLZ**—A **forward lookup zone (FLZ)**, the type you'll work with most often, contains records that translate names to IP addresses, such as A, AAAA, and MX records. It's named after the domain whose resource records it contains, such as w2k8ad99.com or usdoj.gov. After you select the option to create an FLZ, you simply supply a name for the zone, such as mydomain.com or subdomain.mydomain.com, depending on which part of the DNS namespace the zone will be managing.
- **RLZ**—A **reverse lookup zone (RLZ)** contains PTR records that map IP addresses to names and is named after the IP network address (IPv4 or IPv6) of the computers whose records it contains. When you create an RLZ, you select whether it's an IPv4 or IPv6 zone, and then enter the network ID portion of the zone (see Figure 9-8). The zone name is created automatically by using the network ID's octets in reverse order and appending in-addr.arpa to the name, shown in the Reverse lookup zone name text box. PTR records stored in an RLZ contain only one item of information: the FQDN of the computer identified by the

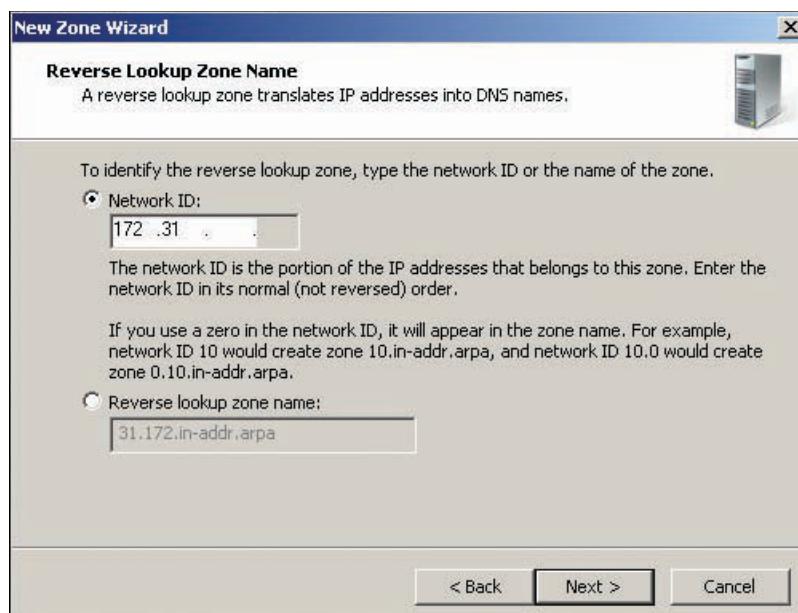
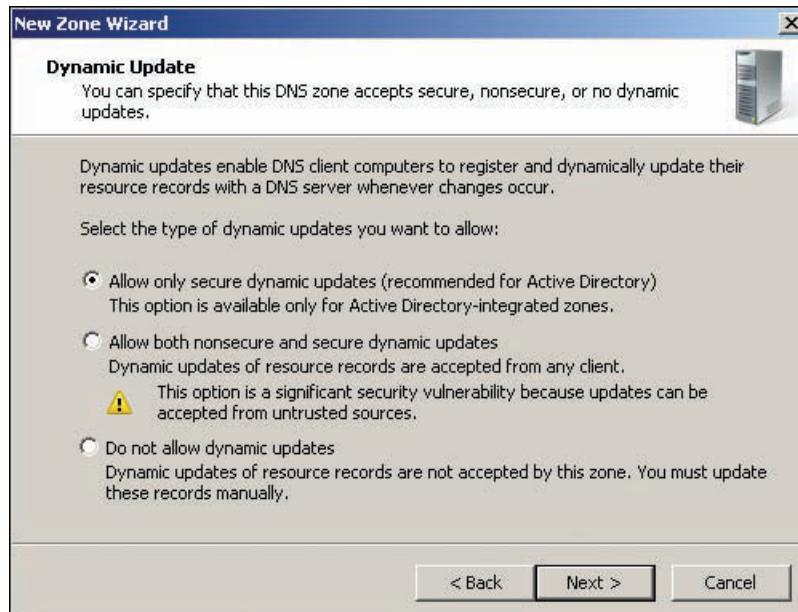


Figure 9-8 Creating a reverse lookup zone

IP address. When computers use DHCP for IP configuration, DHCP can create PTR records automatically when the computer's IP address changes. Otherwise, PTR records can be created manually.

Dynamic Updates The final step in creating a new zone is to select whether and how to use dynamic updates, shown in Figure 9-9. Dynamic updates can be configured in one of three ways:



9

Figure 9-9 Selecting dynamic update options

- *Allow only secure dynamic updates*—Available only for Active Directory-integrated zones, this option ensures that the host initiating the record creation or update has been authenticated by Active Directory.
- *Allow both nonsecure and secure dynamic updates*—Both authenticated Active Directory clients and non-Active Directory clients can create and update DNS records. This option isn't recommended because it allows rogue clients to create DNS records with false information. A rogue DNS client can impersonate a server by updating the server's A record with its own IP address, thereby redirecting client computers to a fraudulent server.
- *Do not allow dynamic updates*—All DNS records must be entered manually. This option helps secure the environment, but on a network with many hosts that must be accessed by name, and on networks using DHCP, it's an administrative nightmare. However, this option does work well for a DNS server that manages names for public resources, such as Web and mail servers with addresses that are usually assigned statically and don't change often.



Activity 9-4: Creating a Forward Lookup Zone

Time Required: 15 minutes

Objective: Create a forward lookup zone.

Description: Your company has resources your employees must access that aren't part of the Windows domain. You think the names of these resources should be resolved by the DNS servers running on domain controllers. You decide to create a new zone that doesn't accept dynamic updates, so all entries must be created manually.

1. Log on to **ServerXX** as Administrator and open DNS Manager, if necessary.
2. Click to expand **ServerXX** in the left pane, if necessary. Right-click **Forward Lookup Zones** and click **New Zone**. Click **Next** in the welcome window of the New Zone Wizard.

3. In the Zone Type window, make sure the **Primary zone** option button and the **Store the zone in Active Directory** check box are selected (the default settings). Click **Next**.
4. In the Active Directory Zone Replication Scope window, make sure the **To all DNS servers in this domain** option button is selected, and then click **Next**.
5. Type **W2k8adXX-External.com** in the Zone name text box, and then click **Next**.
6. In the Dynamic Update window, click the **Do not allow dynamic updates** option button, and then click **Next**. Click **Finish**.
7. In DNS Manager, click to expand the **Forward Lookup Zones** folder, if necessary, and then click to expand the **W2k8adXX-External.com** folder. Notice there are two records in the zone file: the SOA record and an NS record.
8. Right-click **W2k8adXX-External.com** and click **New Host (A or AAAA)**. Type **ServerXX-Ext** in the Name text box (the FQDN is filled in automatically) and **192.168.100.XX** in the IP address text box.
9. Click to clear the **Create associated pointer (PTR) record** check box and then click the **Add Host** button. Click **OK** to the “successfully created” message, and then click **Done**.
10. To test your new entry, open a command prompt window, type **ping serverXX-Ext.w2k8adXX-External.com**, and press **Enter**. You should get a successful reply. If not, check your spelling and syntax in the Ping command and when creating the host record and zone.
11. Type **ping serverXX-ext** and press **Enter**. You should get a message that host serverXX-ext could not be found. This error happens when the domain name isn’t included in the name to look up. In this case, only the default domain name is used (w2k8adXX.com), and there’s no DNS entry for serverXX-Ext in the w2k8adXX.com domain. To solve this problem, work through the next few steps.
12. Type **ipconfig /all | more** and press **Enter**. The first few lines of output are mostly DNS client configuration information. The Primary Dns Suffix and DNS Suffix Search List lines should show your domain name. Close the command prompt window.
13. Open the Local Area Connection Properties dialog box. (To do this, open Network and Sharing Center, click **Manage network connections**, right-click **Local Area Connection**, and click **Properties**.)
14. Double-click **Internet Protocol Version 4 (TCP/IPv4)**. In the Properties dialog box, click **Advanced** to open the Advanced TCP/IP Settings dialog box, and then click the **DNS** tab.
15. Click **Append these DNS suffixes (in order)**. Click **Add**, and type **w2k8adXX-External.com**. Click **Add**, and then click **Add** again. Type **w2k8adXX.com**, and then click **Add**. Click the green **up arrow** to move **w2k8adXX.com** to the top of the list because it’s the domain you’ll be accessing most often. Click **OK** until the Local Area Connection Properties dialog box is closed. Close all open windows.
16. Open a command prompt window, type **ipconfig /all | more**, and press **Enter**. Notice that the DNS Suffix Search List reflects the information you just entered in the DNS tab of the Advanced TCP/IP Settings dialog box. Press the **spacebar** until you get the command prompt.
17. Type **ping serverXX-Ext** and press **Enter**. You should get a successful reply.
18. Close all open windows and stay logged on for the next activity.



Activity 9-5: Working with Reverse Lookup Zones

Time Required: 15 minutes

Objective: View the properties of reverse lookup zones and create an RLZ.

Description: You’re unfamiliar with reverse lookup zones, so you want to explore existing RLZs on your server to see how they differ from FLZs. You assign a new IP address to your server that doesn’t already have an RLZ associated with it, and then create a new RLZ for the IP address.

1. Log on to **ServerXX** as Administrator and open DNS Manager, if necessary.
2. First, you need to assign an IP address for an RLZ that doesn't exist yet. Open the Network and Sharing Center and click **Manage network connections**. Right-click **Local Area Connection** and click **Properties**.
3. Double-click **Internet Protocol Version 4 (TCP/IPv4)**. Click the **Advanced** button to open the Advanced TCP/IP Settings dialog box. Click the **IP Settings** tab, if necessary, click the **192.168.100.XX** address in the IP addresses list box, and then click **Remove**. Next, you assign an address that doesn't have an RLZ associated with it.
4. Click the **Add** button. In the IP address text box, type **192.168.200.XX**. The Subnet mask text box is filled in automatically with 255.255.255.0. Click **Add**. Click **OK** three times. Close the Network Connections and Network and Sharing Center windows.
5. Open DNS Manager and click to expand **ServerXX**, if necessary, and click **Reverse Lookup Zones**.
6. Right-click **Reverse Lookup Zones** and click **New Zone**. In the New Zone Wizard's welcome window, click **Next**.
7. In the Zone type window, select the settings to create a primary zone stored in Active Directory, and then click **Next**. Select the option to replicate the zone to all DNS servers in the domain, and then click **Next**.
8. You want to create an IPv4 reverse lookup zone, so click **Next**. Type **192.168.200** in the Network ID text box. The Reverse lookup zone name text box is filled in automatically with **200.168.192.in-addr.arpa**. Click **Next**.
9. In the Dynamic Update window, click **Do not allow dynamic updates**. Click **Next**, and then click **Finish**.
10. In DNS Manager, click the **200.168.192.in-addr.arpa** zone folder in the left pane. You should see an SOA and an NS record. There are no PTR records yet.
11. Under Forward Lookup Zones, click the **w2k8adXX-External.com** folder, and double-click **ServerXX-Ext**. In the IP address text box, type **192.168.200.XX**. Make sure the **Update associated pointer (PTR) record** check box is selected, and then click **OK**.
12. In the left pane of DNS Manager, click the **200.168.192.in-addr.arpa** folder. If the PTR record isn't there, click **Action**, **Refresh** from the menu until you see it.
13. Open a command prompt window, type **nslookup 192.168.200.XX**, and press **Enter**. You should see **serverXX-ext.w2k8adXX-external.com** returned. Close the command prompt window.
14. After this point, you won't be using the secondary IP address in this book, so you should remove the **192.168.200.XX** address from your IPv4 settings. You can also delete the RLZ you just created by right-clicking the **200.168.192.in-addr.arpa** zone and clicking **Delete**. Click **Yes** when prompted if you want to delete the zone. Click **Yes** when warned that it's an Active Directory-integrated zone.
15. Leave DNS Manager open and stay logged on for the next activity.

9

Creating Zones from the Command Line If you have a lot of zones to create, you can wear out your clicking finger by using DNS Manager. For those who enjoy using the command line, Dnscmd.exe has DNS creation and configuration options. To see the syntax for Dnscmd.exe and get help information, type **dnsclmd /?** at a command prompt. The basic syntax is **dnsclmd server /command** plus command parameters, if required. Following are some examples with **server99** as the DNS server name:

- Create a new primary Active Directory-integrated zone named **zone1** that allows only secure dynamic updates:

```
dnsclmd server99 /ZoneAdd zone1 /DsPrimary
```

- Add an A record for the host named host1 in zone1 with the IP address 192.168.200.99:

```
dnscmd server99 /RecordAdd zone1 host1 A 192.168.200.99
```

Dnscmd.exe has dozens of command options. As you can see, with a little practice, you can learn its syntax and manage all your DNS zones without a single mouse click.

Configuring DNS Zones

After a zone is created, you can view and change its properties in DNS Manager by right-clicking the zone and clicking Properties. In the General tab of a zone's Properties dialog box (see Figure 9-10), you can view and change the following options (some have been discussed previously):

- *Status*—Pause a running DNS zone or start a paused DNS zone. When a zone is paused, queries made to it are refused.
- *Type*—Change the zone type (primary, secondary, or stub) and choose whether the zone should be Active Directory integrated.
- *Replication*—Change the replication scope.
- *Dynamic updates*—Choose Secure only, Nonsecure and secure, or None.
- *Aging*—Click this button to configure aging and scavenging options (discussed in the next section), which specify how often stale resource records are removed from the zone database.

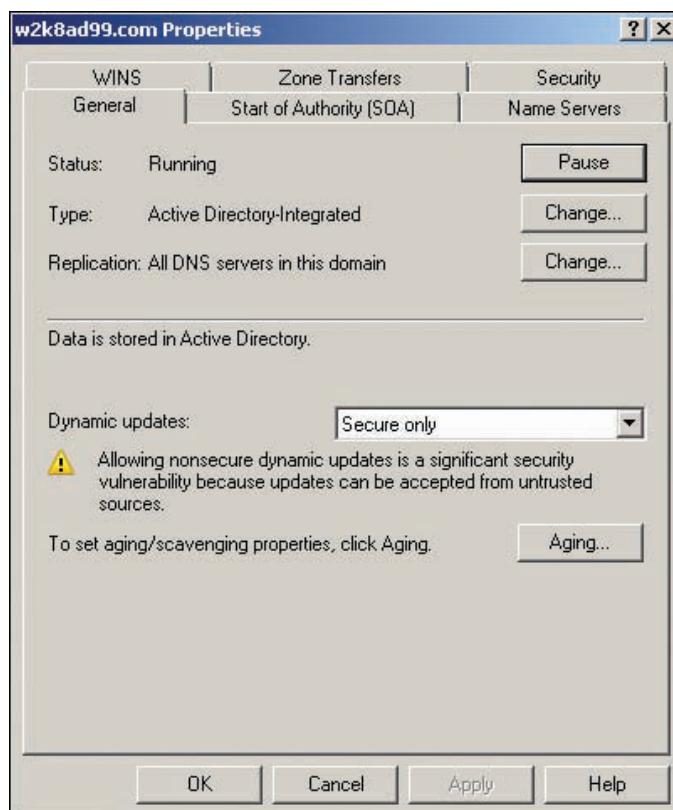


Figure 9-10 A zone's Properties dialog box

Aging and Scavenging Resource Records

When a resource record is created with DDNS, the record receives a timestamp based on the server's time and date. When a resource goes offline, it should contact the DNS server to delete its resource records. Unfortunately, this process doesn't always occur, and records that are no

longer valid are left in the database. In fact, Windows clients usually delete their DNS records only when they release or renew their IP address, not when they shut down.

Over time, these “stale” resource records can degrade server performance, provide incorrect information to DNS queries, and generally make DNS less reliable and efficient. Figure 9-11 shows the Zone Aging/Scavenging Properties dialog box. When **scavenging** is enabled, the server checks the zone file for stale records periodically and deletes those meeting the criteria for a stale record. The options in the Zone Aging/Scavenging Properties dialog box are as follows:

- **Scavenge stale resource records**—When this check box is selected, scavenging is enabled for the zone. However, the scavenging frequency must also be set in the Advanced tab of the DNS server’s Properties dialog box. By default, scavenging on the server isn’t enabled.
- **No-refresh interval**—To prevent DNS record timestamps from being updated too often, the No-refresh interval timer starts when a DNS record has been updated (refreshed). During the no-refresh period, DNS doesn’t accept a timestamp change to the record. Timestamp changes can occur, for example, when a computer renews its IP address lease from DHCP, but no actual changes to DNS data occur. The No-refresh interval prevents excessive replication of DNS data because even a timestamp change requires record replication. The default No-refresh interval setting is 7 days.
- **Refresh interval**—After the no-refresh period expires, the Refresh interval timer begins. During the refresh period, timestamp changes are accepted. If the Refresh interval timer expires, the record is considered stale and available for scavenging. If the record is refreshed during this period, the No-refresh interval timer begins again. The default Refresh interval setting is 7 days.
- **The zone can be scavenged after**—This setting is the earliest time and date that zone data can be scavenged. It’s based on the current time and date plus the refresh interval. To see this information, you must have the Advanced view option enabled in DNS Manager.

9

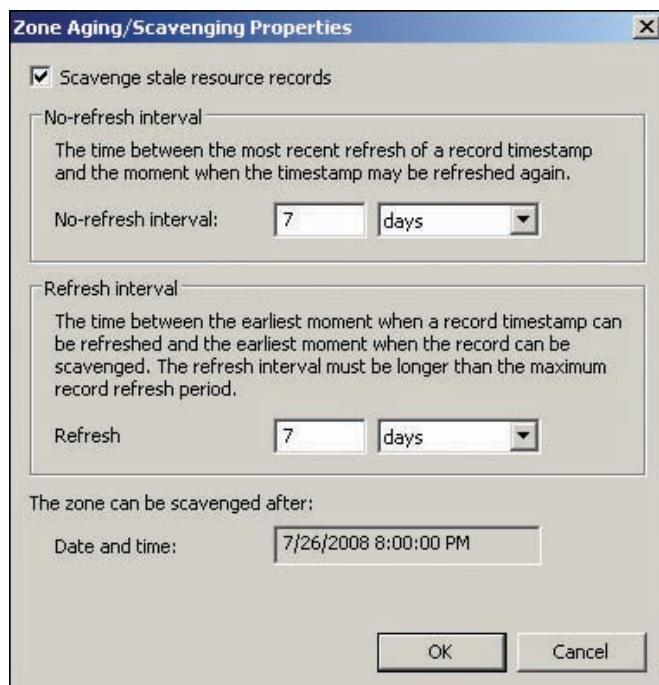


Figure 9-11 The Zone Aging/Scavenging Properties dialog box

The process by which DNS records are aged and scavenged isn't obvious from reading descriptions of the no-refresh and refresh intervals, so a step-by-step example is in order, in which the No-refresh and Refresh intervals are set to their default seven days:

1. A DNS client computer gets a new IP address from a DHCP server and registers an A and a PTR record with the DNS server. Each record has its own set of timers, so the interval timers in this example apply to both the A and PTR records.
2. The No-refresh interval timer starts, and no timestamp refreshes are accepted for the record for seven days.
3. The No-refresh interval timer expires.
4. The Refresh interval timer starts, and record refreshes are accepted for seven days.
5. The computer is shut down one day after the Refresh interval starts and isn't started again.
6. The Refresh interval timer expires.
7. The scavenging process deletes the expired DNS record.

The scavenging process, when enabled, is also set for seven days by default. In the preceding example, the computer was shut down one day after the Refresh interval timer began, so six days elapsed before the record was available for scavenging. If the scavenging process had just finished a scavenging run before the refresh interval expired, the record could remain in the database for an additional seven days, totaling 13 days from the time the computer was shut down and the time the record was actually deleted.

Although you can configure aging/scavenging for each zone separately, you can set scavenging for all zones at the same time by right-clicking the DNS server in DNS Manager and clicking Set Aging/Scavenging for All Zones. You have the same options shown in Figure 9-11 and are asked whether you want the settings to apply to all existing zones.

As mentioned, it's not enough to enable scavenging for zones. You must also enable scavenging on the server in the Advanced tab of its Properties dialog box. You don't need to enable scavenging on every DNS server, however. Because zone data, including aging/scavenging parameters, is replicated to all DNS servers, scavenging needs to be enabled on only one server. Scavenging does consume server resources, so enabling it on a DNS server with a fairly light workload is best.



Activity 9-6: DNS Aging and Scavenging

Time Required: 15 minutes

Objective: Configure aging and scavenging.

Description: You have noticed quite a few obsolete DNS entries on your server, particularly for laptop computers that connect to the network briefly and then sometimes don't connect again for days, weeks, or longer. You want to reduce the number of obsolete records, so you enable and configure aging/scavenging.

1. Log on to **ServerXX** as Administrator and open DNS Manager, if necessary.
2. In the left pane of DNS Manager, right-click **ServerXX** and click **Properties**. Click the **Advanced** tab, and click to select the **Enable automatic scavenging of stale records** check box, which enables scavenging on the server. Leave the scavenging period set to 7 days, and then click **OK**.
3. Right-click **ServerXX** in the left pane and click **Set Aging/Scavenging for All Zones**. Click the **Scavenge stale resource records** check box to enable scavenging on all zones. Leave the No-refresh and Refresh interval timers set at 7 days, and then click **OK**.
4. In the Server Aging/Scavenging Confirmation list box, click **Apply these settings to existing Active Directory-integrated zones**, and then click **OK**.
5. In DNS Manager, click **Forward Lookup Zones** and, if necessary, click to expand **w2k8adXX.com**. Right-click **w2k8adXX.com** and click **Properties**. Click the **Aging** button. The settings for the zone should be the same as you set in Step 3. (If they aren't, click **Cancel** twice, click the zone in the left pane, and click **Action**, **Refresh** from the menu. Then right-click **w2k8adXX.com** again and click **Properties**. Click **Aging**.) Click **OK** twice.
6. Leave DNS Manager open for the next activity.

Start of Authority Records

The SOA record is found in every zone and contains information that identifies the server primarily responsible for the zone as well as some operational properties for the zone. Shown in Figure 9-12, the SOA record contains the following information:

- *Serial number*—A revision number that increases each time data in the zone changes. This number is used to determine when zone information should be replicated.
- *Primary server*—On a primary Active Directory-integrated zone, this field displays the name of the server where DNS Manager is currently running. For a standard zone, it displays the primary DNS server's name.
- *Responsible person*—The e-mail address of the person responsible for managing the zone. A period rather than an @ sign is used to separate the username from the domain name (according to RFC 1183, which defines DNS resource record types).
- *Refresh interval*—Specifies how often a secondary DNS server attempts to renew its zone information. When the interval expires, the server requests the SOA record from the primary DNS server. The serial number in the retrieved SOA record is then compared with the serial number in the secondary server's SOA record. If the serial number has changed, the secondary server requests a new copy of the zone data. After the transfer is completed, the refresh interval begins anew. The default value is 15 minutes.
- *Retry interval*—The amount of time a secondary server waits before retrying a zone transfer that has failed. This value should be less than the refresh interval and defaults to 10 minutes. The retry interval begins after the refresh interval expires, and the primary server can't be contacted or the zone transfer fails.
- *Expires after*—The amount of time before a secondary server considers its zone data obsolete if it can't contact the primary DNS server. If the refresh interval expires without a successful zone transfer, this timer begins. If it expires without an update to the zone data (or an indication that the zone data hasn't changed), the DNS server stops responding to queries. This value must be higher than the refresh and retry intervals combined; the default is 1 day.

9

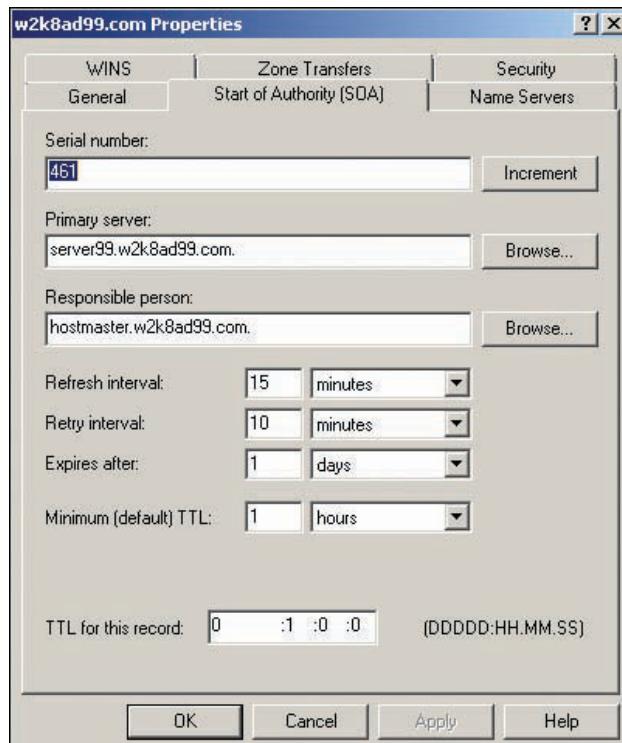


Figure 9-12 SOA record information

- *Minimum (default) TTL*—This setting specifies a default TTL value for zone data when a TTL isn't supplied. The TTL value tells other DNS servers that cache records from this zone how long to keep cached data and should be adjusted according to how often data in the zone is likely to change. For example, a zone that maintains only static entries for resources that aren't changed, added, or removed often can specify a high TTL value. If a zone maintains dynamic records or records for resources that are going online and offline constantly, this value should be lower. If a redesign of your network will cause many changes to zone data, this value can be lowered temporarily. Then wait until the previous TTL time has elapsed before making the changes. This way, servers caching records that will be changed don't store them very long. The TTL set on resource records overrides this default value, which is 1 hour.

Name Server Records

NS records specify FQDNs and IP addresses of authoritative servers for a zone. A typical configuration with Active Directory-integrated zones has an NS record for each domain controller configured as a DNS server in the domain or forest, depending on the scope of zone replication.

NS records are also used to refer DNS queries to a name server that has been delegated authority for a subdomain. For example, com TLD servers refer queries for resources in the technet.microsoft.com subdomain to a DNS server that's authoritative for the microsoft.com domain. The microsoft.com domain name server can then refer the query to another DNS server that has been delegated authority for the technet subdomain of microsoft.com. Subdomains need not be delegated; they can simply be created under the zone representing their parent domain. If the subdomain has many resources and traffic on it is heavy, however, zone delegation (explained in more detail in the next section) is a wise approach.

An NS record technically consists of just the name server's FQDN, but for the name to be useful, there must be a way to resolve it to an IP address. DNS does this with a **glue A record**, which is an A record containing the name server's IP address. In DNS Manager, glue records are created automatically, if possible, by a DNS lookup on the NS record's FQDN; they don't appear as an A record anywhere in the zone database. Figure 9-13 shows the interface for creating and

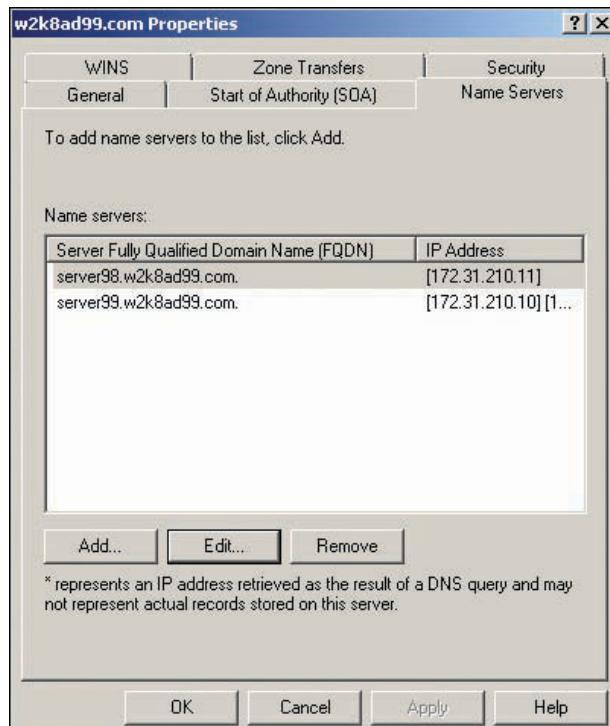


Figure 9-13 The Name Servers tab

editing NS records. If Windows fails to resolve the name server's FQDN, you can edit the record and add an IP address manually.

Zone Delegation

Zone delegation is transferring authority for a subdomain to a new zone, which can be on the same server or another server. Typically, you use zone delegation when a business unit in an organization is large enough to warrant its own subdomain and has the personnel to manage its own DNS server for the subdomain. Even if the business unit won't be managing the subdomain, delegating the handling of the subdomain to other servers might make sense for performance reasons.

When a subdomain has been delegated to a zone on another server, the DNS server hosting the parent zone maintains only an NS record pointing to the DNS server hosting the delegated zone. When the parent DNS server receives a query for the subdomain, it refers the query to the DNS server hosting the subdomain.



If changes are made to the name servers hosting the delegated zone, the NS records on the server hosting the parent domain must be updated manually.

NOTE

You might have noticed a zone called `_msdcs.w2k8adXX.com` on your DNS server. Every Windows domain zone has an `_msdcs` subdomain, which holds all the SRV records for Microsoft-hosted services, such as the global catalog, LDAP, and Kerberos. In the forest root domain, this subdomain is delegated to a new zone on the same server, not on a different server. For example, in DNS Manager in Figure 9-14, the `_msdcs.w2k8ad99.com` zone is located under Forward Lookup Zones, and an `_msdcs` icon under this subdomain signifies that it has been delegated.

9

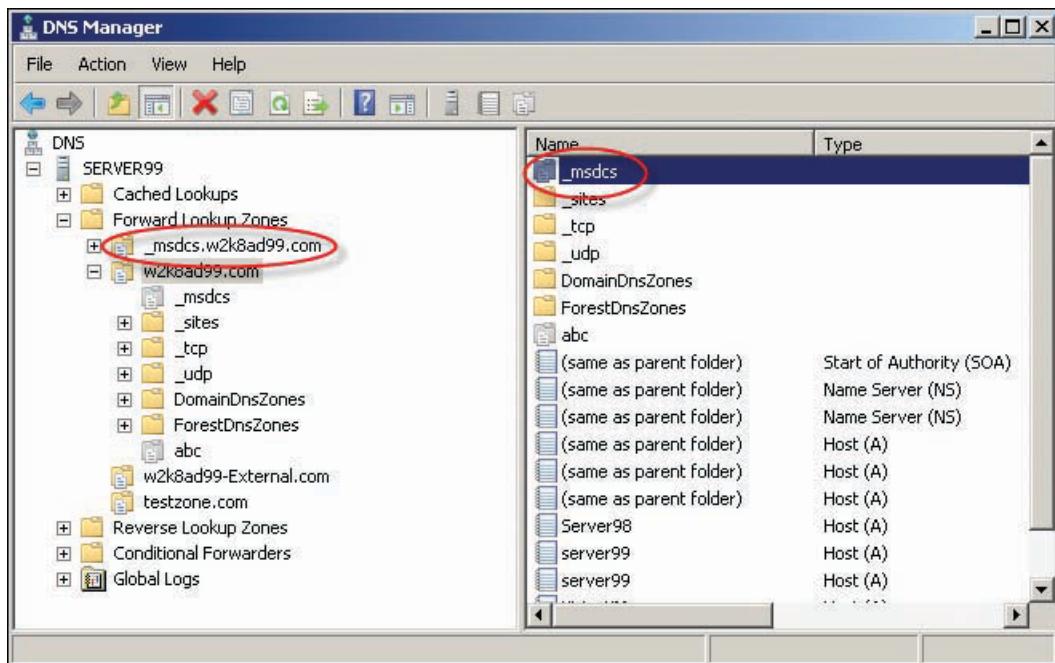


Figure 9-14 Viewing a delegated zone in DNS Manager

The reason `_msdcs` is created as a subdomain is so that Windows clients and other clients specifically looking for a Microsoft service can query DNS for the service in the `_msdcs` subdomain. Remember: It's possible for non-Microsoft OSs to be operating in the same domain, and they might offer some of the same services, such as Kerberos and LDAP. The reason `_msdcs` is delegated to a separate zone in the forest root domain is to change the zone's replication scope from domain-wide to forest-wide. Because the forest root contains specialized functions, such as global catalog servers, replication of this domain's SRV records to the entire forest is critical.

If the_msdc subdomain isn't delegated to its own zone, the records it contains are replicated according to the parent zone's setting, which is often only domain-wide, not forest-wide.



Activity 9-7: Creating a New Zone and a Delegation

Time Required: 20 minutes

Objective: Create a new zone and a delegation for the new zone.

Description: You recently installed a domain controller (Server1XX) for a subdomain (subXX), and then installed DNS on the new domain controller. Now you want your new server to host the zone for subXX.w2k8adXX.com and create a delegation for the zone on ServerXX.

1. Log on to **Server1XX** as Administrator (with Password02) and open DNS Manager.
2. First, you create the new zone on the server that will host it. In the left pane, click to expand **Server1XX**, if necessary. Right-click **Forward Lookup Zones** and click **New Zone**. In the New Zone Wizard, click **Next**.
3. In the Zone Type window, make sure the **Primary zone** option button and the **Store the zone in Active Directory** check box are selected (the default settings). Click **Next**.
4. In the Active Directory Zone Replication Scope window, leave the default setting **To all DNS servers in this domain** selected, and then click **Next**.
5. In the Zone name text box, type **subXX.w2k8adXX.com**, and then click **Next**.
6. In the Dynamic Update window, leave the default selection, click **Next**, and then click **Finish**.
7. In the left pane of DNS Manager, click to expand **subXX.w2k8adXX.com**. Notice that two records are created automatically: the SOA and NS records. Double-click the **Name Server** record, which opens the zone's Properties dialog box to the Name Servers tab. Click the **Edit** button. If no IP addresses are shown, click the **Resolve** button. Windows should resolve the IP address from a DNS lookup to your other DNS server. You can add addresses, delete addresses, change the order of addresses in the list, and provide a TTL value for the NS record. Click **OK** twice.
8. Click the **subXX.w2k8adXX.com** folder in the left pane. If the A record for Server1XX hasn't appeared yet, click the **Refresh** button (or click **Action**, **Refresh** from the menu).
9. Log on to **ServerXX** as Administrator and open DNS Manager, if necessary.
10. Click the **w2k8adXX.com** folder in the left pane, and double-click the **subXX** folder. Notice that it contains several subfolders and two A records pointing to Server1XX.
11. You need to delete the subdomain before you can delegate it. Right-click **subXX** and click **Delete**. Click **Yes** in the warning message.
12. Now you can create the delegation. Right-click **w2k8adXX.com** and click **New Delegation**. In the New Delegation Wizard's welcome window, click **Next**.
13. In the Delegated domain text box, type **subXX**. The FQDN text box is filled in automatically and should be "subXX.w2k8adXX.com." Click **Next**.
14. In the Name Servers window, click **Add**. In the Server fully qualified domain name (FQDN) text box, type **server1XX.subXX.w2k8adXX.com** and click **Resolve**. The IP address of Server1XX should be listed in the IP Addresses of this NS record list box. Click **OK**. Click **Next**, and then click **Finish**.
15. Notice a gray zone icon named subXX under w2k8adXX.com, which indicates the zone has been delegated. Double-click **subXX**. You should see an NS record pointing to Server1XX.subXX.w2k8adXX.com.
16. Stay logged on to both servers, and leave DNS Manager open for the next activity.

Using Stub Zones Stub zones, as previously discussed, are a special type of zone that contain only an SOA record, one or more NS records, and the necessary glue A records to resolve NS records. Essentially, a stub zone points to another DNS server that's authoritative for the zone.

The records in a stub zone, like other Active Directory-integrated zones and secondary zones, are updated regularly through Active Directory replication and zone transfers. Reasons for using stub zones include the following:

- *Maintenance of zone delegation information*—If changes are made to addresses of the name servers hosting a delegated zone, the NS records on the parent DNS server must be updated manually. If a stub zone is created for the delegated zone on the parent DNS server, the NS records are updated automatically. The use of a stub zone effectively eliminates manual maintenance of the delegated zone’s NS records.
- *In lieu of conditional forwarders*—If changes are made to addresses of domain name servers that are conditionally forwarded, the IP addresses for the conditional forwarder records must be changed manually. If a stub zone is created instead of using a conditional forwarder, the NS records in the stub zone are updated automatically. In addition, because stub zones can be Active Directory integrated, creating them on all DNS servers isn’t necessary, as it is with conditional forwarders.
- *Faster recursive queries*—When a DNS server receives a query for a resource record in the stub zone, it can perform a recursive query by using the stub zone’s NS records rather than accessing a root server.
- *Distribution of zone information*—When a network consists of many zones, distribution of those zones is necessary to make the entire DNS namespace accessible throughout the network. Typically, this distribution requires secondary zones or Active Directory-integrated zones. Stub zones can be used strategically to reduce the number of secondary zones or full Active Directory-integrated zones; reducing the number of these zones cuts down network traffic caused by zone transfers and replication.

9

Zone Transfers

A **zone transfer** copies all or part of a zone from one DNS server to another and occurs as a result of a secondary server requesting the transfer from another server. The server requesting the zone transfer is sometimes called the slave, and the server providing the zone information is sometimes called the master. The master server can host a primary or secondary zone, but the slave server always hosts a secondary zone. Although Active Directory-integrated zones use Active Directory replication to transfer zone information, you can configure standard zone transfers if the target is a standard secondary zone. Zone transfers can be initiated in two ways:

- *Refresh interval*—As discussed, a secondary zone server requests zone information from another server (a primary or another secondary master) when the zone’s refresh interval expires, which is every 15 minutes by default.
- *DNS notify*—A master server can be configured to send a DNS notify message to secondary servers when zone information changes. The secondary server can then request the zone transfer immediately without waiting for the refresh interval to expire.

Zone transfers are configured in the Zone Transfers tab of a zone’s Properties dialog box (see Figure 9-15), which has the following options:

- *Allow zone transfers*—When this check box is selected, zone transfers are enabled. By default, zone transfers in Active Directory-integrated zones are disabled. In standard zones, zone transfers are enabled for all other name servers listed for that zone. Options for configuring zone transfers are as follows:
 - To any server: Allows any server to request a zone transfer. This option isn’t recommended for most environments, as it allows any host to request network information, which is not secure.
 - Only to servers listed on the Name Servers tab: This option is the default for standard zones.
 - Only to the following servers: You can specify servers to which zone information can be transferred.

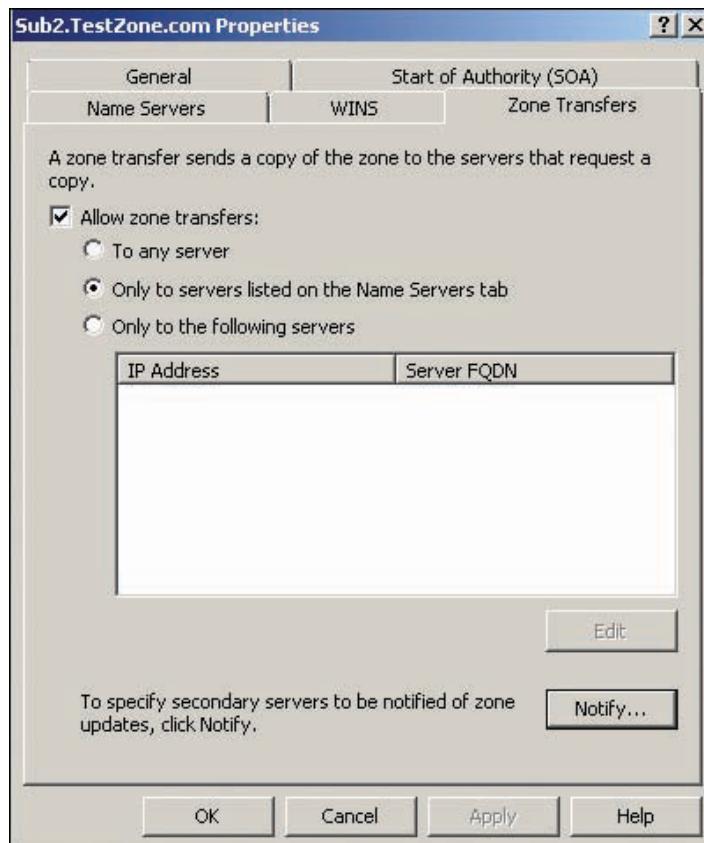


Figure 9-15 Configuring zone transfers

- **Notify**—Clicking this button opens a dialog box where you can specify servers that should receive notifications of changed zone information. By default, the notify option is enabled in standard zones for servers listed in the Name Servers tab.



If all zones are hosted on Windows domain controllers and are Active Directory integrated, there's no need to configure zone transfers because Active Directory replication handles this process.

NOTE

Incremental Zone Transfers There are two types of zone transfer: full zone transfers and incremental zone transfers. A full zone transfer was the only transfer method in earlier DNS versions. As DNS databases grew larger and zone files became more numerous and much bigger, incremental zone transfers were defined. Both the master and slave DNS servers must support incremental zone transfers to use them.

When a secondary server requests a zone transfer, it can request an incremental transfer. (If the secondary zone is newly configured on the server, it requests a full zone transfer.) If the serial number of the slave's zone is lower than the master's, the master determines the differences between its current zone data and the slave's zone data. The master then transfers only the resource records that have changed. For incremental zone transfers to work, the master must keep a record of incremental changes with each serial number change. For example, if a slave server requests an incremental zone transfer, and its zone serial number is 500 and the master's zone serial number is 502, the master sends all changes that have occurred to the zone between serial number 500 and 502. Even if an incremental transfer is requested, the master can still respond with a full zone transfer if it doesn't support incremental transfers or have sufficient change history to respond accurately with an incremental transfer.



Activity 9-8: Configuring Zone Transfers

Time Required: 10 minutes

Objective: Configure an Active Directory-integrated zone to allow zone transfers.

Description: You plan to create some secondary zones for your primary Active Directory-integrated zone, so you need to enable and test zone transfers.

1. Log on to **ServerXX** as Administrator and open DNS Manager, if necessary.
2. Open a command prompt window. Type **nslookup** and press **Enter**.
3. Type **ls -d w2k8adXX.com** and press **Enter**. This command is supposed to display all the zone records via a zone transfer. You should get an error message stating that the DNS server refused to transfer the zone. Next, you enable zone transfers.
4. In the left pane of DNS Manager, click to expand **ServerXX**, if necessary, and click to expand **Forward Lookup Zones** and then **w2k8adXX.com**. Right-click **w2k8adXX.com** and click **Properties**.
5. Click the **Zone Transfers** tab, and then click the **Allow zone transfers** check box. By allowing zone transfers to any server, no further zone configuration is needed to transfer the zone. On a server that's accessible from the Internet, be aware that you don't want to allow zone transfers to just any server. Click **OK**.
6. Go back to the command prompt window where Nslookup is running. Type **ls -d w2k8adXX.com** and press **Enter**. You should see a lengthy display of the zone information.
7. Leave DNS Manager open for the next activity.

9



Activity 9-9: Creating a Standard Primary Zone

Time Required: 15 minutes

Objective: Create and configure a standard primary zone.

Description: You have a server configured with the DNS Server role that's not running Active Directory. You need to create a standard primary zone for a group of UNIX and Linux computers. (In this activity, you create the zone on **Server1XX**, even though it does have Active Directory installed.)

1. Log on to **Server1XX** as Administrator and open DNS Manager, if necessary.
2. Right-click **Forward Lookup Zones** and click **New Zone**. In the New Zone Wizard's welcome window, click **Next**.
3. In the Zone Type window, leave the default setting for the zone type (primary), click to clear the **Store the zone in Active Directory** check box, and then click **Next**.
4. In the Zone name text box, type **TestZone.com**. (If you're creating a zone for internal use only, following DNS namespace syntax isn't necessary, so you could have named the zone **TestZone**.) Click **Next**.
5. Accept the default filename **TestZone.com.dns**, and then click **Next**.
6. In the Dynamic Update window, verify that the default setting **Do not allow dynamic updates** is selected, click **Next**, and then click **Finish**.
7. In the left pane of DNS Manager, click to expand **TestZone.com**. Notice that the SOA and NS records are created automatically. Right-click **TestZone.com** and click **New Host (A or AAAA)**.
8. In the New Host dialog box, type **test1** in the Name text box and **192.168.110.1** in the IP address text box. (The address you use doesn't matter in this case because this record is just used as a test. Normally, of course, you enter the address assigned to the host computer.) Click to clear the **Create Associated pointer (PTR) record** check box, and then click **Add Host**.
9. You should get a success message. Click **OK**, and then click **Done**.

10. Open a command prompt window. Type **nslookup test1** and press **Enter**. You should get an error message such as “can’t find test1” because by default, Nslookup appends the primary DNS suffix to any name lookups, and test1 isn’t in your primary DNS suffix domain.
11. Type **nslookup test1.testzone.com** and press **Enter**. You should get a reply with the IP address you entered for the A record in Step 8.
12. Close the command prompt window, and stay logged on to both servers for the next activity.



Activity 9-10: Creating a Secondary Zone and Configuring Zone Transfers

Time Required: 15 minutes

Objective: Create a secondary zone and configure zone transfers.

Description: You want a backup for fault tolerance and load sharing of the standard primary zone you created, so you decide to create a secondary zone on ServerXX and configure zone transfers.

1. Log on to **ServerXX** as Administrator and open DNS Manager, if necessary.
2. Right-click **Forward Lookup Zones** and click **New Zone**. In the New Zone Wizard’s welcome window, click **Next**.
3. In the Zone Type window, click the **Secondary zone** option button, and then click **Next**. Type **TestZone.com** in the Zone name text box, and then click **Next**.
4. In the Master DNS Servers window type **192.168.100.1XX** in the Master Servers text box, and press **Enter**. Click **Next**, and then click **Finish**.
5. Log on to **Server1XX** as Administrator and open DNS Manager, if necessary.
6. Right-click **TestZone.com** and click **Properties**. Click the **Zone Transfers** tab.
7. Make sure the **Allow zone transfers** check box is selected, and then click the **Only to the following servers** option button.
8. Click the **Edit** button. Click in the IP addresses of secondary servers text box, type **192.168.100.2XX** (the address of ServerXX), press **Enter**, and then click **OK**. Click **OK** again to close the zone’s Properties dialog box.
9. On ServerXX, click **TestZone.com** in the left pane of DNS Manager, and then click the **Refresh** toolbar button. The zone data should have been transferred successfully, and you should see the SOA, NS and A records for TestZone.com.
10. Test the zone by opening a command prompt window on ServerXX, typing **nslookup test1.testzone.com**, and pressing **Enter**. You should get a successful reply. Close the command prompt window.
11. Close all open windows, and log off both servers.

Using WINS with DNS

Windows Internet Name Service (WINS) is a legacy name service used to resolve NetBIOS names, sometimes referred to as single-label names. WINS has similarities to DDNS, in that a central database of name-to-address mappings is maintained on a server where client computers update their own records dynamically. Windows clients do a WINS lookup by contacting the server with the name of the host whose IP address is required. WINS supports only IPv4 and is slowly becoming obsolete. You should configure your DNS server to use WINS only if you have older Windows clients, such as Windows 9x, and non-Windows clients that use only DNS. DNS/WINS integration allows non-Windows clients to resolve the names of older Windows clients that require NetBIOS name resolution. WINS might also be a part of your network if you’re running older applications that depend on NetBIOS name resolution. Figure 9-16 shows the WINS tab, which has the following configuration options:

- **Use WINS forward lookup**—When this option is enabled for the zone, the DNS server attempts to contact a WINS server to resolve the name, if it couldn’t be resolved through DNS. WINS forward lookup is disabled by default.

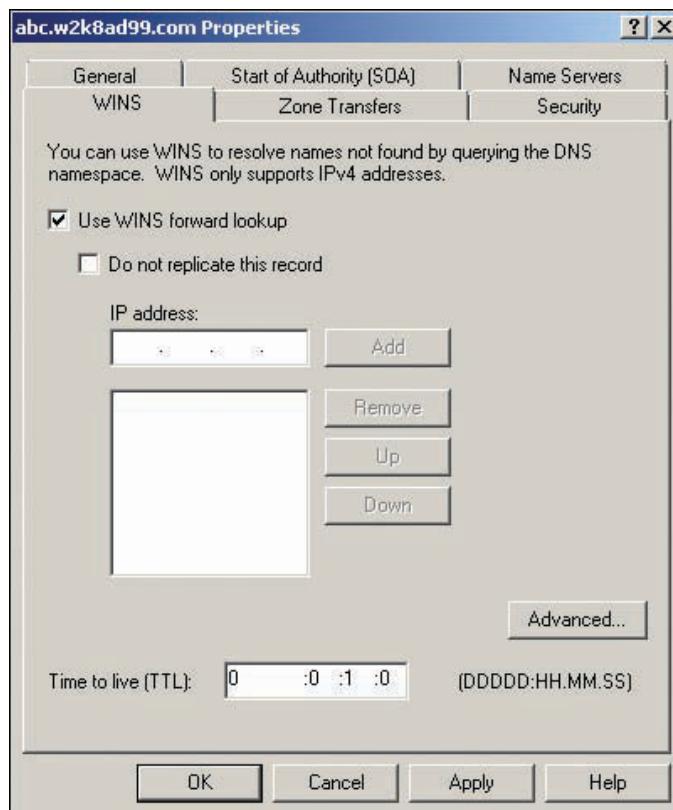


Figure 9-16 WINS configuration options

- *Do not replicate this record*—If WINS forward lookups are enabled, selecting this check box prevents the WINS resource record from being replicated to other DNS servers. This option should be selected if you have non-Windows DNS servers in your environment because WINS resource records are Windows specific, and including them in a zone transfer could corrupt the zone or prevent its transfer.
- *IP address*—Enter the IP addresses of WINS servers that should be contacted for name resolution.
- *Time to live (TTL)*—This text box specifies how long a cached WINS resource record is kept.

Using the GlobalNames Zone Although WINS is still supported in Windows Server 2008 and Vista, Windows Server 2008 includes a new feature to help IT administrators migrate away from WINS. This new feature, the **GlobalNames zone (GNZ)**, provides a method for IT administrators to add single-label names (computer names that don't use a domain suffix) to DNS, thereby allowing client computers to resolve these names without including a DNS suffix in the query. The GNZ is not a replacement for a dynamically created WINS database because records in this zone must be added manually. For important servers with names currently being resolved by WINS, however, a GNZ is an option worth considering, especially if only a few hosts are the sole reason for maintaining WINS.

GNZ functionality is not just a partial replacement for WINS, however. If your network supports mobile users whose laptops and other mobile devices are unlikely to have the correct DNS suffixes configured, GNZ can make access to servers these users need more convenient. Instead of mobile users having to remember resource FQDNs, they can simply access them by using a single-label name, such as Web1.

GNZ functionality must be enabled on servers hosting this zone by using Dnscmd.exe. Before you create a GNZ, enter the following command:

```
Dnscmd server /config /EnableGlobalNamesSupport 1
```

After GNZ support is enabled, you create a new zone that can be (but need not be) Active Directory integrated and named GlobalNames (not case sensitive). Dynamic updates should be disabled because GNZ doesn't support DDNS. For each host to be accessed with a single-label name, create a CNAME record in the GNZ that references the host's A record. You must enable GNZ support on each server to which the zone is replicated.

Advanced DNS Server Settings

So far, you have focused on DNS zone creation and configuration—and rightly so because zones are where all the data is and where most DNS configuration takes place. However, you should be familiar with several DNS server settings to configure an optimal DNS environment and solve DNS problems when they occur. The following settings are discussed in this section:

- Forwarders
- Root hints
- Round robin
- Recursion
- Debug logging

DNS Forwarders

Forwarders were defined previously in “DNS Server Roles,” but this section goes into more detail on when to configure and use them. Recall how a typical DNS query is processed: A DNS server receives a lookup request from a client and, if it’s unable to satisfy the request, a recursive query ensues, starting with a root server. This process works well, but in situations such as the following, referring the query to a forwarder is more efficient:

- *When the DNS server address for the target domain is known*—Suppose a company has a department working on highly confidential research, and this department is segmented from the rest of the network by routers and firewalls. This department maintains its own domain controllers and DNS servers that aren’t part of the organization’s domain. However, department members often need access to resources on the corporate servers. In addition, the research department’s DNS servers aren’t permitted to contact the Internet. For computers in this department network to resolve names for corporate resources, a forwarder can be configured on its DNS server that points to a corporate DNS server. The corporate DNS server not only resolves queries for corporate domain resources, but also performs recursive lookups for external domains on behalf of the research department’s DNS server.
- *When only one DNS server in a network should make external queries*—A network consisting of several DNS servers might want to limit external queries to a single DNS server. This strategy has several benefits. First, network security can be enhanced by limiting exposure to the Internet to only one server. Second, because a single server is making all the queries to Internet domains, overall DNS performance can be enhanced because the server builds an extensive cache of Internet names. To use this strategy, all DNS servers on the network, except the actual forwarder, should be configured with the forwarder.
- *When a forest trust is created*—Windows requires DNS name resolution between the two forests involved in a trust relationship. Configuring conditional forwarders in the forest root name servers of both forests that point to each other is a good way to accomplish this.
- *When the target domain is external to the network and an external DNS server’s address is known*—A company running a small network with limited bandwidth might find that

the traffic caused by an internal DNS server's recursive lookups is excessive. The internal DNS server can provide name resolution for all internal resources and forward queries for external names to the DNS server of the company's ISP.

Starting with Windows Server 2003, Microsoft introduced conditional forwarding. Traditional forwarding means "If you can't resolve the query, forward it to this address." Conditional forwarding enables administrators to forward queries for particular domains to particular name servers and all other unresolved queries to a different server.

Configuring Traditional Forwarders Configuring a traditional forwarder is straightforward. Right-click the server node in DNS Manager, click Properties, and click the Forwarders tab (see Figure 9-17).

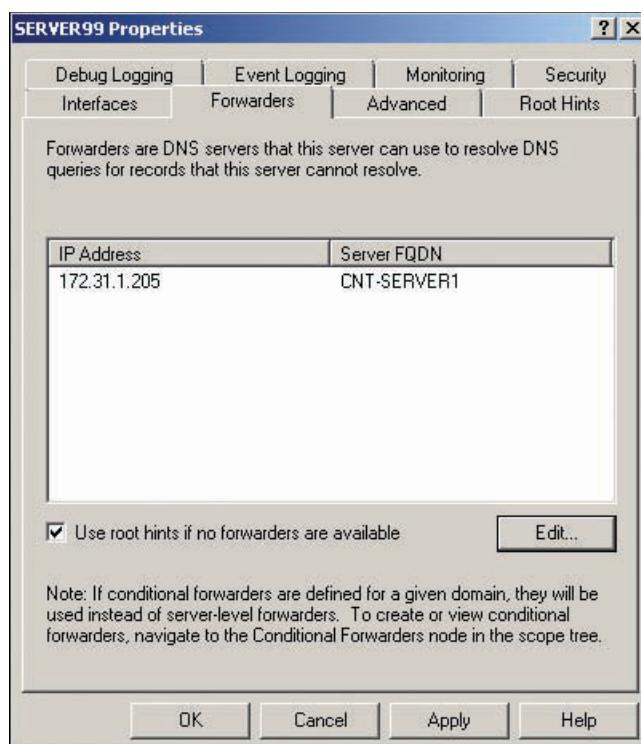


Figure 9-17 Configuring traditional forwarders

After clicking the Edit button, you can enter the IP address or FQDN of DNS servers to which unresolved requests should be sent. If more than one server is specified, they are queried in the order in which they're listed. Additional servers are queried only if no response is received from the first server. If no response is received from any forwarder, by default, the normal recursive lookup process is initiated, starting with a root server. If the "Use root hints if no forwarders are available" check box (see Figure 9-17; discussed later in the chapter) is not selected and no forwarders respond, the DNS server sends a failure reply to the client.

Configuring Conditional Forwarders In Windows Server 2003, both traditional and conditional forwarders were configured in the Forwarders tab, but in Server 2008, Microsoft moved configuring conditional forwarders to a node in DNS Manager. To create a new conditional forwarder, expand the Conditional Forwarders node, and then right-click Conditional Forwarders and click New Conditional Forwarder to open the dialog box shown in Figure 9-18.

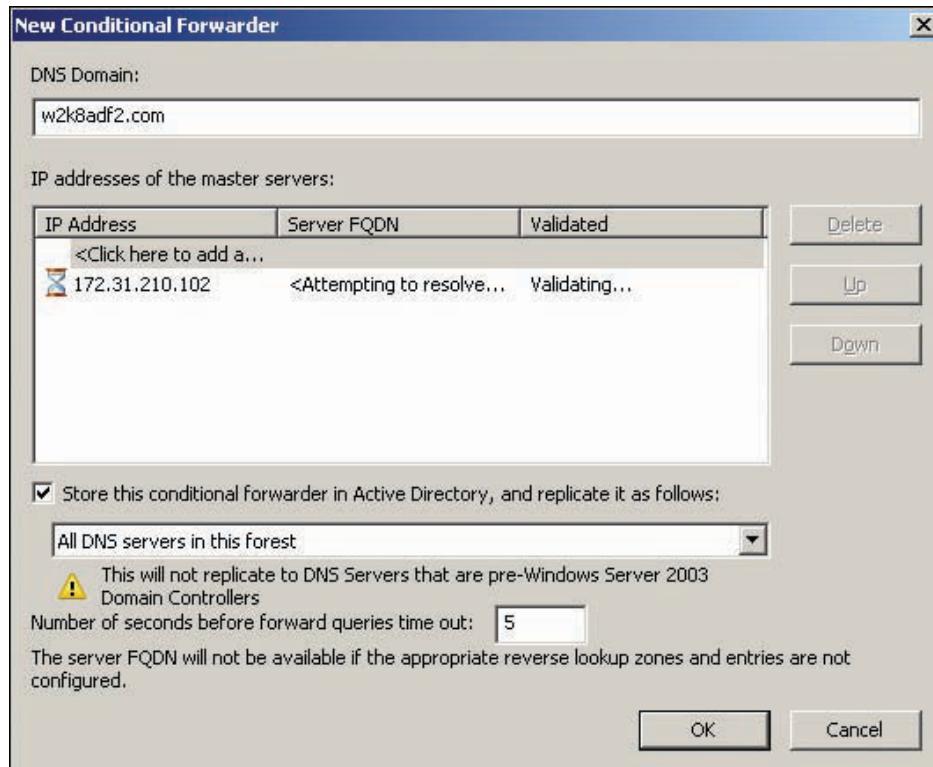


Figure 9-18 Configuring conditional forwarders

Enter the domain name for which you want to forward queries, and then add IP addresses for DNS servers that are authoritative for the domain. After you enter the IP address, Windows attempts to resolve the IP address to the server's FQDN. You can store the forwarder in Active Directory and have it replicated forest-wide or domain-wide. With forwarders and/or conditional forwarders configured, the DNS server attempts to resolve DNS queries in this order:

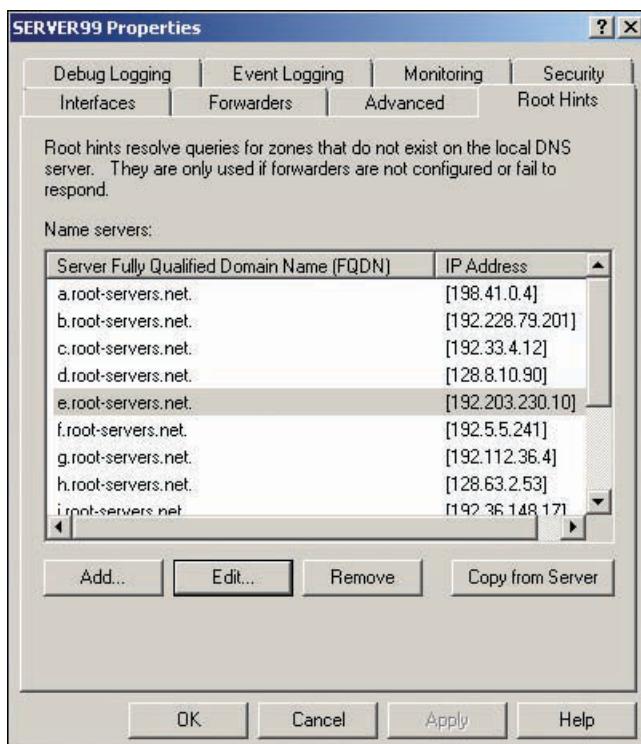
1. From locally stored zone resource records
2. From the DNS cache
3. From conditional forwarders (if configured and the domain name matches)
4. From traditional forwarders (if configured)
5. Recursively by using root hints (only if no traditional forwarder is configured)



Root hints aren't used if a traditional forwarder is configured because after the forwarder is queried, the recursive lookup process is complete.

Root Hints

Root hints consist of a list of name servers preconfigured on Windows DNS servers that point to Internet root servers, which are DNS servers located on the Internet and managed by the Internet Assigned Numbers Authority (IANA). These servers contain lists of name servers that are responsible for top-level domains. Root hints are configured in the Root Hints tab of a DNS server's Properties dialog box (see Figure 9-19).



9

Figure 9-19 Configuring root hints

The root hints data comes from the Cache.dns file located in the %SystemRoot%\System32\DNS folder on a DNS server. Why is this file called the root hints file? As you can imagine, if the file is loaded during DNS installation, its data (root server IP addresses, for the most part) can become obsolete quickly. Instead of using the addresses in Cache.dns to perform recursive lookups, Windows selects one of the addresses randomly to request an up-to-date list of root server addresses. Windows then caches this list to use for queries to TLD servers. The Cache.dns file is also updated with this list. The query for the list of root servers occurs each time the DNS server is started. The root hints file can also be copied from another DNS server by clicking the Copy from Server button in the Root Hints tab. In addition, root hints can be updated through the Windows Update service.

You can configure an internal DNS server as a root server if your network is isolated from the public Internet. You do this by creating an FLZ named “.”. This server is then considered authoritative for all domains. After you create this new root zone, your root hints file is disabled, and you can't create any forwarders. Next, configure your other DNS servers to point to your new root server. Remove the existing root hints entries and add an entry that points to your new root server. If you ever decide to remove the root server, simply delete the root FLZ, and Windows prompts you to reload the root hints file.

Round Robin

You can configure load sharing among servers running mirrored services. With a mirrored service, data for a service running on one server is duplicated on another server (or servers). For example, you can set up an FTP server or a Web server on servers that synchronize their content with one another regularly. Then configure DNS with multiple A records, using the server's name in both records, but with each entry configured with a different IP address.

For example, suppose you have a Web server with the FQDN www.coolgadgets.com that is heavily used, responding slowly, and dropping connections. You can set up two additional Web

servers and configure a mechanism for synchronizing files between the servers, such as DFSR or a third-party file synchronization service. Next, you create two additional DNS A records (you already have one for the existing Web server) in the coolgadgets.com domain that use the same hostname, www, but different IP addresses. The Windows DNS service responds to queries for the www host by sending all three IP addresses in the response but varying the order of IP addresses each time.

This process is called **round robin** because each IP address is placed first in the list an equal number of times. Hosts receiving the DNS response always attempt to use the first address listed. You can improve the results of round robin DNS by configuring a shorter TTL on the three A records so that remote DNS servers don't cache IP addresses for an extended period. By default, the round robin option is enabled on Windows DNS servers, but you can disable it in the Advanced tab of the DNS server's Properties dialog box (see Figure 9-20 in the next section).

Recursive Queries

Recursive queries, used in DNS queries, were defined earlier in “The DNS Lookup Process.” Typically, resolving DNS queries involves iterative queries to a root server first, then to a TLD server, and finally to an authoritative server for the domain name being resolved. However, a recursive query might involve a forwarder instead, in which the DNS server sends a recursive query to the forwarder. The forwarder resolves the query and responds to the DNS server or performs a recursive query starting with a root server.

Recursion is enabled on Windows DNS servers by default, but there are two ways to change this setting. The first involves configuring forwarders. As shown previously in Figure 9-17, there's the check box “Use root hints if no forwarders are available.” If this check box isn't selected, recursion is disabled, but only if forwarders do not respond. The second is the “Disable recursion (also disables forwarders)” option in the Advanced tab of the DNS server's Properties dialog box (see Figure 9-20). If this check box is selected, the DNS server doesn't

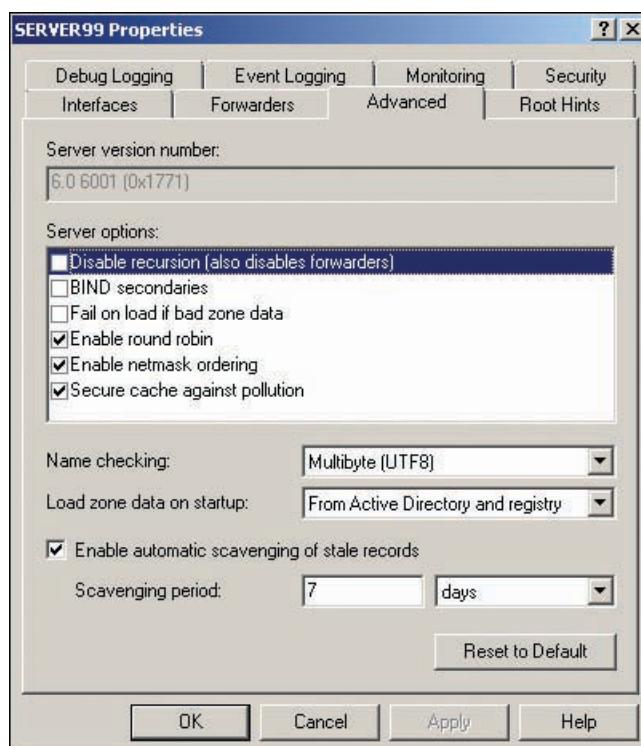


Figure 9-20 The Advanced tab of a DNS server's Properties dialog box

attempt to contact any other DNS servers, including forwarders, to resolve a query. For example, you might want to disable recursion when you have a public DNS server containing resource records for your publicly available servers (Web, e-mail, and so forth). The public DNS server is necessary to resolve iterative requests from other DNS servers for your public domain, but you don't want unauthorized Internet users using your DNS server to field recursive client requests.

Event and Debug Logging

When DNS is installed, a new event log is created to record informational, error, and warning events generated by the DNS server. You can configure which event types should be logged in the Event Logging tab of the server's Properties dialog box (shown in Figure 9-21). Events you're likely to find in the DNS Server log include zone serial number (referred to as version number in the DNS Server log) changes, zone transfer requests, and DNS server startup and shutdown events. The event log can help you diagnose problems, such as when an error causes the server to stop or keeps it from starting or when communication between servers for replication or zone transfers has failed. When DNS problems are evident and can't be traced easily to misconfiguration, the event log is the first place to look.

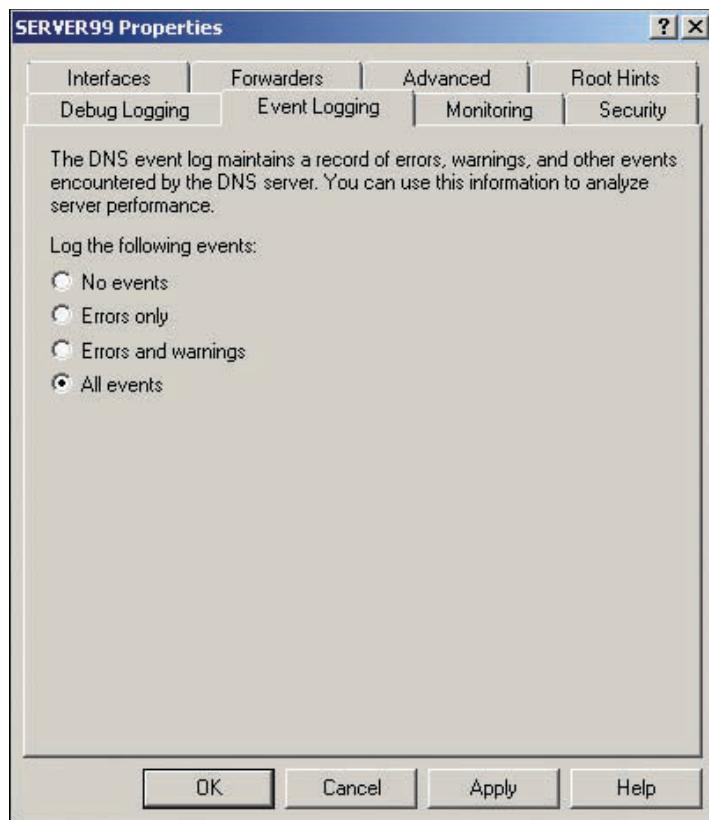


Figure 9-21 The Event Logging tab

When serious DNS debugging is warranted, you can enable debug logging in the server's Properties dialog box. Debug logging records selected packets coming from and going to the DNS server in a text file. Figure 9-22 shows the packet-capturing options for debug logging.

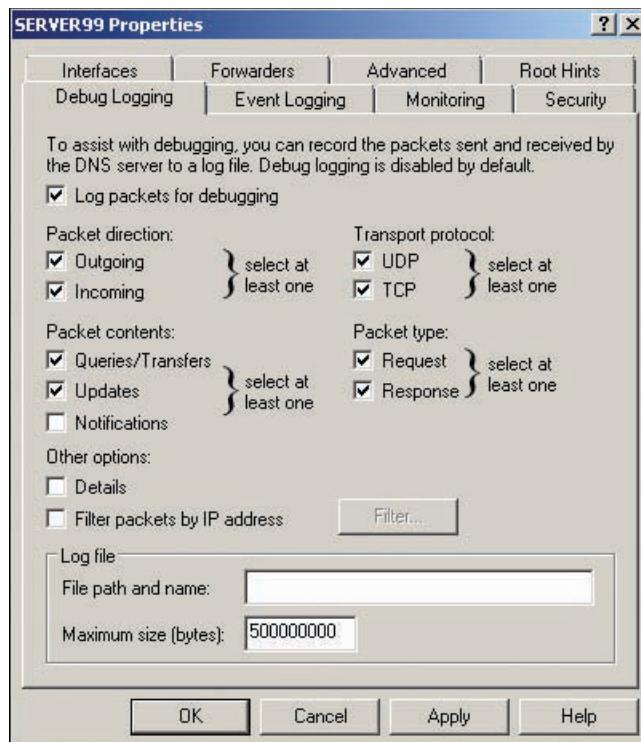


Figure 9-22 The Debug Logging tab

Figure 9-23 shows a sample of debug logging output. The first part of the file is a key to help you interpret the captured data. Each line of the file starting with date and time is a summary of a captured packet. If necessary, you can enable logging of detailed packet contents. The information from debug logging can help you solve problems related to “Web page not found” errors, zone transfer problems, redirect errors, and other DNS operational errors that aren’t easy to find by examining the DNS configuration and event logs alone.

```

dnslog2.txt - Notepad
File Edit Format View Help
DNS Server log file creation at 8/13/2008 12:50:32 PM
Message logging key (for packets - other items use a subset of these fields):
Field # Information values
-----
1 Date
2 Time
3 Thread ID
4 Context
5 Internal packet identifier
6 UDP/TCP indicator
7 Send/Receive indicator
8 Remote IP
9 Xid (hex)
10 Query/Response R = Response
     blank = Query
     Q = Standard Query
     N = Notify
     U = Update
     ? = Unknown
11 Opcode
12 [ Flags (hex) ]
13 Flags (char codes) A = Authoritative Answer
     T = Truncated Response
     D = Recursion Desired
     R = Recursion Available
14 ResponseCode ]
15 Question Name
16 Question Type

8/13/2008 7:52:51 PM 0D60 PACKET 02F38038 UDP Snd 127.0.0.1 4d3f R Q [8385 A DR NXDOMAIN] SRV (5)_ldap(4)_tcp(18)Site217-Pit
8/13/2008 7:53:02 PM 0D60 PACKET 036246C8 UDP Rcv 127.0.0.1 6efa Q [0001 D NOERROR] SRV (5)_ldap(4)_tcp(8)Server99(8)v
8/13/2008 7:53:02 PM 0D60 PACKET 036246C8 UDP Snd 127.0.0.1 6efa R Q [8385 A DR NXDOMAIN] SRV (5)_ldap(4)_tcp(8)Server99(8)v
8/13/2008 7:53:09 PM 0D60 PACKET 0364FB08 UDP Rcv 172.31.210.1 0003 Q [0001 D NOERROR] A (11)coolgadgets(6)tomsho(3)com
8/13/2008 7:53:09 PM 0D60 PACKET 036AD630 UDP Snd 172.31.1.205 bb6c Q [0001 D NOERROR] A (11)coolgadgets(6)tomsho(3)com
8/13/2008 7:53:09 PM 0D60 PACKET 032E46C8 UDP Rcv 172.31.1.205 bb6c R Q [8385 A DR NXDOMAIN] A (11)coolgadgets(6)tomsho(3)com
8/13/2008 7:53:09 PM 0D60 PACKET 032E46C8 UDP Snd 172.31.210.1 0003 R Q [8385 A DR NXDOMAIN] A (11)coolgadgets(6)tomsho(3)com

```

Figure 9-23 Debug logging output

Monitoring and Troubleshooting DNS

A network's DNS structure can range from a basic single-domain, single-server scheme to a complex multidomain scheme with subdomains, secondary zones, forwarders, delegations, and stub zones. In addition, many environments use more than one name resolution service; for example, some Windows applications and services depend on WINS and NetBIOS lookups. To troubleshoot a DNS problem, such as a failed name resolution, first you need to know that DNS is actually used for name resolution. After determining that DNS is part of the process, you can begin monitoring DNS, if the problem is performance related, or troubleshooting DNS queries and zone activities when there are query failures.

DNS Troubleshooting

Windows has several tools to administer, monitor, and troubleshoot DNS server operation, including the following commonly used tools:

- *DNS Manager*—The main DNS configuration tool, used to perform most DNS configuration tasks, monitor zone data and the DNS cache's contents, and configure event logging and debug logging.
- *Dnscmd.exe*—A powerful command-line tool that enables administrators to perform basic to advanced configuration and monitoring. Some available command options are as follows (commands aren't case sensitive but use capitalization for better readability):
 - /Info—Displays server information
 - /Config—Allows detailed configuration of Registry values that affect DNS server and zone operation, such as setting a Registry value to prevent the server from caching recursive lookup records
 - /Statistics—Displays or clears server statistics
 - /ClearCache—Clears the server cache
 - /ZoneInfo—Displays zone information
 - /ZoneAdd—Creates a new zone
 - /ZoneDelete—Deletes a zone
 - /RecordAdd—Adds a resource record
 - /RecordDelete—Deletes a resource record
 - /CreateDirectoryPartition—Creates a custom directory partition
 - /ExportSettings—Exports DNS settings to a text file
- *Event Viewer*—Used to view the DNS Server event log (can also be viewed in the Global Logs node in DNS Manager).
- *Dnslint*—A command-line program used to check for resource records on a server, verify delegations, verify resource records needed for Active Directory replication, and perform e-mail connectivity tests. You can download Dnslint from the Microsoft Web site and find information on using it at <http://support.microsoft.com/kb/321045>.
- *Nslookup*—Used to test DNS queries with the default DNS server or a specific DNS server.
- *Ipconfig*—Used to check DNS client configuration and the DNS suffix search list; also used to cause a client to register its DNS name and display and delete locally cached DNS records.
- *Performance Monitor*—Found in Server Manager under the Diagnostics node; you can monitor more than 60 performance counters related to DNS.
- *Protocol analyzer*—This type of tool provides information similar to debug logging but with more flexibility. Network Monitor no longer ships with Windows Server 2008 and Vista, but you can download it from the Microsoft Download Center. An excellent freeeware protocol analyzer, Wireshark, can be downloaded from www.wireshark.org.

Before you can begin troubleshooting DNS queries efficiently, you need a clear picture in your mind of the DNS lookup process. Earlier in the chapter, an example was given but didn't factor in variables such as the Hosts file, cache, and forwarders. Taking these factors into account, a DNS lookup involves the following steps, starting with the DNS client:

1. Check the local DNS cache, which contains the contents of the Hosts file.
2. Query the DNS server with a recursive lookup.

If the address is resolved in Step 1, it's returned to the requesting application, and the process is completed. After Step 2 has been initiated, the query is in the hands of the DNS server being queried, and the following steps occur on this server:

3. Check local zone data.
4. Check locally cached data.
5. Query root server or configured forwarders.

Remember that Step 3 can include primary zones, secondary zones, and stub zones as well as delegated zones. At Step 5, the recursive query process continues until the name is resolved or a failed message is returned. At this point, however, the lookup process is largely out of the local administrator's hands.

When troubleshooting a query, you want to eliminate the easy things first, which usually means verifying the client configuration. To verify DNS configuration, use these Ipconfig options:

- /all—Displays IP addresses of the configured DNS servers as well as the DNS suffix search list.
- /displaydns—Displays the local DNS cache, which also has the contents of the Hosts file.
- /flushdns—Deletes the local DNS cache. Sometimes the local cache is big, and spotting a problem could be difficult. Deleting the cache is harmless and can save you from wading through dozens of cached entries.

After these steps, double-check the Hosts file to make sure you didn't miss something when you displayed the local cache.

If everything checks out on the client, your job just got tougher. You'll probably want to proceed with analyzing the DNS server the client uses, including examining the following:

- *Locally cached data*—Stale records can return incorrect results. If you suspect records are stale, delete the cache or the suspect domains in the cache.
- *DNS Server log*—Use Event Viewer to view the DNS Server log, or use DNS Manager to view the DNS Events node under the Global Logs node. Both applications record the same information. Look for warning or error messages indicating service failures or zone transfer or replication failures.
- *Verify Active Directory replication*—You can use Dnslint to verify that the correct resource records exist for Active Directory replication. The dnsllint /ad /s localhost /v command generates a report in HTML format and opens the report in Internet Explorer. Warnings and errors are color-coded in the report.
- *Verify zone transfers*—Nslookup can request records from an entire zone. On a server hosting secondary zones, use Nslookup in interactive mode by typing nslookup and pressing Enter. Change the server to the primary DNS server for the zone with the server *server-name* command, and then use ls -d *domain* (substituting the name of the zone you want to verify for *domain*). If zone transfers aren't working, you get a "query refused" message. Otherwise, the zone data is displayed. Also, verify the settings in the Zone Transfer tab on the primary server to make sure the secondary server is in the server list or that any server can request zone transfers.
- *Verify zone delegations*—Dnsllint can be used for this task, too. Use the dnsllint /d *delegated-zone* /s *IP_of_authoritative_server* command to produce a report to verify the delegation.

- *Ping*—Use Ping to verify connectivity to remote DNS servers that might be part of the lookup process.
- *Verify PTR records*—It's easy to forget to create the zones needed for PTR records and to make sure PTR records are created when entering a new A record manually. Certain processes require reverse lookups, so make sure critical servers have PTR records as well as A records. To do this, check for the reverse lookup zone in DNS Manager, or use Nslookup to first do a forward lookup for the host's IP address and then do a reverse lookup, using the returned IP address. If the lookup fails, the PTR record doesn't exist. The process is shown in Figure 9-24.

Administrator: Command Prompt - nslookup

```
C:\>Users\Administrator>nslookup
Default Server: localhost
Address: 127.0.0.1

> host1.testzone.com
Server: localhost
Address: 127.0.0.1

Name: host1.testzone.com
Address: 172.31.210.155

> 172.31.210.155
Server: localhost
Address: 127.0.0.1

*** localhost can't find 172.31.210.155: Non-existent domain
>
```

9

Figure 9-24 Use Nslookup to verify PTR records

The procedures and tools described in this section should arm you with the necessary knowledge to start the DNS troubleshooting process and solve at least minor problems. More complex problems take some perseverance with these tools and perhaps debug logging and protocol analysis. The better you understand the DNS process, the more quickly you can solve problems. Use debug logging and a protocol analyzer periodically to examine DNS operation when it's working correctly, and save these results. This way, you have something to compare with troubleshooting output when problems happen.

Monitoring DNS Performance

DNS performance can degrade over time because of increased database size and increased client activity. Performance can also suffer because of poor design decisions that use excessive bandwidth for zone transfers or Active Directory replication. Dnscmd.exe can display a snapshot of server statistics with the dnscmd /statistics command, but Performance Monitor is a more powerful tool. As discussed, you can gather information on more than 60 performance counters related to DNS. Figure 9-25 shows Performance Monitor graphing the following counters:

- *AXFR Request Received*—Total full zone transfer requests received
- *Total Query Received/sec*—The average number of queries received each second
- *Zone Transfer Success*—The total number of successful zone transfers during the monitoring period

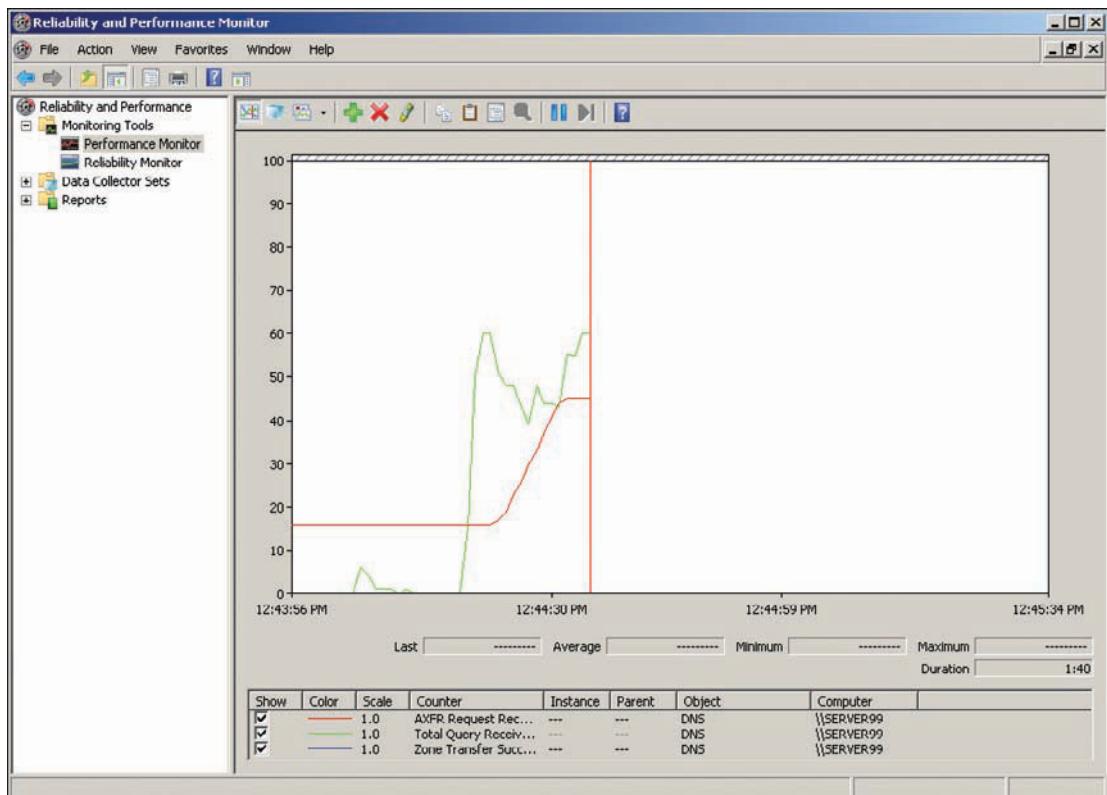


Figure 9-25 Viewing counters in Performance Monitor

You should sample some key DNS counters periodically when DNS is performing well because this information is useful for troubleshooting. In Performance Monitor, you can view performance in real time or save the data to a log to be viewed later. You can save logs of key counters for which you have collected data during peak and off-peak hours. These saved logs constitute your baseline for DNS performance. Later, if DNS performance is degrading, you can compare baseline logs to current data to see which counters differ significantly, allowing you to pinpoint the bottleneck. Because queries and dynamic updates are among the most frequent tasks a server handles, these two counters should be included in your baseline logs: Total Query Received/sec and Dynamic Update Received/sec.

Chapter Summary

- DNS is based on a hierarchical naming structure and a distributed database. DNS names use the structure *host.domain.top-level-domain* or perhaps *host.subdomain.domain.top-level-domain*. This name is referred to as the fully qualified domain name (FQDN).
- DNS can be described as an inverted tree with the root domain at the top, TLDs branching off the root, and domains and subdomains branching off TLDs. The entire DNS tree is called the DNS namespace. Every domain has one or more authoritative name servers.
- The DNS database is composed of zones containing resource records, such as Start of Authority (SOA), Host (A), and Service (SRV) records. Host (A) resource records can be updated with static or dynamic updates.
- DNS lookups involve iterative and recursive queries. Most lookups start from the DNS resolver with a recursive query to a DNS server. The DNS server satisfies the query or performs a series of iterative queries, starting with a root server.
- DNS servers can perform one or more of the following roles: authoritative server, forwarder, conditional forwarder, and caching-only server. DNS databases consist of the

following zone types: primary zone, secondary zone, and stub zone. Primary and stub zones can also be Active Directory-integrated zones.

- Active Directory-integrated zones have the advantages of automatic replication, multimaster replication and update, secure updates, and efficient replication. The scope of Active Directory zone replication can be forest-wide, domain-wide, or custom.
- A zone can be a forward lookup zone or a reverse lookup zone. FLZs contain host records primarily. Reverse lookup zones contain PTR records.
- SOA records contain information about a zone, including its serial number and a number of timers used for zone transfers. NS records specify the name of a server that's authoritative for the zone.
- Subdomains can be delegated to a zone on another server to improve performance and control replication scope. Stub zones are often used to keep delegation records up to date. Zone transfers can be full or incremental and occur from a primary or secondary zone to a secondary zone.
- Advanced DNS settings include configuring forwarders, root hints, round robin, recursive queries, and logging.
- Tools for monitoring and troubleshooting DNS include Dnscmd, Dnslint, Nslookup, Ipconfig, and Performance Monitor. You need to understand the DNS query process to troubleshoot DNS problems efficiently. Performance Monitor is used to gather counter data on DNS activities. You can save data to a log as a baseline and compare it with data gathered later when there are problems.

Key Terms

Active Directory-integrated zone A primary or stub zone with the DNS database stored in an Active Directory partition rather than a text file. Because Active Directory zones are replicated to other domain controllers automatically, only primary and stub zones can be Active Directory integrated.

authoritative server A DNS server that holds a complete copy of a zone's resource records (typically a primary or secondary zone).

caching-only DNS server A DNS server with no zones. Its sole job is to field DNS queries, do recursive lookups to root servers, or send requests to forwarders, and then cache the results.

conditional forwarder A DNS server to which other DNS servers send requests targeted for a specific domain.

DNS namespace Defines the structure of the names used to identify resources in Internet domains. It consists of a root name (defined as a period), top-level domains, second-level domains, optionally one or more subdomains, and hostnames separated by periods.

Dynamic DNS (DDNS) A DNS name-registering process whereby computers in the domain can register or update their own DNS records.

forwarder A DNS server to which other DNS servers send requests they can't resolve themselves.

forward lookup zone (FLZ) A DNS zone containing records that translate names to IP addresses, such as A, AAAA, and MX records. It's named after the domain whose resource records it contains.

GlobalNames zone (GNZ) A new feature in Windows Server 2008 that provides a method for IT administrators to add single-label names (computer names that don't use a domain suffix) to DNS, thereby allowing client computers to resolve these names without including a DNS suffix in the query.

glue A record An A record used to resolve the name in an NS record to its IP address.

iterative query A type of DNS query to which a DNS server responds with the best information it has to satisfy the query. The DNS server doesn't query additional DNS servers in an attempt to resolve the query.

primary zone A DNS zone containing a read/write master copy of all resource records for the zone; this zone is authoritative for the zone.

recursive query A query in which the DNS server processes the query until it responds with an address that satisfies the query or with an “I don’t know” message. The process might require the DNS server to query several additional DNS servers.

referral A response to an iterative query in which the address of another name server is returned to the requester.

resolver A DNS client that sends a recursive query to a DNS server.

resource record Data in a DNS database that contains information about network resources, such as hostnames, other DNS servers, and services, and is identified by a letter code.

reverse lookup zone (RLZ) A DNS zone containing PTR records that map IP addresses to names; it’s named with the IP network address (IPv4 or IPv6) of the computer whose records it contains.

root hints A list of name servers preconfigured on Windows DNS servers that point to Internet root servers, which are DNS servers located on the Internet and managed by IANA.

root servers DNS servers that keep a database of addresses of other DNS servers managing top-level domain names.

round robin A method of responding to DNS queries when more than one IP address exists for the queried host. Each IP address is placed first in the list of returned addresses an equal number of times so that hosts are accessed alternately.

scavenging A process whereby the DNS server checks the zone file for stale records periodically and deletes those meeting the criteria for a stale record.

secondary zone A DNS zone containing a read-only copy of all resource records for the zone. Changes can’t be made directly on a secondary DNS server, but because it contains an exact copy of the primary zone, it’s considered authoritative for the zone.

standard zone A primary, secondary, or stub zone that isn’t Active Directory integrated.

stub zone A DNS zone containing a read-only copy of only the zone’s SOA and NS records and the necessary A records to resolve NS records. A stub zone forwards queries to a primary DNS server for that zone and is not authoritative for the zone.

top-level domain (TLD) servers DNS servers that maintain addresses of other DNS servers that are authoritative for second-level domains that use the top-level domain. For example, a TLD server for the com top-level domain contains NS records for authoritative DNS servers for all domains ending in .com.

zone A grouping of DNS information that represents one or more domains and possibly subdomains.

zone delegation The transfer of authority for a subdomain to a new zone, which can be on the same server as the parent zone or on another server.

zone transfer An operation that copies all or part of a zone from one DNS server to another and occurs as a result of a secondary server requesting the transfer from another server.

Review Questions

1. Which of the following best describes DNS? (Choose all that apply.)

- a. Hierarchical database
- b. Flat database
- c. Monolithic database
- d. Distributed database

2. Which of the following accurately represents an FQDN?

- a. host.top-level-domain.subdomain.domain
- b. domain.host.top-level-domain

- c. host.subdomain.domain.top-level-domain
d. host.domain.top-level-domain.subdomain
3. A DNS server that can't resolve a query from its local data sends a recursive query to a root server. True or False?
4. A resource record containing an alias for another record is which of the following record types?
a. A
b. CNAME
c. NS
d. PTR
5. What type of resource record is necessary to get a positive response from the command nslookup 192.168.100.10?
a. A
b. CNAME
c. NS
d. PTR
6. When a DNS server responds to a query with a list of name servers, what is the response called?
7. You're scanning the local cache on a DNS client, and you run across the notation ::1. What does this notation mean?
8. Your company just opened a small branch office where 10 computer users will work. You have installed a single Windows Server 2008 computer configured as a member server for basic file and print server needs. Users require DNS for Internet access and access to company resources. You decide to install DNS on the existing server. Which of the following types of installations makes the most sense?
a. A primary server hosting a standard zone
b. An Active Directory-integrated zone hosting the zone in which the server is a member
c. A caching-only DNS server
d. A server that's a forwarder
9. You have a DNS server outside your corporate firewall that's a stand-alone Windows Server 2008 server. It hosts a primary zone for your public Internet domain name, which is different from your internal Active Directory domain names. You want one or more of your internal servers to be able to handle DNS queries for your public domain and to serve as a backup for the primary DNS server outside the firewall. Which configuration should you choose for internal DNS servers?
a. Configure a standard secondary zone.
b. Configure a standard stub zone.
c. Configure a forwarder to point to the primary DNS server.
d. Configure an Active Directory-integrated stub zone.
10. DNS ServerA forwards a query to ForwarderB, which replies with a "not found" message. DNS ServerA continues the lookup by querying a root server. True or False?
11. Which of the following is true about a stub zone? (Choose all that apply.)
a. They are authoritative for the zone.
b. Their records are updated by the primary server automatically.
c. They can't be Active Directory integrated.
d. They contain SOA and NS records.

12. You have Windows Server 2008 DNS servers, Windows Server 2003 DNS servers, and Windows 2000 DNS servers. You just created a new zone, newzone.com, that you want replicated by Active Directory to all DNS servers. Where should you store the zone?
 - a. ForestDNSZones partition
 - b. Newzone.com.dns
 - c. DomainDNSZones partition
 - d. Domain partition
13. The DNS server at your headquarters holds a standard primary zone for the abc.com domain. A branch office connected by a slow WAN link holds a secondary zone for abc.com. Updates to the zone aren't frequent. How can you decrease the amount of WAN traffic caused by the secondary zone checking for zone updates?
 - a. In the SOA tab of the zone's Properties dialog box, increase the minimum (default) TTL.
 - b. In the Advanced tab of the DNS server's Properties dialog box, increase the expire interval.
 - c. In the SOA tab of the zone's Properties dialog box, increase the refresh interval.
 - d. In the Zone Transfers tab of the SOA Properties dialog box, decrease the retry interval.
14. You have delegated a subdomain to a zone on another server. Several months later, you hear that DNS clients can't resolve host records in the subdomain. You discover that the IP address scheme was changed recently in the building where the server hosting the subdomain is located. What can you do to make sure DNS clients can resolve hostnames in the subdomain?
 - a. Configure a forwarder pointing to the server hosting the subdomain.
 - b. Edit the NS record in the delegated zone on the parent DNS server.
 - c. Edit the NS record in the delegated zone on the DNS server hosting the subdomain.
 - d. Configure a root hint pointing to the server hosting the subdomain.
15. You want a DNS server to handle queries for a domain with a standard primary zone hosted on another DNS server. You don't want your server to be authoritative for that zone. How should you configure your server? (Choose all that apply.)
 - a. Configure a secondary zone on your DNS server.
 - b. Configure a stub zone on your DNS server.
 - c. Configure a forwarder on your DNS server.
 - d. Configure a delegation on your Web server.
16. You're in charge of a standard primary zone for a large network with frequent changes to the DNS database. You want changes to the zone to be transmitted as quickly as possible to all secondary servers. What should you configure and on what servers?
17. You have several hundred client computers using WINS to resolve names of some enterprise servers. Many of the client computers are laptops used to connect to the network remotely. You're trying to eliminate WINS from your network to reduce the number of protocols and services you must support. What can you do, with the least administrative effort, that allows you to stop using WINS yet still allows clients computers to use a single-label name for accessing enterprise servers?
 - a. Create a GlobalNames zone and add CNAME records for enterprise servers.
 - b. Create a Hosts file containing servers' names and addresses and upload the Hosts file to each client that needs it.
 - c. Configure each client computer with the correct domain suffix.
 - d. Create a stub zone and add CNAME records for each enterprise server.

18. You manage the DNS structure on your network. The network security group has decided that only one DNS server should contact the Internet. Under no circumstances should other servers contact the Internet for DNS queries, even if the designated server is down. You have decided that the DNS server named DNS-Int should be the server allowed to contact the Internet. How should you configure your DNS structure to accommodate these requirements?
- On each DNS server except DNS-Int, configure a forwarder pointing to DNS-Int. Configure DNS-Int as a forwarder by enabling forwarded requests in the Forwarders tab of the server's Properties dialog box.
 - On each DNS server except DNS-Int, configure a root hint to point to DNS-Int and delete all other root hints. Configure a root zone on DNS-Int.
 - On each DNS server except DNS-Int, configure a forwarder pointing to DNS-Int. Disable the use of root hints if no forwarders are available. No changes are necessary on DNS-Int.
 - On each DNS server except DNS-Int, in the Advanced tab of the server's Properties dialog box, disable recursion. No changes are necessary for DNS-Int.
19. You have a zone containing two A records for the same hostname, but each A record has a different IP address configured. The host records point to two servers hosting a high-traffic Web site, and you want the servers to share the load. After some testing, you find that you're always accessing the same Web server, so load sharing isn't occurring. What can you do to solve the problem?
- Enable the load sharing option on the zone.
 - Enable the round robin option on both A records.
 - Enable the load sharing option on both A records.
 - Enable the round robin option on the server.
20. Which is the correct order in which a DNS client tries to resolve a name?
- Cache, DNS server, Hosts file
 - Hosts file, cache, DNS server
 - Cache, Hosts file, DNS server
 - DNS server, cache, Hosts file
21. You want to verify whether a PTR record exists for the AHost.ADomain.com host, but you don't know the IP address. Which of the following commands should you use?
- Ping -a AHost.ADomain.com, and then Ping *IPAddress* returned from the first Ping
 - Nslookup AHost.ADomain.com, and then Nslookup *IPAddress* returned from the first Nslookup
 - Dnscmd /PTR AHost.ADomain.com
 - Dnslint /PTR AHost.ADomain.com
22. You have been communicating with ComputerB from your workstation for the past several hours. A colleague informs you that he has just made some changes to the IP addressing scheme on the network where ComputerB is located. You find that you can no longer communicate with ComputerB. What tool can you use on your workstation to solve the problem?
- Ping
 - Nslookup
 - Ipconfig
 - Dnslint
23. To resolve a query, a DNS server looks in its local cache first. True or False?

24. You have just finished setting up your DNS infrastructure, and the DNS process seems to be working well. You want to be able to create a baseline of performance data so that if slowdowns occur later, you have information for comparison purposes. Which tool should you use?
 - a. Dnscmd.exe
 - b. Debug logging
 - c. Performance Monitor
 - d. Event logging
25. You're trying to track down a DNS name resolution problem. So far, you haven't been able to get the data you need to see exactly what's happening when DNS queries fail. You need to see the actual data packets being sent to and from DNS servers. Which tool should you use?
 - a. Dnslint
 - b. Debug logging
 - c. Performance Monitor
 - d. Nslookup

Case Projects



Case Project 9-1: Providing Zone Fault Tolerance

In this project, you work in groups of at least three people. You want to have at least two other servers that are authoritative for your domain. Work with others in your group so that the zone for each user's domain is supported by two other servers that are authoritative for the zone. Write down the details of how you will accomplish this task. Have your instructor review your solution before you implement it. After implementing your solution, test its effectiveness from your server (without looking at your partner's servers). Write down what you did to perform your test.

Case Project 9-2: Expanding Your Reach

Now that you can communicate by using DNS lookups with the servers and workstations in your partner's domains, you want to be able to use DNS to contact resources in the rest of the domains in your class. You don't want your server to be authoritative for any more domains. If the NS records of the other domains change, you don't want to have to make manual changes on your server. Write down the solution you plan to use, submit it to your instructor for approval, and then implement your solution. Test the solution and write down how you tested it.

Case Project 9-3: Stress-Testing Your DNS Server

You can work in groups on this project. You have just finished DNS installation and want to stress-test your DNS server to see how well it handles a lot of queries, both to local zones as well as zones requiring your server to do recursive lookups. You want to monitor the server's performance while it's being stressed. Devise a plan to stress-test the server and monitor its performance. Be specific. If feasible, implement your solution after your instructor has approved it.

Configuring and Maintaining the Active Directory Infrastructure

After reading this chapter and completing the exercises, you will be able to:

- Describe and configure Active Directory functional levels
- Add and remove domains from a forest
- Configure Active Directory trusts
- Configure intrasite replication
- Work with sites
- Manage operations master roles

The majority of day-to-day work in an Active Directory environment involves managing objects in a domain. With a single-domain, single-site environment, administrators rarely need to use other tools besides Active Directory Users and Computers. However, multidomain, multisite, and multiforest environments require maintenance and configuration of the Active Directory infrastructure in addition to user, group, and computer objects. For example, a Windows network that has been in operation for years often has a mix of server OSs. Your understanding of domain and forest functional levels is critical to maintain this environment. In addition, multiple forests or multiple trees in the same forest might require trust configuration. A multisite network requires a solid understanding of site configuration and how domain controllers at different sites replicate with one another. Finally, maintenance of operations master roles is critical in all but the smallest networks. These topics are paramount to maintaining an Active Directory environment and are especially important in the 70-640 certification exam.

Examining Active Directory Functional Levels

With each release of a Windows server OS, features have been added to make the Active Directory environment more capable and easier to manage. However, features added to a new OS release often aren't compatible with earlier releases. Instead of requiring administrators to upgrade their current servers before installing a new server version, Windows allows administrators to configure functional levels on new domain controllers to maintain backward compatibility.

When you install the first domain controller in a forest root domain, the forest functional level defaults to Windows 2000, and the domain functional level defaults to Windows 2000 native. These levels provide the most backward compatibility with older OSs. However, for optimum operation, functional levels should be set to the highest version that domain controllers on the network support. Be aware that domain and forest functional levels are specific to domain controllers. Member servers and workstation computers don't have this setting and can be domain members of domains and forests running at any functional level. The following sections discuss the features and requirements of each forest and domain functional level.



A functional level called Windows 2000 mixed provides backward compatibility with Windows NT domain controllers. This functional level has been deprecated in Windows Server 2008, and Windows NT domain controllers are no longer supported in the same network as a Windows Server 2008 domain controller.

Forest Functional Levels

The forest functional level determines the features of Active Directory that have forest-wide implications and which server OSs are supported on domain controllers in the forest. A Windows Server 2008 domain controller supports the following functional levels:

- Windows 2000
- Windows Server 2003
- Windows Server 2008

The forest functional level can be raised from an earlier version to a newer version, but it can't be changed from a newer version to an earlier version. The following sections describe the available features and supported OSs for each functional level.

Windows 2000 The Windows 2000 forest functional level supports all the default features of an Active Directory forest. Because Windows 2000 was the first server OS supporting Active Directory, this functional level is considered the baseline for forest operation. Some notable features not supported at this functional level include creating forest trusts and renaming a domain. This level supports running Windows 2000 Server through Windows Server 2008 on domain controllers.

Windows Server 2003 The Windows Server 2003 forest functional level requires all domain controllers in all domains to be running at least Windows Server 2003. If there's a possibility of using a Windows 2000 Server computer as a domain controller in your network, don't raise the forest functional level to Windows Server 2003.

This level supports all the forest-wide features of the Windows 2000 functional level and adds the following features:

- *Forest trusts*—Create a trust relationship between forests (discussed in Chapter 4). The Windows 2000 functional level allows trusts between two domains in different forests but not between two forests.
- *Knowledge Consistency Checker (KCC) improvements*—Large networks with more sites are supported by the Intersite Topology Generator (ISTG), a function the KCC performs on a domain controller in each site.
- *Linked-value replication*—At the Windows 2000 functional level, when group membership changes, the entire group membership is replicated. The Windows Server 2003 functional level replicates only changes to group membership, thereby saving network and processor bandwidth.
- *Rename a domain*—Domains in a Windows Server 2003 forest can be renamed by using the Rdom.exe and Gpfixup.exe command-line tools. Domain renaming is a complex process and should be attempted only after reviewing the documentation on the Microsoft Web site carefully.
- *Read only domain controller (RODC) deployment*—RODCs can be deployed in a Windows Server 2003 forest, but they must be running Windows Server 2008 (because RODCs were introduced in Server 2008). In addition, a writeable Windows Server 2008 domain controller must be installed first to replicate with the RODC. A writeable domain controller is a server with Active Directory installed without the RODC option; it supports making changes to the local Active Directory database.
- *Additional features*—Other features, related mostly to the Active Directory schema, include creating the dynamic auxiliary class named dynamicObject, converting the inetOrgPerson object (used by some LDAP applications) to a user object and vice versa, creating new group types to support role-based authorization, and deactivating schema attributes and classes.

Windows Server 2008 No forest-wide features have been added to this functional level, but new features could be added later. Therefore, to operate at this forest functional level, all domain controllers must be running at the Windows Server 2008 domain functional level and, therefore, must be running Windows Server 2008.

Domain Functional Levels

Windows Server 2008 supports three domain functional levels that have nearly identical names as the forest functional levels. A domain controller can't be configured to run at a lower functional level than the functional level of the forest in which it's installed. Like forest functional levels, domain functional levels can be raised but not lowered. After a domain's functional level has been raised, no domain controllers running earlier versions of the OS can be installed in the domain. The following sections summarize the features available at each level.

Windows 2000 Native The Windows 2000 native domain functional level includes all the original features given to domains by Active Directory. Windows Server 2003 and Windows 2000 Server support the Windows 2000 mixed functional level, which provides backward compatibility with Windows NT domains. Windows Server 2008 no longer supports this functional level, so Windows 2000 native is the baseline functional level for Windows Server 2008 domain controllers. The following list of features can be thought of as upgrades to the Windows NT domain system. Most of these features were discussed in Chapter 5.

- *Universal groups*—Allow administrators to assign rights and permissions to forest-wide resources to users from any domain.
- *Group nesting*—Allows most group types to be members of most other group types.
- *Group conversion*—Allows administrators to convert between security and distribution groups.
- *Security identifier (SID) history*—Facilitates migrating user accounts from one domain to another (which changes users' SIDs). A user's original SID is kept in the sIDHistory

(meaning “SID history”) attribute to determine the user’s group memberships in the original domain and maintain the user’s access to resources in the original domain.

This level supports running Windows 2000 Server and later on domain controllers.

Windows Server 2003 This level supports all the features in the Windows 2000 native functional level. All domain controllers must be running Windows Server 2003 or later. Added features for this functional level include the following:

- *Domain controller renaming*—The Netdom.exe command-line tool makes renaming a domain controller possible without undue latency. Using the System Properties dialog box to rename a domain controller doesn’t update DNS and Active Directory replication parameters completely, which could cause client authentication problems. Netdom does perform these updates.
- *Logon timestamp replication*—The lastLogonTimestamp user account attribute is updated with the time and date of a user’s last logon. This attribute is replicated to all domain controllers in the domain.
- *Selective authentication*—With this feature, an administrator can specify users and groups from a trusted forest who can authenticate to servers in a trusting forest.
- *Users and Computers container redirection*—When creating users, groups, and computers with command-line tools that don’t allow specifying a target OU (or if the location is omitted), these accounts are placed in the Users or Computers container. You can use the Redirusr (for users and groups) and Redircmp (for computers) commands to specify an alternate default location.
- *Additional features*—This level includes constrained delegation, Authorization Manager policy support, and the userPassword attribute set as the effective password on inetOrgPerson and user objects. These features are beyond the scope of this book, however.

Windows Server 2008 This functional level supports all features in the Windows Server 2003 functional level with several additions, described in the following list. All domain controllers must be running Windows Server 2008 or later.

- *Distributed File System (DFS) replication*—DFS is used to replicate the contents of the Sysvol share, which provides a more robust replication process.
- *Fine-grained password policies*—Discussed in Chapter 7, fine-grained password policies enable administrators to assign different password and account lockout policies for users and groups.
- *Interactive logon information*—Enabled through group policies, this option displays information about a user’s most recent successful and unsuccessful logon attempts each time the user logs on. If you enable this policy in a domain with a functional level lower than Windows Server 2008, users who attempt to log on receive a warning message explaining that the information couldn’t be retrieved, and the user will be unable to log on.
- *Advanced Encryption Standard (AES) support*—AES 128 and AES 256 are supported encryption standards that can be used for Kerberos authentication to increase user logon security.



Activity 10-1: Verifying Current Functional Levels and Enabling Last Interactive Logon Information



If you aren’t running at the Windows Server 2008 functional level, you must not proceed with this activity. In Step 2, you determine the forest and domain functional levels. If the domain isn’t at the Windows Server 2008 functional level, you must raise it. You can’t log on after you complete this activity if the domain functional level is not Windows Server 2008.

Time Required: 15 minutes

Objective: Verify your current functional level and enable last interactive logon information.

Description: For security reasons, you want users to be able to see when their account was last used to log on and whether there were any unsuccessful logons. This information is also important for your servers. Because this feature is available only with the Windows Server 2008 domain functional level, you need to verify that you're running at that level.

1. Log on to your server as Administrator, and open Active Directory Users and Computers.
2. Right-click the domain node in the left pane and click **Properties**. If necessary, click the **General** tab, where the domain functional level and forest functional level should be listed. Verify that both are Windows Server 2008. If not, notify your instructor. Click **Cancel**. Close Active Directory Users and Computers.
3. Open the Group Policy Management Console (GPMC). Right-click the domain node and click **Create a GPO in this domain, and Link it here**. Type **CompWinLogonGPO** in the Name text box, and then click **OK**.
4. In the left pane of GPMC, right-click **CompWinLogonGPO** under the domain node and click **Edit** to open the Group Policy Management Editor (GPME).
5. Expand **Computer Configuration, Policies, and Administrative Templates**, and then click **Windows Components**. Click to expand **Windows Logon Options**.
6. Double-click **Display information about previous logons during user logon** in the right pane. In the Setting tab for the policy, click **Enabled**, and then click **OK**. Close the GPME and GPMC windows.
7. Open a command prompt window, type **gpupdate**, and press **Enter**. Close the command prompt window after Gpupdate.exe has finished running.
8. Log off the server. Log on again as Administrator, but mistype the password so that the logon fails the first time. Log on successfully after one failed attempt. You should see a screen similar to Figure 10-1. Click **OK**, and then log off your server.

10

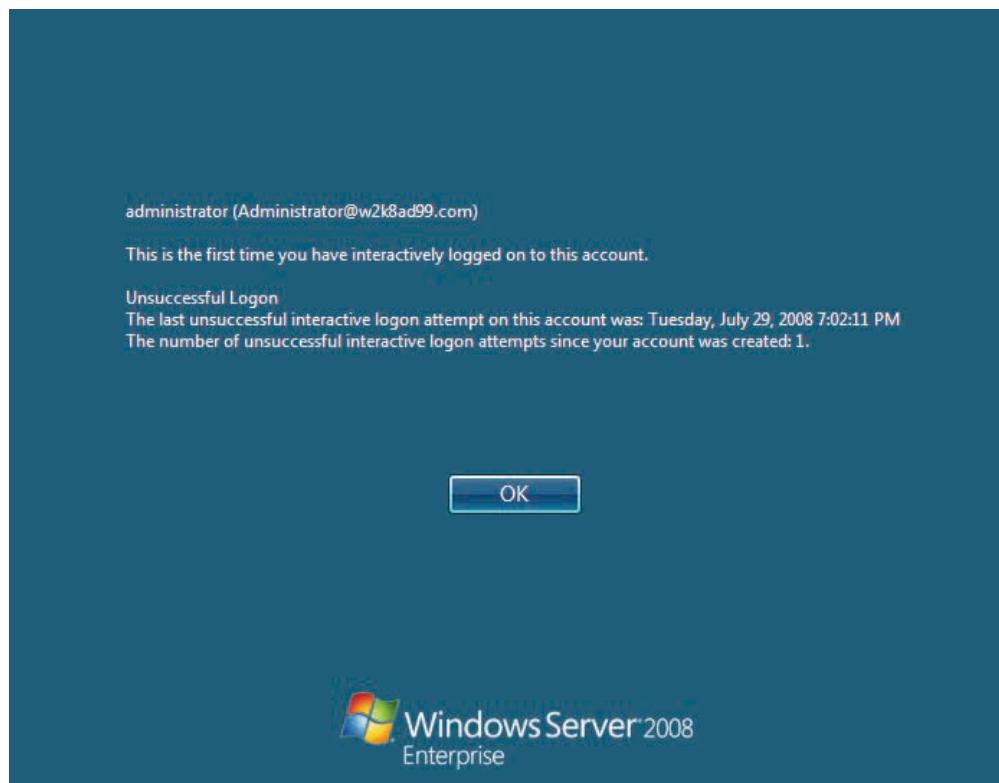


Figure 10-1 Last interactive logon information

Raising Domain and Forest Functional Levels

As stated, forest and domain functional levels are set at Windows 2000 and Windows 2000 native, respectively, by default. You can raise the functional levels when you run Dcpromo.exe to install Active Directory (the recommended method), or you can raise them manually. Before you raise functional levels, be sure your domain controllers meet the requirements for the functional level you want.



Functional levels apply only to domain controllers. Member servers can run any version of Windows Server, regardless of the domain or forest functional level.

NOTE

Raising the Domain Functional Level All domain controllers in the domain must be running the Windows version that supports the functional level you want. When you raise the domain functional level, the change affects all domain controllers in the domain. However, you need to raise the functional level on only one domain controller; all other domain controllers reflect the change. To raise the domain functional level, in Active Directory Domains and Trusts, right-click the domain node and click Raise Domain Functional Level. Figure 10-2 shows the Raise domain functional level dialog box.

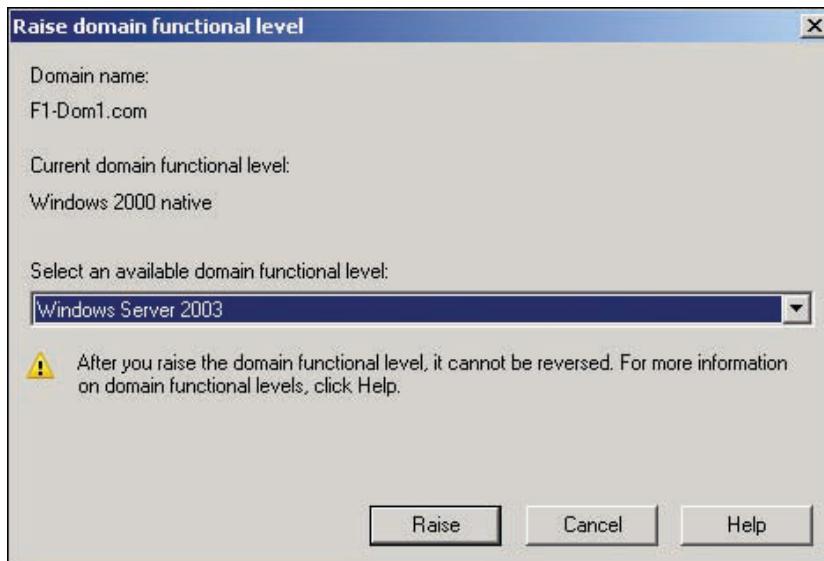


Figure 10-2 The Raise domain functional level dialog box

Raising the Forest Functional Level You must be a member of the Domain Admins or Enterprise Admins group to raise the forest functional level. In addition, if you’re raising both the forest and domain functional levels, you must raise the domain functional level first to at least the level you’re raising the forest functional level. Remember, after a functional level is raised, it can’t be changed back to a lower level, so be sure your domain controllers meet the functional level’s requirements.

To change the forest functional level, you use Active Directory Domains and Trusts. Right-click the Active Directory Domains and Trusts node and click Raise Forest Functional Level. If the forest is already at the Windows Server 2008 level, you get a message informing you that the forest is operating at the highest possible functional level. If not, you see a dialog box similar to Figure 10-3.

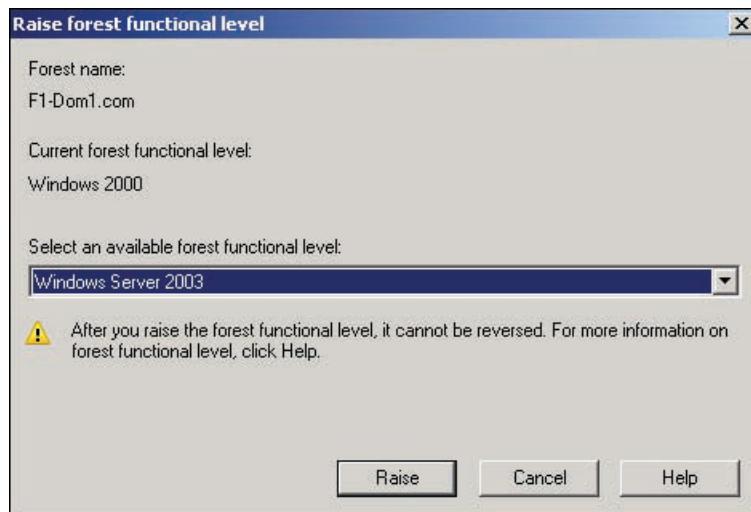


Figure 10-3 The Raise forest functional level dialog box

To clear up any confusion about which configurations for forest and domain functional levels are valid, examine Figure 10-4. The first forest is set at the Windows Server 2008 level with domains at the Windows Server 2003 and Windows 2000 levels. This configuration isn't valid because domain functional levels must be equal or greater than forest functional levels. The second forest is set at the Windows Server 2003 level with domains at the Windows Server 2008 and Windows Server 2003 levels, which is a valid configuration.

10

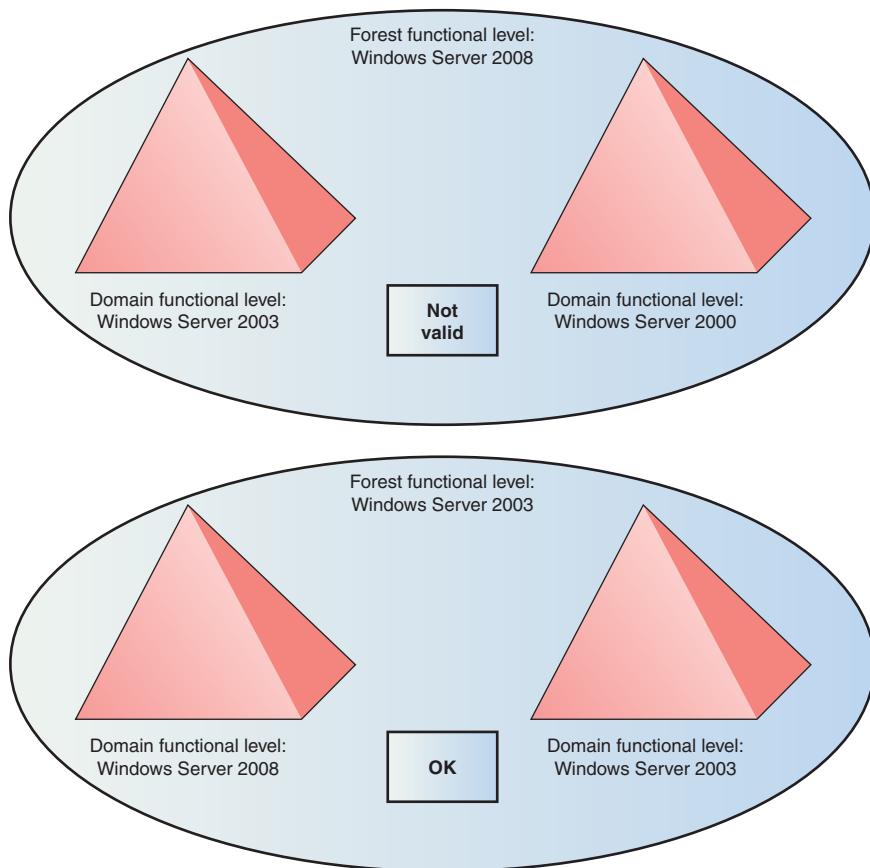


Figure 10-4 Valid and invalid configurations for forest and domain functional levels

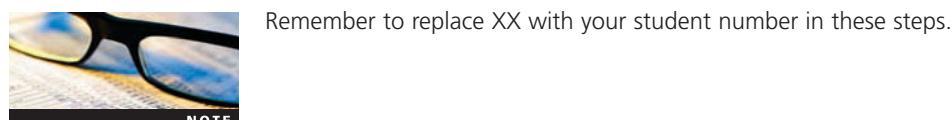


Activity 10-2: Demoting a Domain Controller to a Member Server

Time Required: 30 minutes

Objective: Demote a domain controller to a member server.

Description: Some of the following activities require a domain controller in a new forest. In this activity, you demote Server1XX to a member server and in the next activity, you install AD DS again as a new DC in a new forest.



Remember to replace XX with your student number in these steps.

NOTE

1. Log on to **Server1XX** as Administrator.
2. Click **Start**, type **dcpromo** in the Start Search text box, and press **Enter** to start the Active Directory Domain Services Installation Wizard. Click **Next** in the welcome window.
3. In the Delete the Domain window, make sure the **Delete the domain** check box is selected, and then click **Next**.
4. If you see the Remove DNS Delegation window, click **Next**. In the Windows Security window, type **Administrator** and **Password01** in the corresponding text boxes, and then click **OK**.
5. In the Administrator Password window, type **Password02** in the Password and Confirm password text boxes. Note that you're using the password to log on to the local computer because this server is no longer a domain controller. Click **Next**.
6. In the Summary window, verify your selections. Note that the server will become a member server after the process is finished. Click **Next**.
7. If you see a message stating that the DNS delegations couldn't be removed, click **OK**. When the wizard is completed, click **Finish**. When prompted to restart the computer, click **Restart Now**.
8. After your computer restarts, log on to the domain as Administrator with **w2k8adXX\administrator** as the username and **Password01** as the password, and then open Server Manager.
9. In the left pane of Server Manager, click the **Roles** node, and in the right pane, click **Remove Roles**. When the Remove Roles Wizard starts, click **Next** in the welcome window.
10. Click to clear the **Active Directory Domain Services** check box, and then click **Next**. In the Confirm Removal Selections window, click **Remove**. After the removal is finished, click **Close**. When prompted to restart, click **Yes**.
11. After the computer restarts, log on to the domain from Server1XX as Administrator (following the procedure in Step 8). The removal of Active Directory Domain Services continues. When it's finished, click **Close**.
12. Next, you should remove the DNS Server role. Because Server1XX is no longer a domain controller, DNS doesn't contain Active Directory-integrated zones. Click **Remove Roles**, and then click **Next**.
13. Click to clear the **DNS Server** check box, and then click **Next**. Click **Remove**. When the removal is finished, click **Close**. When prompted to restart, click **Yes**.
14. After the computer restarts, log on to the domain from Server1XX as Administrator (again, following the procedure in Step 8). The removal of DNS Server continues. After it's finished, click **Close**.
15. Stay logged on, and leave Server Manager open for the next activity.



Activity 10-3: Installing a New Domain Controller in a New Forest

Time Required: 30 minutes

Objective: Install a new domain controller in a new forest.

Description: This activity doesn't provide step-by-step instructions; instead, it specifies parameters to select for the new domain controller.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. In Server Manager, install the Active Directory Domain Services Role. When it's finished, run **Dcpromo.exe**.
3. Choose to install the DC in a new domain in a new forest, and name the domain **w2k8ad1XX.com**.
4. Leave the forest and domain functional levels at the default Windows 2000 and Windows 2000 native, respectively.
5. When prompted, choose to install DNS. Close all open windows.



Activity 10-4: Trying to Use Unsupported Forest and Domain Features

Time Required: 20 minutes

Objective: Attempt to create a forest trust and redirect the default Users container.

Description: You have just installed a new Windows Server 2008 domain controller. You want to know how Windows behaves when you attempt to use unsupported features while running at the default Windows 2000 forest and domain functional levels.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Active Directory Domains and Trusts**. Right click the **W2k8ad1XX.com** node and click **Properties**. Click the **Trusts** tab.
3. Click **New Trust**. Notice that your choices include three different trust types but not an option to create a trust with another forest. In the next activity, after you raise the forest functional level, this option is available.
4. Click **Cancel** twice, and close Active Directory Domains and Trusts.
5. Open Active Directory Users and Computers. Click **View, Advanced Features** from the menu, if necessary, to enable this view option so that you can see the Attribute Editor for objects.
6. In the left pane, click to expand the **Users** container. Right-click **Administrator** and click **Properties**.
7. Click the **Attribute Editor** tab. Scroll down to find the **lastLogonTimestamp** attribute. The value is **<not set>**. The attribute exists because it's included in the schema of a Windows Server 2008 domain, but it's not used until the domain functional level is set to at least Windows Server 2003. Click **Cancel**.
8. Next, you test the feature for redirecting the default Users and Computers containers. Open a command prompt window. First, create a new OU by typing **dsadd ou "ou=NewCompOU,dc=w2k8ad1XX,dc=com"** and pressing **Enter**.
9. Next, redirect new computer accounts to this new OU by typing **redircmp "ou=NewCompOU,dc=w2k8ad1XX,dc=com"** and pressing **Enter**. You should get an error message stating that the functional level must be at least Windows Server 2003, and the redirection wasn't successful.
10. Close all open windows, but stay logged on to Server1XX for the next activity.



Activity 10-5: Raising the Domain and Forest Functional Levels

Time Required: 10 minutes

Objective: Raise the forest and domain functional levels for the new forest.

Description: You have just installed a new Windows Server 2008 domain controller in a new forest. You want to be able to use some features of the Windows Server 2008 functional level, so you raise the domain and then the forest functional level.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Open Active Directory Domains and Trusts. Right-click the **W2k8ad1XX.com** node and click **Raise Domain Functional Level**.

3. In the Raise domain functional level dialog box, click the **Select an available domain functional level** list arrow, and then click **Windows Server 2008**. Click the **Raise** button. In the warning message informing you that the process can't be reversed, click **OK**. Click **OK** in the message box stating the functional level was raised successfully.
4. Right-click the **Active Directory Domains and Trusts** node and click **Raise Forest Functional Level**.



If you want to raise forest and domain functional levels to the same level, you can raise the forest functional level first, and the domain functional level is raised automatically in all domains to match the forest's new functional level. All domain controllers must be running an OS version that supports the chosen functional level.

5. In the Raise forest functional level dialog box, click the **Select an available forest functional level** list arrow, and then click **Windows Server 2008**. Click the **Raise** button. In the warning message informing you that the process can't be reversed, click **OK**. Click **OK** in the message stating the functional level was raised successfully.
6. Now that you're at the Windows Server 2008 functional level for the forest and domain, verify that some of the added features are available. Right-click the **W2k8ad1XX.com** node and click **Properties**. Click the **Trusts** tab.
7. Click **New Trust**. Notice that your choices are now four different trust types, including the option to create a trust with another forest. Click **Cancel** twice, and close Active Directory Domains and Trusts.
8. Open a command prompt window. Try the redircmp command again by typing **redircmp "ou=NewCompOU,dc=w2k8ad1XX,dc=com"** and pressing **Enter**.
9. The command you typed should have completed successfully. To test it, create a new computer with the Net computer command, which doesn't allow using the Active Directory path when creating new objects. Type **net computer \\NewComputer /Add** and press **Enter**. The command should complete successfully.
10. Open Active Directory Users and Computers and click the **NewCompOU** OU to verify that the NewComputer account you created has been added.
11. Log off the server and log back on as Administrator.
12. Open Active Directory Users and Computers and click the **Users** container. Open the Properties dialog box for the Administrator account, and click the **Attribute Editor** tab. Scroll down to the lastLogonTimeStamp attribute and verify that it contains a value.
13. Close all open windows, and stay logged on to Server1XX for the next activity.

Adding and Removing Domains

When you're installing Windows Server 2008 domain controllers in a new forest, the process is straightforward, as you have seen. However, installing new Windows Server 2008 domain controllers in existing Windows Server 2003 or Windows 2000 Server domains and forests is also common. With each successive version of the Windows OS, new features are added, and the schema changes, with new objects and object attributes. Before you can install a Windows Server 2008 server as a domain controller in an existing Windows Server 2003 or Windows 2000 Server domain, you must prepare existing domain controllers for the Windows Server 2008 domain controller and the schema changes it will bring.

Preparing a Forest and Domain for Windows Server 2008 with Adprep

The Adprep command-line program prepares an existing forest or domain for the addition of a Windows Server 2008 domain controller. Adprep.exe is on the Windows Server 2008 installation

CD/DVD in the \sources\adprep folder. Copy this folder to the domain controllers where you need to run Adprep.

To prepare the forest, first run the adprep /forestprep command on an existing Windows Server 2003 or Windows 2000 Server domain controller acting as the schema master. To determine which domain controller has this role, in the Active Directory Schema snap-in, right-click the Active Directory Schema node and click Operations Master. You must log on to the schema master DC as a member of all three of these groups: Enterprise Admins, Schema Admins, and Domain Admins.

After adprep /forestprep runs and changes have been replicated to all DCs in the forest, you must run adprep /domainprep in each domain where you plan to add a Windows Server 2008 DC. Windows 2000 domains require an extra parameter: adprep /domainprep /gpprep. The command must be run on the infrastructure master DC for the domain. To determine the infrastructure master DC, in Active Directory Users and Computers, right-click the domain node and click Operations Masters. The Infrastructure tab lists the DC with this role. To run the adprep /domainprep command, you must be logged on as a member of Domain Admins for the domain.

Preparing for a Read Only Domain Controller

Before you can install an RODC in an existing domain that isn't running all Windows Server 2008 domain controllers, you must follow these steps:

- Verify that the forest functional level is Windows Server 2003 or higher.
- Prepare the forest by running adprep /forestprep while logged on to any computer as a user who's a member of Enterprise Admins. It doesn't matter which computer you run this command from because it contacts the infrastructure master for each domain in the forest to update its application directory partition.
- Install at least one writeable DC running Windows Server 2008.
- Install an RODC on a full Windows Server 2008 installation or a Server Core installation.

10

Remember, you must first copy the Adprep files from the Windows Server 2008 installation CD/DVD to the computer on which you'll run it.

Removing Domain Controllers and Domains

You might need to remove a DC from a domain because of server consolidation or upgrades or remove an entire domain from your network because of company reorganization or a redesign of your Active Directory infrastructure.

Removing a Domain Controller Removing a DC from your domain is a straightforward procedure, but you need to be aware of some potential issues:

- If the DC performs any operations master roles, you must first transfer the role to another DC (discussed later in "Managing Operations Master Roles").
- If the DC is a global catalog server, make sure at least one other DC in the domain is a global catalog server.
- If it's the only DC in the domain, you'll also remove the domain.

To remove a DC, you use Dcpromo to remove domain services from the domain controller. Dcpromo is used to make a Windows Server 2008 server a DC, but it's also used to make a DC a regular server. When you run Dcpromo on a DC, the Active Directory Domain Services Installation Wizard detects that the server is already a domain controller. If it's also a global catalog server, you're warned that global catalog servers are required for user logon and one must be available in the domain. Figure 10-5 shows the second window of the wizard, where you specify whether it's the last DC in the domain. Next, you're prompted for an Administrator password. After domain services have been removed, your server remains a member of the domain (assuming it wasn't the last DC).

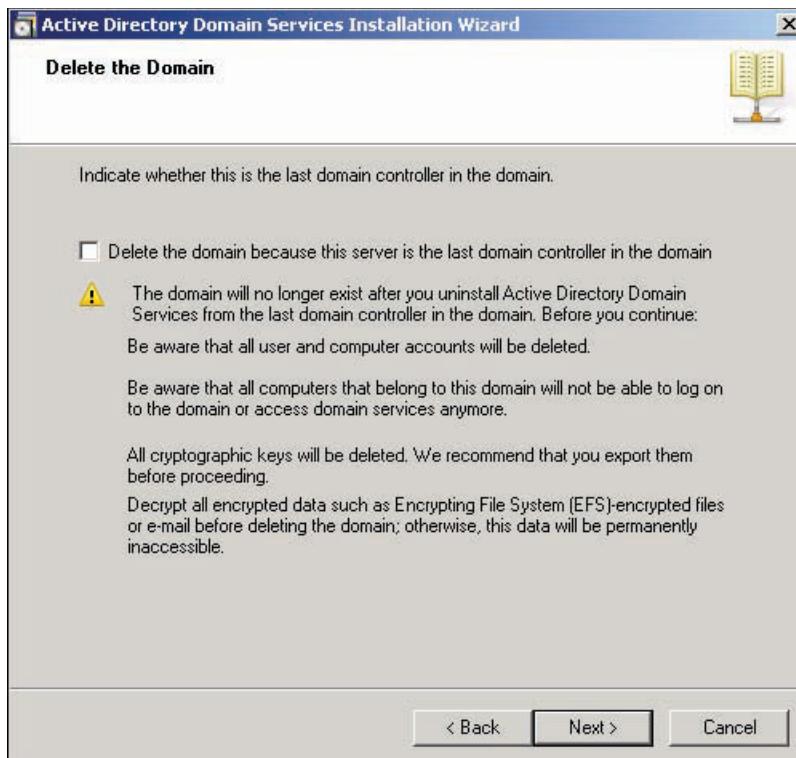


Figure 10-5 Removing domain services

Removing a Domain There are two ways to remove a domain, depending on how you removed DCs: Dcpromo and Ntdsutil. If you used Dcpromo to remove the last DC, you’re finished with domain removal because Dcpromo handles removing all vestiges of the domain from the rest of the forest.

However, if the last DC crashed or was simply taken offline without using Dcpromo to demote it to a regular server, you must use Ntdsutil to remove the domain. This process is called removing an orphaned domain. The following steps explain how to remove an orphaned domain with Ntdsutil. The procedure is called metadata cleanup, which removes all selected domain data from the rest of the forest, and you must be a member of Enterprise Admins to perform this procedure:

1. Log on to a domain controller.
2. Open a command prompt window and run Ntdsutil. Ntdsutil is an interactive command-line program, like Nslookup.
3. Type **metadata cleanup** and press **Enter** to display the Metadata Cleanup prompt.
4. Type **connections** and press **Enter**.
5. Type **connect to server DCName** and press **Enter**, replacing *DCName* with the name of the domain naming master DC. (To determine which DC performs this role, open Active Directory Domains and Trusts, right-click the Active Directory Domains and Trusts node, and click Operations Master.) Type **quit** and press **Enter**.
6. At the Metadata Cleanup prompt, type **select operation target** and press **Enter**.
7. Type **list domains** and press **Enter**. A list of domains is displayed.
8. Type **select domain n**, replacing *n* with the number in the list for the domain to be removed, and press **Enter**.
9. Type **quit** and press **Enter** to get back to the Metadata Cleanup prompt.
10. Type **remove selected domain** and press **Enter**. You should get a message indicating that removal was successful.

Migrating Domain Objects

In today's business world, companies grow, reorganize, and merge with other companies. Active Directory is designed to accommodate this dynamic environment by allowing user, group, and computer accounts to be moved between domains in the same forest and in different forests. You can't simply delete an account in one domain and re-create it in another without losing the original account's security identifiers (SIDs), however. For this purpose, Windows provides the Active Directory Migration Tool so that administrators can migrate Active Directory objects without losing their security assignments.

Using the Active Directory Migration Tool The Active Directory Migration Tool (ADMT) allows moving objects and restructuring Active Directory without users losing access to network resources. ADMT has three main types of migration:

- *Intraforest migration*—Moving objects between domains in the same forest. The domain from which objects are moved is the source domain, and the domain to which they're being moved is the target domain. **Intraforest migration** is often done when a company reorganizes, causing users to change their primary domain memberships, or when several domains are consolidated into fewer domains. After an intraforest migration, objects that were moved no longer exist in the original domain.
- *Interforest migration*—Moving objects between domains in different forests. **Interforest migration** might be indicated when companies merge or a company breaks up into multiple divisions. Migrated objects are actually copied and exist in both domains simultaneously so that users can continue working while the migration is in progress. You can also roll back the migration, if necessary, with little effort.
- *Migration of an NT 4.0 domain to an Active Directory domain*—Migrating Windows NT 4.0 domains to Windows Server 2008 domains isn't supported. However, you can migrate NT 4.0 domains to Windows 2000 Server or Windows Server 2003 domains.

ADMT isn't included in Windows Server 2008, but you can get it from the Microsoft download Web site. ADMT 3.1 is the required version for Windows Server 2008. ADMT can be run in wizard mode, from a command line, or from a script.

Active Directory migration is a complex procedure. Before attempting a migration, you should review the Active Directory Migration guide thoroughly (a document weighing in at more than 200 pages), which is available on the Microsoft Web site. The following list explains some terms used for migration planning and implementation:

- *SID history*—When an account is migrated to another domain, it's assigned a new SID. As you learned in Chapter 4, the SID is used to assign an object rights and permissions to resources and to determine group membership. If an object's SID changes, the object loses resource access as well as group memberships. When an object is migrated to another domain, its SID from the source domain is copied to the object's SIDHistory attribute in the target domain. When a user logs on to the new domain, the SID in SIDHistory is used along with the new SID for determining the object's rights and permissions. Because most permissions are assigned via global group memberships, global groups must be migrated before user accounts. Group objects also maintain SID history.
- *Security translation*—In this process, ADMT examines every resource's ACL for an occurrence of the migrated account's SID in the source domain and changes it to the account's SID in the target domain. In a large network with many resources and objects being migrated, this process can be extensive. Most migrations use SID history to maintain user access to resources during migration, and then perform security translation after the migration is finished.
- *Password Export Server (PES)*—PES, a separate program, is used to migrate passwords during an interforest migration. It must be installed on a domain controller in the source domain.

Configuring Active Directory Trusts

Active Directory trusts were described in Chapter 4. This chapter discusses trust configuration, trust administration, and trust authentication options. Recall that all domains in a forest trust one another automatically through two-way transitive trusts, which you can't remove. In review, here are the types of trusts you can configure:

- Shortcut trust
- Forest trust
- External trust
- Realm trust

One important requirement before creating any trust is that DNS must be configured so that FQDNs of DCs in all participating domains can be resolved. DNS configuration might require Active Directory-integrated forest-wide replication of zones, conditional forwarders, or stub zones, depending on the type of trust being created and the OSs involved. Before you attempt to create a trust, make sure you can resolve the FQDN of both domains from both domains by using Nslookup or a similar tool.

Configuring Shortcut Trusts

A shortcut trust is a one-way or two-way transitive trust between two domains in the same forest or two domains in trusting forests. Although all domains in a forest trust each other through transitivity, a shortcut trust shortens or eliminates the path through domains that authentication requests must travel. For example, a user who's a member of DomainA attempts to access resources in DomainF. Assuming Domains B, C, D, and E lie in the trust path between DomainA and DomainF, the authorization for resource access must traverse these four domains to be validated. This process can cause delays or, if no domain controller is available in a domain along the path, the access attempt could fail. A shortcut trust eliminates the full trust path by creating a direct trust between DomainA and DomainF.

If you're creating a shortcut trust between domains in different forests, a forest trust between the two forests must exist. To create a shortcut trust between domains in the same forest, open Active Directory Domains and Trusts, and then open the Properties dialog box of the domain node. Follow these steps:

1. In the Trusts tab, click the New Trust button to start the New Trust Wizard, and click Next.
2. In the Trust Name window, type the DNS name of the target domain (see Figure 10-6), and then click Next.

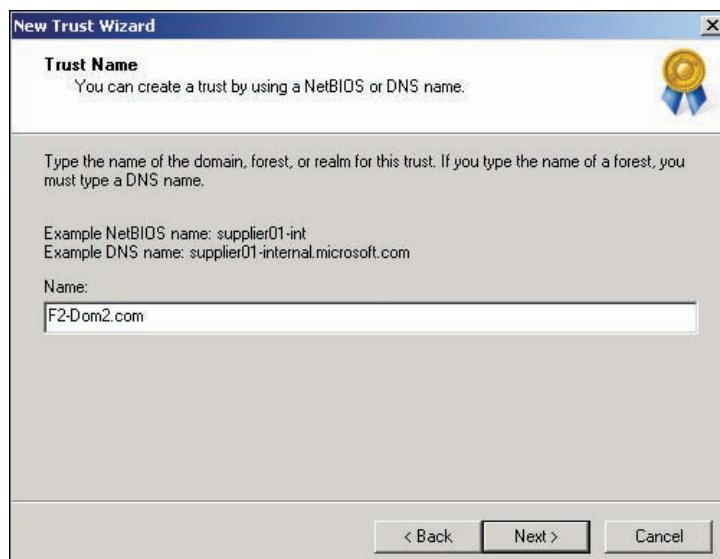


Figure 10-6 Entering the target domain for the trust

3. In the Trust Type window (see Figure 10-7), click the Trust with a Windows domain option button to create a shortcut trust. Type the target domain's name again, if necessary, and then click Next.

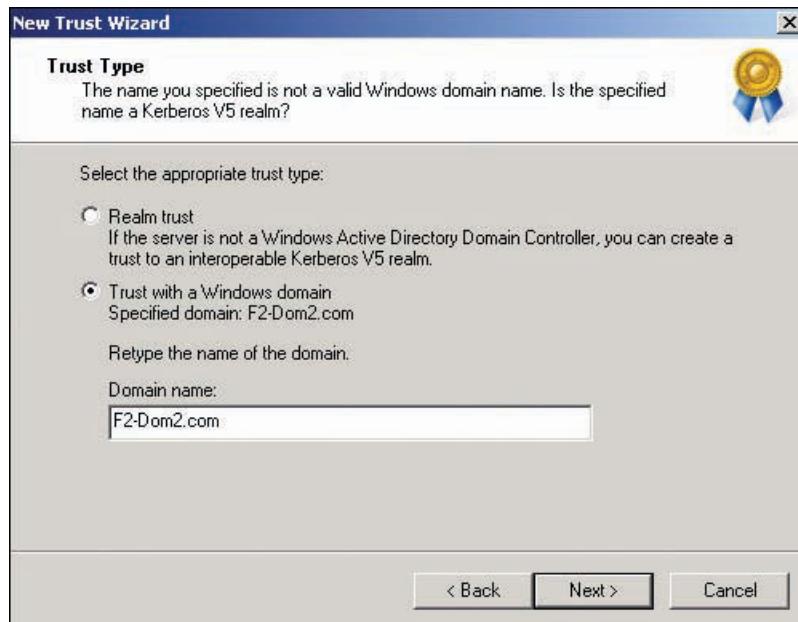


Figure 10-7 Selecting the trust type

4. In the Direction of Trust window (see Figure 10-8), leave the default setting, Two-way, selected, and then click Next.

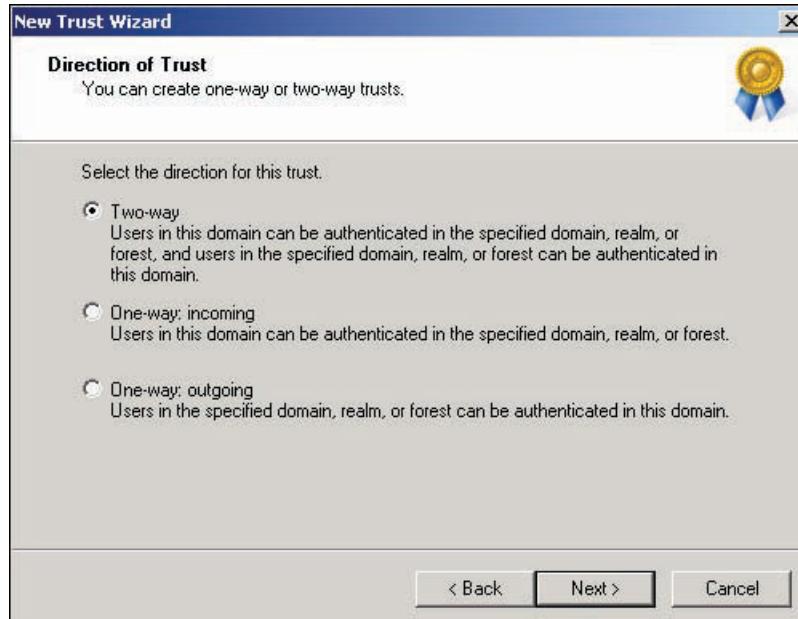


Figure 10-8 Selecting the trust direction

5. In the Sides of Trust window, the next choice is specifying whether to create the trust only in the local domain or in both the local domain and the target domain specified in Step 2. If you choose the latter, you must have the proper credentials to create a trust in the target domain. If you choose to create the trust only in the local domain, an administrator in the target domain must create the other side of the trust. Click Next.
6. In the User Name and Password window, if you choose to create the trust in both domains, you're prompted for credentials for an account in the target domain that can create the trust. You must be an administrator in the target domain and have to enter your credentials with the *username@domain* or *domain\username* syntax. If you're creating only the local side of the trust, you are prompted to enter a trust password. This password must also be used when creating the other side of the trust, so it must be communicated to the administrator who creates the trust in the other domain.
7. In the Trust Selections Complete window, you can review your choices. This window is the only place where you actually see the word "Shortcut" describing the trust type (see Figure 10-9). After reviewing your choices, click Next to create the trust.

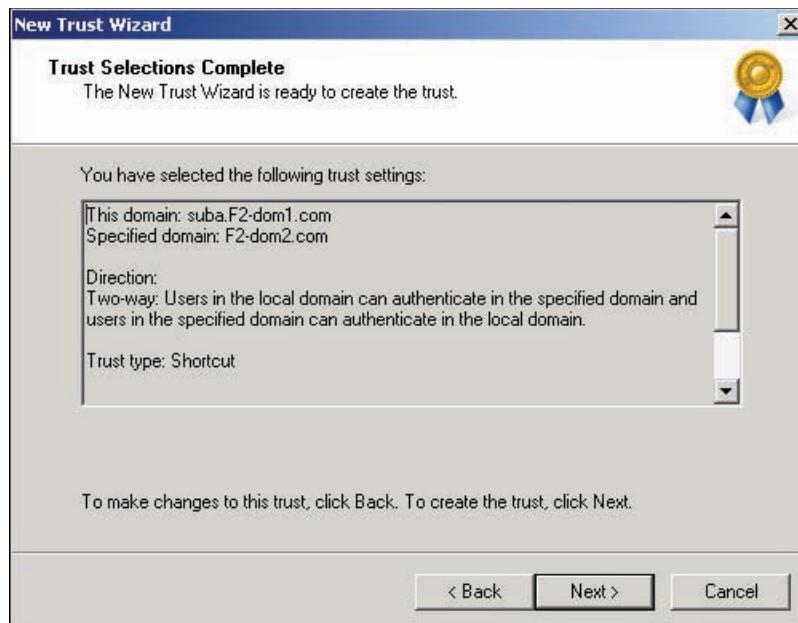


Figure 10-9 Reviewing your trust settings

8. The next window shows the status of the trust and summarizes the trust parameters again. After reviewing the information, click Next.
9. Next, you can confirm the trust, which you should do if you created both sides of the trust. After the wizard is finished, the Trusts tab shows the trust relationship and trust type. In Figure 10-10, the Trusts tab for domain suba.F2-dom1.com shows an automatic parent trust between F2-dom1.com and suba.F2-dom1.com and the shortcut trust that was just created. Figure 10-11 depicts the entire forest and its trust relationships.

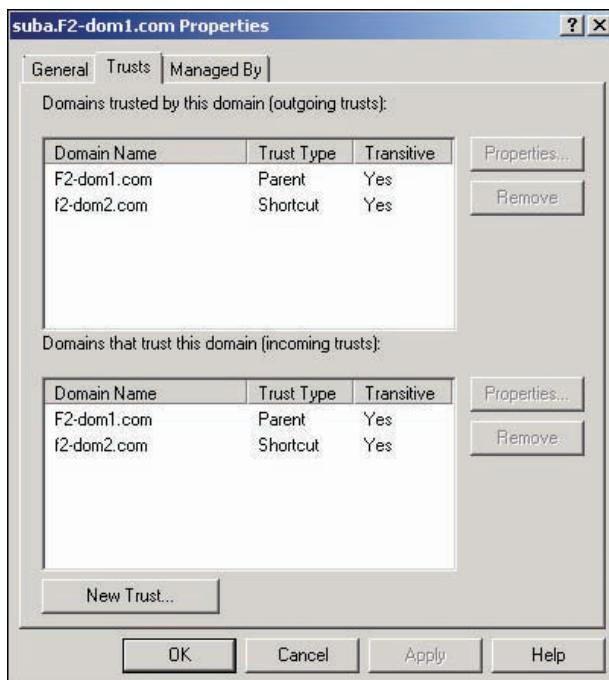


Figure 10-10 Reviewing trust relationships and types

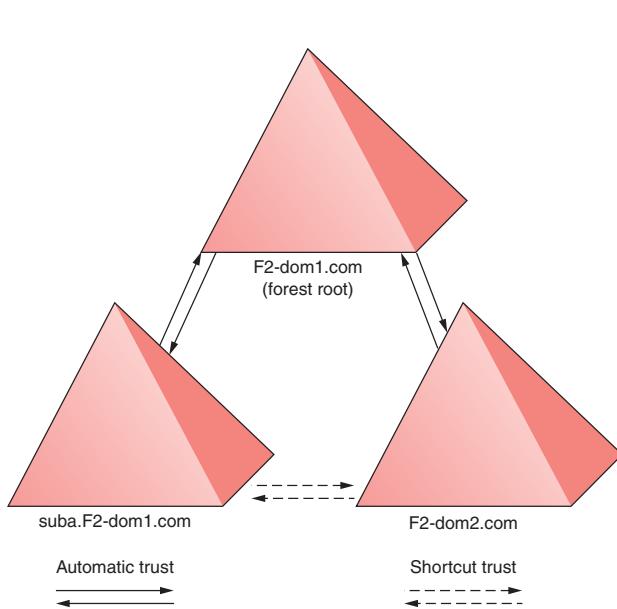


Figure 10-11 A forest and its trusts

The forest shown in Figure 10-11 is a small forest of only two trees and three domains. The path between suba.F2-dom1.com and F2-dom2.com is only two referrals away, so normally you don't need to create a shortcut trust between suba.F2-dom1.com and F2-dom2.com. However, if four or five other domains were along the path between these two domains, a shortcut trust makes sense if users from these domains access each other's resources frequently.

In the preceding example, because all the domains are in the same forest, the DNS domains could be configured as Active Directory-integrated zones, and zone replication could be configured so that zones are replicated to all DNS servers in the forest. No further DNS configuration is necessary because the DNS servers in F2-dom1.com store the zone for F2-dom2.com, and vice versa. Trusts between forests and external trusts might require additional DNS configuration.

Configuring Forest Trusts

Configuring a forest trust is similar to creating a shortcut trust. The main consideration before you begin is making sure DNS is configured correctly in both forest root domains. The following are the three most common ways to configure DNS for a forest trust:

- *Conditional forwarders*—As you learned in Chapter 9, a conditional forwarder forwards all DNS requests for a domain to a DNS server specified in the conditional forwarder record. Setting up a conditional forwarder is easy, but if the IP address on the DNS server in the target domain changes, forwarding no longer works. With this method, you create a conditional forwarder in the forest root domain pointing to a DNS server in the other forest root domain. Do this in both forests involved in the trust.
- *Stub zones*—Stub zones are much like conditional forwarders, except they’re updated dynamically if DNS servers’ addresses change. The only real downside of stub zones is the additional traffic created by replicating zone information, which is minimal. To use this method, create a stub zone in the forest root domain of both forests pointing to the forest root domain of the other forest.
- *Secondary zones*—Creating a secondary zone for the purpose of configuring forest trusts is probably overkill. With secondary zones, you need to configure zone transfers, which causes more network traffic than with stub zones, especially if the primary zone’s forest root domain contains a lot of records. However, you might want to use secondary zones as fault tolerance for the primary zone and to facilitate local hosts’ name resolution for hosts in the primary domain.

You can also configure a DNS server to act as the root server for the DNS namespaces of both forests. On the root server, you must delegate the namespaces for each forest, and then configure root hints on DNS servers in the two forests to point to the root server.

After DNS is configured and you can resolve the forest root domain of both forests from both forests, you’re ready to create the trust. The procedure is essentially the same as creating a shortcut trust, but there are a few important differences. You must initiate the forest trust in Active Directory Domains and Trusts from the forest root domain. After the New Trust Wizard starts, follow these steps:

1. Specify the forest root domain of the target forest.
2. In the Trust Type window, Windows recognizes that the specified domain is a forest root domain and gives you the option of creating an external trust or a forest trust (see Figure 10-12). Click the Forest trust option button, and then click Next.

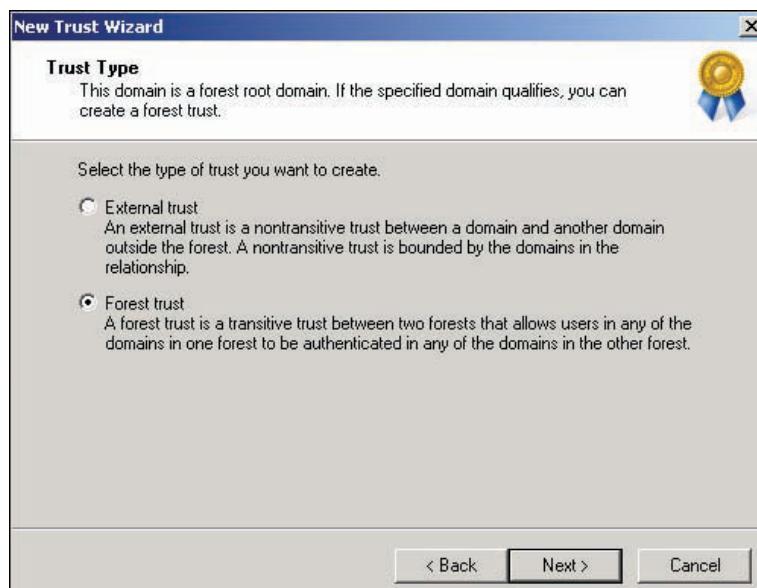


Figure 10-12 Creating a forest trust

3. In the Sides of Trust window, choose whether you're creating the trust for the local domain only or for both domains, and then click Next.
4. In the Outgoing Trust Authentication Level—Local Forest window, the choices are forest-wide authentication or selective authentication (see Figure 10-13). **Forest-wide authentication** means Windows should authenticate all users in the specified forest for all resources in the local forest. With **selective authentication**, you can choose which local forest resources that users in the specified forest can be authenticated to. Authenticating a user for a resource doesn't grant the user access; permissions must also be set. Microsoft recommends forest-wide authentication when both forests belong to the same company and selective authentication when the forests belong to different organizations. Select your authentication level, and then click Next.



10

Figure 10-13 Selecting an authentication level

5. In the Routed Name Suffixes—Specified forest window, if multiple trees exist in one of the forests, you're asked whether you want to prevent authentication requests from any of the name suffixes. A name suffix generally represents a second-level domain name.
6. Last, you're asked to confirm the trust.



Activity 10-6: Creating Stub Zones and Conditional Forwarders

Time Required: 15 minutes

Objective: Create a stub zone and a conditional forwarder.

Description: You want to create a forest trust between w2k8adXX.com and w2k8ad1XX.com, but first you must configure DNS. You decide to create a stub zone on the w2k8adXX.com DNS server and a conditional forwarder on the w2k8ad1XX.com DNS server.

1. Log on to **ServerXX** as Administrator, if necessary, and open DNS Manager.
2. Right-click **Forward Lookup Zones** and click **New Zone**. In the New Zone Wizard's welcome window, click **Next**.
3. In the Zone Type window, click the **Stub zone** option button verify that the **Store the zone in Active Directory** check box is selected and then click **Next**.
4. In the Active Directory Zone Replication Scope window, make sure **To all DNS servers in this domain** is selected, and then click **Next**. (If you had multiple domains, you might want to choose To all DNS servers in this forest.)
5. In the Zone name text box, type **w2k8ad1XX.com**, and then click **Next**.

6. In the Master DNS Servers window, type the IP address of Server1XX (**192.168.100.1XX**) and press **Enter**. Click **Next**, and then click **Finish**.
7. In DNS Manager, click to expand **Forward Lookup Zones**, if necessary, and then double-click the **w2k8ad1XX.com** zone to verify that SOA, NS, and A records are present. Close DNS Manager.
8. To test the stub zone, open a command prompt window, type **nslookup w2k8ad1XX.com**, and press **Enter**. The IP addresses of all DNS servers for the w2k8ad1XX.com domain are displayed. Close the command prompt window.
9. Log on to **Server1XX** as Administrator, if necessary.
10. Open DNS Manager. Click to expand the server node, and then click to select **Conditional Forwarders**. Right-click **Conditional Forwarders** and click **New Conditional Forwarder**.
11. In the New Conditional Forwarder dialog box, type **W2k8adXX.com** in the DNS Domain text box. Then click **<Click here to add an IP Address or DNS Name>**, type **192.168.100.1XX**, and press **Enter**. (If you had multiple DNS servers that should get a copy of the conditional forwarder record, you would click the “Store this conditional forwarder in Active Directory and replicate it as follows” check box.) Click **OK**.



If you get an error message that the IP address isn't authoritative for the zone, wait a few minutes, and then come back to this dialog box. Usually, the wait clears the error message.

NOTE

12. To test your forwarder, open a command prompt window, type **nslookup w2k8adXX.com**, and press **Enter**. The IP addresses of all DNS servers for w2k8adXX.com are displayed.
13. Close the command prompt window. Stay logged on to both servers for the next activity.



Activity 10-7: Testing Access Between Untrusting Forests

Time Required: 10 minutes

Objective: Test access between two forests before creating a trust.

Description: You plan to create a forest trust between w2k8adXX.com and w2k8ad1XX.com, but first, you want to see what happens when you try to access resources across forests.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start**, type **\ServerXX.w2k8adXX.com** in the Start Search text box, and press **Enter**.
3. You should see a Connect to dialog box asking for your username and password. Type **administrator** and **Password02**, and then click **OK**. The logon should be unsuccessful. Without a trust between the two forests, you can't log on to a domain in the other forest. Click **Cancel**.
4. Try to access the server again by clicking **Start**, typing **\ServerXX.w2k8adXX.com** in the Start Search text box, and pressing **Enter**.
5. In the Connect to dialog box, type **w2k8adXX.com\Administrator** and **Password01** for the password, and then click **OK**. You're trying to log on with credentials from the other domain. This logon should be successful, and a list of shares available on the server should be displayed.
6. When no forest trust exists, you can still access a domain in another forest, but you need the logon credentials of a user in this domain. The trust precludes the need for credentials in multiple domains. Close all open windows.
7. Log off both servers to clear the existing connection between the two domains.



Activity 10-8: Creating a Forest Trust

Time Required: 10 minutes

Objective: Create a forest trust.

Description: Now that you have DNS set up between the two forests, you can create the forest trust.

1. Log on to **ServerXX** as Administrator, and open Active Directory Domains and Trusts.
2. Right-click **w2k8adXX.com** and click **Properties**.
3. Click the **Trusts** tab, and click the **New Trust** button to start the New Trust Wizard. Click **Next** in the wizard's welcome window.
4. Type **w2k8ad1XX.com** in the Name text box, and then click **Next**.
5. Click the **Forest trust** option button for the trust type. You can also create an external trust in this window, but an external trust isn't transitive. Windows 2000 Server forests and NT domains don't support forest trusts, so you must select an external trust if you're using these OSs. Click **Next**.
6. In the Direction of Trust window, verify that the default **Two-way** is selected, and then click **Next**.
7. In the Sides of Trust window, click **Both this domain and the specified domain**. If you're creating only one side of the trust, you're asked to enter a trust password, which must be used to create the second side of the trust. Click **Next**.
8. Type **w2k8ad1XX.com\administrator** in the User name text box and **Password02** in the Password text box, and then click **Next**. (If you enter incorrect credentials, you must restart the trust creation from the beginning.)
9. In the Outgoing Trust Authentication Level—Local Forest window, verify that **Forest-wide** is selected for the authentication level, and then click **Next**.
10. In the Outgoing Trust Authentication Level—Specified Forest window, verify that **Forest-wide** is selected, and then click **Next**.
11. Review your settings in the Trust Selections Complete window, and then click **Next**.
12. In the Trust Creation Complete window, the status of the trust creation and a summary of your choices are displayed. Click **Next**.
13. In the Confirm Outgoing Trust window, click **Yes, confirm the outgoing trust**, and then click **Next**.
14. In the Confirm Incoming Trust window, click **Yes, confirm the incoming trust**, and then click **Next**.
15. Click **Finish**. The Trusts tab should list w2k8ad1XX.com in both the outgoing trusts and incoming trusts lists. Click **OK**.
16. Close all open windows, and stay logged on for the next activity.

 10

Activity 10-9: Confirming Cross-Forest Access

Time Required: 10 minutes

Objective: Access resources from one forest to another.

Description: Try to access resources in the w2k8adXX.com domain from the w2k8ad1XX.com domain.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start, Run**. Type **\ServerXX.w2k8adXX.com** and click **OK**. A Windows Explorer window should open that lists all shares on ServerXX.
3. Double-click **Shared**. It should open. When you try to create a file, you should be successful. The Shared share has Full Control permission assigned to the Everyone group, which includes authenticated users from other forests.
4. In Windows Explorer, click the **back arrow** to see the list of shared folders on ServerXX. Double-click **TestShare1**. (Don't click TestShare because the Everyone group has permission to it.) You should get a "Windows cannot access" message. Click **Diagnose**. Windows should report that TestShare1 is available, but you were denied access. Click **Cancel**.
5. Log on to **ServerXX** as Administrator, if necessary.

6. In Windows Explorer, click to expand the **Q:** volume. Right-click **TestShare1** and click **Properties**. Click the **Sharing** tab, and then click the **Advanced Sharing** button. Click **Permissions**.
7. In the Permissions for TestShare1 dialog box, click **Add**. In the Select Users, Computers, or Groups dialog box, click **Locations**. Click **w2k8ad1XX.com**, and click **OK**.
8. Type **Administrator** and click **Check Names**. Click **OK**. In the Share Permissions list box, Administrator (w2k8ad1XX\Administrator) is added. Click the **Full Control** check box in the Allow column of the Permissions for Administrator list box, and then click **OK** twice.
9. Click the **Security** tab, and then click **Edit**. Click **Add**. In the Select Users, Computers, or Groups dialog box, click **Locations**. Click **w2k8ad1XX.com**, and then click **OK**.
10. Type **Administrator** and click **Check Names**. Click **OK**. Click the **Full Control** check box in the Allow column of the Permissions for Administrator list box, click **OK**, and then click **Close**.
11. On Server1XX, try again to open **TestShare1**. You should be successful. When you try to create a file, you should be successful.
12. On both servers, close all open windows and log off.

Configuring External and Realm Trusts

External trusts and realm trusts are configured in Active Directory Domains and Trusts. An external trust is created between domains in different forests or between domains in a Windows Server 2003/2008 forest and a Windows 2000 Server forest or Windows NT domain. Recall that Windows 2000 Server and Windows NT don't support forest trusts, so an external trust is the only way to build a trust relationship between forests in these OSs and Windows Server 2003/2008 forests. An external trust involves Windows domains on both sides of the trust, but a realm trust is created between a Windows domain and a non-Windows OS running the Kerberos v5 authentication protocol.

Unlike a forest trust, an external trust is not transitive and need not be created between the forest root domains of two forests. In addition, SID filtering (discussed later in this chapter) is enabled by default. Aside from these differences, creating an external trust is nearly identical to creating a forest trust.

The only real consideration when creating a realm trust is whether it should be transitive. If it's transitive, the trust extends to all child domains and child realms. Otherwise, the procedure is much the same as configuring other trust types.

Configuring Trust Properties

After creating a trust, you might need to view or change its settings. To do this, in Active Directory Domains and Trusts, open the domain's Properties dialog box and click the Trusts tab. Select the trust you want to configure and click the Properties button. The Properties dialog box of a forest trust contains three tabs—General, Name Suffix Routing, and Authentication—discussed in the following sections.

The General Tab The General tab, shown in Figure 10-14, contains the following fields and information:

- *The other domain supports Kerberos AES Encryption*—Kerberos AES encryption enhances authentication security and is supported by Windows Server 2008 and Vista. If the forest trust is between two Windows Server 2008 domains, you can select this option.
- *Direction of trust*—This field is for informational purposes only. You can't change the trust direction without deleting and re-creating the trust.
- *Transitivity of trust*—This field is for informational purposes only. You can't change the transitivity without re-creating the trust. Some trusts, such as forest and shortcut trusts, are always transitive.
- *Validate*—Click this button to confirm the trust. It performs the same action as the confirmation process at the end of the New Trust Wizard. If you didn't create both sides of the trust with the wizard, you should validate the trust with this option after both sides have been created.
- *Save As*—Click this button to create a text file containing details of the trust.

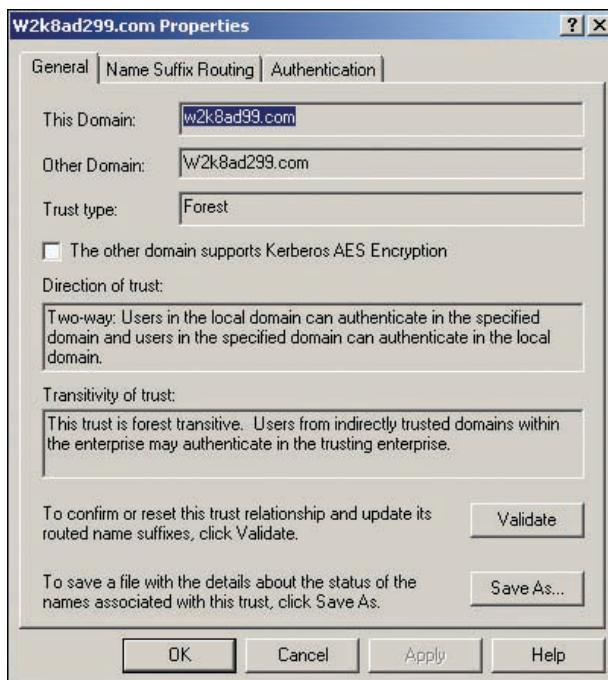


Figure 10-14 Settings in the General tab

10

The Name Suffix Routing Tab In the Name Suffix Routing tab, you can control which name suffixes used by the trusted forest are routed for authentication. For example, ForestA contains multiple trees—coolgadgets.com and niftytools.com—and ForestA is trusted by ForestB. Only users from coolgadgets.com should have access to ForestB resources, however. To do this, the ForestB administrator can disable authentication requests containing the name suffix niftytools.com. The Name Suffix Routing tab displays all available name suffixes in the trusted forest, and you can disable or enable them. In Figure 10-15, two name suffixes in the w2k8ad299.com forest are listed. The second suffix was added after the forest trust was created and is set to disabled.

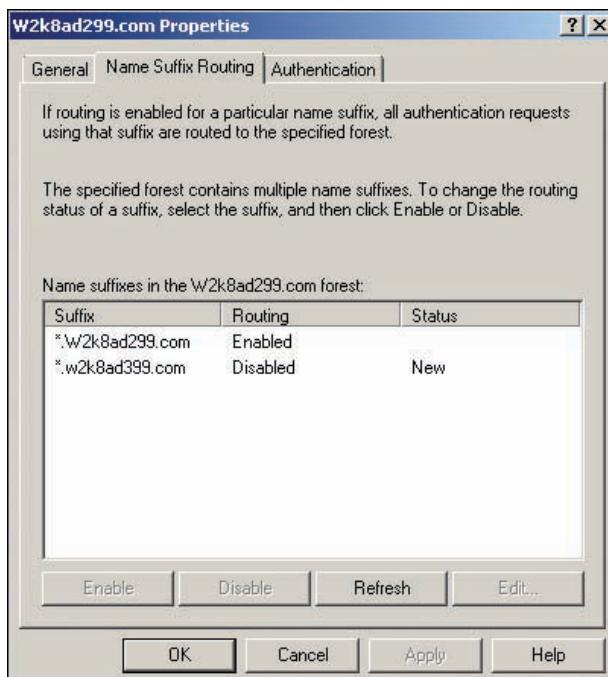


Figure 10-15 The Name Suffix Routing tab

Two or more trees in a forest is one way to have multiple name suffixes. An administrator can also create other name suffixes, called **alternate UPN name suffixes**, that can be assigned as a user's UPN suffix for logon purposes. The UPN suffix enables the user to log on with the format *username@domain*. By default, the user's domain is set as the UPN suffix. An administrator can create an alternate UPN suffix to enhance logon security by disassociating the domain name from the user logon name. Assigning alternate UPN suffixes can also simplify logons. If a domain name is lengthy, such as ny.america.niftytools.com, an administrator could allow users to log on with just the name *user@nifty*. UPN suffixes don't have to comply with domain-naming standards, so including a top-level domain in the suffix isn't necessary.

To create a UPN suffix, right-click the root node in Active Directory Domains and Trusts and click Properties. The UPN Suffixes dialog box opens, where you can enter a new UPN suffix and click Add.

The Authentication Tab The Authentication tab has the same options as the Outgoing Trust Authentication Level window shown previously in Figure 10-13: forest-wide or selective authentication. As discussed, forest-wide authentication is recommended for forest trusts when both forests belong to the same organization. Selective authentication, recommended for forests in different organizations, enables you to specify users who can authenticate to selected resources in the trusting forest. After choosing selective authentication, you add users and groups from the trusted forest to the DACL of computer accounts in the trusting forest and assign the “Allowed to authenticate” permission to these computer accounts. When selective authentication is enabled, by default, users from the trusted forest can't authenticate to the trusting forest. If users try to authenticate to a computer in the trusting domain and haven't been granted authentication permission, they get an error message similar to Figure 10-16.



Figure 10-16 Selective authentication error message



Activity 10-10: Configuring Selective Authentication

Time Required: 10 minutes

Objective: Configure selective authentication.

Description: Configure selective authentication and try to access resources in the w2k8adXX.com domain from the w2k8ad1XX.com domain. Then add the Administrator account from w2k8ad1XX.com to the DACL of serverXX.w2k8adXX.com with the Allowed to authenticate permission.

1. Log on to **ServerXX** as Administrator, and open Active Directory Domains and Trusts.
2. Right-click **w2k8adXX.com** and click **Properties**. Click the **Trusts** tab.
3. Click **w2k8ad1XX.com** in the top list box and click the **Properties** button. Review the options in the General tab, and then click the **Name Suffix Routing** tab to review the available options.
4. Click the **Authentication** tab, click the **Selective authentication** option button, and then click **OK** twice.
5. Log on to **Server1XX** as Administrator with **Password02**.

6. Click **Start**, type **\serverXX.w2k8adXX.com**, and press **Enter**. You should get an error message similar to Figure 10-16 indicating that the machine you’re logging on to is protected by an authentication firewall. Click **OK**.
7. On *ServerXX*, open Active Directory Users and Computers. Click the **Domain Controllers** OU. Right-click **ServerXX** and click **Properties**.
8. Click the **Security** tab. Click **Add** to open the Select Users, Computers, and Groups dialog box, and then click **Locations**. Click the **w2k8ad1XX.com** forest, and then click **OK**.
9. Type **Domain Admins** and click **Check Names**. All users who are members of the Domain Admins group in the w2k8ad1XX.com domain are allowed to authenticate to ServerXX. Click **OK**.
10. Make sure **Domain Admins (w2k8ad1XX\Domain Admins)** is selected at the top of the Security tab, click the **Allowed to authenticate** check box in the Allow column, and then click **OK**.
11. On *Server1XX*, try again to access **\serverXX.w2k8adXX.com**. You should be successful.
12. In case you want other users to be able to access resources on ServerXX from the w2k8ad1XX.com domain, you should change the authentication type back to forest-wide authentication. On *ServerXX*, open Active Directory Domains and Trusts. Right-click **w2k8adXX.com** and click **Properties**. Click the **Trusts** tab. Click **w2k8ad1XX.com** in the top list box, and then click the **Properties** button. Click the **Authentication** tab, click the **Forest-wide authentication** option button, and then click **OK** twice.
13. Close all open windows on both servers, and stay logged on for the next activity.

SID Filtering The “Active Directory Migration Tool” section explained that the **sIDHistory** attribute is used when migrating accounts from one domain to another. This attribute can also be used for nefarious purposes to gain administrative privileges in a trusting forest. Suppose ForestA is trusted by ForestB. An administrator in ForestA can edit the **sIDHistory** attribute of a user in ForestA to include the SID of a privileged account in ForestB. When this user logs on to a domain in ForestB, he or she has the same access as the privileged account.

10

To counter this security risk, Windows provides a feature called **SID filtering** (also called SID filter quarantining). SID filtering is enabled by default on external trusts but is disabled on forest trusts. It causes the trusting domain to ignore any SIDs that aren’t from the trusted domain. Essentially, the trusting domain ignores the contents of the **sIDHistory** attribute. SID filtering should be enabled or disabled from the trusting side of the domain and should be used only between forests or with external domains. It shouldn’t be used between domains in the same forest because it would break Active Directory replication and automatic transitive trusts.

For Active Directory migration purposes, SID filtering can be disabled but should be reenabled after the migration. To disable SID filtering, use the following command:

```
netdom trust TrustingDomainName /domain:TrustedDomainName  
/quarantine:No
```

To enable SID filtering, simply change the No to Yes. To check the status of SID filtering, omit the Yes or No at the end of the command.



You can view and clear the contents of **sIDHistory** in Attribute Editor and ADSI Edit, but you can’t add or change existing values. If you attempt to do so, you get an access denied error.

Configuring Intrasite Replication

Efficient and accurate replication of changes made to the Active Directory database is critical in a Windows domain. In Chapter 4, you were introduced to intrasite and intersite replication. This section expands on the concepts of intrasite replication, and the next section, “Understanding and Configuring Sites,” discusses intersite replication in more detail.

Intrasite and intersite replication use the same basic processes to replicate Active Directory data; the primary goal is to balance replication timeliness and efficiency. To that end, the replication strategy between DCs within a site (intrasite) are optimized for high-speed, low-latency LAN links. Intersite replication is optimized to take slower WAN links into account.

Intrasite replication can be initiated in one of two ways:

- *Notification*—When a change is made to the Active Directory database, the DC on which the change was made notifies its replication partners. The partners then request replication from the notifying DC.
- *Periodic replication*—To account for missed updates, DCs request replication from their partners periodically. The interval can be configured in the connection object's Properties dialog box (explained later in the “Connection Objects” section).

Intrasite replication involves two main components: Knowledge Consistency Checker (KCC) and connection objects.

Knowledge Consistency Checker (KCC)

The KCC, introduced in Chapter 4, is a process that runs on every DC and, for intrasite replication, builds a replication topology among DCs in a site and establishes replication partners. As shown in Figure 10-17, each DC in a site has one or more replication partners. For example,

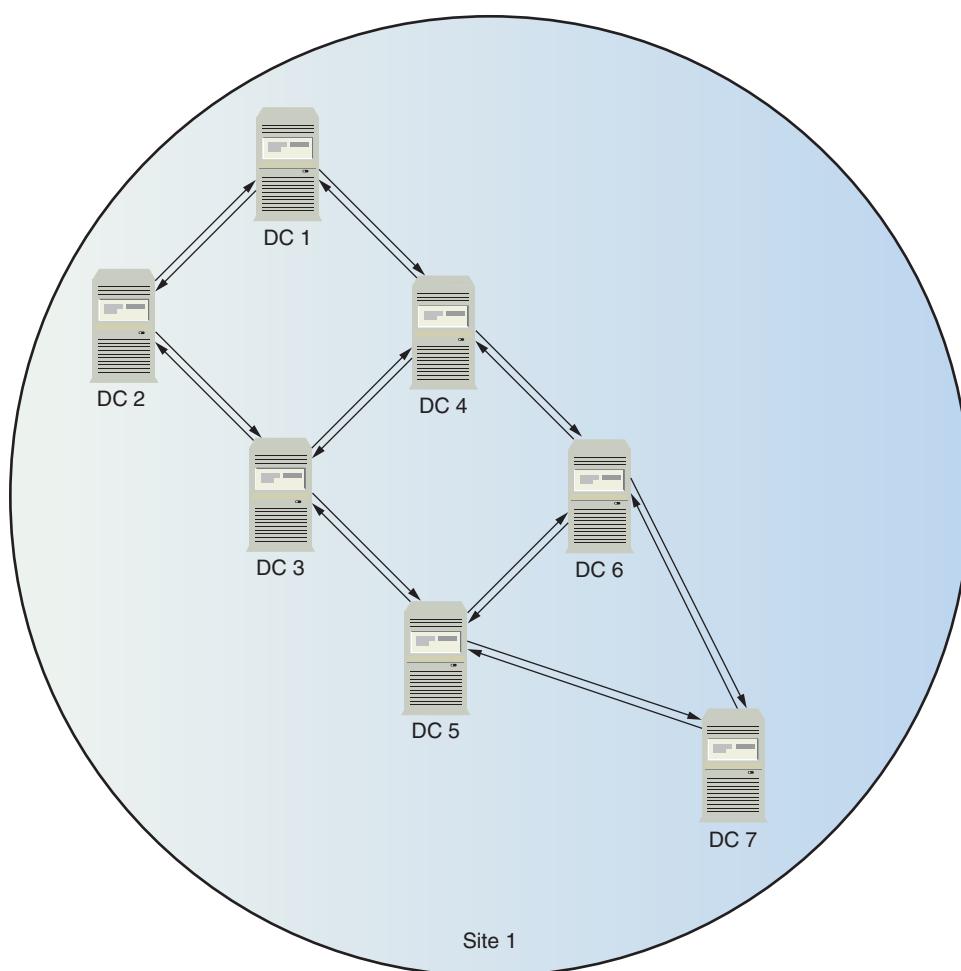


Figure 10-17 Intrasite replication partners

DC3 is partners with DC2, DC4, and DC5. The topology is designed to ensure that no more than two DCs lie in the replication between two domain controllers. To put it another way, data in a replication transfer doesn't have to travel more than three hops to reach its destination DC. For example, if Active Directory data on DC1 changes, the changes have to hop through DC4, DC6, and DC7 to reach DC7. A domain controller waits 15 seconds after an Active Directory change before replicating with its partners, with a 3-second delay between partners. This arrangement guarantees that all DCs in a site receive changes in less than a minute.

The KCC on each domain controller uses data stored in the forest-wide configuration directory partition to create the replication topology. The configuration directory partition is replicated to all DCs in the forest, so the KCCs need not communicate with one another. Because they all run the same algorithm on the same data, the KCCs on domain controllers create the same replication topology. The KCC recalculates the replication topology every 15 minutes by default to ensure that the topology accurately reflects DCs that come online or go offline. If necessary, the replication topology can be recalculated manually in Active Directory Sites and Services. To do so, right-click the NTDS Settings node under a domain controller, point to All Tasks, and click Check Replication Topology. You must be logged on to the DC as an administrator to perform this task. The partnership between DCs is controlled by a connection object, which the KCC creates automatically for intrasite replication.

Connection Objects

Connection objects define the connection parameters between two replication partners. The KCC generates them automatically between intrasite DCs. Generally, you don't need to make changes to intrasite connection objects, but if you do, they can be changed in Active Directory Sites and Services. Figure 10-18 shows connection objects in Active Directory Sites and Services, and Figure 10-19 shows the Properties dialog box for one of the objects.

10

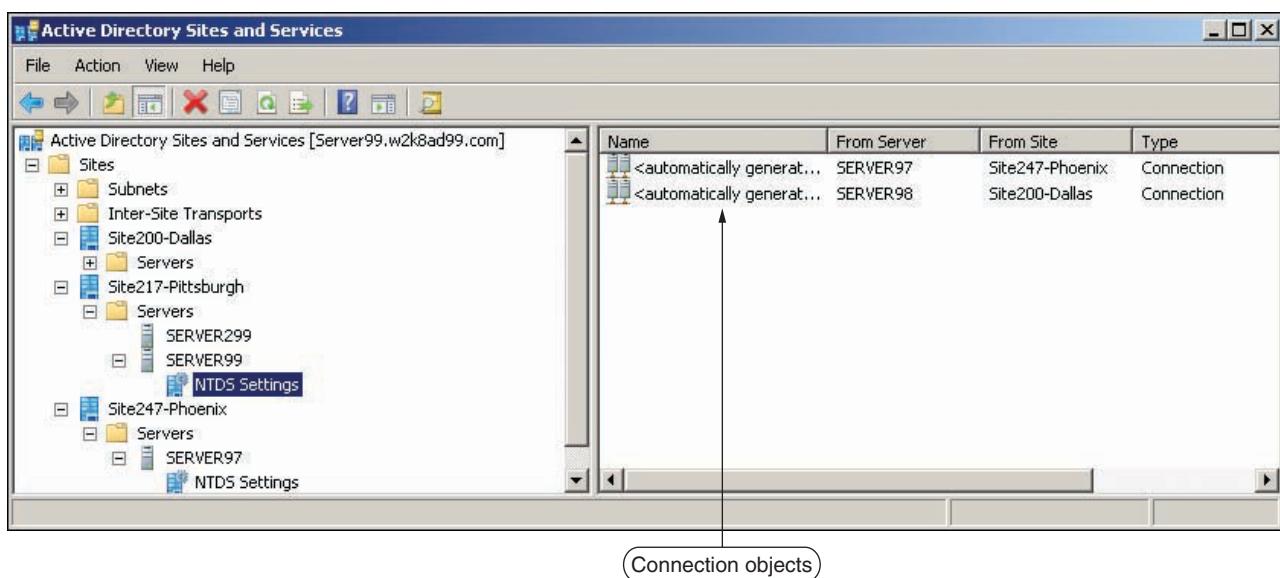


Figure 10-18 Connection objects in Active Directory Sites and Services

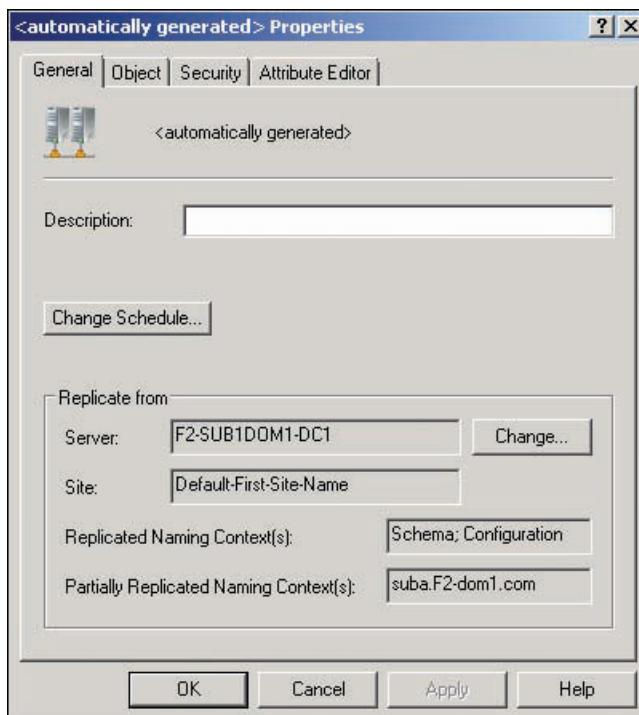


Figure 10-19 The Properties dialog box for a connection object

The General tab in the Properties dialog box is the only one of interest for connection objects; the other three tabs are the same for all Active Directory objects and were discussed in Chapter 4. The General tab contains the following fields:

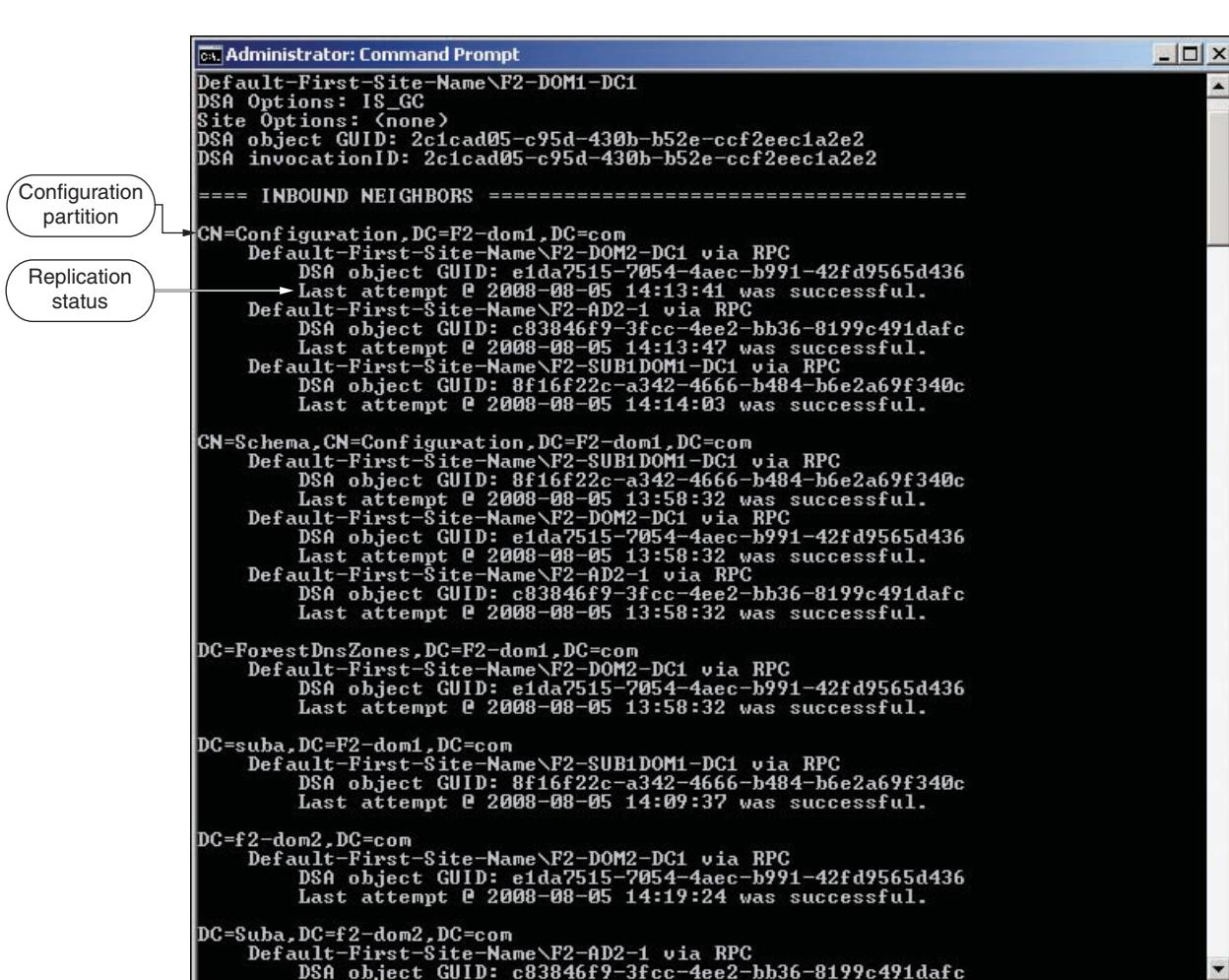
- *Change Schedule*—Click this button to view and change the KCC’s default schedule (once per hour) for periodic replication. Periodic replication occurs in addition to triggered replication, which occurs after changes to Active Directory have been made. If you attempt to change the schedule on a KCC-generated connection object, Windows warns you that changes are overwritten by Active Directory, unless you mark the object as not automatically generated.
- *Replicate from Server*—Replication is a pull process whereby a DC requests replication from its partners after being notified of changes and at the periodic replication interval. The name of the connection object’s replication partner is specified in this field; to change it, click the Change button. For intrasite replication, in which the KCC creates the connection object, changing the server isn’t recommended. As with the replication schedule, Windows warns you if you attempt to change the server name.
- *Replicate from Site*—The name of the site where the replication partner can be found. When only one site exists, this name is usually Default-First-Site-Name.
- *Replicated Naming Context(s)*—Specifies which partitions are replicated and from where. You might not see the full list because the text box isn’t very wide. In Figure 10-19, the schema directory partition and configuration partition are replicated from the specified server.
- *Partially Replicated Naming Context(s)*—Usually, a domain name is listed in this text box if the DC you’re configuring is a global catalog server and there are multiple domains in the forest. In Figure 10-19, the domain controller is getting global catalog information from the suba.F2-dom1.com domain. This text box is usually empty if the DC isn’t a global catalog server.

Creating Connection Objects You can create connection objects for intrasite replication if you want to alter the replication topology manually. You might want to alter the topology if

a site includes WAN links that could benefit from a different replication schedule. To do so, right-click NTDS Settings under the applicable server and click New Active Directory Domain Services Connection. You're asked to select a DC as a replication partner, and the connection object is named after this server by default. By default, the schedule for a new connection object is set to every 15 minutes, but you can change this value. Creating a connection object should be unnecessary in most cases, but it can be useful for troubleshooting replication problems. The KCC uses the new connection object in its topology calculations and might alter the topology as a result. You must be sure of what you're doing before making manual changes to the intrasite replication topology, or you could break replication.

If you do make changes, right-click the NTDS Settings node, point to All Tasks, and click Check Replication Topology to run the KCC algorithm. If you created a connection object, the KCC might alter the existing topology. If you created a connection manually to a server that already exists, the KCC deletes the automatically generated connection and leaves the manually created connection. If you remove the manually created connection, the KCC generally re-creates the original topology.

Checking Replication Status You can use Active Directory Sites and Services to force the KCC to check the replication topology, but if you want to view detailed information about connections and replication status, use the command-line program Repadmin.exe. Many arguments can be used with this command, but to view replication status, use repadmin /showrepl. Figure 10-20 shows the output of this command in a forest containing two trees, each with two domains and a total of four DCs. Each replication partner is listed.



```

C:\Administrator: Command Prompt
Default-First-Site-Name\F2-DOM1-DC1
DSA Options: IS_GC
Site Options: <none>
DSA object GUID: 2c1cad05-c95d-430b-b52e-ccf2eec1a2e2
DSA invocationID: 2c1cad05-c95d-430b-b52e-ccf2eec1a2e2

===== INBOUND NEIGHBORS =====
CN=Configuration,DC=F2-dom1,DC=com
  Default-First-Site-Name\F2-DOM2-DC1 via RPC
    DSA object GUID: e1da7515-7054-4aec-b991-42fd9565d436
    Last attempt @ 2008-08-05 14:13:41 was successful.
  Default-First-Site-Name\F2-AD2-1 via RPC
    DSA object GUID: c83846f9-3fcc-4ee2-bb36-8199c491dafc
    Last attempt @ 2008-08-05 14:13:47 was successful.
  Default-First-Site-Name\F2-SUB1DOM1-DC1 via RPC
    DSA object GUID: 8f16f22c-a342-4666-b484-b6e2a69f340c
    Last attempt @ 2008-08-05 14:14:03 was successful.

CN=Schema,CN=Configuration,DC=F2-dom1,DC=com
  Default-First-Site-Name\F2-SUB1DOM1-DC1 via RPC
    DSA object GUID: 8f16f22c-a342-4666-b484-b6e2a69f340c
    Last attempt @ 2008-08-05 13:58:32 was successful.
  Default-First-Site-Name\F2-DOM2-DC1 via RPC
    DSA object GUID: e1da7515-7054-4aec-b991-42fd9565d436
    Last attempt @ 2008-08-05 13:58:32 was successful.
  Default-First-Site-Name\F2-AD2-1 via RPC
    DSA object GUID: c83846f9-3fcc-4ee2-bb36-8199c491dafc
    Last attempt @ 2008-08-05 13:58:32 was successful.

DC=ForestDnsZones,DC=F2-dom1,DC=com
  Default-First-Site-Name\F2-DOM2-DC1 via RPC
    DSA object GUID: e1da7515-7054-4aec-b991-42fd9565d436
    Last attempt @ 2008-08-05 13:58:32 was successful.

DC=suba,DC=F2-dom1,DC=com
  Default-First-Site-Name\F2-SUB1DOM1-DC1 via RPC
    DSA object GUID: 8f16f22c-a342-4666-b484-b6e2a69f340c
    Last attempt @ 2008-08-05 14:09:37 was successful.

DC=f2-dom2,DC=com
  Default-First-Site-Name\F2-DOM2-DC1 via RPC
    DSA object GUID: e1da7515-7054-4aec-b991-42fd9565d436
    Last attempt @ 2008-08-05 14:19:24 was successful.

DC=Suba,DC=f2-dom2,DC=com
  Default-First-Site-Name\F2-AD2-1 via RPC
    DSA object GUID: c83846f9-3fcc-4ee2-bb36-8199c491dafc

```

Figure 10-20 Output of the repadmin /showrepl command

Each section of the output in Figure 10-20 lists a directory partition followed by the DCs from which the partition is replicated. For example, the first line under INBOUND NEIGHBORS specifies the configuration partition, and the second line shows that the F2-DOM2-DC1 domain controller is a replication partner for that partition. The next two lines show the connection object's GUID and the status of the last replication attempt. Each partition is represented in the subsequent lines of output.

Repadmin can also be used to show the partitions being replicated by each connection object, force replication to occur, force the KCC to recalculate the topology, and other actions.



Typing repadmin /? doesn't show all the available command parameters. To learn more about this command and see the full list of command parameters, visit <http://technet.microsoft.com/en-us/library/cc736571.aspx>.



Activity 10-11: Demoting Server1XX to a Stand-Alone Server

Time Required: 15 minutes

Objective: Demote Server1XX to a stand-alone server.

Description: You're in the process of consolidating your Active Directory structure and need to demote the last domain controller for the w2k8ad1XX.com domain.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start**, type **dcpromo** in the Start Search text box, and press **Enter**. In the Active Directory Domain Services Installation Wizard's welcome window, click **Next**.
3. In the message box warning that the domain controller is a global catalog server, click **OK**.
4. In the Delete the Domain window, click the **Delete the domain because this server is the last domain controller in the domain** check box, and then click **Next**.
5. In the Application Directory Partitions window, click **Next**. Click the **Delete all application directory partitions on this Active Directory domain controller** check box, and then click **Next**.
6. If you see the Remove DNS Delegation window, click **Next**. In the Windows Security window, enter **Administrator** and **Password02** in the corresponding text boxes, and then click **OK**.
7. In the Administrator Password window, type **Password02** in the Password and Confirm password text boxes, and then click **Next**.
8. In the Summary window, verify your choices, and then click **Next**. Removal of Active Directory begins. If you get an error message about DNS delegations, click **OK**. When the wizard has completed, click **Finish**.
9. Click **Restart Now**. When your server restarts, log on as **Administrator** with **Password02**. In a later activity, you promote the server to a domain controller in the w2k8adXX.com domain.

Global Catalog Replication

Domain controllers configured as global catalog servers require special attention to ensure proper replication of this important directory partition. As you learned in Chapter 4, the global catalog contains a partial replica of all objects in the forest, maintains universal group memberships, provides cross-domain logon support, and is used to locate objects throughout the forest.

Global catalog servers maintain an inbound connection with a DC in each domain the global catalog is built from (see Figure 10-21). Furthermore, connections between global catalog servers always include replication of the global catalog partition. You can see evidence of transferring the global catalog partition when viewing the properties of a connection object between global catalog servers. The Partially Replicated Naming Context(s) field shows "All other domains." Replication of the global catalog doesn't create a separate topology, but it does influence the connections the KCC creates.

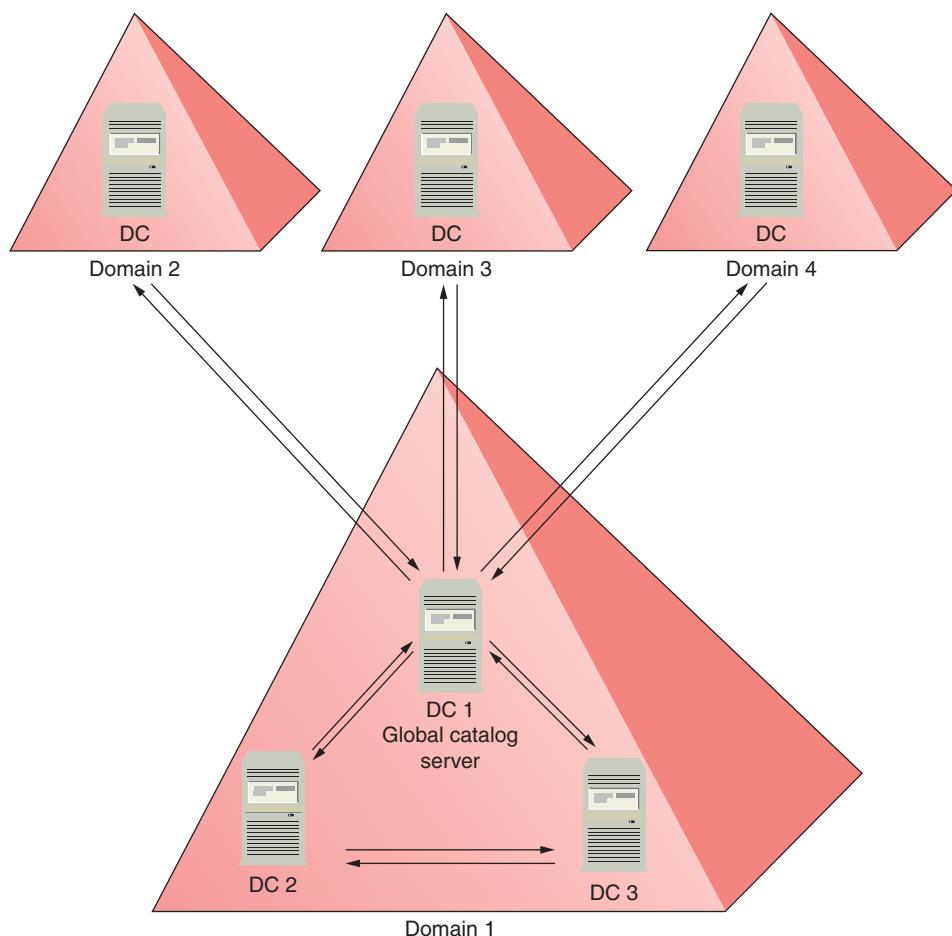


Figure 10-21 Global catalog replication

10

Special Replication Situations

Most Active Directory database changes follow the regular replication rules: Wait 15 seconds after a change is made before notifying partners, and then forward the changes with 3-second intervals between changes. However, certain changes require special processing:

- *Urgent replication events*—The following events trigger change notifications immediately, without waiting the normal 15 seconds:
 - Account lockouts, which occur when an account has a certain number of failed logon attempts
 - Changes to the account lockout policy
 - Changes to the domain password policy
 - Changes to non-security principal passwords, such as the password used to create a trust relationship
 - Password change to a domain controller computer account
 - Changes to the RID master DC
- *User account password changes*—Special replication processing occurs when a user's password is changed. A user whose password is changed can be authenticated by a DC different from the one where the change originates. To avoid delays between password changes and a user's ability to log on, Active Directory forwards password changes with urgent processing to the PDC emulator DC. If a user attempts to log on with the new password before the authenticating DC has this information, the logon attempt is forwarded to the

PDC emulator for the domain instead of denying the logon. You can use group policies to configure DCs to not contact the PDC emulator when a logon fails, however, which you might want to do if there's no PDC emulator in the local site.

RODC Replication

An RODC is treated like any other domain controller when considering replication topology. However, RODCs have some limitations you should keep in mind when you're creating the topology:

- The connection between an RODC and a writeable DC is a one-way connection because changes can't originate on an RODC.
- Two RODCs can replicate with one another, as long as one has an incoming connection with a writeable DC.
- The domain directory partition can be replicated only to an RODC from a Windows Server 2008 DC. Windows Server 2003 DCs can replicate other partitions to an RODC.
- When upgrading a domain from Windows Server 2003, the first Windows Server 2008 DC must be writeable.

RODCs are a new configuration option in Windows Server 2008. Because they can be made more secure than a writeable domain controller, they're often used in branch offices where physical server security can be a concern. For this reason, administrators are likely to use them in Active Directory site design.

Understanding and Configuring Sites

Chapter 4 discussed the reasons for creating additional sites and described basic site components, and you learned how to create new subnets in preparation for creating new sites. This section covers the components of intersite replication, explains how to configure sites for optimal efficiency, and includes the following topics:

- Creating new sites
- Configuring site links
- Intersite transport protocol
- Bridgehead servers
- Site link bridges
- Global catalog and universal group membership caching

Creating Sites

As you learned in Chapter 4, a site is an Active Directory object containing domain controllers and replication settings and is usually associated with IP subnets and site links. Sites are usually geographically dispersed and connected by WAN links, but sites can also be different buildings on a campus or different floors of a building, for example. The only criteria for a site is that it's associated with one or more IP subnets and no two sites share the same subnet. When you create a site in Active Directory Sites and Services, as you did in Activity 4-9, you're asked to select a site link. DEFAULTTIPSITELINK is the only choice unless you've created other site links.

The Significance of Subnets After creating a site, you must associate one or more subnets with it, which essentially means you're assigning a range of IP addresses to the site. Active Directory uses this information in two important ways:

- *Placing new domain controllers in the appropriate site*—Correct placement is necessary to determine the optimum intrasite and intersite replication topology and to associate clients with the nearest domain controllers. When a new DC is installed, it's automatically placed in the site corresponding with its assigned IP address (see Figure 10-22). If the DC existed before the site was created, you need to move the DC manually from Default-First-Site-Name to the new site.

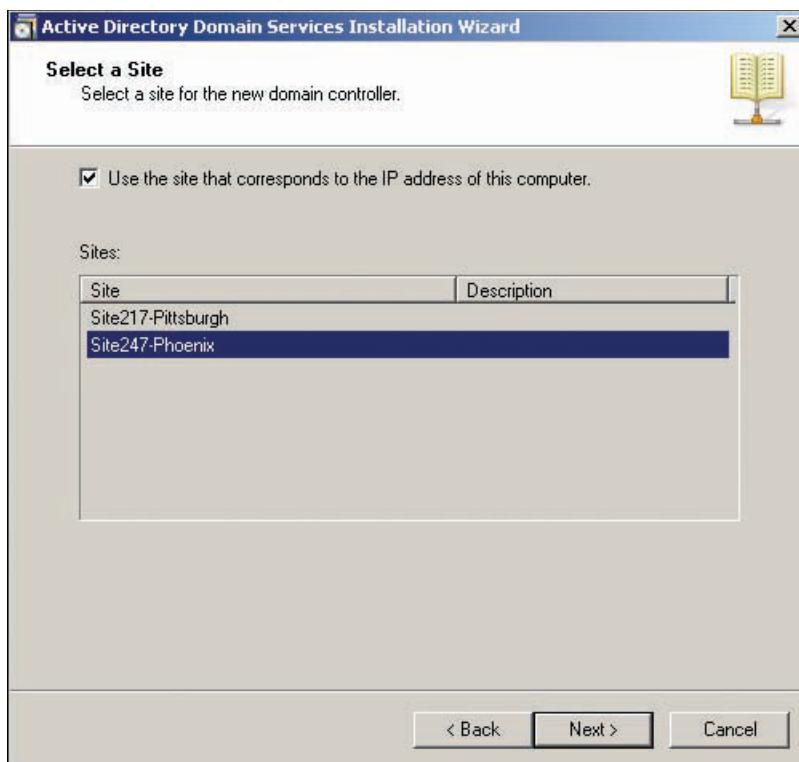


Figure 10-22 Selecting a site for a new domain controller

10

- *Determining which site a client computer belongs to*—When a client requests a domain service, such as logon to the domain or access to a DFS resource, the client request can be directed to a DC or member server in the same site. Use of a local resource is usually preferable, especially when remote sites are connected via slower WAN links.

Defining your subnets is important when you have multiple sites. If a client's IP address doesn't match a subnet in any of the defined sites, communication efficiency could degrade because the client might request services from servers in remote sites instead of locally.



Activity 10-12: Creating a New Site

Time Required: 10 minutes

Objective: Create a new site.

Description: Your business has opened a new location. To prepare Active Directory for this new location, you're creating a new site. You want to rename the default site with a more descriptive name, so you use the third octet of the subnet's network address as part of the name. You configure the site in subsequent activities.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Open Active Directory Sites and Services. Click to expand the **Sites** folder. You should see a **Subnets** folder, an **Inter-Site Transports** folder, and the **Default-First-Site-Name** site object.
3. Click to expand the **Subnets** folder. The subnet you created in Activity 4-9 should be there (192.168.100.0/24). Right-click the **192.168.100.0/24** subnet and click **Properties**. The General tab of the subnet's Properties dialog box shows that the subnet is assigned to **Default-First-Site-Name**. Click **Cancel**.
4. Right-click **Default-First-Site-Name** and click **Rename**. Type **Site100** and press **Enter**. Giving each site a descriptive name is a good idea; in this case, the 100 just indicates the subnet the site is associated with.

5. Right-click the **Sites** folder and click **New Site**. In the New Object - Site dialog box, type **Site200** in the Name text box. Notice that you're prompted to select a site link object for the site. (Site links are discussed in the next section.) Click **DEFAULTTIPSITELINK**, and then click **OK**.
6. You should see a message from Active Directory Domain Services informing you that more steps are necessary to finish configuring your site. You need to make sure your site links are appropriate, add subnets for the site in the Subnets folder, and add a domain controller to the site. Click **OK**.
7. Close Active Directory Sites and Services.



Activity 10-13: Promoting Server1XX to a Domain Controller

Time Required: 20 minutes

Objective: Promote a server to a domain controller in the w2k8adXX.com domain.

Description: You have finished deleting a domain as part of your Active Directory consolidation and want to promote the server that was demoted in Activity 10-11 to a DC in the w2k8adXX.com domain. (Note that ServerXX must be running when you perform this activity.)

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start**, type **dcpromo**, and press **Enter**. When the wizard starts, click **Next**. In the Operating System Compatibility window, click **Next**.
3. In the Choose a Deployment Configuration window, click **Existing forest**. Make sure **Add a domain controller to an existing domain** is selected, and then click **Next**.
4. In the Network Credentials window, type **w2k8adXX.com** in the text box, and then click the **Set** button. Type **administrator@w2k8adXX.com** for the username and **Password01** for the password, and then click **OK**. Click **Next**.
5. In the Select a Domain window, click **Next**.
6. Because you have more than one site defined, Windows selects a site for you based on the server's IP address; in this case, Site100 should be selected by default. Click **Next**.
7. DNS was installed on the DC when this server was part of the w2k8ad1XX.com domain. You can make the DC a global catalog server and an RODC at this point, but you make this DC a global catalog server later. Click to clear the **Global catalog** check box, and then click **Next**.
8. You get a "Infrastructure Master Configuration Conflict" message. Click **Do not transfer the infrastructure master role to this domain controller. I will correct the configuration later**.
9. You get an message about dynamically assigned IP addresses because your IPv6 address is dynamically assigned. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.
10. You might get a message about DNS delegation. When asked if you want to continue, click **Yes**.
11. In the Location for Database, Log Files, and SYSVOL window, accept the default settings, and then click **Next**.
12. In the Directory Services Restore Mode Administrator Password window, type **Password02** in the Password and Confirm password text boxes, and then click **Next**.
13. In the Summary window, click **Next**. When the wizard completes the Active Directory installation, click **Finish**, and then click **Restart Now**.
14. When the server restarts, log on as **Administrator** with **Password01**. Note that you're now logging on to the w2k8adXX.com domain, so you use the password defined for the domain administrator.
15. Open Active Directory Users and Computers to verify that the domain information from ServerXX has replicated to Server1XX. You should see all the OUs and users created for the w2k8adXX.com domain. Click the **Domain Controllers** OU. You should see both ServerXX

and Server1XX. Notice that the Site column shows in which site the DC is located. Close Active Directory Users and Computers, and stay logged on to Server1XX. Both servers must remain running for the next activity.



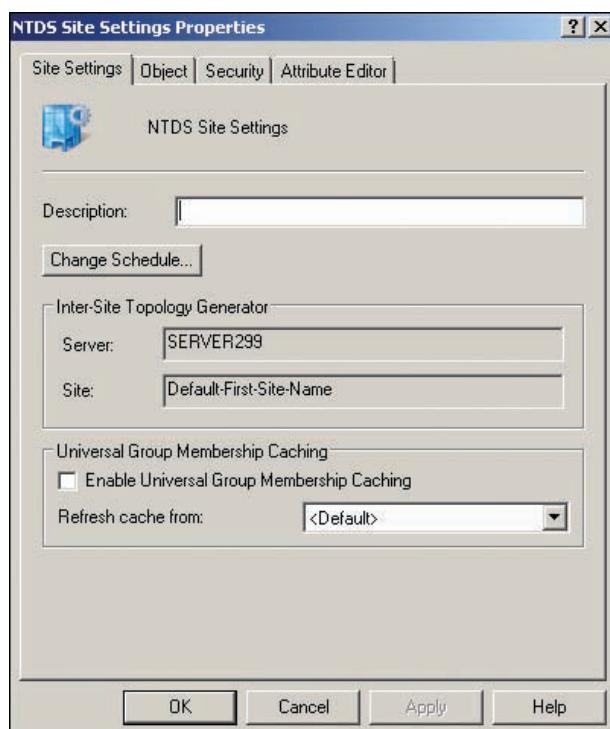
Activity 10-14: Viewing Site Properties

Time Required: 15 minutes

Objective: View and change some site properties.

Description: You're trying to familiarize yourself with sites and site objects, so you explore the properties of NTDS Site Settings, server NTDS Settings, and connection objects.

1. Log on to **Server1XX** as Administrator, if necessary, and open Active Directory Sites and Services.
2. Click to expand **Sites**, and then click **Site100**. Two objects are displayed in the right pane: the Servers folder, which lists the DCs in the site, and NTDS Site Settings. The NTDS Site Settings Properties dialog box (see Figure 10-23) has a variety of settings that affect intrasite and intersite replication.



10

Figure 10-23 The NTDS Site Settings Properties dialog box

3. In the right pane, double-click to expand the **Servers** folder and then **Server1XX**. Right-click **NTDS Settings** and click **Properties**. Note that there are NTDS Settings associated with server objects and NTDS Site Settings associated with site objects (as in Figure 10-23).
4. In the General tab, you can configure the server as a global catalog server. Click the **Connections** tab. You should see ServerXX in both the Replicate From and Replicate To text boxes. Click **Cancel**.
5. In the right pane, double-click to expand **NTDS Settings**. Right-click the connection object for ServerXX. Notice that Replicate Now is an option, which you can use to force replication to occur immediately. Click **Properties**.
6. Click the **Change Schedule** button. The regular schedule for intrasite replication is once per hour. Click **OK**, and then click **Cancel**.
7. Click **Site100** again. Right-click **NTDS Site Settings** and click **Properties**.

8. In the Site Settings tab, click **Change Schedule**. In the Schedule for NTDS Site Settings dialog box, click **All**. Click **Four Times per Hour**. Changing the replication schedule here changes it for all automatically generated connections in the site. Click **OK** twice.
9. Verify that the schedule has changed. Click **NTDS Settings** under Server1XX again. Double-click the connection object to open its Properties dialog box, and click the **Change Schedule** button. Notice that the schedule for replication has changed. (If the schedule doesn't seem to have changed, close and reopen Active Directory Sites and Services, and check again.) Click the **All** button at the upper left of the day/time table, click the **Once per Hour** option button, and then click **OK**.
10. Click **Apply**. You get a message indicating that changes to the connection will be overwritten because it's generated automatically and are asked whether you want to mark the connection as not automatically generated. Click **Yes**, which changes the replication schedule for this connection only. Any other connections have their schedule set in NTDS Site Settings. Click **OK**. Notice that the connection object's name changes to a numeric GUID instead of being generated automatically.
11. Stay logged on and keep Active Directory Sites and Services open for the next activity.

Configuring Site Links

Any new sites you create use the default site link, DEFAULTIPSITELINK, for their connection with other sites. If all your company locations are connected via network links of similar speeds, you can use a single site link for all site connections. However, if connections between locations differ in speed or traffic volume, for example, you might want to create additional site links so that you can adjust the replication schedule according to your network links' characteristics.

Site links are located in the Inter-Site Transports folder in Active Directory Sites and Services. This folder has two subfolders—IP and SMTP—and the DEFAULTIPSITELINK site link is in the IP folder. To configure the site link, right-click it and click Properties to open the dialog box shown in Figure 10-24. (Intersite transport protocols are discussed in the next section.)

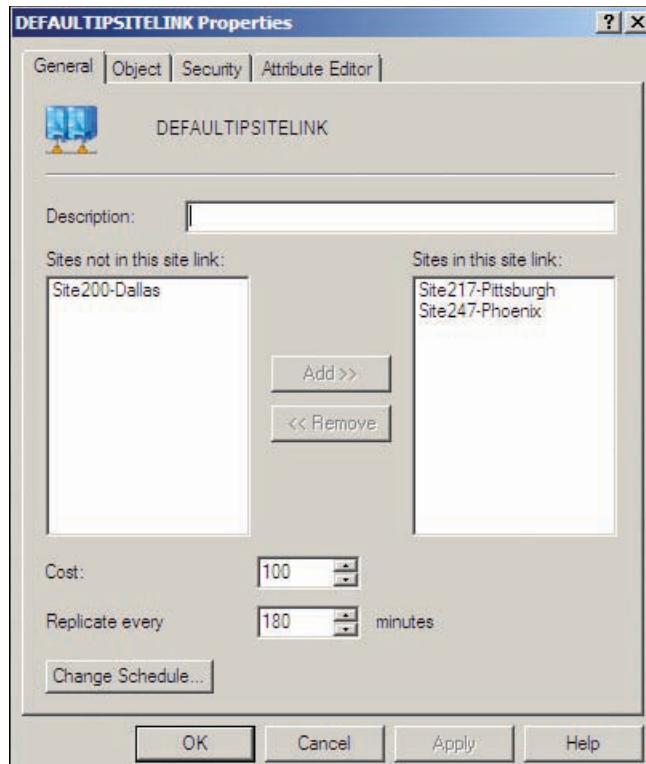


Figure 10-24 The Properties dialog box for a site link

In a site link's Properties dialog box, you can add or remove sites that use the link for replication. In Figure 10-24, Site217-Pittsburgh and Site247-Phoenix use the site link, but Site200-Dallas does not. You can change the replication cost and frequency in this dialog box, too. (The cost attribute was discussed in Chapter 4.) By default, intersite replication occurs every 180 minutes, seven days a week. If you click Change Schedule, you can deselect days or times when replication can occur. For example, if your WAN link is busiest on Monday through Friday from 9 a.m. to noon, you could exclude these days and times from the replication schedule. Replication then occurs every three hours at all other times and days.

To create a new site link that uses the IP protocol, right-click the IP folder and click New Site Link. You should provide a descriptive name for the site link. A site link must contain at least two sites. A site can exist in more than one site link, however; for example, suppose your configuration includes three sites: Pittsburgh, Dallas, and Phoenix. Pittsburgh and Dallas could be contained in one site, and Dallas and Phoenix could be in the other site. Dallas, in this case, is contained in both sites. This arrangement makes sense if Dallas has WAN connections between both Pittsburgh and Phoenix. Domain controllers between Pittsburgh and Phoenix can still replicate with one another because of the transitive nature of site links. Because Pittsburgh can replicate with Dallas and Dallas can replicate with Phoenix, Pittsburgh can replicate with Phoenix.

Two other site link configuration options can be configured only in the Attribute Editor tab of a site link's Properties dialog box. By default, notification of changes doesn't occur between sites, and replication is based solely on the schedule. You can enable notifications by setting the options attribute to 1. In addition, data is compressed by default when it's replicated between sites. To turn compression off, set the options attribute to 4. To combine multiple options, simply add the values together. Therefore, to enable notification and disable compression, set the options attribute to 5.

10



Activity 10-15: Creating a Site Link

Time Required: 15 minutes

Objective: Create a new site link.

Description: You have created a site and now have a domain controller in the site. Next, you create a site link to configure replication between Site100 and Site200.

1. Log on to **Server1XX** as Administrator and open Active Directory Sites and Services, if necessary.
2. Click to expand **Sites** and **Inter-Site Transports**, if necessary.
3. Right-click the **IP** folder and click **New Site Link**. In the Properties dialog box, type **Site100-200** in the Name text box.
4. In the Sites not in this site link list box, click **Site100**, and then click the **Add** button. In the same list box, click **Site200**, and then click **Add** again. Click **OK**.
5. If necessary, click to expand **IP** in the left pane. In the right pane of Active Directory Sites and Services, right-click **Site100-200** and click **Properties**. Click the **Change Schedule** button. Notice that replication takes place all day every day.
6. Drag to form a box around Monday through Friday from 8 a.m. to 3 p.m., and then click **Replication Not Available**. Now Site 100 and Site 200 won't attempt to replicate during these times. Click **OK**.
7. Click in the **Cost** text box and type **200**. Recall that the higher the cost of the link, the less attractive it is when the topology is generated. If there are multiple paths between destinations, the lower cost path is selected. Click **OK**.
8. Close Active Directory Sites and Services, and log off Server1XX.

Bridgehead Servers To determine the intersite replication topology for a site, the KCC on one DC is designated as the Intersite Topology Generator (ISTG). To that end, the ISTG is responsible for assigning a bridgehead server for each directory partition in the site. Bridgehead servers are responsible for all intersite replication.

You might need to designate bridgehead servers manually sometimes. Perhaps you've identified a DC in a site that's less burdened by other server tasks and is better able to handle the task than the server identified by the ISTG. You can use the repadmin /bridgeheads command to list which DCs in a site are acting as bridgehead servers to other sites.

After you have determined which DCs are currently acting as bridgehead servers, you can designate preferred bridgehead servers in Active Directory Sites and Services. Find the server in the Servers folder under the site, right-click the server object, and click Properties. Select the intersite transport protocol on the left (see Figure 10-25), and add it to the "The server is a preferred bridgehead server for the following transports" list box. You need to make sure all directory partitions in the site are contained on the bridgehead servers you configure. If you don't, Windows warns you about which partitions the configured bridgehead servers won't replicate. Replication still takes place for these partitions because Windows configures the necessary bridgehead servers automatically, but relying on this automatic configuration defeats the purpose of assigning bridgehead servers manually.

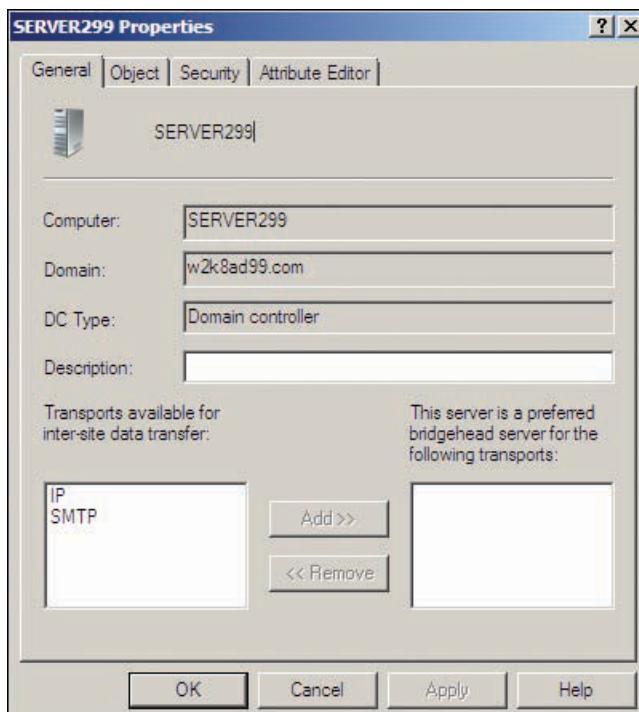


Figure 10-25 Configuring a bridgehead server



If a manually configured bridgehead server fails, replication for the partitions it contains stops. The ISTG doesn't configure a new bridgehead server automatically for a failed manually configured one. However, if the ISTG assigns the bridgehead server and it fails, the ISTG automatically attempts to assign a new one.

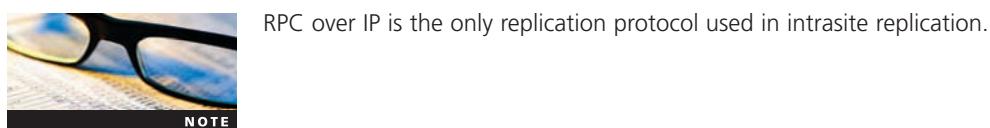
Intersite Transport Protocols Two protocols can be used to replicate between sites: IP and SMTP. By default, IP is used in the DEFAULTIPSITELINK site link and is recommended in most cases. To be precise, when you choose IP as the intersite transport protocol, you're choosing Remote Procedure Call (RPC) over IP. RPC over IP uses synchronous communication, which requires a reliable network connection with low latency. With synchronous communication, when a request is made, a reply is expected immediately, and the entire process of replication with one DC finishes before the process can begin with another DC.

If your network connections don't lend themselves to RPC over IP, you can use Simple Mail Transport Protocol (SMTP). SMTP, used primarily for e-mail, is an asynchronous protocol that

works well for slower, less reliable, or intermittent connections. The advantage of SMTP is that a DC can send multiple replication requests simultaneously without waiting for the reply; the reply can occur sometime later. So if you think of SMTP as an e-mail conversation, you can liken RPC over IP to a chat session.

SMTP requires fairly complex configuration, and the administrative hassle is rarely worth it, particularly with today's fast and reliable WAN connections. In addition, SMTP can't be used to replicate domain directory partitions, so it can't be used in domains spanning multiple sites. It can be used only to replicate the schema, global catalog, and configuration partitions. In a nutshell, here are requirements for the bridgehead servers on both ends of an SMTP-configured site link:

- The SMTP feature must be installed on both servers.
- An enterprise certification authority must be configured on the network.
- The site link path must have a lower cost than an RPC over IP site link.
- You can't have DCs from the same domain in both sites.
- The DCs must be configured to receive e-mail.



Site Link Bridges By default, **site link bridging** is enabled, which makes site links transitive. In some circumstances, you don't want all site links to be transitive, such as when some WAN links are slow or available only sporadically, as with a dial-up connection. To change the transitive behavior of site links, turn off site link bridging and create site link bridges manually, which enables you to manage replication traffic between sites more efficiently with some network topologies.

Figure 10-26 shows a network with a hub-and-spoke WAN topology. Because of the transitive nature of site links, Site1 replicates with bridgehead servers in Site2 and can also replicate with bridgehead servers in Site2A, Site2B, and Site2C. If WAN connections between all sites are fast and reliable, with plenty of bandwidth for replication traffic, this default behavior works well.

Keep in mind, however, that the same replication traffic is crossing the WAN links four times, one for each site. On slower or heavily used WAN links between Site1 and Site2, this extra traffic could be excessive. To better control the flow of replication traffic, disable automatic site link bridging and create site link bridges between Site1 and Site2 and between Site2 and its satellites. Replication traffic still flows between Site1 and Site2, but Site2 distributes the traffic to satellite sites, so replication traffic crosses the Site1-Site2 WAN link only one time. You would probably want to create site link bridges in the opposite direction as well.

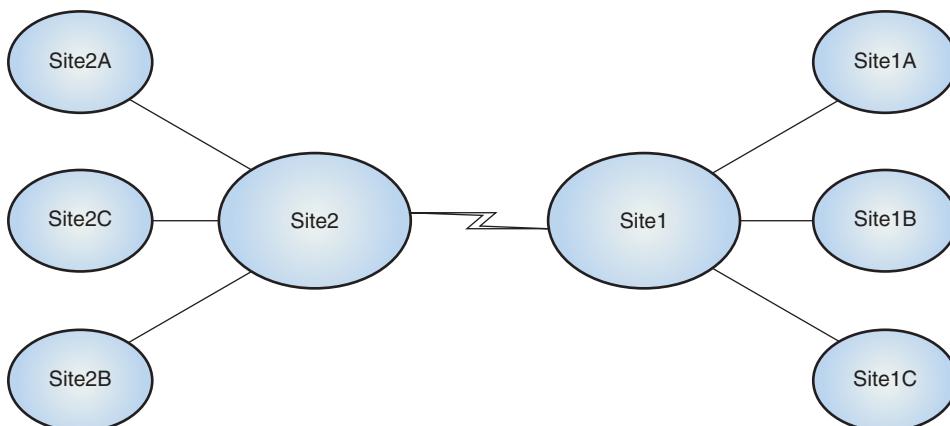


Figure 10-26 Hub-and-spoke topology

Other reasons to create site link bridges manually include the following:

- *Control traffic through firewalls*—You might want to limit which DCs can communicate with one another directly through firewalls. You can configure firewalls to allow traffic between DCs at specific sites and create site link bridges as needed.
- *Accommodate partially routed network*—Normally, the KCC considers all possible connections when determining the replication topology. If sites are connected only intermittently, you can configure site link bridges between only the sites that map to full-time network connections, which bypasses intermittent links.
- *Reduce confusion of the KCC*—A complex network that involves many alternate paths between sites can cause confusion when the KCC and ISTG create the replication topology. You can force what kind of topology is created by using custom site link bridges and disabling transitivity.

To disable transitivity of site links, right-click the IP or SMTP folder under Inter-Site Transports, and click Properties. Click to clear the Bridge all site links check box. To create a site link bridge, right-click the IP or SMTP folder and click New Site Link Bridge. Give a descriptive name to the site link bridge, and then add at least two site links to it.

The Global Catalog and Universal Group Membership Caching

As you know, the global catalog is a critical component for many Active Directory operations, so access to a global catalog server must be considered when designing sites and configuring site replication. Having a global catalog server used to be critical in sites with more than a few users because it speeded logons and forest-wide searches for Active Directory objects. However, replication traffic is increased considerably in sites with global catalog servers.

Windows Server 2008 resolves the potential conflict between faster logons and increased replication traffic by introducing **universal group membership caching**. When this feature is enabled, the first time a user logs on to a domain in the site with no global catalog server, the user's universal group membership information is retrieved from a global catalog server in a different site. Thereafter, the information is cached locally on every DC in the site and updated every 8 hours, so there's no need to contact a global catalog server. Having this feature available, however, doesn't mean a global catalog server should never be placed in a site. Microsoft recommends placing a global catalog server in the site when the number of accounts (user and computer) exceeds 500 and the number of DCs exceeds two. With 500 cached accounts, the traffic created by refreshing every 8 hours might be higher than global catalog replication traffic. In addition, you need to determine whether the other benefits of having a global catalog server (faster forest-wide searches, faster updates of universal groups) outweigh the reduced replication traffic of universal group membership caching.

To configure universal group membership caching, in Active Directory Sites and Services, expand the site object, and then open the Properties dialog box of the NTDS Site Settings object. In the Site Settings tab, click the Enable Universal Group Membership Caching check box. In addition, you can select which global catalog server is used to refresh the cache.

Working with Operations Master Roles

As discussed in Chapter 4, Active Directory uses a multimaster replication scheme to synchronize copies of most information in the Active Directory database. However, some critical information is subject to a single master replication scheme to avoid any possibility of the information becoming unsynchronized. The servers that keep this critical information are assigned a Flexible Single Master Operation (FSMO) role. FSMO roles were described in Chapter 4 and can be summarized as follows:

- *Forest-wide FSMO roles*—Only one DC per forest performs these roles: domain naming master and schema master.
- *Domain-wide FSMO roles*—Only one DC per domain performs these roles: PDC emulator, RID master, and infrastructure master.

This chapter discusses best practices for locating these DCs in your network for optimal reliability and replication efficiency. Furthermore, this chapter explains how to transfer and seize FSMO roles when you need to assign a role to a different domain controller.

Operations Master Best Practices

The decision of where to place an FSMO role holder is part of your overall Active Directory design strategy. If you build a new forest, the first DC installed performs all five FSMO roles. When a new domain is created in the forest, the first DC performs all three domain-wide FSMO roles for that domain. In a smaller network, having all these critical roles on a single server can work, but in a large network with multiple domains and sites, you might want to transfer some roles to different servers. Placement of the DCs functioning in these roles can affect replication and the capability to recover from a server failure. In addition, being able to restore functionality of FSMO roles quickly after a server failure is critical. However, not all FSMOs have equal importance; some roles must be functioning almost continuously for proper domain operation, but other roles can be offline for a while with little disturbance to the network.

Here are some common rules for operations masters:

- Unless your domain is very small, transfer operations master roles from the first DC installed in the forest to other DCs because some FSMO roles can be quite resource intensive.
- Place the servers performing these roles where network availability is high.
- Designate an alternate DC for all roles. The alternate assumes the role if the original server fails, and it should be a direct replication partner with the original FSMO role holder. Document your plan to make sure alternate DCs aren't burdened with other services that could impede their performance as an FSMO role holder.

The following sections explain issues involved with FSMO roles in more detail.

10

Domain Naming Master The domain naming master is needed when a domain or domain controller is added or removed from the forest. In most cases, neither users nor administrators notice its absence until one of these operations is attempted. If the DC performing this role goes offline, you should probably wait until it comes back online before attempting to add or remove a domain or DC. The exception, of course, is if you need to add a domain to the network immediately. If you decide to install this role on another DC, the original domain naming master must not be put back into service unless you uninstall Active Directory.

When possible, the domain naming master should be a direct replication partner with another DC that's also a global catalog server in the same site. Ideally, the domain naming master should also be a global catalog server. If the role must be moved, the direct replication partner is the preferred choice because it should be most fully replicated with the original FSMO. The domain naming master and the other forest-wide FSMO role, the schema master, can be, but need not be, on the same server.

Schema Master The schema master is needed when the Active Directory schema is changed, including raising the forest functional level. Its absence isn't apparent to users or administrators unless a schema change is attempted. Generally, the schema master should be transferred to another server only when you're certain the original server will be down permanently.

PDC Emulator The PDC emulator processes password changes for older Windows clients (Windows 9x and NT) and is used during logon authentication, as discussed earlier. The DC performing this role should be centrally located where there's a high concentration of users to facilitate logons. The PDC emulator is the most heavily used of the FSMO roles and should be placed on a suitable DC, which shouldn't be a global catalog server because global catalog servers are also used heavily. If the PDC emulator role fails, you might want to move the role to another server immediately. After the original server returns to service, the role can be transferred back to it.

RID Master Every Active Directory object uses an RID to create the object's SID. The RID master provides these RIDs to domain controllers. Given that, the RID master should be placed

in an area where Active Directory objects are created most often, such as near the administrator's office. This FSMO role must be highly available to other DCs and is ideally placed with the PDC emulator because the PDC emulator uses the RID master's services frequently. Because the RID master doles out RIDs to DCs in blocks of 500, temporary downtime might not be noticed. However, if a DC has exhausted its pool of RIDs, and the RID master is not available, new objects can't be created. In the event of an RID master failure, moving this role to another server should be considered only if the original RID master is down permanently.

Infrastructure Master A temporary interruption of this role's services probably won't be noticed. This role is most needed when many objects have been moved or renamed. The infrastructure master role shouldn't be performed by a DC that's also a global catalog server, unless all servers in the forest have been configured as global catalog servers or there's only one domain in the forest. However, a global catalog server should be in the same site as the infrastructure master because there's frequent communication between these two roles. In the event of an infrastructure master failure, the role can be moved to another DC, if necessary, and returned to the original server when it's back in service.



The only time the infrastructure master and global catalog can be on the same DC is when there's only one domain in the forest or all DCs are configured as global catalog servers. If neither is the case, and the infrastructure master is also a global catalog server, the infrastructure master never finds out-of-date data, so it never replicates changes to other DCs in the domain.

Managing Operations Master Roles

Because of the critical nature of the functions FSMO role holders perform, administrators should be familiar with two important FSMO management operations: transferring and seizing. These two functions enable administrators to change the DC performing the FSMO role to make the Active Directory design more efficient and to recover from server failure. Of course, system backups should always be part of managing disaster recovery. Chapter 13 covers backup and restore of Active Directory.

Transferring Operations Master Roles Transferring an operations master role means moving the role's function from one server to another while the original server is still in operation. This transfer is generally done for one of the following reasons:

- The DC performing the role was the first DC in the forest or domain and, therefore, holds all domain-wide or domain- and forest-wide roles. Unless you have only one DC, distributing these roles to other servers is suggested.
- The DC performing the role is being moved to a location that isn't well suited for the role.
- The current DC's performance is inadequate because of the resources the FSMO role requires.
- The current DC is being taken out of service temporarily or permanently.

The five FSMO roles and the MMCs used to transfer them are listed in Table 10-1.

Table 10-1 The MMCs for transferring FSMO roles

FSMO Role	MMC
Schema master	Active Directory Schema
Domain naming master	Active Directory Domains and Trusts
RID master, PDC emulator master, and infrastructure master	Active Directory Users and Computers



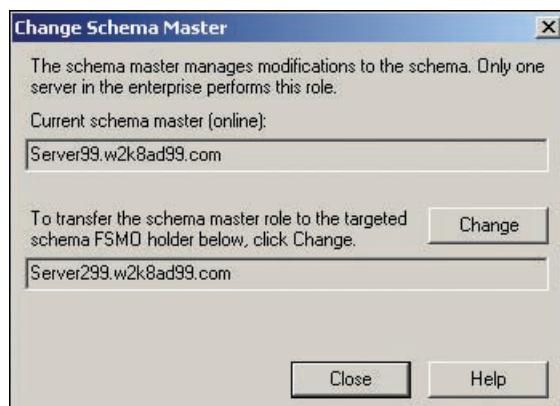
Activity 10-16: Transferring the Schema Master Role

Time Required: 15 minutes

Objective: Transfer the schema master role.

Description: You want to distribute the FSMO load, so you transfer the schema master role to your second domain controller.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Open a new MMC and add the Active Directory Schema snap-in to it, if necessary.
3. Under Console Root, right-click **Active Directory Schema** and click **Change Active Directory Domain Controller**.
4. In the Change Directory Server dialog box, click **Server1XX.w2k8adXX.com** and click **OK**. You get a message warning you that because the schema snap-in isn't connected to the schema operations master, you can't make any changes. Click **OK**.
5. Right-click **Active Directory Schema** and click **Operations Master**. The Change Schema Master dialog box shows you the current schema master and asks whether you want to transfer the role to the new DC (see Figure 10-27). Click the **Change** button.



10

Figure 10-27 The Change Schema Master dialog box

6. When prompted to confirm, click **Yes**. In the success message box, click **OK**. Notice that the Change Schema Master dialog now shows Server1XX as the schema master. Click **Close**.
7. Close the MMC window.

To change the domain naming master, the steps are similar to Activity 10-16, except you use Active Directory Domains and Trusts. Because the global catalog is currently on the same DC as the infrastructure master, which isn't recommended, you transfer the infrastructure master role next.



Activity 10-17: Transferring the Infrastructure Master Role

Time Required: 15 minutes

Objective: Transfer the infrastructure master role.

Description: You understand the problem of having the infrastructure master role on the same DC as a global catalog server, so you transfer the role to another DC.

1. Log on to **ServerXX** as Administrator, if necessary, and open Active Directory Users and Computers.
2. Right-click the **Active Directory Users and Computers** node and click **Change Domain Controller**.
3. In the Change Directory Server dialog box, click **Server1XX.w2k8adXX.com** and click **OK**.

4. Right-click the **Active Directory Users and Computers** node again, point to **All Tasks**, and click **Operations Masters**.
5. In the Operations Masters dialog box, click the **Infrastructure** tab. Click the **Change** button to transfer the infrastructure master to Server1XX.
6. Click **Yes** when asked to confirm the transfer, and then click **OK** in the success message. Notice that Server1XX is shown as the operations master in the Infrastructure tab. Click **Close**.
7. Close Active Directory Users and Computers.

The procedure to transfer the PDC emulator and RID master roles is similar to transferring the infrastructure master role.

Seizing Operations Master Roles An operations master role is seized when the current role holder is no longer online because of some type of failure. Seizing should never be done when the current role holder is accessible and should usually be done only when it's unlikely the original server can be restored to service. If a DC is scheduled to be decommissioned, you should transfer the role while the DC is still online. If the operations master DC becomes inaccessible because of network failure or a temporary hardware failure, you should wait until this server is back online rather than seize the operations master role.

An exception might be the PDC emulator role, which can affect user logons, or the RID master, which might be needed to create Active Directory objects. If either role holder is going to be offline for an extended period, seizing the role and then transferring it to the original DC when it's back online might be best for continued Active Directory operation. To seize an operations master role, follow these steps:

1. Open a command prompt window, type **ntdsutil**, and press **Enter**.
2. Type **roles** and press **Enter** to get the FSMO Maintenance prompt.
3. Type **connections** and press **Enter** to get the Server Connections prompt.
4. Type **connect to server DCName**, replacing *DCName* with the domain controller where you're transferring the FSMO role.
5. Type **quit** to get back to the FSMO Maintenance prompt.
6. Type **seize RoleName** and press **Enter**, replacing *RoleName* with the name of the role you want to seize. Possible role names are domain naming master, schema master, PDC, RID master, and infrastructure master.
7. Windows attempts to transfer the role first, and if a transfer fails, the role is seized. Type **quit** and press **Enter** to exit Ntdsutil.

Chapter Summary

- Instead of requiring administrators to upgrade all current servers before installing a new server version, administrators can configure functional levels on new domain controllers to maintain backward compatibility.
- Functional levels can be raised from an earlier version to a newer version but can't be changed from a newer version to an earlier version.
- Windows Server 2008 supports three forest functional levels: Windows 2000, Windows Server 2003, and Windows Server 2008. The supported domain functional levels have nearly identical names. A domain controller can't be configured to run at a lower domain functional level than the functional level of the forest in which it's installed.
- You can raise the functional levels when you run Dcpromo.exe to install Active Directory (the recommended method), or you can raise them manually. Before you raise functional levels, be sure your domain controllers meet the requirements for the functional level you want.

- Before you can install a Windows Server 2008 server as a domain controller in an existing Windows Server 2003 or Windows 2000 Server domain, you must prepare existing domain controllers for the Windows Server 2008 domain controller and the schema changes it will bring.
- Before you can install an RODC in an existing domain that isn't running all Windows Server 2008 domain controllers, you must verify that the forest functional level is Windows Server 2003 or higher, prepare the forest with Adprep, and install a writeable Windows Server 2008 domain controller.
- To remove a domain controller, you use Dcpromo to remove domain services from the domain controller. You can use Dcpromo or Ntdsutil to remove a domain from a forest.
- Use the Active Directory Migration Tool to migrate accounts from one domain or forest to another.
- Before creating a trust of any type, DNS must be configured so that FQDNs of domain controllers in all participating domains can be resolved. Typically, you configure DNS between forests by using conditional forwarders, stub zones, and occasionally secondary zones.
- Some trust properties you can configure include the trust direction and transitivity, name suffix routing, and authentication.
- Both intrasite and intersite replication use the same basic processes to replicate Active Directory data; the main goal is to balance data replication timeliness and efficiency. Intrasite replication involves two major components: Knowledge Consistency Checker (KCC) and connection objects.
- A site is an Active Directory object containing domain controllers and default settings for replication within the site and is usually associated with one or more IP subnets and site links. To create a new site, you use Active Directory Sites and Services.
- Connection objects provide the connection and replication parameters between two servers. You can add or remove sites that use a particular site link for replication. Two protocols can be used to replicate between sites: IP and SMTP. By default, IP is used in the DEFAULTTIPSITELINK site link and is recommended in most cases.
- Bridgehead servers are responsible for all intersite replication. By default, site link bridging is enabled, which makes site links transitive.
- Universal group membership caching resolves the potential conflict between faster logons and additional replication traffic.
- Deciding where to place the FSMO role holder is part of your overall Active Directory design strategy. Two important operations for managing FSMOs are transferring and seizing operations master roles.



10

Key Terms

alternate UPN name suffixes This method enables users to log on with another name in place of the “domain” in the typical UPN suffix format *username@domain*. These suffixes are used for security reasons or to simplify logons with lengthy suffixes.

connection object An Active Directory object created in Active Directory Sites and Services that defines the connection parameters between two replication partners.

forest-wide authentication A property of a forest trust in which all users in a trusted forest can be authenticated to the trusting forest.

interforest migration Moving objects between domains in different forests. Migrated objects are actually copied and exist in both domains simultaneously so that users can continue working while the migration is in progress.

intraforest migration Moving objects between domains in the same forest. The domain from which objects are moved is the source domain, and the domain to which they're being moved is the target domain.

selective authentication A property of a forest trust that enables administrators to specify users who can authenticate to selected resources in the trusting forest.

SID filtering When enabled, this option causes the trusting domain to ignore any SIDs that aren't from the trusted domain.

site link bridging A default property of a site link that makes it transitive. To control the transitive nature of site links, you can create site link bridges manually.

universal group membership caching When enabled for a site, this Windows Server 2008 feature stores universal group membership information retrieved from a global catalog server, so the global catalog server doesn't have to be contacted for each user logon.

Review Questions

1. Which of the following is the default forest functional level for a Windows Server 2008 domain controller installed in a new forest?
 - a. Windows 2000 mixed
 - b. Windows 2000
 - c. Windows Server 2003
 - d. Windows Server 2008
2. Which of the following is true about forests running at the Windows Server 2003 functional level? (Choose all that apply.)
 - a. You can rename a domain.
 - b. You can create a forest trust with a Windows 2000 forest.
 - c. RODCs can be part of the forest.
 - d. Windows 2000 domain controllers can be part of the forest.
3. The Windows 2000 native domain functional level supports universal groups. True or False?
4. Which of the following is a feature introduced with the Windows Server 2008 domain functional level? (Choose all that apply.)
 - a. Shortcut trusts
 - b. Fine-grained password policies
 - c. DFS replication of Sysvol
 - d. Selective authentication
5. You're going to introduce a Windows Server 2008 domain controller into a Windows Server 2003 forest. Which of the following should you do?
 - a. First, prepare the forest by running adprep /forestprep on a Windows Server 2003 domain controller performing the schema operations master role. Then run adprep /domainprep in each domain that will have a Windows Server 2008 domain controller.
 - b. First, run adprep /domainprep in each domain that will have a Windows Server 2008 domain controller. Then prepare the forest by running adprep /forestprep on a Windows Server 2003 domain controller performing the infrastructure operations master role.
 - c. First, run adprep /domainprep on a Windows Server 2003 domain controller that holds the schema operations master role. Then run adprep /forestprep on a domain controller performing the infrastructure operations master role.
 - d. First, prepare the forest by running adprep /forestprep on the new Windows Server 2008 domain controller. Then run adprep /domainprep on each new Windows Server 2008 domain controller in each domain.
6. If you need to remove a domain from a forest in which the last domain controller has failed, which program should you use?

7. What is the program for migrating users from one forest to another?
8. Which of the following is associated with Active Directory migration? (Choose all that apply.)
- Ntdsutil
 - Adprep
 - SID history
 - Security translation
9. You're going to configure a forest trust between ForestA and ForestB and are logged on to a domain controller in the root of ForestA. You try to ping a domain controller in the root domain of ForestB and get the reply "Please check the name and try again." You have the IP address of the domain controller in the other forest, so you try pinging again with this IP address, and it's successful. You know you have the correct server and domain name. What should you do before you attempt to create the trust?
- Verify the IP address assignment of the remote domain controller.
 - Configure a stub zone.
 - Verify that Kerberos v5 is configured correctly in both forests.
 - Configure a standard primary zone.
10. If you configure a trust between ForestA and ForestB, and a trust exists between ForestB and ForestC, then ForestA trusts ForestC. True or False?
11. Which of the following should you configure if you want users in a trusted forest to have access only to certain resources in your forest, regardless of permission settings on these resources?
- SID filtering
 - Trust transitivity
 - Selective authentication
 - One-way trust
12. Bob is an administrator in a trusted forest, and you have some concerns about his trustworthiness. You want to be sure he can't gain privileged access to resources in your forest while masquerading as a user in his forest who doesn't normally have privileged access in your forest. What should you configure in the forest trust?
- SID filtering
 - Trust transitivity
 - Selective authentication
 - One-way trust
13. You want to change the replication schedule between two domain controllers in the same site—and only these two domain controllers—to occur four times per hour. The KCC has generated all your intrasite connection objects. What's the best way to make this change?
- In the General tab of the connection object's Properties dialog box, click Change Schedule, and change the replication schedule to four times per hour. Make sure the object is marked as automatically generated.
 - Create a new connection object for the two domain controllers, and set the schedule to four times per hour. Tell the KCC to check the replication topology.
 - In the Site Settings tab of the NTDS Site Settings Properties dialog box, click Change Schedule, and set the schedule to four times per hour.
 - In the Schedule tab of the server's Properties dialog box, click Change Schedule, and set the schedule to four times per hour.

14. A user calls the help desk to change her forgotten password. A minute later, she attempts to log on with the new password but gets a logon failed message. She verifies that the correct password is being entered. She tries logging on again about 30 minutes later and is successful. What's the most likely cause of the delay in the user's ability to log on?
 - a. The domain controller where the password was changed was in a different site, and normal replication between sites caused the delay.
 - b. The domain controller that authenticated the user must have gone down and didn't receive the password change until it was brought back online.
 - c. The domain controller holding the PDC emulator role wasn't contacted by the domain controller that authenticated the user.
 - d. The intrasite replication schedule is set for 30 minutes instead of 15 seconds.
15. You want to install an RODC in your Windows Server 2003 forest, which currently has all Windows Server 2003 domain controllers. How should you go about doing this?
 - a. Change the forest functional level to Windows Server 2008 first, run Adprep in the forest and domain, and then install the RODC.
 - b. Install the RODC in the forest; no additional steps are necessary.
 - c. Run Adprep in the forest and domain, and then install the RODC.
 - d. Run Adprep for the forest and domain, install a Windows Server 2008 writeable domain controller, and then install the RODC.
16. Users of a new network subnet have been complaining that logons and other services are taking much longer than they did before being moved to the new subnet. You discover that many logons and requests for DFS resources from workstations in the new subnet are being handled by domain controllers in a remote site instead of local domain controllers. What should you do to solve this problem?
17. You have three sites: Boston, Chicago, and LA. You have created site links between Boston and Chicago and between Chicago and LA with the default site link settings. What do you need to do to make sure replication will occur between Boston and LA?
 - a. Do nothing; replication will occur between Boston and LA with the current configuration.
 - b. Create a new connection object between Boston and LA.
 - c. Create a site link bridge between Boston and LA.
 - d. Configure a site link between Boston and LA with SMTP.
18. Which of the following is true about using SMTP in site links? (Choose all that apply.)
 - a. A certification authority must be installed.
 - b. Domains can span the sites included in the site link.
 - c. It's best used on slow or unreliable network links.
 - d. It's the preferred transport protocol for intersite links.
19. A partition stored on a domain controller in SiteA isn't being replicated to other sites, but all other partitions on domain controllers in SiteA are being replicated. The problem partition is stored on multiple domain controllers in SiteA. What should you investigate as the source of the problem?
 - a. An automatically configured bridgehead server
 - b. A manually configured bridgehead server
 - c. A failed site link bridge
 - d. A failed ISTG
20. Your network is configured in a hub and spoke topology. You want to control the flow of replication traffic between sites, specifically reducing the replication traffic traveling across network links between hub sites to reach satellite sites. What should you configure?
 - a. Connection objects between domain controllers in each site
 - b. Intersite transports

- c. Site link bridges
 - d. NTDS settings
21. You want to decrease users' logon time at SiteA but not increase replication traffic drastically. You have 50 users at this site with one domain controller. Overall, your network contains 3000 user and computer accounts. What solution can decrease logon times with the least impact on replication traffic?
- a. Configure the domain controller as a domain naming master.
 - b. Configure the domain controller as a global catalog server.
 - c. Configure multiple connection objects between the domain controller in SiteA and a remote global catalog server.
 - d. Enable universal group membership caching.
22. Which of the following configurations should you avoid?
- a. Domain naming master and schema master on the same domain controller
 - b. PDC emulator and RID master on the same computer
 - c. Infrastructure master configured as a global catalog server
 - d. Schema master configured as a global catalog server
23. Users usually notice a failure of the domain naming master immediately. True or False?
24. User authentications are taking a long time. The domain controller performing which FSMO role will most likely decrease authentication times if it's upgraded?
- a. RID master
 - b. PDC emulator
 - c. Infrastructure master
 - d. Domain naming master
25. You're taking an older server performing the RID master role out of service and will be replacing it with a new server configured as a domain controller. What should you do to ensure the smoothest transition?
- a. Transfer the RID master role to the new domain controller, and then shut down the old server.
 - b. Shut down the current RID master and seize the RID master role from the new domain controller.
 - c. Back up the domain controller that's currently the RID master, restore it to the new domain controller, and then shut down the old RID master.
 - d. Shut down the current RID master, and then transfer the RID master role to the new domain controller.

10

Case Projects



Case Project 10-1: Working with Trusts

Examine the network in Figure 10-28. You need to configure this network to meet the following requirements:

1. All users in the abc.com forest should be authenticated to all resources in the xyz.com forest.
2. Selected users in the xyz.com domains should be authenticated to selected resources in the abc.com forest.
3. No users in the jkl.com domain tree should be authenticated to the abc.com forest.
4. Users in the uk.jkl.com domain access resources in the phx.usa.abc.com domain frequently. Latency should be kept to a minimum.

5. Users in the phx.usa.abc.com domain access resources in the gb.uk.abc.com domain frequently. Latency should be kept to a minimum.
6. Users in the Linux network need to access resources in the xyz.com forest frequently.

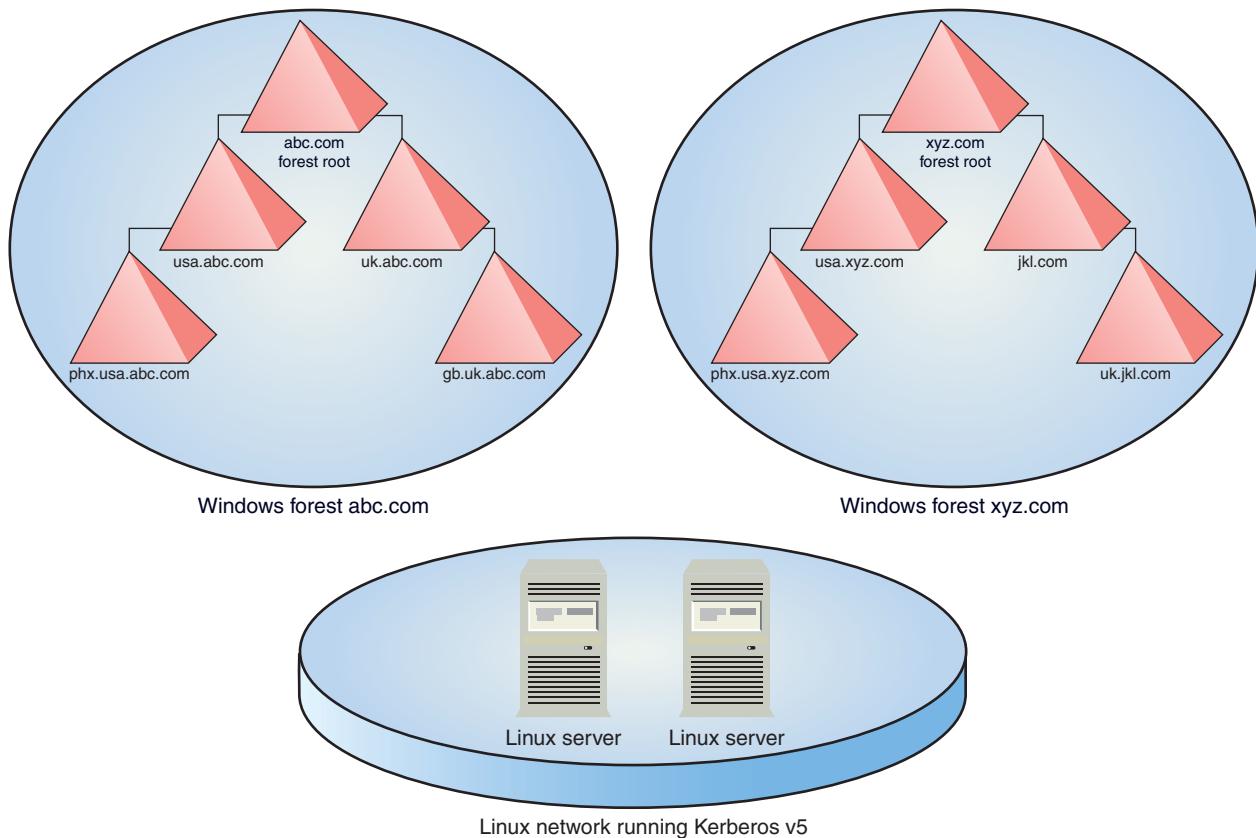


Figure 10-28 The network for Case Project 10-1

Given the preceding requirements, write a report of one to two pages describing how you would configure trust relationships and cite configuration options, such as one-way or two-way, transitivity, authentication, and so forth.

Case Project 10-2: Designing Sites

You're called in as a consultant to create a site design. The company has a network consisting of four hub sites and six satellite sites (see Figure 10-29). There are four domains, one for each city. Note the following facts about the company's site requirements:

- The satellite sites are in the same domain as the city to which they're connected.
- No sites contain domain controllers from outside their domain.
- Each hub site has 750 to 1000 users and 10 to 15 domain controllers.
- Each satellite site has 50 to 100 users and 2 to 4 domain controllers.

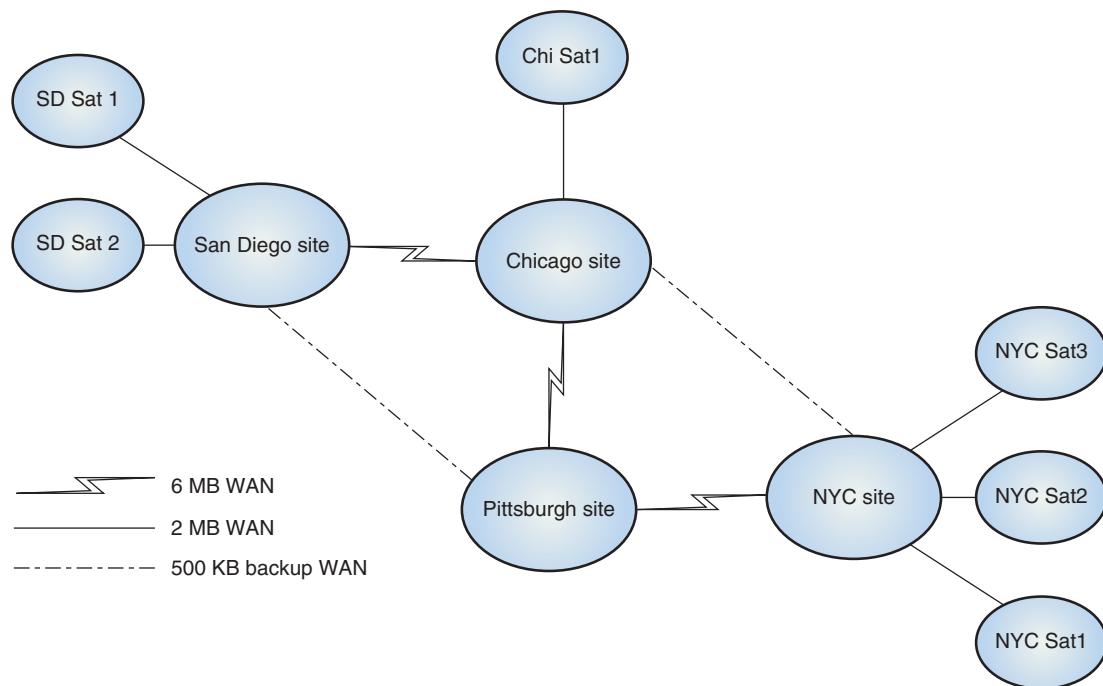


Figure 10-29 The site for Case Project 10-2

10

Write a memo of one to two pages describing some factors to consider when designing this site, and take the following into account:

- Site links
- Intersite transport protocols
- Site link bridges
- Bridgehead servers
- FSMO role holders
- Global catalog servers

What additional information do you need to choose an efficient site design for this network?

This page intentionally left blank

Active Directory Certificate Services

After reading this chapter and completing the exercises, you will be able to:

- Describe the components of a PKI system
- Deploy the Active Directory Certificate Services role
- Configure a certification authority
- Maintain a PKI

It's a matter of trust. Whether you're shopping on a Web site, engaging in online banking, or even reading a corporate e-mail, you must have a certain level of trust that the entity you're exchanging information with is actually who it says it is. Unfortunately, digital fraud and scams have become all too common. Fortunately, there are ways to protect yourself and your organization in the form of digital certificates.

Microsoft Active Directory Certificate Services provides the infrastructure for issuing and validating digital certificates in a corporate environment. With digital certificates, users can provide proof of their identities to corporate resources and confirm the identity of resources they access. Active Directory Certificate Services is Microsoft's implementation of a public key infrastructure (PKI), which secures information transfer and identity management and verification. This chapter describes how a PKI works and defines the terms used to discuss a PKI and Active Directory Certificate Services. You learn how to install and configure the Active Directory Certificate Services role and how to configure and manage key elements of the role, such as certification authorities and certificate enrollments and revocations.

Introducing Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is a server role in Windows Server 2008, referred to as Certificate Services in previous Windows versions. AD CS provides the services for creating a public key infrastructure (PKI) that administrators can use to issue and manage public key certificates. With AD CS, you can add a level of security for a variety of applications, including e-mail, wireless networks, virtual private networks (VPNs), Encrypting File System (EFS), smart cards for user logons, Secure Socket Layer/Transport Layer Security (SSL/TLS), and others. This section describes the basic components of a PKI and defines several terms used in implementing PKIs and AD CS.

Public Key Infrastructure Overview

A **public key infrastructure (PKI)** is a security system that binds a user's or device's identity to a cryptographic key that secures data transfer with encryption and ensures data authenticity with digital certificates. PKI provides the following services to a network:

- **Confidentiality**—Data and communications are protected by encryption algorithms, allowing only the authorized parties to access information.
- **Integrity**—Ensures that data received is the same as data sent.
- **Nonrepudiation**—Ensures that a party in a communication can't dispute the validity of the transaction, much like a signature on a letter or contract is used to verify that the signatory wrote the letter.
- **Authentication**—Verifies the identity of a person or system involved in a transaction.

Before going into the details of a PKI, first you need to understand why this service is necessary. Suppose you want to do some online banking, a transaction you want to be confidential. You open your Web browser and go to *www.mybank.com*. You enter your logon information and proceed with your transaction. Without some type of security system in place, a number of things can go wrong with this procedure, as in the following examples:

- DNS servers could be compromised, replacing the IP address of *www.mybank.com* with the IP address of a fraudulent site. All your logon information, including, perhaps, your account number, is actually being sent to the fraudulent Web site and could be used to access your real account. Without some type of security system in place, you can't be sure of the authenticity of the server you're communicating with.
- Someone could be electronically eavesdropping on your conversation. You might actually be communicating with *www.mybank.com*, but someone could be "listening" to the conversation with a packet-capturing program, which means your transaction is not confidential. The packets can be examined to find your logon information and account information for later use.

A public key security system, such as your Web browser using HTTPS instead of HTTP in a URL, can thwart both of the preceding situations. In the first example, using digital certificates can authenticate the Web site's identity. If your browser is directed to a fraudulent site, the digital certificate doesn't match the site's URL. In the second example, encryption would provide confidentiality and prevent an eavesdropper from interpreting information in captured packets.

Of course, for the security system to work, users have the responsibility of checking that the Web browser is using secure communication (usually indicated by a padlock icon in the browser). In addition, users must be vigilant in heeding warning messages about Web sites' certificate validity. PKI is commonly used in many other situations, but whenever a secure transaction is necessary between two parties that don't know each other, PKI is likely to be part of the transaction.

PKI Terminology

Before you delve into PKI transactions, review the following list of components that compose a PKI:

- *Plaintext*—Data that has been unaltered; as used in cryptography, this term defines the state of information before it's encrypted or after it has been decrypted.
- *Ciphertext*—Data that has been encrypted; it's the result you get when plaintext is transformed by an encryption algorithm.
- *Key*—In encryption, a key is a numeric value used by a cryptographic algorithm to change plaintext into ciphertext (encrypt) and ciphertext back to plaintext (decrypt).
- *Secret key*—A key used to both encrypt and decrypt data in a secure transaction. The secret key must be known by both parties because it's used in both ends of the cryptography process. The terms symmetric key and shared secret key are also used. Secret keys are used in symmetric cryptography, defined later in this list, and provide a lower-overhead secure transaction than using a public/private key pair.
- *Private key*—A key that's held by a person or system and is unknown to anyone else. A private key is part of a key pair used in asymmetric cryptography (defined later in this list) and is most often used by the owner to decrypt data that has been encrypted with the corresponding public key.
- *Public key*—A key owned by a person or system that's distributed to whoever wants to have a secure communication session with the key owner. The public key, part of the key pair used in asymmetric cryptography, is used to encrypt data, which can then be decrypted only by using the owner's private key. A public key is also used to verify a digital signature.
- *Symmetric cryptography*—An encryption/decryption process that uses a single secret key to encrypt and decrypt a message (also called private key cryptography or secret key cryptography). The key is often referred to as a shared secret because both parties involved in the communication must have the same key. Symmetric cryptography is vulnerable to attack because the shared secret must be transmitted to both parties, and the key used in the encryption algorithm tends to be easier to crack than those used in asymmetric cryptography.



NOTE

Although symmetric cryptography is sometimes referred to as private key cryptography or private key encryption, these terms are somewhat imprecise. A private key is used as part of a pair in asymmetric cryptography and should never be shared with another party.

- *Asymmetric cryptography*—An encryption/decryption process, used in a PKI system, that uses both a public key and a private key. Asymmetric cryptography is more complex and requires more computing resources than symmetric cryptography, but it's also more secure. Because of its higher resource requirements, asymmetric cryptography is often used along with symmetric cryptography. Asymmetric cryptography is used to exchange secret keys, which are then used symmetrically for the bulk of data encryption and decryption.

- *Digital certificate*—A digital document containing identifying information about a person or system; it's a central component of a PKI. Information in the certificate typically includes a person's or organization's name or a system's URL and IP address as well as the holder's public key, an expiration date, and the digital signature of the certification authority that issued the certificate. The certificate also defines the purpose for which it's used.
- *Digital signature*—A numeric string created by a cryptographic algorithm, called a hash (discussed later in “Installing the AD CS Role”), that's used to validate a message or document's authenticity. The signature is verified by an algorithm that uses the stated owner of the signature's public key to accept or reject the signature as authentic. In a PKI, a certification authority's digital signature is used to verify the authenticity of digital certificates and other documents.
- *Certification authority (CA)*—An entity that issues and manages digital certificates and associated public keys and is an integral part of a PKI. Windows Server 2008, with the Active Directory Certificate Services role installed, can be a CA for a corporate network. Companies such as VeriSign, Comodo, and GlobalSign are examples of universally trusted public CAs that issue certificates to people and systems needing to engage in secure communication with the public.

Now that you have a few terms down, take another look at the online banking session discussed earlier. The following steps are general because an actual secure Web session involves many variables, but these steps are the basic framework for most secure Web transactions (see Figure 11-1):

1. The Web browser requests a secure transaction with *www.mybank.com* using HTTPS. HTTPS is a secure form of HTTP using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol, both of which use a PKI.
2. The Web server sends information about the encryption protocols it will use and its certificate containing its public key.
3. The Web client verifies the certificate and extracts the CA's public key to verify the digital signature of the issuing CA. If the CA is trusted and the signature is verified, the Web client sends additional parameters to the server that are encrypted with the server's public key. One parameter is a session key, which is a shared secret key used to encrypt and decrypt data transferred during the rest of the communication session.
4. The Web server decrypts the session key with its private key. The session key is now used to encrypt and decrypt information communicated between the parties.

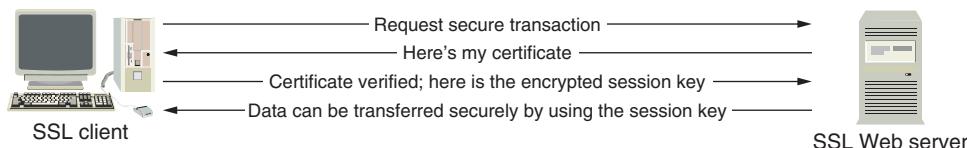


Figure 11-1 Steps of a secure Web transaction

Notice in the preceding steps that both asymmetric and symmetric encryption are used. Asymmetric encryption is used in the beginning of the conversation to transmit several parameters, including the session key. After that point, symmetric encryption is used. So why not use asymmetric encryption throughout the conversation? Doing so requires both client and server to have a public/private key pair, and assuming every client has one might be unreasonable. Also, the additional processing asymmetric encryption requires slows communication. Because the shared secret key (session key) is exchanged by using more secure asymmetric encryption, the transaction remains highly secure.

The online banking transaction example was used because of its familiarity to most people. A Windows network with Active Directory Certificate Services installed is typically used to add

an extra layer of security to corporate network communication. AD CS not only ensures confidential communication, but can also protect corporate users and resources by providing data integrity and authenticity.



Don't confuse a PKI in which publicly trusted CAs are used to secure public transactions with a PKI used in a private organization. The fact that you set up a CA in your company doesn't mean certificates issued by your CA are trusted by the outside world.

NOTE

AD CS Terminology

Now that you have a general understanding of a PKI, review some terms used when implementing AD CS to give you an overview of this server role:

- **Certificate revocation list (CRL)**—A list of certificates that have been invalidated before their expiration date by the CA administrator. Reasons for certificate revocation include a private key that has been compromised or is suspected of having been compromised or a certificate deemed no longer necessary, such as when an employee leaves the company that issued the certificate.
- **Certificate template**—A shell or model of a certificate used to create new certificates. **Certificate templates** define characteristics of the certificate, such as the intended use and expiration date. In Windows Server 2008, AD CS includes more than 30 predefined certificate templates named for their intended purpose, such as Web Server for authenticating the identity of Web servers and Smart Card Logon, which enables users to authenticate by using smart cards. You can also create custom certificate templates.
- **Certificate distribution point (CDP)**—Identifies where the CRL for a CA can be retrieved; can include URLs for HTTP, FILE, FTP, and LDAP locations.
- **Delta CRL**—A list of certificates revoked since the last base, or complete, CRL was published. Using Delta CRLs reduces the amount of traffic created when downloading CRLs.
- **Enterprise CA**—A CA installation on a Windows Server 2008 server that's integrated with Active Directory.
- **Standalone CA**—A CA installation that isn't integrated with Active Directory.
- **Enrollment agent**—A user authorized to enroll for smart cards on behalf of other users. A new function in Windows Server 2008 is a **restricted enrollment agent**, which limits the agent to enrolling only specific users or security groups. Restricted enrollment agents are available only with an enterprise CA.
- **CA hierarchy**—The first CA installed in a Windows network is called the root CA. The root CA's certificate is self-signed and distributed to Windows clients that automatically trust the root CA. Additional CAs, called subordinate CAs, can be installed. A subordinate CA's certificate is signed by the root CA, and because Windows clients trust the root CA, by extension they trust subordinate CAs.
- **Online responder**—A server that supports Online Certificate Status Protocol (OCSP). This protocol is an alternative to clients downloading CRLs periodically to check certificate status. Clients can instead query an online responder for a certificate's status.
- **Certificate enrollment**—The process of issuing a certificate to a client. AD CS supports a number of enrollment methods, including autoenrollment, Web enrollment, smart card enrollment, and manual enrollment. In addition, AD CS supports Network Device Enrollment Service (NDES), which allows network devices to obtain certificates.
- **Key management**—Users' private keys are stored in their profiles. If a private key gets lost or corrupted, it might need to be restored. Key archival provides a method for storing a backup of a private key, and key recovery is the process of restoring a private key.
- **Authority Information Access (AIA)**—The AIA is a path configured on a CA server that specifies where to find the certificate for a CA.

Deploying the Active Directory Certificate Services Role

Before you decide to deploy AD CS on your network, you should have a clear understanding of how it will be used in your network and the options for implementing AD CS. For example, if your reason for issuing certificates to employees is to give them secure access to external resources, such as Web servers and Internet e-mail, you should probably use a well-known external third-party CA. After all, a certificate your internal CA issues is unlikely to be trusted by outside entities. However, if your goal is to enhance the security of internal communication, that's the primary purpose of AD CS. All your internal clients and resources can be configured to trust the internal CA.



NOTE

It's possible to have a third-party CA as part of your PKI. In this case, the third-party CA acts as a root CA and issues certificates to your internal subordinate CAs. With this setup, your client computers can access external resources securely because the third-party CA is a point of common trust between internal computers and external entities.

Some AD CS options you should be aware of before deploying this server role include the following:

- Standalone and enterprise CAs
- Online and offline CAs
- AD CS hierarchy
- Certificate practice statement

Standalone and Enterprise CAs

An **enterprise CA** is a server running Windows Server 2008 with the Active Directory Certificate Services role installed. Enterprise CAs integrate with Active Directory and offer several advantages to the PKI running in a domain environment. A **standalone CA** is a server running Windows Server 2008 with the Active Directory Certificate Services role installed, but it has little Active Directory integration. If you're issuing certificates only to domain member users and computers, you can install all enterprise CAs. If your network consists of non-Windows devices, you need at least one standalone CA. Although standalone CAs can be integrated with Active Directory somewhat for storing configuration information, the CA certificate, and CRL data, the integration must be done manually. Table 11-1 compares standalone and enterprise CAs.

Table 11-1 Standalone and enterprise CAs

Standalone CA server	Enterprise CA server
Active Directory not required	Active Directory required; server must be a member server (preferred) or domain controller
Can operate offline	Must operate online
Certificate requests must be approved manually	Certificate requests approved manually or automatically by using Active Directory information
No certificate templates available	Certificate templates available
Certificates not published in Active Directory	Certificates published in Active Directory
Requester must enter identifying information in certificate request manually	Identifying information is taken from Active Directory
CA's certificate distributed to clients manually	CA's certificate distributed to clients automatically
CRL optionally published to Active Directory	CRL automatically published to Active Directory



NOTE

You must be running Windows Server 2008 Enterprise or Datacenter Edition to install an enterprise CA. Standard Edition supports only standalone CAs.

Online and Offline CAs

A CA server is a critical component in a network's security. If a CA is compromised, all certificates the CA has issued are also compromised and must be revoked immediately. Given the critical nature of servers acting as CAs, it's common practice to run one or more servers in the CA hierarchy in offline mode.

An offline CA isn't connected to the network, which makes it less vulnerable to attacks. However, all certificates and CRLs must be distributed with removable media. In a small network, using removable media to process certificate transactions works fine, but in a large network, depending on an offline CA for all your certificate needs isn't practical. Typically, when a hierarchy of CAs is necessary, a mix of offline and online CAs is used.

The root CA is the most critical and is the server typically configured for offline operation. An offline CA must also be a standalone CA. The root CA issues certificates only to CAs in the next level of the hierarchy that can be accommodated by using removable media. The next section on CA hierarchies discusses this concept in more detail.

Creating a CA Hierarchy

A small organization might require only a root CA if certificate requirements are modest. Large organizations, however, might want to create a hierarchy of CAs, consisting of a root CA, intermediate CAs, and issuing CAs. A CA hierarchy is used to distribute the load placed on CA servers and augment security.

The **root CA** is the first CA installed in a network. If the root CA is an enterprise CA, its certificate is distributed to clients automatically via group policies. If it's a standalone CA, manual configuration of group policies is required to distribute its certificate. In either case, after clients are configured to trust the root CA's certificate, they also trust the certificate of any CA that's subordinate to the root. Administrators can use this fact to create a hierarchy that insulates the root CA from network exposure. This hierarchical arrangement is how you can operate a root CA in offline mode. The root CA needs to grant issuing certificates only to subordinate CAs, which are trusted by the clients to which they issue access certificates.

Depending on an organization's needs, a CA hierarchy can be single-level, consisting of only the root CA; two-level, consisting of the root CA and one or more issuing CAs; or three-level, consisting of the root CA, one or more intermediate CAs, and one or more issuing CAs. Figure 11-2 shows two-level and three-level hierarchies.

11

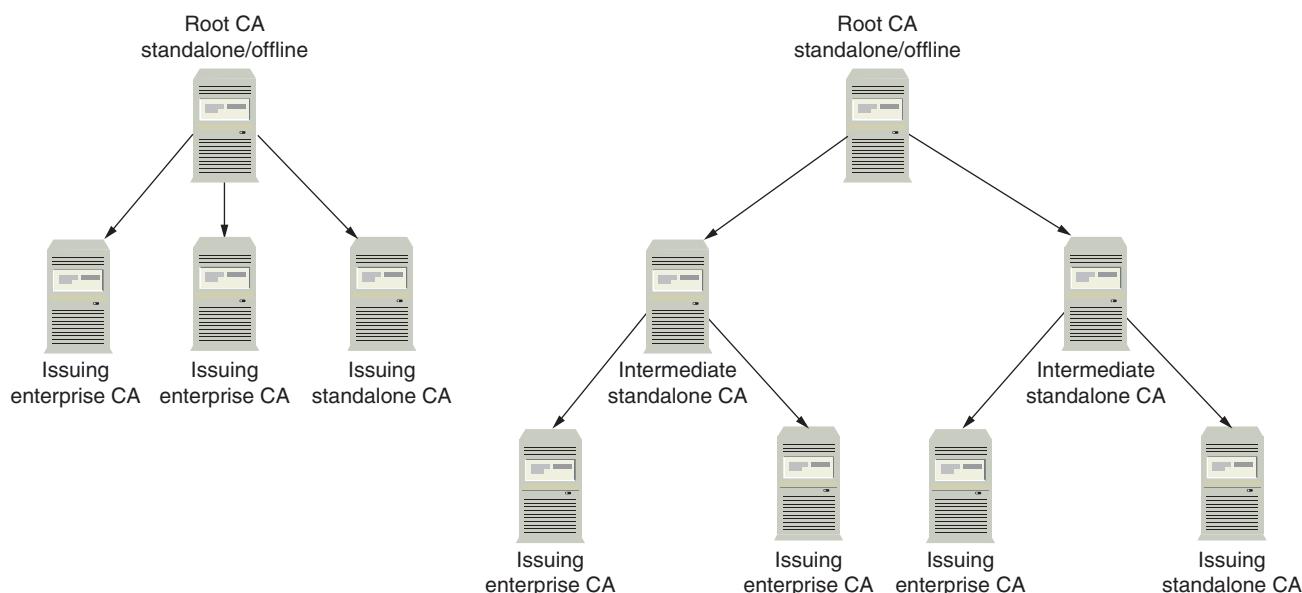


Figure 11-2 Two-level and three-level CA hierarchies

In the two-level hierarchy, the root CA issues certificates to subordinate CAs and then is usually taken offline for security. The subordinate CAs are referred to as **issuing CAs** because they interact with clients to field certificate requests and maintain the CRL. Because the root CA issues certificates to issuing CAs and the clients trust the root CA, they also trust the issuing CAs. Issuing CAs are generally enterprise CAs or can be a combination of enterprise and standalone if the network includes non-Windows clients.

The three-level hierarchy is a common configuration and offers the most security because the issuing CAs, where user certificate requests are made, is farther removed from the root CA. In this arrangement, the root CA issues certificates to **intermediate CAs** (sometimes called policy CAs), authorizing them to issue certificates to other CAs. Intermediate CAs issue certificates to issuing CAs, which respond to user and device certificate requests. The root CA and intermediate CAs can be standalone and operate in offline mode. Issuing CAs can be a mix of enterprise and standalone CAs and operate in online mode.

Multilevel CA hierarchies are often used to distribute the certificate-issuing load in organizations that have multiple locations. Each intermediate CA is responsible for one or more issuing CA in each location. In Figure 11-2, for example, one intermediate CA and its subordinate issuing CAs might handle certificate management for the U.S. location, and the other intermediate and issuing CAs handle certificates for the Europe location.

Certificate Practice Statement

A **certificate practice statement (CPS)** is a document describing how a CA issues certificates. A CPS is not a required component of a PKI, but it should be developed as part of the planning process when an organization is designing its PKI. The document is usually published on the Internet, and every certificate the CA issues has a URL pointing to the CPS so that people examining the certificate can read the statement. Because the CPS describes the process used to issue certificates, it can be used as a guide when deploying your CA design. A CPS usually contains the following elements:

- Identification of the CA
- Security practices used to maintain CA integrity
- Types of certificates issued
- Policies and procedures used when issuing, revoking, recovering, and renewing certificates
- Cryptographic algorithms used
- Certificate lifetimes
- CRL-related policies, including where CRL distribution points are located
- Renewal policy of the CA's certificate

The CPS is installed by creating a CAPolicy.inf file and placing the file in the CA server's %systemroot% directory before the AD CS role is installed. For more about creating a CAPolicy.inf file, see <http://technet.microsoft.com/en-us/library/cc728279.aspx>.

Installing the AD CS Role

Best practices dictate that the AD CS role shouldn't be installed on a domain controller. In fact, for optimum security, AD CS should probably be the only role installed on the server. If you're installing a standalone CA, the server can be a member server if you want to take advantage of the limited Active Directory integration possible with standalone CAs. An enterprise CA must be installed on a member server running Windows Server 2008 Enterprise or Datacenter Edition.



Activity 11-1: Demoting Server1XX to a Member Server

Time Required: 20 minutes

Objective: Demote Server1XX to a member server.

Description: You're ready to begin implementing AD CS. You have an excess of domain controllers on your network, and you don't want to install AD CS on a domain controller. You demote one of your DCs to a member server in preparation for installing AD CS.

1. Log on to **Server1XX** as Administrator.
2. Click **Start**, type **dcpromo** in the Start Search text box, and press **Enter**. When the Active Directory Domain Services Installation Wizard starts, click **Next**.
3. In the Delete the Domain window, make sure the **Delete the domain** check box is *not* selected, and then click **Next**.
4. If you see the Remove DNS Delegation window, click **Next**. When prompted for credentials to remove the DNS delegation, enter **Administrator** for the username and **Password01** for the password, and then click **OK**.
5. In the Administrator Password window, type **Password02** in the Password and Confirm password text boxes. Note that this password is used to log on to the local computer because this server is no longer a domain controller. Click **Next**.
6. In the Summary window, verify your selections. Note that the server becomes a member server after this process is completed. Click **Next**.
7. If you get a message stating that the DNS delegations couldn't be removed, click **OK**. When the wizard has completed, click **Finish**. When prompted to restart the computer, click **Restart Now**.
8. After your computer restarts, log on to the domain as Administrator with **Password01**, and open Server Manager.
9. Click the **Roles** node in the left pane, and then click **Remove Roles** in the right pane. In the Remove Roles Wizard's welcome window, click **Next**.
10. In the Remove Server Roles window, click to clear the **Active Directory Domain Services** check box, and then click **Next**. In the Confirm Removal Selections window, click **Remove**. When the removal is complete, click **Close**. When prompted to restart, click **Yes**.
11. After the computer restarts, log on to the domain from Server1XX as Administrator. The removal of Active Directory Domain Services continues. When it's finished, click **Close**.
12. Next, you should remove the DNS Server role. Because Server1XX is no longer a domain controller, DNS contains no Active Directory-integrated zones. Click **Remove Roles**, and then click **Next**.
13. Click to clear the **DNS Server** check box, and then click **Next**. Click **Remove**. When the removal is finished, click **Close**. When prompted to restart, click **Yes**.
14. After the computer restarts, log on to the domain from Server1XX as Administrator. The removal of DNS Server continues, and when it's finished, click **Close**.
15. Now you must change the DNS server address in Server1XX's IP configuration. Change the preferred DNS server in the TCP/IP properties of the Local Area Connection to **192.168.100.2XX** (the address of ServerXX).
16. Stay logged on and leave Server Manager open for the next activity.

AD CS is installed in Server Manager by adding the AD CS role. During installation, you have several options, and your selections depend on how the CA will be used in your network. What's the name of your CA? Is it the root CA or a subordinate CA? Is it an enterprise or standalone CA? Will the CA issue certificates to users and devices or to other CAs? Keep in mind that many of the selections you make, including the CA name, can't be changed after AD CS is installed.

11



Activity 11-2: Installing the AD CS Role

Time Required: 20 minutes

Objective: Install the AD CS role.

Description: You want to set up a PKI on your network to augment security. You have researched AD CS and decided to install that server role on a member server and configure it as an enterprise CA.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. Click the **Roles** node in the left pane and click **Add Roles** in the right pane to start the Add Roles Wizard. Click **Next** in the welcome window.

3. In the Select Server Roles window click **Active Directory Certificate Services**, and then click **Next**.
4. In the Introduction to Active Directory Certificate Services window, read the description and the paragraph under Things to Note. In particular, note that you can't change the computer name, join a different domain, or promote the server to a domain controller after the role is installed. Click **Next**.
5. In the Select Role Services window, the Certification Authority option is selected by default. Click to select **Online Responder**. The Online Responder role service requires the Web Server role service, so when you're prompted to add this role service, click **Add Required Role Services**. If the server were going to be a standalone root CA in a multilevel hierarchy, you would install only Certification Authority. You can't install NDES until the Certification Authority role has been installed. Click **Next**.
6. In the Specify Setup Type window, make sure **Enterprise** is selected. If you did not change this server's DNS address to the address of ServerXX, Enterprise is grayed out. Click **Next**.
7. In the Specify CA Type window, make sure **Root CA** is selected, and then click **Next**.
8. In the Set Up Private Key window, make sure **Create a new private key** is selected. If this CA were replacing a failed CA, you would click "Select a certificate and use its associated private key." If you had a private key from a previous installation or from an external source, you would click "Select an existing private key on this computer." Click **Next**.
9. In the Configure Cryptography for CA window, accept the default selections and click **Next**.
10. The next window requests a name for the CA. By default, the name is generated automatically to include the domain name and server name followed by "CA." For example, if the domain is w2k8ad99.com and the server name is Server199, the default CA name is w2k8ad99-Server199-CA. You can also enter the distinguished name suffix, but usually, the default is fine. Click **Next**.
11. In the Set Validity Period window, you can set the validity period of the certificate issued to this CA. The validity period should be specified in the certificate practice statement. The period you choose depends on how this CA is used and the types of certificates it will issue. If the certificate expires, the CA is no longer valid, nor are any certificates it has issued. Certificates can be renewed as needed. Accept the default of 5 years, and then click **Next**.
12. In the Configure Certificate Database window, you can choose where certificates and the certificate log should be stored. If the CA will be used heavily, these two databases should be stored on separate drives and shouldn't be placed on the same drive as the Windows folder. For testing purposes, you can use the default location of C:\Windows\system32\CertLog for both databases. Click **Next**.
13. Because you chose to install the Online Responder role service, which requires the Web Server role service, the Web Server (IIS) window is displayed. Click **Next**.
14. You're prompted to select role services for the Web Server role service. If necessary, you can make changes to the default selections. For now, accept the defaults and click **Next**.
15. In the Confirm Installation Selections window, review the options you have chosen. You're also warned that you can't change the computer name or domain name after the CA has been installed. Click **Install**.
16. When the installation is finished, click **Close**.
17. In Server Manager, you probably have a warning event for AD CS. Click the **Active Directory Certificate Services** link next to the yellow warning message, and then double-click the **Warning** message. Read the event information. It explains how you can verify that the CA certificate was published correctly in Active Directory. Click **Close**.
18. Open a command prompt window, type **gpupdate /force**, and press **Enter** to update the certificate store (database where certificates are stored). After gpupdate has finished, type

certutil -viewstore and press **Enter**. The View Certificate Store dialog box opens (see Figure 11-3), which lists all certificates currently published in Active Directory. Click the **w2k8adXX-Server1XX-CA** certificate, and then click the **View Certificate** button.

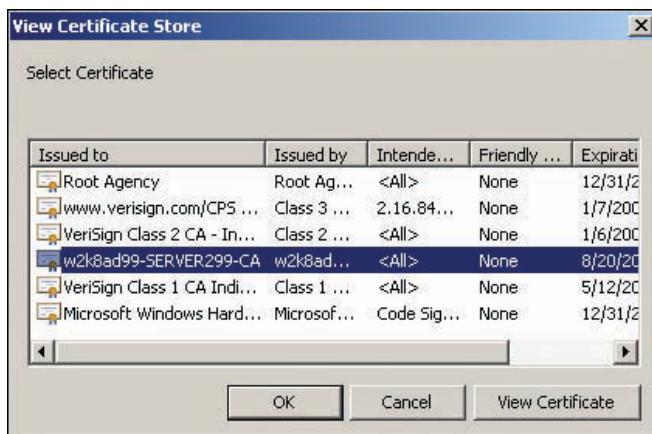


Figure 11-3 Viewing the certificate store

19. Figure 11-4 shows the certificate for your new CA. Notice that the **Issuer Statement** button is grayed out. If you publish a CPS, this button becomes active and links to your CPS. Click the **Details** tab to view more information about the certificate. Click the **Certification Path** tab, which shows the path through the CA hierarchy to the root CA where the certificate originates. In this case, only the current server is listed because you don't have a multilevel CA hierarchy. Click **OK**.

11



Figure 11-4 The General tab for the CA certificate

20. Click **OK** in the View Certificate Store dialog box to close it. Close the command prompt window.
21. Stay logged on for the next activity.

A few windows you saw in the preceding activity need some additional explanation. The Configure Cryptography for CA window from Step 9 of the AD CS installation includes several options (see Figure 11-5), described in the following list:

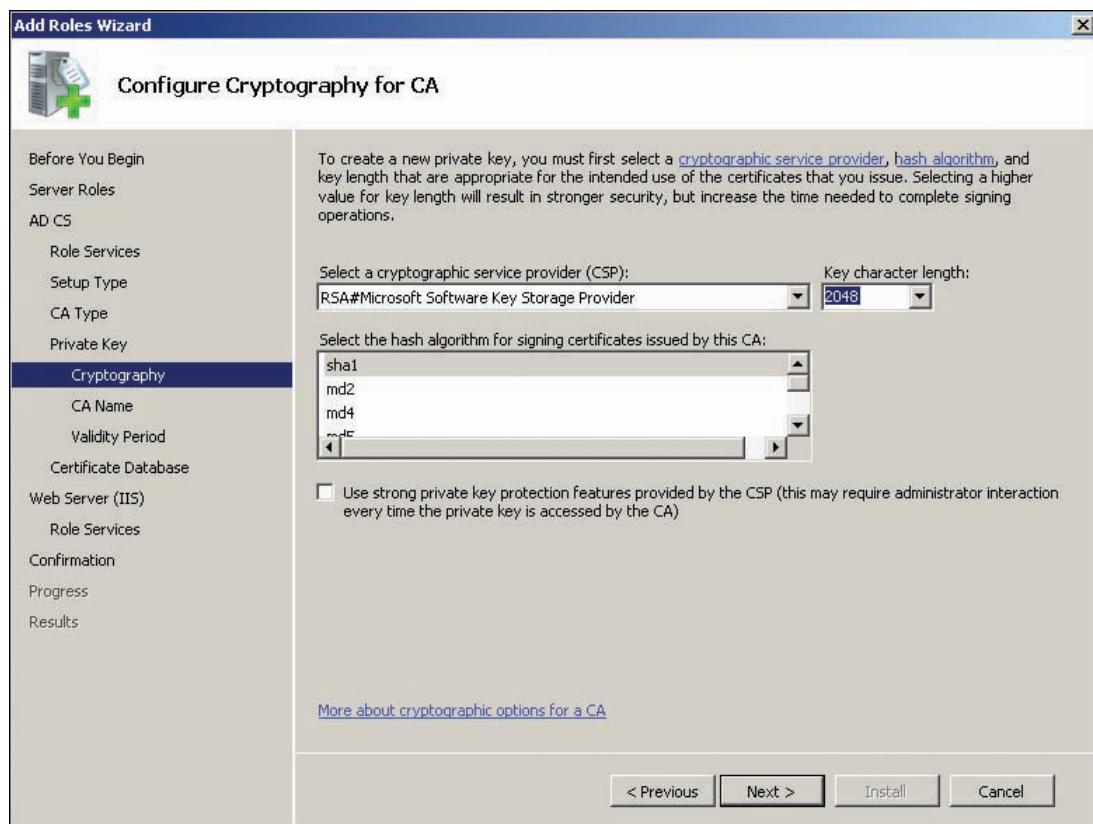


Figure 11-5 The Configure Cryptography for CA window

- **Select a cryptographic service provider (CSP)**—This list box displays the CSPs already configured in Windows Server 2008. A CSP is a library of algorithms that perform cryptographic functions, such as creating hashes and encrypting and decrypting data.
- **Key character length**—This text box defines the number of bits that make up keys used in the cryptography algorithms. Generally, the longer the key, the more difficult it is to crack. However, longer keys also take more CPU resources to perform cryptographic functions.
- **Select the hash algorithm for signing certificates issued by this CA**—A **hash algorithm** is a mathematical function that takes a string of data as input and produces a fixed-size value as output. Hash values are used to verify that the original data hasn't been changed and to sign the CA certificate and certificates issued by the CA.
- **Use strong private key protection features provided by the CSP**—If this check box is selected, cryptographic operations require the administrator to enter a password, which helps prevent unauthorized use of the CA and its private key.

The Details tab you viewed in Step 19 of Activity 11-2 contains a considerable amount of information (see from Figure 11-6). The following list describes some items in this tab:

- **Version**—This field specifies the version of the X.509 standard the certificate uses. X.509 is an international standard that defines many aspects of a PKI, including certificate formats.

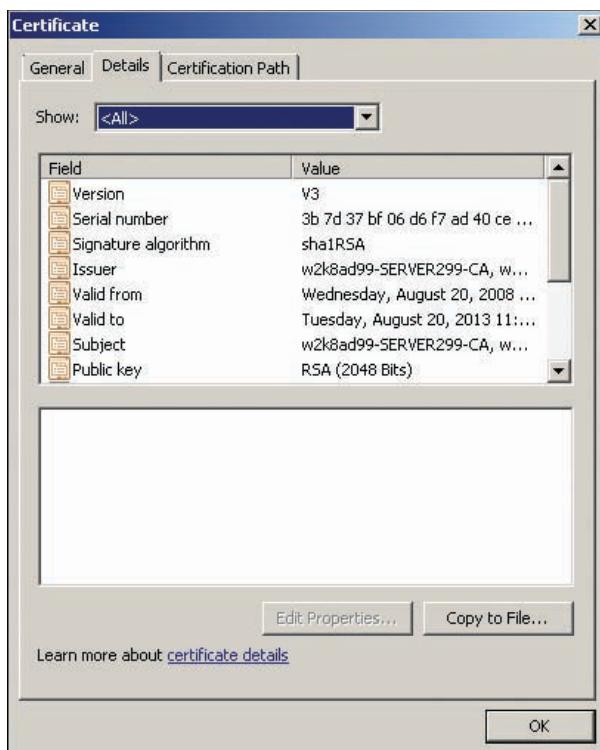


Figure 11-6 The Details tab for a certificate

11

- *Signature algorithm*—The hash algorithm used to sign the certificate.
- *Issuer*—The CA that issued the certificate. In this case, the certificate is self-signed, as all root CA certificates are.
- *Subject*—The device, computer, user, or other entity that has been issued the certificate. In this case, it's the CA itself.
- *Public key*—Defines the algorithm and bit length for the public key.
- *Key usage (not shown in the figure)*—Specifies the purposes for which the certificate can be used. Examples are digital signature and certificate signing.

Configuring a Certification Authority

After installing AD CS on a server, you must perform several configuration tasks, including the following, before using your new CA:

- Configure certificate templates
- Configure enrollment options
- Configure the online responder
- Create a revocation configuration

Configuring Certificate Templates

If you install an enterprise CA, a number of predefined certificate templates can be configured to generate certificates. Windows Server 2008 supports three versions of certificate templates:

- *Version 1 templates*—Provided for backward compatibility; Windows Server 2003 Standard Edition and Windows 2000 Server support only version 1 templates. These templates can't be modified or removed, and autoenrollment is not an option. Windows Server

2008 includes several version 1 templates. You can duplicate these templates, and then they're converted to version 2 or 3 templates, which can be modified.

- *Version 2 templates*—Allow customization of most certificate settings and permit auto-enrollment. They are supported by Windows Server 2003 Enterprise Edition and later.
- *Version 3 templates*—Provide advanced cryptographic functions; they can be issued only from Windows Server 2008 enterprise CAs and can be used only on Windows Server 2008 and Vista clients.

Certificate templates are created and modified in the Certificate Templates snap-in, which is automatically added under the Active Directory Certificate Services node in Server Manager (see Figure 11-7). You can modify a template listing Windows Server 2003 Enterprise or Windows Server 2008 in the Minimum Supported CAs column. Templates listing Windows 2000 in this column must be duplicated before modifying them. The recommended method is modifying the duplicate rather than the template. Each template type has a different set of properties and a varying number of tabs in the template Properties dialog boxes.

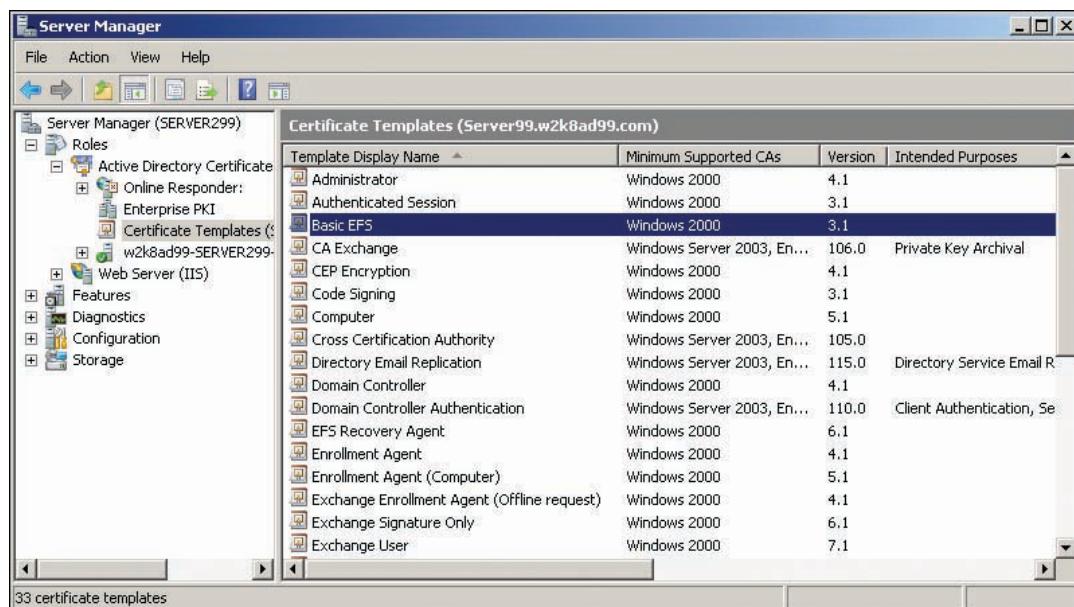


Figure 11-7 The Certificates Templates snap-in

A common certificate type is one used for EFS, which allows users to encrypt and decrypt files on a hard drive. The Basic EFS template is used to issue certificates to users so that they can protect files with EFS. The EFS Recovery Agent template is used to issue certificates to users who are designated as recovery agents so that EFS-encrypted files can be recovered if a user's EFS certificate becomes unusable for some reason.



Activity 11-3: Creating an EFS Certificate Template

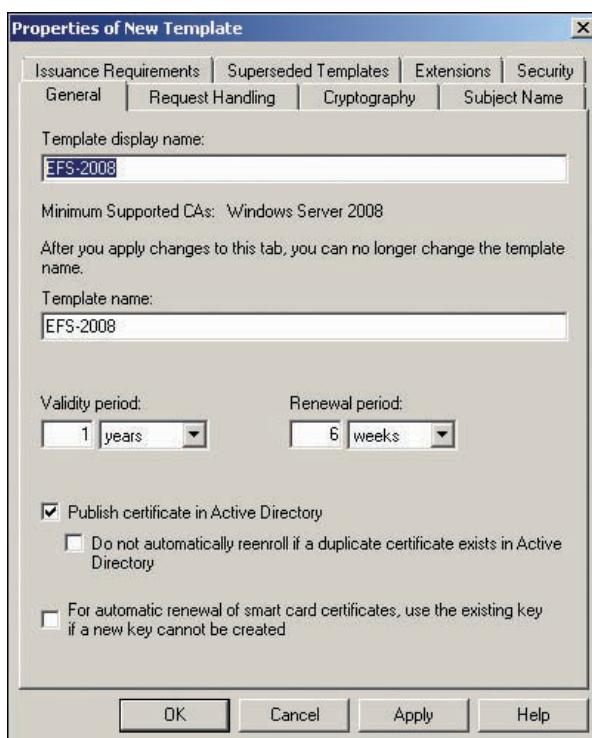
Time Required: 10 minutes

Objective: Create an EFS certificate template.

Description: You want to issue certificates to employees so that they can use EFS throughout the domain. You duplicate the version 1 Basic EFS template and create a version 3 EFS template for use on Vista clients.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. In the left pane, click to expand **Roles** and then **Active Directory Certificate Services**. Click **Certificate Templates** to list the available templates in the right pane. (If nothing appears below Active Directory Certificate Services, try closing Server Manager and then reopening it.)

3. Right-click **Basic EFS** in the right pane and click **Properties**. Notice that all options are grayed out because you must duplicate the version 1 template to make changes. Click **Cancel**.
4. Right-click **Basic EFS** and click **Duplicate Template**. In the Duplicate Template dialog box, you can select the minimum version of Windows Server that you want the certificate to be compatible with. Click **Windows Server 2008, Enterprise Edition**, and then click **OK**.
5. In the General tab of the Properties of New Template dialog box (see Figure 11-8), type **EFS-2008** in the Template display name text box.



11

Figure 11-8 The Properties of New Template dialog box

6. Review the options for configuring the EFS certificate. Click in the Validity period text box and type **2**.
7. Click the **Request Handling** tab. Click the **Purpose** list arrow to view the options for certificates created with this template. Leave **Encryption** as the selected purpose. Review the other options in this tab.
8. Click the **Superseded Templates** tab. Click **Add**, click **Basic EFS** in the Certificate templates list box, and then click **OK**. Now when a request for an EFS certificate is made, only the new EFS-2008 certificate is used.
9. Browse through the options in other tabs to see the configuration settings available for this template, and click **OK** when you're finished. Notice that the new template lists Windows Server 2008 in the Minimum Supported CAs column.
10. Close all open windows, and log off Server 1XX.

The following list describes some configuration options in the General tab for certificate templates in more detail:

- *Template display name/Template name*—By default, these two fields have the same value, but they can be different. However, after the template has been created, you can't change either name.

- *Validity period*—The length of time the certificate is valid if it's not renewed. If the period elapses, the certificate expires; it's invalid and can no longer be renewed. You can specify the validity period in units of years, months, weeks, or days.
- *Renewal period*—The time window before a certificate's validity period expires in which the certificate can be renewed. For example, if a certificate is issued January 1, 2009 and has a validity period of 1 year and a renewal period of 1 month, the certificate can be renewed any time between December 1, 2009 and January 1, 2010. After a certificate is renewed, it's valid for another length of time specified by the validity period.
- *Publish certificate in Active Directory*—When this check box is selected, information about the template is available throughout the network.
- *Do not automatically reenroll if a duplicate certificate exists in Active Directory*—When this check box is selected, if a Windows XP or later computer makes an enrollment request, a new enrollment request isn't made if a duplicate certificate already exists in Active Directory. Certificates can be renewed, but duplicate certificates aren't issued.
- *For automatic renewal of smart card certificates, use the existing key if a new key cannot be created*—When this check box is selected, this option helps prevent smart card renewal failures if a smart card is out of storage space for a new key.

Configuring Certificate Enrollment Options

Certificate enrollment occurs when a user or device requests a certificate, and the certificate is granted. Enrollment can occur with several methods:

- Autoenrollment
- Certificates MMC
- Web enrollment
- Network Device Enrollment Service (NDES)
- Smart card enrollment

Configuring Certificate Autoenrollment When autoenrollment is configured, users and devices don't have to make explicit certificate requests to be issued certificates. Autoenrollment options are configured through group policies and the certificate template. In addition, the CA must be configured to allow autoenrollment, which is an option only on enterprise CAs.

Certificate autoenrollment is commonly used for EFS. A user must have a certificate to encrypt and decrypt a file with EFS. If no certificate server is operating on the network, Windows creates the certificate automatically but only on the computer where the encrypted file is created. Without a central store of certificates, certificates created this way could be deleted or lost too easily, resulting in loss of access to the encrypted file. In addition, the user would have to be logged on to the computer where the encrypted file is stored to access it; network access of the encrypted file wouldn't be possible.

By setting up autoenrollment for EFS certificates, a user's EFS certificate is created the first time he or she logs on to the domain after autoenrollment is configured. Furthermore, the certificate is available anywhere in the domain and is centrally stored, which makes backup and restore of the certificate easier. Because autoenrollment is configured through group policies, a user must first be authenticated by a domain controller before a certificate is issued to make the process secure.

Autoenrollment is enabled in the Computer Configuration or User Configuration node of the Group Policy Management Console. The Certificate Services Client—Auto-Enrollment policy, which has the options shown in Figure 11-9, controls autoenrollment settings. The following list describes these options:

- *Configuration Model*—Options are Enabled, Disabled, and Not configured. If Enabled is selected, the Active Directory objects affected by the policy can autoenroll for certificates.
- *Renew expired certificates, update pending certificates, and remove revoked certificates*—When this check box is selected, autoenrollment is extended so that certificates are renewed, updated, and removed (for revoked certificates) automatically.



Figure 11-9 Options for the Auto-Enrollment policy

- *Update certificates that use certificate templates*—When this check box is selected, certificates created with a certificate template can be updated through autoenrollment if the template changes.

Autoenrollment is configured for certificate templates in the Request Handling, Issuance Requirements, and Security tabs of a template's Properties dialog box. In the Request Handling tab, you can configure the amount of user interaction required during autoenrollment with the following options:

- *Enroll subject without requiring any user input*—This option is required for autoenrollment of computers and services. You can also select it if you want user autoenrollment to occur in the background without user interaction.
- *Prompt the user during enrollment*—Users must respond to prompts during autoenrollment.
- *Prompt the user during enrollment and require user input when the private key is used*—Users must enter a password during autoenrollment and each time their private keys are used. This option is the most secure but least user friendly.

The Issuance Requirements tab has options for specifying enrollment requirements for certificates issued from the template:

- *CA certificate manager approval*—If selected, a CA manager must approve the certificate request before it's issued.
- *This number of authorized signatures*—If enabled and the number of signatures is more than zero, certificate enrollment requests must be signed with a digital signature. If more than one signature is required, autoenrollment is disabled.
- *Require the following for reenrollment*—Two options are available. If “Same criteria as for enrollment” is selected, users must use the same process for renewal that's required for initial enrollment. If “Valid existing certificate” is selected, renewal is automatic as long as the current certificate is valid.

The Security tab of a certificate template is similar to the Security tab of most Active Directory objects. By default, Domain Users group members have the Enroll permission. The Autoenroll permission must be set for users in the domain to autoenroll in the certificate.

The CA must be set to allow autoenrollment by configuring request-handling options (see Figure 11-10). The default option is “Follow the settings in the certificate template, if applicable. Otherwise, issue the certificate automatically.” This option enables the CA to autoenroll applicable templates, so normally there’s no need to change it unless you want to disallow autoenrollment. The “Set the certificate request status to pending option” accepts certificate requests but requires an administrator to issue the certificate manually in the Certificates MMC. Activity 11-4 explains this procedure.

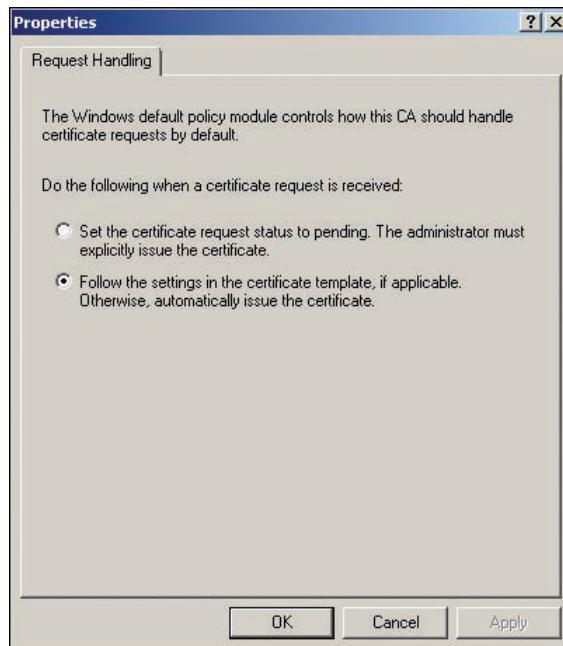


Figure 11-10 Request-handling options

The following list summarizes the steps for configuring autoenrollment after you have installed an issuing CA:

1. Create a certificate template.
2. Set options as needed in the Issuance Requirements and Request Handling tabs of the Properties dialog box.
3. Configure the template to allow autoenrollment by setting the Autoenroll permission for the users or groups who should autoenroll for the certificate.
4. Configure the Certificate Services Client - Auto-Enrollment policy.
5. Make sure the CA’s request-handling options are configured to allow autoenrollment.
6. Add the template to the Certificate Templates folder under the CA server node.



Activity 11-4: Configuring Certificate Autoenrollment

Time Required: 20 minutes

Objective: Configure autoenrollment for users to use EFS.

Description: Configure autoenrollment by configuring group policy and certificate template properties.

1. Log on to **ServerXX** as Administrator and open Group Policy Management (GPMC).
2. Right-click the **Group Policy Objects** folder and click **New**. Type **CertAutoGPO** in the Name text box, and then click **OK**.

3. Right-click **CertAutoGPO** and click **Edit**. In Group Policy Management Editor (GPME), click to expand **User Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Public Key Policies**. Click **Public Key Policies** in the left pane. In the right pane, double-click **Certificate Services Client - Auto-Enrollment**.
4. In the Define Policy Settings tab, click the **Configuration Model** list arrow and click **Enabled**. Click the **Renew expired certificates, update pending certificates, and remove revoked certificates** check box and the **Update certificates that use certificate templates** check box. Click **OK**.
5. Close GPME. In GPMC, right-click the domain node and click **Link an Existing GPO**. In the Select GPO list box, click **CertAutoGPO**, and then click **OK**. Close GPMC.
6. Log on to **Server1XX** as Administrator and open Server Manager.
7. In the left pane, click to expand the **Roles** node and the **Active Directory Certificate Services** node. Click **Certificate Templates** to list the available templates in the right pane.
8. Double-click **EFS-2008** to open its Properties dialog box, and then click the **Security** tab. Click **Domain Users**, click the **Autoenroll** permission in the Allow column, and then click **OK**.
9. In the left pane of Server Manager, right-click the CA server node (**w2k8adXX-Server1XX-CA**), and click **Properties**.
10. Click the **Policy Module** tab, and then click **Properties**. In the Request Handling tab, verify that the **Follow the settings in the certificate template, if applicable** option button is selected. Click **Cancel** twice.
11. Click the CA server node, and then double-click the **Certificate Templates** folder. The listed templates represent the certificates this CA can issue. Right-click the **Certificate Templates** folder, point to **New**, and click **Certificate Template to Issue**.
12. In the Enable Certificate Templates dialog box, click **EFS-2008**, and then click **OK**. Your CA is now ready to issue EFS certificates through autoenrollment.
13. Stay logged on and leave Server Manager open.

11



Activity 11-5: Testing EFS Certificate Autoenrollment

Time Required: 20 minutes

Objective: Test EFS certificate autoenrollment.

Description: You have configured a certificate template to autoenroll Domain Users with an EFS certificate. You test the configuration by logging on to the domain from your Vista computer, and then verifying that a new certificate has been issued. (Note: Your domain controller and CA server as well as your Vista computer must be running. If you're using virtual machines and can't accommodate three running simultaneously, you can log on to the domain controller instead of the Vista computer.)

1. Log on to the domain from your Vista computer as **salesperson1**.
2. When you log on, autoenrollment of user certificates takes place. To verify that the EFS-2008 certificate has been issued, you can view your certificates. Click **Start**, type **MMC** in the Start Search text box, and press **Enter**.
3. Click **File, Add/Remove Snap-in** from the MMC menu. In the Available snap-ins list box, click **Certificates**, and then click **Add**. Click **OK**.
4. In the left pane, click to expand **Certificates - Current User** and **Personal**, and then click **Certificates**. The issued EFS-2008 certificate is displayed in the right pane (see Figure 11-11).
5. In the left pane, click to expand **Trusted Root Certification Authorities** and click the **Certificates** folder to view certificates of CAs your computer trusts. Your CA should be listed at the bottom.

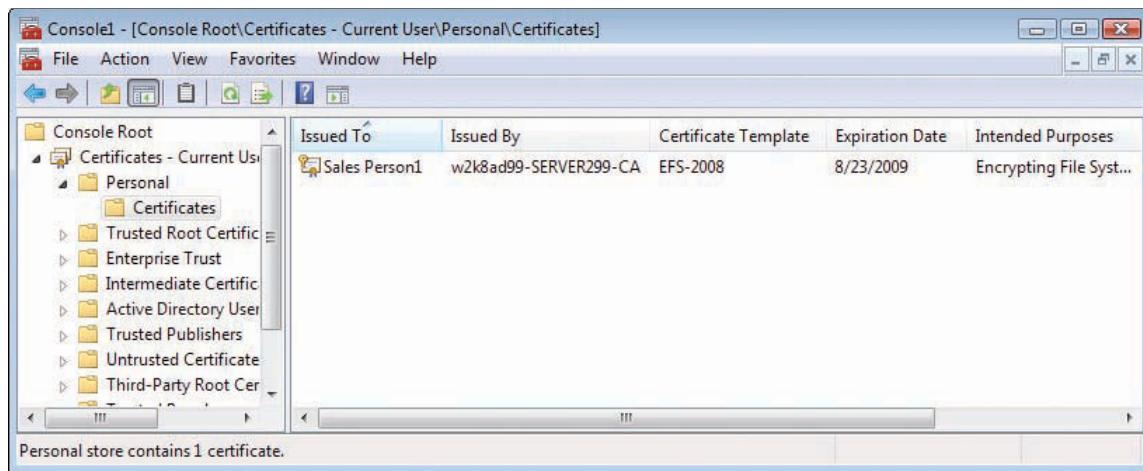


Figure 11-11 Viewing issued certificates

6. On Server1XX (your CA), click to expand the CA server node, and then click the **Issued Certificates** folder. The salesperson1 certificate should be listed. You might also see a certificate issued to your domain controller.
7. Close all open windows. When prompted to save console settings, click **No**. Log off your Vista computer.

Requesting a Certificate with the Certificates Snap-in Users can request certificates that aren't configured for autoenrollment by using the Certificates snap-in. To do so, make sure you're logged on to the domain. Then right-click the Certificates folder under the Personal folder, point to All Tasks, and click Request New Certificate to start the Certificate Enrollment Wizard.

The Request Certificates window (Figure 11-12) lists the certificates available with this method. If you click the "Show all templates" check box, other templates are listed but have a

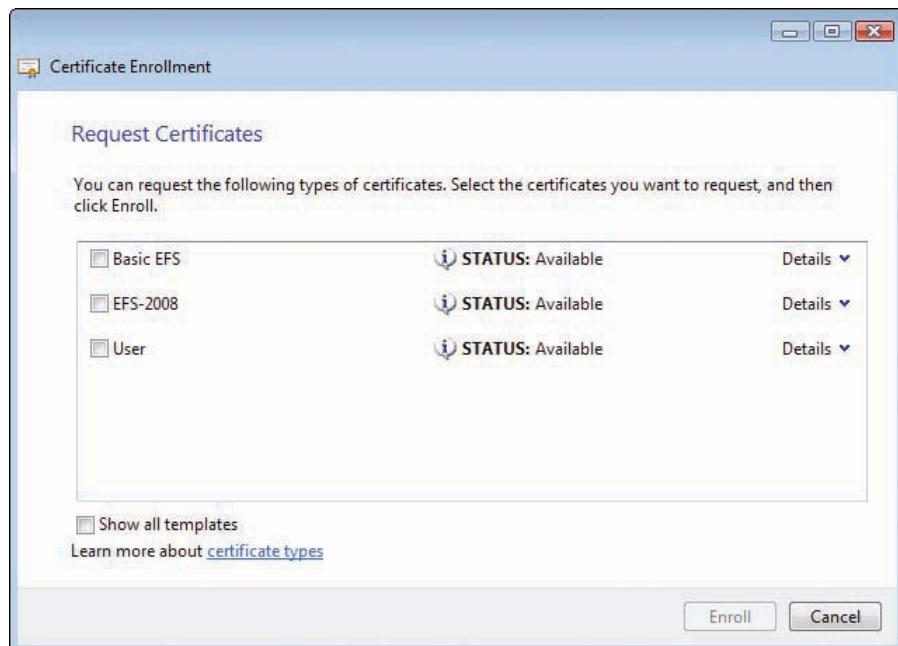


Figure 11-12 Using the Certificate Enrollment Wizard

status of Unavailable. Select the certificates you want to enroll in, and click the Details item to see how the certificate key can be used and the certificate's validity period. This method for requesting certificates can be used only with enterprise CAs.

In most cases, autoenrollment is preferred over manual requests. If you want users to know their certificate information or if you have specialized templates that only a few users require, you might want to use manual requests.

Configuring Web Enrollment After autoenrollment, the most common certificate request method is Web enrollment, which requires installing the Certification Authority Web Enrollment role service in Server Manager. This role service enables users to request and renew certificates, retrieve CRLs, and enroll for smart card certificates via their Web browsers. Web enrollment is the main method for accessing CA services on a standalone CA because, as mentioned previously, autoenrollment and the Certificates snap-in can be used only with enterprise CAs.

To access the Certification Authority Web Enrollment role service, users simply open a browser and go to <http://CAServer.domain/certsrv>; *CAServer* is the name of the CA server, and *domain* is the domain name. The server with the Web Enrollment role service installed can be, but need not be, the CA server. A server configured for Web enrollment is called a **registration authority** or a **CA Web proxy**.



Activity 11-6: Installing Web Enrollment

Time Required: 20 minutes

Objective: Install Web enrollment.

Description: You have several certificates that you don't want to use autoenrollment for and have found that using the Certificates snap-in is cumbersome for users. You install the Certification Authority Web Enrollment role service and test it by requesting a certificate from your Vista computer. (If you want to test the configuration from your CA Server or domain controller, you must enable IE to run ActiveX controls.)

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. In the left pane, click to expand the **Roles** node and then click **Active Directory Certificate Services**. Click **Add Role Services** in the right pane.
3. Click **Certification Authority Web Enrollment**. When prompted, click **Add Required Role Services**, and then click **Next**.
4. In the Web Server (IIS) window, click **Next**. In the Select Role Services window, click **Next**. In the Confirm Installation Selections window, click **Install**.
5. When the installation is finished, click **Close**.
6. IIS must have a Web Server Certificate. To request one, click **Start**, point to **Administrative Tools**, and click **Internet Information Services (IIS) Manager**.
7. In the left pane of IIS Manager, click the **Server1XX** node. In the middle pane, double-click **Server Certificates**.
8. In the Actions pane, click **Create Domain Certificate** to start the Create Certificate Wizard. In the Distinguished Name Properties window shown in Figure 11-13, fill in the following information:
 - Common name: **server1XX.w2k8adXX.com**
 - Organization: **Server 2008 AD Class**
 - Organizational unit: **Your name**
 - City/locality: **Your city**
 - State/province: **Your state or province**
 - Country/region: **Your country**
9. Click **Next**. In the Online Certification Authority window, click **Select**, click **w2k8adXX-Server1XX-CA**, and then click **OK**. In the Friendly name text box, type **server1XX.w2k8adXX.com**, and then click **Finish**.

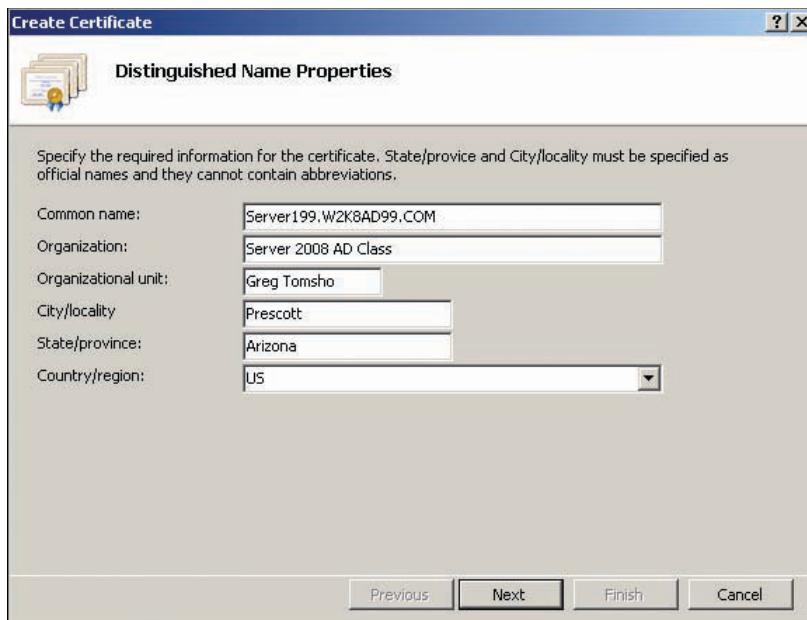


Figure 11-13 Entering distinguished name information

10. In the left pane of IIS Manager, click the **Sites** node. Right-click **Default Web Site** and click **Bindings**.
11. In the Site Bindings dialog box, click **Add**.
12. In the Add Site Binding dialog box, click the **Type** list arrow and click **https**. Click the **SSL certificate** list arrow, click **server1XX.w2k8adXX.com**, and then click **OK**. Click **Close**.
13. In the left pane of IIS Manager, click to expand **Sites** and **Default Web Site**, and then click **CertSrv**. In the middle pane, double-click **SSL Settings**. In the SSL Settings dialog box, click **Require SSL**. Notice the options under Client certificates. You can have the Web server ignore, accept, or require client certificates. If you want client computers to connect to the Web server to verify their identity, you would select **Require**. For now, leave the default **Ignore** selected.
14. Click **Apply** in the Actions pane, and then close IIS Manager.
15. To test your configuration, log on to the domain from your Vista computer as **salesperson1**. Open Internet Explorer, type **https://server1XX.w2k8adXX.com/certsrv** in the Address text box, and press **Enter**. When prompted for a username and password, log on as salesperson1 with the UPN (salesperson1@w2k8adXX.com) or w2k8adXX.com\salesperson1 syntax. The Web enrollment home page opens (see Figure 11-14).
16. Click the **Request a certificate** link, and then click **User Certificate**. The User-Certificate - Identifying Information window is displayed, which informs you that no more information is required. However, you must install an ActiveX control, as indicated by the yellow information bar.
17. Click the yellow information bar at the top of the Web page and click **Run ActiveX Control**. Click **Run**, click **Allow**, and then click **Submit**. (If you get an error message stating that the CA Web site must be configured to use HTTPS authentication, add the CA Web site to the Trusted Sites list in Internet Explorer.)
18. When asked whether you want to request a certificate now, click **Yes**. Click **Allow** in the Internet Explorer Security message box.
19. In the Certificate Issued window, click **Install this certificate**. In the Web Access Confirmation message box, click **Yes**. You see a message indicating the certificate has been installed.
20. Close Internet Explorer and IIS Manager. Log off your Vista computer, but stay logged on to Server 1XX.

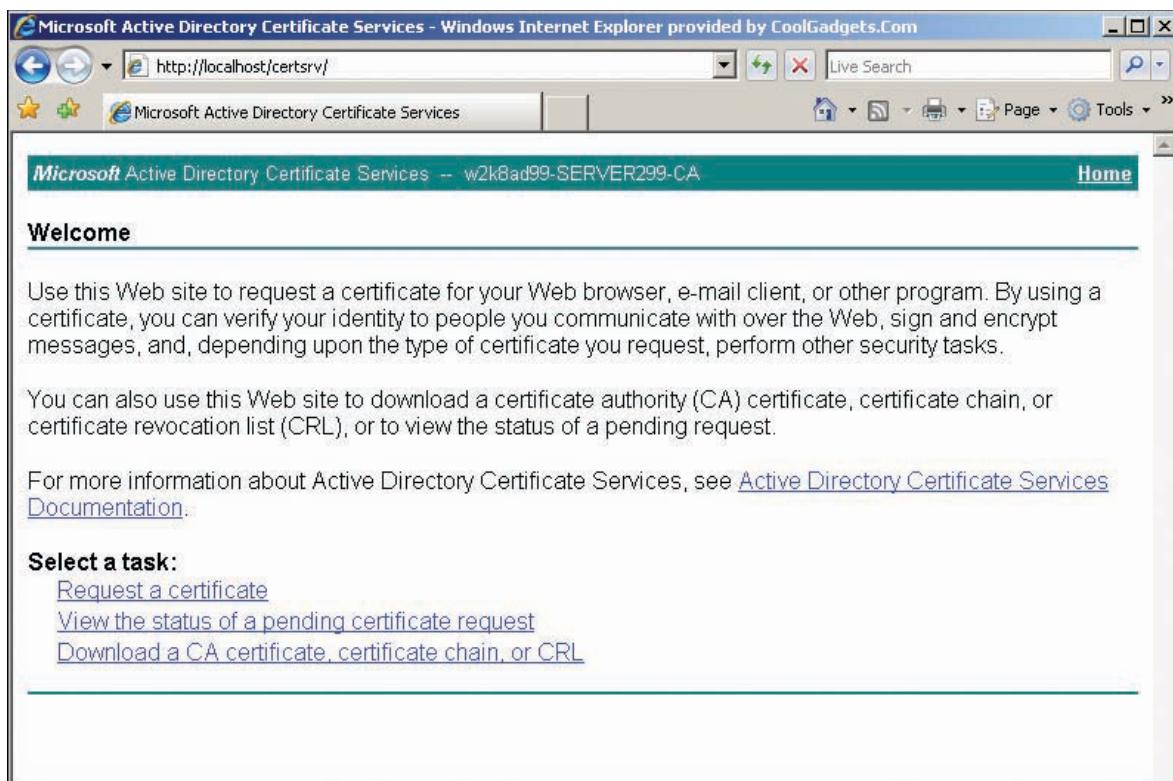


Figure 11-14 The Web enrollment home page

11

Network Device Enrollment Service Network Device Enrollment Service (NDES) allows network devices, such as routers and switches, to obtain certificates by using Simple Certificate Enrollment Protocol (SCEP), a Cisco proprietary protocol. With this protocol, Cisco internetworking devices can request and obtain certificates to run IPSec, even if they don't have domain credentials. The procedure for installing and configuring NDES involves the following steps:

1. Create a user for NDES and add it to the IIS_USRS group.
2. Configure a certificate template with enroll permissions assigned to the NDES user.
3. Install the NDES role service.
4. Create a public/private key pair, using the network device's OS to enroll.
5. Forward the key pair to the registration authority on the server hosting NDES.
6. Submit a certificate request from the device to the NDES server.



For more information on using NDES, see <http://technet.microsoft.com/en-us/library/cc753784.aspx>.

NOTE

Smart Card Enrollment Smart card enrollment is not so much an enrollment method as a specialized type of certificate template. It takes place through Web enrollment at a smart card station. After a user supplies credentials to request the smart card certificate and presents his or her card, the certificate information is embedded in the card.

Smart cards are used to enhance security. Users can log on to a network by presenting the card to a station with a card reader and entering their PINs, much like using an ATM card. A user designated as an enrollment agent can enroll smart card certificates on behalf of users to simplify the process. However, enrollment agents can enroll on behalf of any user, including administrators, which could pose a security risk. After a smart card is created for a user, the card

can be used to log on as that user. Enrollment agents must be issued an Enrollment Agent certificate to perform this task, but considering the power an enrollment agent has, these people must be highly trusted in the organization.

To mitigate the security concerns, Windows Server 2008 offers restricted enrollment agents. With this feature, administrators can configure smart card certificate templates to specify which users or groups an enrollment agent can enroll in the certificate. To do this, use the Restrict enrollment agents option in the Enrollment Agents tab of the CA server's Properties dialog box. By default, enrollment agents are not restricted.

Configuring the Online Responder

An **online responder (OR)** enables clients to check a certificate's revocation status without having to download the CRL. To use an OR, you install the Online Responder role service when you install the CA role or later. You can install this role service on the same server as the CA role or a different server, and it requires the Web Server role service.

After the OR role service is installed, it must be configured with these steps:

1. Configure an OCSP Response Signing certificate template. This certificate is used to sign the response the OR provides to certificate revocation queries. (OCSP stands for Online Certificate Status Protocol.)
2. Configure the CA to support the online responder. An Authority Information Access (AIA) extension is configured on a CA to indicate the OR's location.
3. Add the OCSP Response Signing Certificate template to the CA, and enroll the OR with this certificate.
4. Configure revocation for the OR, including the settings required for the OR to reply to certificate status requests.



Activity 11-7: Configuring an OCSP Response Signing Certificate Template

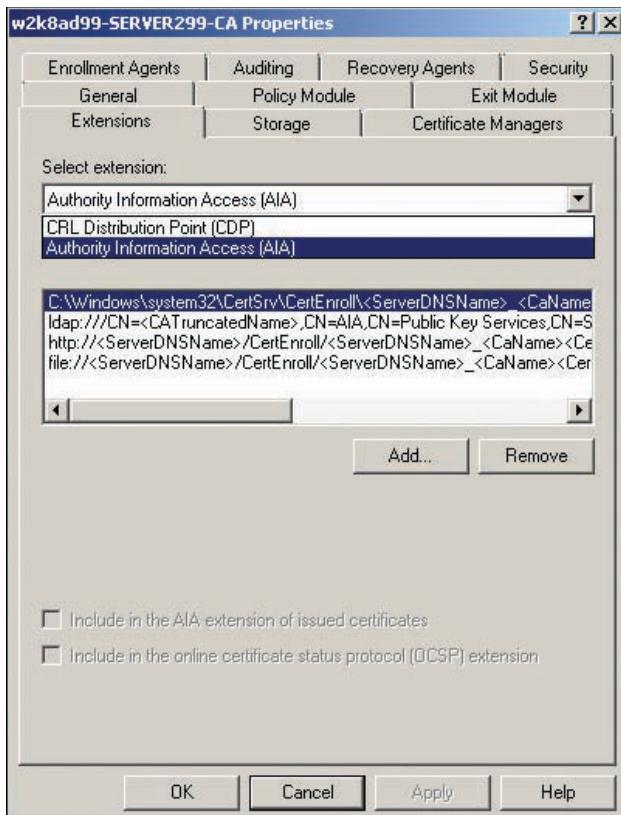
Time Required: 20 minutes

Objective: Configure an OCSP Response Signing Certificate template.

Description: Now that you have configured your CA to issue certificates via autoenrollment and Web enrollment, you want to configure an online responder to field certificate status requests instead of requiring clients to download the CRL.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. If necessary, in the left pane, click to expand the **Roles** node and the **Active Directory Certificate Services** node.
3. Click **Certificate Templates**. In the right pane, right-click the **OCSP Response Signing** template and click **Duplicate Template**. Leave the **Windows Server 2008, Enterprise Edition** option button selected, and then click **OK**.
4. In the Properties of New Template dialog box, type **OCSP-2008** in the Template display name text box, and then click the **Publish certificate in Active Directory** check box.
5. Click the **Security** tab, and then click the **Add** button. In the Select Users, Computers, or Groups dialog box, click **Object Types**. Click the **Computers** check box, and then click **OK**. Type **server1XX** and click **Check Names**. Click **OK**.
6. Click the **Enroll** and **Autoenroll** permissions in the Allow column, and then click **OK**.
7. The next step is to add the template to the CA. In the left pane of Server Manager, click the CA server node (**w2k8adXX-Server1XX-CA**). Right-click **Certificate Templates**, point to **New**, and click **Certificate Template to Issue**.
8. In the Enable Certificate Templates list box, click **OCSP-2008**, and then click **OK**.

9. Next, you must inform the CA of the online responder's location. Right-click the CA server node and click **Properties**.
10. Click the **Extensions** tab. Click the **Select extension** list arrow (see Figure 11-15), and then click **Authority Information Access (AIA)**.



11

Figure 11-15 The Extensions tab

11. In the “Specify locations from which users can obtain the certificate for this CA” list box, click the entry starting with **http**. Click the **Include in the online certificate status protocol (OCSP) extension** check box, and then click **OK**.
12. When you're prompted to restart Active Directory Certificate Services, click **Yes**.
13. Now the OR server (Server1XX, in this case) must enroll in the signing certificate you configured earlier in this activity. You can do this by restarting the server or requesting it manually. The next activity goes through the steps to request the certificate manually so that the server doesn't have to be restarted. Stay logged on for the next activity.



Activity 11-8: Requesting the OCSP Response Signing Certificate

Time Required: 10 minutes

Objective: Request the OCSP Response Signing certificate.

Description: To avoid restarting the OR server, you request the OCSP Response Signing certificate in the Certificates snap-in.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. Click **Start**, type **MMC** in the Start Search text box, and press **Enter**. Click **File, Add/Remove Snap-in** from the MMC menu.

3. Click **Certificates**, and then click the **Add** button. In the Certificates snap-in dialog box, click the **Computer account** option button, and then click **Next**. In the Select Computer dialog box, leave the default selection of Local computer, click **Finish**, and then click **OK**.
4. In the left pane, click to expand the **Certificates** node and the **Personal** folder, and then click **Certificates**. Notice that two certificates are issued to this computer.
5. Right-click the **Certificates** folder, point to **All Tasks**, and click **Request New Certificate** to start the Certificate Enrollment Wizard. Click **Next**.
6. In the Request Certificates window, click the **OCSP-2008** check box, and then click the **Enroll** button. In the next window, click **Finish**.
7. Click the **Certificates** folder again. You should see the new OCSP-2008 certificate in the list.
8. The last step is configuring the certificate. Right-click the **OCSP Response Signing** certificate, point to **All Tasks**, and click **Manage Private Keys**.
9. In the Security tab, click **Add**. In the Enter the object names to select text box, type **Network Service**, click **Check Names**, and then click **OK**. Click **OK**, and then close the MMC.
10. Stay logged on to Server1XX for the next activity.

Creating a Revocation Configuration

A revocation configuration tells the CA what methods are available for clients to access CRLs. To create a revocation configuration, you use the Active Directory Certificate Services snap-in, under the Roles node in Server Manager. The steps are described in the following activity.



Activity 11-9: Creating a Revocation Configuration for the OR

Time Required: 10 minutes

Objective: Create a revocation configuration.

Description: You're almost finished configuring the online responder. The last task is creating the revocation configuration so that the CA can direct clients where and how to get their CRL.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. Click to expand **Active Directory Certificate Services**, if necessary, and then click to expand **Online Responder**. Right-click **Revocation Configuration** and click **Add Revocation Configuration**. In the Add Revocation Configuration Wizard's welcome window, click **Next**.
3. In the Name the Revocation Configuration window, type **ORServer1XX** in the Name text box. The name should describe the online responder function and include the server name. Click **Next**.
4. In the Select CA Certificate Location window, leave the default selection of **Select a certificate for an Existing enterprise CA**, and then click **Next**.
5. In the Choose CA Certificate window, click **Browse** next to the Browse CA certificates published in Active Directory text box. The Select Certification Authority message box opens. Because there's only one choice, click **OK**. The Online Responder Signing certificate is loaded automatically. Click **Next**.
6. In the Select Signing Certificate window (see Figure 11-16), accept the defaults, and then click **Next**.
7. In the Revocation Provider window, click the **Provider** button. Select the entry beginning with "http," if necessary, and then click **Edit**. Copy the path listed; you use it in the next step. Click **Cancel**.
8. Under the Delta CRLs text box, click **Add**. In the Add/Edit URL text box, type **http://server1XX.w2k8adXX.com/CertEnroll/w2k8adXX-SERVER1XX-CA.crl** (or paste the path you copied in Step 7), and then click **OK** twice. In the wizard's final window, click **Finish**.
9. Leave Server Manager open and stay logged on for the next activity.

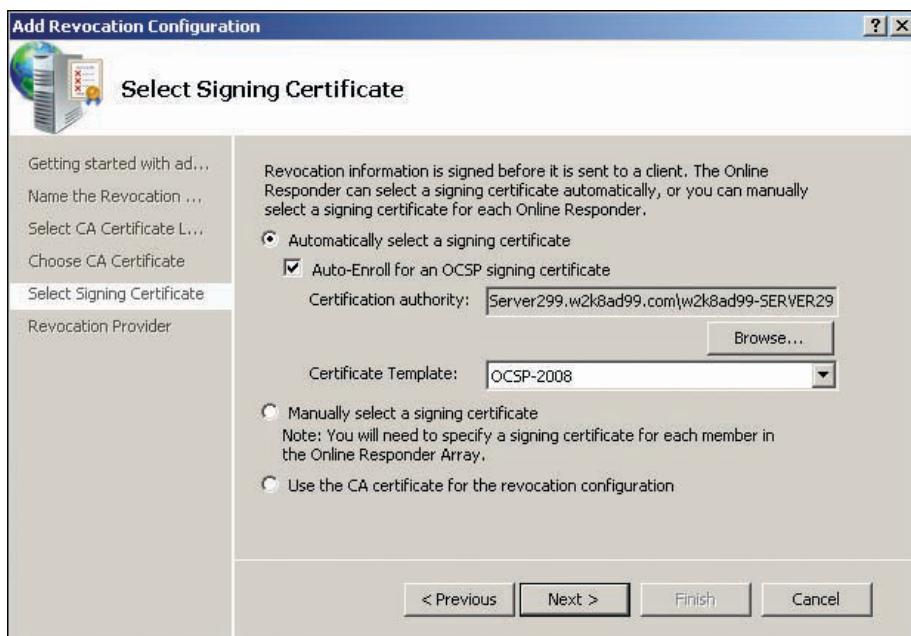


Figure 11-16 The Select Signing Certificate window

One way to test the OR's configuration is to issue and then revoke some certificates. Then open a Web browser and go to <http://server1XX.w2k8adXX.com/CertEnroll/w2k8adXX-SERVER1XX-CA.crl>. After you download this CRL file, open it. The Revocation List tab in Figure 11-17 lists serial numbers and revocation dates for revoked certificates.

11

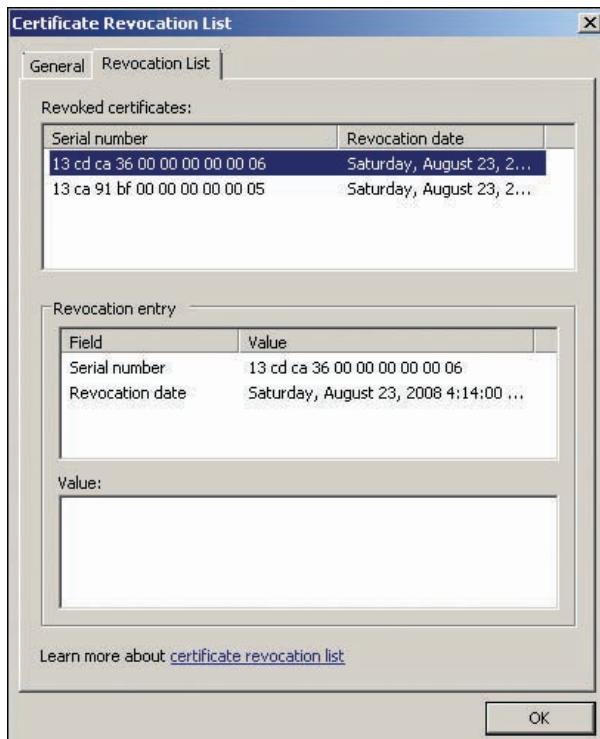


Figure 11-17 Viewing the CRL

Maintaining and Managing a PKI

CA servers, issued certificates, and associated private keys are critical components of a network that depends on a public key infrastructure, so these components must be maintained and protected against disasters. In addition, key CA administrative roles must be assigned to responsible, trusted users to carry out the numerous tasks in maintaining a PKI environment.

Starting with Windows Server 2003, Microsoft introduced CA role-based administration, which limits the PKI tasks a domain administrator account can perform. By default, administrators can perform all tasks on a CA server. However, after roles have been assigned, administrators can perform only tasks related to their assigned roles. Whether you use role-based administration or not, four key roles must be filled to administer a CA and its components:

- **CA Administrator**—Configures and maintains CA servers. This role can assign all other CA roles and renew the CA certificate. To assign this role, give the selected user the Manage CA permission in the Security tab of the CA server’s Properties dialog box.
- **Certificate Manager**—Approves requests for certificate enrollment and revocation. To assign this role, give the selected user the Issue and Manage Certificates permission in the Security tab of the CA server’s Properties dialog box.
- **Backup Operator**—Not so much a CA role as an OS right. Members of the local Backup Operators group or a user who has been assigned the Backup files and directories and Restore files and directories rights can perform this role.
- **Auditor**—Manages auditing logs. Assigning the Manage auditing and security log right confers this role on a user.



For more on CA role-based administration, see <http://technet.microsoft.com/en-us/library/cc739182.aspx>.

NOTE

CA Backup and Restore

Regular backup of all servers in a network is mandatory. When a full backup or system state backup is performed on a CA server, the certificate store is backed up along with other data. You might also want to back up the certificate database on each CA separately. The Active Directory Certificate Services snap-in in Server Manager includes a simple wizard-based backup utility you can use to perform backups with the following options:

- **Private key and CA certificate**—Backs up only the local CA’s certificate and private key.
- **Certificate database and certificate database log**—Backs up the certificates issued by this CA. If your certificate database is large, you can choose to perform incremental backups, which back up only the changes to the database since the last full or incremental backup.

You can also use the Certutil command-line program to back up the CA, and you can automate the process by using the command in a batch file or script and use Windows Task Scheduler to perform periodic backups of the CA database.

Like backup, CA restores can be performed with the Active Directory Certificate Services snap-in or the Certutil program. Before you can restore the CA database, however, the CA service must be stopped. When you start the CA Restore Wizard, you’re prompted to stop the service.



Activity 11-10: Backing Up the CA Server

Time Required: 10 minutes

Objective: Back up the CA server.

Description: Your CA server has been up and running and issuing certificates. You realize the importance of data the CA manages, so you perform a backup of the CA certificate, private key, and certificate database.

1. Log on to **Server1XX** as Administrator and open Server Manager, if necessary.
2. First, you need to create a folder for storing the backup. Normally, this folder is on another server or removable media. For this activity, create a folder named **CABackup** in the root of the C drive.
3. In the left pane of Server Manager, click to expand the **Roles** node and the **Active Directory Certificate Services** node.
4. Right-click the CA server node, point to **All Tasks**, and click **Back up CA** to start the Certification Authority Backup Wizard. Click **Next** in the welcome window.
5. In the Items to Back Up window, click **Private key and CA certificate** and **Certificate database and certificate database log**.
6. Click the **Browse** button next to the Back up to this location text box. In the Browse for Folder dialog box, navigate to and click the **CABackup** folder you just created, and click **OK**. Click **Next**.
7. In the Password and Confirm password text boxes, type **Password01**, and then click **Next**. In the Completing the Certification Authority Backup Wizard window, click **Finish**. The backup begins.
8. Close any open windows, and stay logged on for the next activity.

Key and Certificate Archival and Recovery

If a user's private key is lost or damaged, he or she might lose access to systems or documents. If the key has been used for authentication to a system, a new certificate and key can be issued. However, if the key was used for applications such as EFS, the user loses access to encrypted documents. If a Data Recovery Agent has been assigned to the user's documents, they can be recovered, but Data Recovery Agents should be used only when there's no hope of the document owner regaining access to the files. By using **key archival**, private keys can be locked away and then restored if the user's private key is lost. Private keys can be lost if a user's profile is lost or corrupted or a smart card holding the private key is lost or damaged.

There are two methods for archiving private keys. Manual archival requires users to export their keys to a file by using the Certificates snap-in. The file is password-protected, and the password must be entered to import the key. The certificate the private key is related to must allow the private key to be exported. The default setting for private key export depends on the type of certificate template. For example, the default setting on an EFS or User certificate template is to allow exportation. The default setting on a Computer or IPSec template is to not allow exporting the private key.

The procedure for exporting the private key for a certificate is straightforward:

1. Open the Certificates snap-in.
2. Locate the certificate for the key you want to export.
3. Right-click the certificate, point to All Tasks, and click Export.
4. The Certificate Export Wizard walks you through the process.

The Certificate Export Wizard exports the certificate and optionally exports the private key if allowed. You're prompted to select the format for the certificate export (see Figure 11-18). However, the only format supported for exporting the private key along with the certificate is Personal Information Exchange. If only the certificate is exported, other formats are enabled. You might want to export the certificate without the private key if the certificate is to be used on another computer or OS or for later recovery if the certificate is lost. To import a certificate and/or the private key, in the Certificates snap-in, simply right-click the folder where you want to import the key, point to All Tasks, and click Import. You're asked to supply the password used when the certificate was exported.

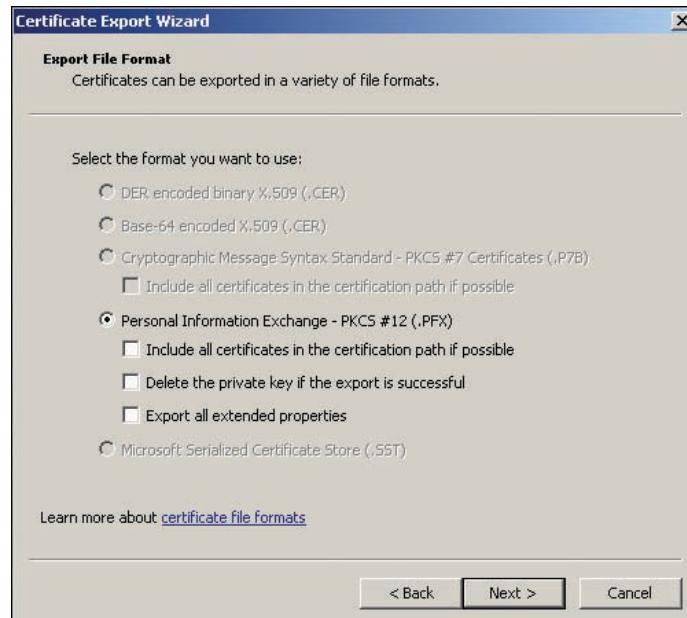


Figure 11-18 Selecting an export format for the certificate

Manual key archival is fine for a network with a small number of users and few keys to manage. However, Windows Server 2008 provides automatic key archival in the Enterprise and Datacenter editions when manual key archival isn't adequate. Automatic key archival uses a key recovery agent (KRA), which is a designated user with the right to recover archived keys. A KRA has a lot of power, so the user should be chosen carefully. The designated user must enroll for a Key Recovery Certificate after the Key Recovery Agent template has been configured to allow the designated user to enroll. The Key Recovery Agent certificate is then added to the Recovery Agents tab of the CA server's Properties dialog box (see Figure 11-19).

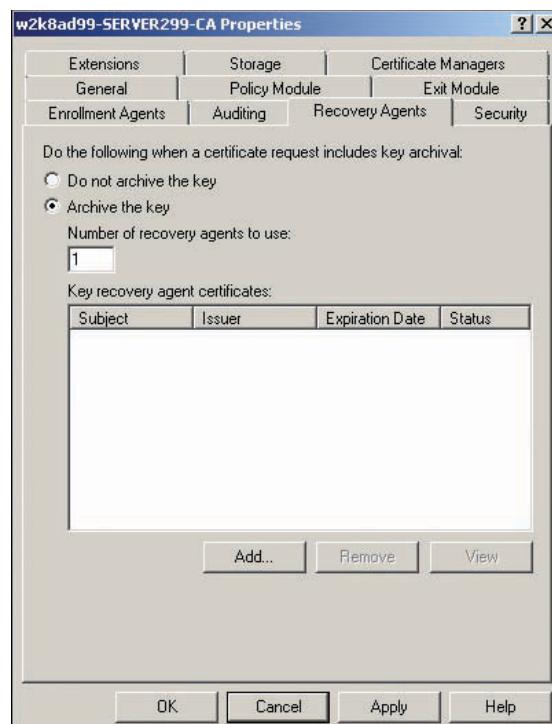


Figure 11-19 Configuring a key recovery agent

After a KRA is assigned, the key for each certificate issued from a certificate template with key export enabled is archived automatically. Multiple KRAs can be assigned to a certificate by entering a value in the Number of recovery agents to use text box. This number should usually be the same as the number of certificates you add to the Key recovery agent certificates list box that allow all installed KRAs to recover keys. The number of recovery agents can't be more than the number of certificates installed. If you specify a number lower than the number of certificates installed, the certificates are selected round-robin for each key archival procedure. In this case, you have to determine which recovery agents can recover an archived key. For example, if two recovery agents are specified and four KRA certificates are installed, two certificates are chosen for each key archival process. Either of the two KRAs can decrypt the key for recovery.

The recovery of a key that has been archived automatically typically follows these steps:

1. The user who has lost his or her private key contacts the Certificate Manager (role holder) to request key recovery.
2. The Certificate Manager locates the key in the CA database.
3. The Certificate Manager inspects the encrypted key's properties to determine which KRAs can recover the key. The Certificate Manager can copy the key from the CA database but can't decrypt the key unless he or she is also a designated KRA.
4. The key is sent to a KRA for decryption.
5. The KRA decrypts the key and sends it to the user in a password-protected file.
6. The user imports the key, using the password supplied by the KRA.



Activity 11-11: Archiving a Key Manually

Time Required: 15 minutes

Objective: Archive a private key.

Description: You have just been issued an EFS certificate and realize you should archive your private key in case it's lost or corrupted.

1. Log on to your Vista computer as **salesperson1**. (If you didn't use your Vista computer to request the EFS certificate for salesperson1, you can log on to ServerXX.)
2. Add the Certificates snap-in to an MMC. (See Activity 11-5 for the steps.)
3. In the left pane, click to expand the **Certificates** node and the **Personal** folder, and then click the **Certificates** folder.
4. Right-click the **EFS-2008** certificate, point to **All Tasks**, and click **Export**. In the Certificate Export Wizard's welcome window, click **Next**.
5. Click the **Yes, export the private key** option button, and then click **Next**.
6. In the Export File Format window, leave the **Personal Information Exchange - PKCS #12 (.PFX)** option button selected, and then click **Next**.
7. In the Password window, type **Password01** in the Password text box and the Type and confirm password (mandatory) text box, and then click **Next**.
8. In the File to Export window, click **Browse**. By default, your Documents folder is selected as the destination folder. Type **EFSCert** in the File name text box, and click **Save**. Click **Next**.
9. In the Completing the Certificate Export Wizard window, click **Finish**. Click **OK** in the success message. Leave the Certificates snap-in open for the next activity.



Activity 11-12: Recovering a Lost Key

Time Required: 15 minutes

Objective: Recover a lost key.

Description: Your user profile, which contained your private key, was accidentally deleted. You need to recover your key from an archived backup.

1. First, you delete your existing certificate and key. In the left pane of the Certificates snap-in, click the **Certificates** folder, if necessary. Right-click the **EFS-2008** certificate and click **Delete**.



2. In the message box explaining that you can't decrypt data encrypted with this certificate, click **Yes**.
3. Right-click the **Certificates** folder, point to **All Tasks**, and click **Import**. (Note that you can request a new certificate, but a new certificate can't decrypt data encrypted with the deleted certificate.)
4. The Certificate Import Wizard starts. Click **Next**.
5. In the File to Import window, click **Browse**. In the File types list box, click **Personal Information Exchange**. Click the **EFSCert** certificate you exported in Activity 11-11, and then click **Open**. Click **Next**.
6. In the Password window, type **Password01** in the Password text box, and then click the **Mark this key as exportable** check box. If you don't select this check box, you can't export the key again. Click **Next**.
7. In the Certificate Store window, accept the default **Personal** option, and then click **Next**.
8. In the Completing the Certificate Import Wizard window, click **Finish**. In the success message box, click **OK**. You should see your EFS-2008 certificate displayed in the Certificates folder.
9. Close all open windows on all computers and log off.

Chapter Summary

- Active Directory Certificate Services (AD CS) provides services for creating a PKI in a Windows Server 2008 environment. A PKI enables administrators to issue and manage certificates, which can add a level of security to a network.
- A PKI binds the identity of a user or device to a cryptographic key. The main services a PKI provides are confidentiality, integrity, nonrepudiation, and authentication.
- Some key terms for describing a PKI and AD CS include private and public keys, digital signature, certification authority, certificate revocation list, online responder, and certificate enrollment.
- An enterprise CA integrates with Active Directory; a standalone CA does not. Windows Server 2008 Enterprise Edition must be installed to install an enterprise CA. For non-Windows devices or users, you need to install a standalone CA.
- A CA can be online or offline. An offline CA is more secure and usually used in a CA hierarchy with one or more online issuing CAs. An issuing CA issues a certificate to users and devices. A CA hierarchy is usually two-level or three-level. The first level is the root CA, and each level created is subordinate to the level above it.
- The AD CS role is installed in Server Manager and should not be installed on a domain controller. An enterprise CA must be installed on a domain member server. A standalone CA can be installed on a member server or a standalone server.
- Configuring a CA involves configuring certificate templates, enrollment options, and an online responder as well as creating a revocation configuration. Certificate templates can be version 1, version 2, or version 3. Version 1 templates can't be changed and are provided for backward compatibility. Version 2 templates are compatible with Windows Server 2003 and later, and version 3 templates are compatible with Windows Server 2008.
- Certificate enrollment occurs when a user or device requests a certificate and the certificate is granted. Enrollment can occur with autoenrollment, the Certificates MMC, Web enrollment, NDES, and smart cards.
- An online responder allows clients to check a certificate's revocation status without having to download the CRL periodically. The Online Responder role service requires installing the Web Server role service, too.

- Role-based administration limits the PKI tasks a domain administrator account can perform. Four key roles must be filled to administer a CA and its components: CA Administrator, Certificate Manager, Backup Operator, and Auditor.
- When a full backup or system state backup is performed on a CA server, the certificate store is backed up along with other data. You use the Active Directory Certificate Services snap-in to back up the certificate database and database log.
- When users' private keys are lost or damaged, they could lose access to systems or documents. Keys can be archived manually with the Certificates snap-in or automatically on enterprise CAs by assigning users as key recovery agents.

Key Terms

CA Web proxy A server configured with the Web Enrollment role service. *See also* registration authority.

certificate practice statement (CPS) A document describing how a CA issues certificates containing the CA identity, security practices used to maintain CA integrity, types of certificates issued, renewal policy, and so forth.

certificate templates A shell or model of a certificate used to create new certificates; it defines characteristics of the certificate, such as the intended use and expiration date.

hash algorithm A mathematical function that takes a string of data as input and produces a fixed-size value as output. Hash values are used to verify that the original data hasn't been changed and to sign CA certificates and certificates issued by the CA.

intermediate CAs A CA in a multilevel CA hierarchy that issue certificates to issuing CAs, which respond to user and device certificate requests. Sometimes called a policy CA.

issuing CAs A CA that interacts with clients to field certificate requests and maintain the CRL.

key archival A method of backing up private keys and restoring them if users' private keys are lost.

Network Device Enrollment Service (NDES) A service that allows network devices, such as routers and switches, to obtain certificates by using Simple Certificate Enrollment Protocol (SCEP), a Cisco proprietary protocol.

online responder (OR) A role service that enables clients to check a certificate's revocation status without having to download the CRL.

public key infrastructure (PKI) A security system that binds a user's or device's identity to a cryptographic key that secures data transfer with encryption and ensures data authenticity with digital certificates.

registration authority A server configured with the Web Enrollment role service. *See also* CA Web proxy.

restricted enrollment agent An enrollment agent that's limited to enrolling only specific users or security groups. Restricted enrollment agents are available only with an enterprise CA.

root CA The first CA installed in a network. Clients are configured to trust the root CA's certificate, and then implicitly trust the certificate of any CA that's subordinate to the root.

11

Review Questions

1. Which of the following is a service provided by a PKI? (Choose all that apply.)
 - a. Confidentiality
 - b. Nonrepudiation
 - c. Authorization
 - d. Antivirus

2. Which of the following is used in both ends of the cryptography process (encrypt and decrypt) and must be known by both parties?
 - a. Public key
 - b. Private key
 - c. Secret key
 - d. Digital signature
3. A PKI is based on symmetric cryptography. True or False?
4. If you want the most security, which of the following should you use?
 - a. Symmetric cryptography only
 - b. Asymmetric cryptography only
 - c. A combination of symmetric and asymmetric cryptography
 - d. Secret key cryptography
5. Camille and Sophie want to engage in secure communication. Both hold a public/private key pair. Camille wants to send an encrypted message to Sophie. Which of the following happens first?
 - a. Camille encrypts the message with her public key.
 - b. Camille sends Sophie her private key.
 - c. Sophie sends Camille her public key.
 - d. Camille encrypts the message with her private key.
6. You have installed your root CA and will be taking it offline. The root CA must be a(n) _____ CA.
7. In a three-level CA hierarchy, the middle-level servers are referred to as _____ CAs.
8. Which of the following identifies the CA and describes the CA's certificate renewal policy?
 - a. Root CA
 - b. Online responder
 - c. CRL
 - d. CPS
9. You're installing AD CS in your network. You need a secure environment and want to require the CA administrator to enter a password each time the CA performs cryptographic operations. Which option should you enable during installation?
 - a. Select the hash algorithm for signing certificates issued by this CA.
 - b. Select a cryptographic service provider (CSP).
 - c. Use strong private key protection features provided by the CSP.
 - d. Change the key length.
10. Version 1 templates can't be modified, but they can be duplicated and then modified. True or False?
11. A certificate is issued on July 1, 2009. Its validity period is 2 years, and its renewal period is 2 months. When can the certificate first be renewed?
 - a. September 1, 2009
 - b. May 1, 2011
 - c. September 1, 2011
 - d. May 1, 2010

12. Which of the following isn't a necessary step to configure autoenrollment?
- Configure a KRA.
 - Configure a certificate template.
 - Configure a group policy.
 - Add the template to the CA.
13. You want to prevent tampering on your internetworking devices by issuing these devices certificates to run IPSec. What should you install?
- Online responder
 - NDES role service
 - Intermediate CA
 - CDP
14. Which of the following steps is necessary to configure an online responder? (Choose all that apply.)
- Configure an OCSP Response Signing certificate template.
 - Enroll the OR with the OCSP Response Signing certificate.
 - Configure the OR enrollment agent.
 - Configure revocation for the OR.
15. Which role can renew the CA certificate?
- CA Administrator
 - Certificate Manager
 - Backup Operator
 - Auditor
16. Your CA has issued several hundred certificates and private keys to several hundred users. More than once, a user's private key has been lost or corrupted, resulting in lost data. You want to make sure your users' private keys can be recovered if needed. What should you do?
17. You want to create a separate backup for the certificate store and make sure the backup occurs every Friday at 11:00 p.m. How should you do this?
- Use Windows Backup to schedule a CA database backup weekly on Fridays at 11:00 p.m.
 - Hire a technician to work Friday nights and instruct him on how to use the AD CS snap-in to back up the certificate store.
 - Use Certutil and Windows Task Scheduler.
 - Use the AD CS snap-in to schedule the backup.
18. To reduce the amount of traffic generated when clients download the CRL, which of the following should you use?
- AIA
 - Delta CRL
 - CDP
 - SCEP
19. You want to begin using smart cards for user logon. The number of enrollment stations you have is limited, so you want department administrators to enroll only other users in their departments in smart card certificates. How should you go about this?
- Issue the designated department administrators an Enrollment Agent certificate. Publish the smart card certificate template. Have the designated enrollment agents use the Certificates snap-in to enroll departmental users in the smart card certificates.
 - Issue the designated department administrators an Enrollment Agent certificate. Configure the smart card certificate templates with the list of users each enrollment

agent can enroll. Have the designated enrollment agents use Web enrollment to enroll departmental users in the smart card certificates.

- c. Issue the designated department administrators an Enrollment Agent certificate. Configure the CA server's properties to restrict enrollment agents. Publish the smart card certificate template. Have the designated enrollment agents use Web enrollment to enroll departmental users in the smart card certificates.
 - d. Configure Enrollment Agent Certificate templates with the list of users agents can enroll. Issue the designated department administrators an Enrollment Agent certificate. Publish the smart card certificate template. Have the designated enrollment agents use Web enrollment to enroll departmental users in the smart card certificates.
20. Your company runs a commercial Web site that enables your business partners to purchase products and manage their accounts. You want to increase the site's security by issuing certificates to business partners to augment logon security and protect data transmissions with encryption. What should you install?
- a. An online enterprise CA
 - b. An online standalone CA
 - c. An offline root CA
 - d. An intermediate CA

Case Projects



Case Project 11-1: Designing a PKI and CA Hierarchy

You're called in as a consultant to create a CA hierarchy for a company. The company has three locations: one in the United States, one in South America, and one in Europe. Each location has approximately 1000 users who need certificates. About 75% of the users in each location are domain members running Windows XP and Vista. The others are running a non-Windows OS and aren't domain members. Some features of the PKI should include the following:

- Web enrollment
- Autoenrollment
- Smart card enrollment, in which designated users can enroll other users
- EFS
- Automatic key archival
- Network device certificates
- Real-time query for certificate revocation status

Design the CA hierarchy, and label each CA according to its function and status (stand-alone, enterprise, root, intermediate, issuing, online, offline). The design should include a drawing showing the hierarchy as well as a detailed description, including how users and clients interact with the systems you selected. In addition, list the role services that need to be installed and the certificate template types that must be configured.

Additional Active Directory Server Roles

After reading this chapter and completing the exercises, you will be able to:

- Describe and configure Active Directory Lightweight Directory Services
- Describe Active Directory Federation Services
- Describe Active Directory Rights Management Services
- Implement a read only domain controller

Active Directory Domain Services is the foundation on which a Windows

Server 2008 network is built. By now, you should have enough knowledge to install and implement a secure, reliable Active Directory network. However, although AD DS is the core technology in Windows Server 2008, some complementary technologies installed as server roles can augment AD DS features and flexibility.

This chapter discusses three server roles introduced in Chapter 1: Active Directory Lightweight Directory Services, Active Directory Federation Services, and Active Directory Rights Management Services. All these roles use or integrate with AD DS technology to give users flexible, secure access to applications and network resources. In addition, you learn how to implement read only domain controllers (RODCs) in a branch office environment.

Active Directory Lightweight Directory Services

When you need a highly capable forest-wide directory service that's tightly integrated with your network OS, Active Directory Domain Services fits the bill. Suppose you want a directory service that's only loosely coupled with the OS, however? Perhaps you need one that can accommodate directory-enabled applications with diverse schema requirements yet doesn't affect the current AD DS schema operating throughout your forest? Active Directory Lightweight Directory Services (AD LDS) is the ideal server role to handle this task.

A **directory-enabled application** uses a directory service to store program data or configuration information, user information for authentication and authorization purposes, or a combination of program, configuration, and user information. The Microsoft Exchange e-mail system is an example of this type of application because it's tightly integrated with Active Directory. Some organizations prefer a different e-mail system—one that's directory enabled but requires schema changes that aren't compatible with the AD DS schema. AD LDS provides the environment for just this situation.

Active Directory LDS Overview

AD LDS, based on LDAP, was formerly known as Active Directory Application Mode (ADAM). This server role provides most of the functionality of AD DS without the requirements of forests, domains, and domain controllers. The primary purpose of AD LDS is to support directory-enabled applications with flexibility that AD DS can't match. For example, the AD DS schema is forest-wide, and changes to it affect all domains and can adversely affect replication times when changes are considerable. AD LDS, on the other hand, can be installed on a single server or a group of servers with a schema unique to the application it's intended to serve. Furthermore, you can install multiple instances of AD LDS on the same server to support multiple directory-integrated applications, each with its own schema requirements.

AD LDS does not rely on AD DS, but it can use the services of AD DS if necessary, when directory-enabled applications require authentication of security principals. The two services can coexist on the same network, or AD LDS can even be used in a non-domain environment. The following are some key features of the AD LDS server role:

- Supports directory-enabled applications without the overhead of a domain infrastructure.
- Multiple application directory partitions are supported, allowing more than one application to use a single AD LDS instance. Application directory partitions hold the data used by directory-enabled applications.
- Multiple AD LDS instances on the same server are supported to accommodate several directory-enabled applications with unique schema requirements.
- Directory replication provides fault tolerance and load sharing, which ensures highly available and reliable access to application data.

AD LDS has some similarities with AD DS but also a number of differences, summarized in the following list:

- No global catalog
- No support for group policy
- No computer objects

- No integration with AD CS
- No trust relationships
- No support for Windows security principals

As you can see, most of the features not supported by AD LDS are enterprise features that support the infrastructure of a Windows Active Directory network. AD LDS doesn't support these features because its intended use is more narrowly focused.

When to Use AD LDS

AD LDS is an ideal solution when a directory-enabled application isn't needed by the entire enterprise. For example, a human resources application that's directory enabled is likely to be used only by the HR Department. AD LDS is a good candidate for this type of application because there's no need to modify the schema in AD DS.

Perhaps you want to evaluate an application that requires directory support. In this situation, installing the application in a production environment that modifies the schema is not ideal. After new objects and attributes are created in an Active Directory schema, these changes remain, even if the application is no longer needed. With AD LDS, you can install the role on a server, evaluate the application, and then remove the role with no disturbance to your existing infrastructure.

Besides supporting directory-enabled applications, AD LDS can be used for a host of other purposes:

- *Authentication for Web applications*—Although AD LDS doesn't support using Windows security principals for accessing network resources, it does support using user objects to store identity information for external applications. For example, your company hosts a Web portal application that requires authenticating external users who need access to corporate business applications. AD LDS can be deployed on servers outside the corporate firewall along with Web servers requiring its authentication services. The Web applications can run on any platform that supports LDAP.
- *Directory consolidation*—Large organizations might have several sources of user identity information, including multiple forests, phone directories, other LDAP directory services, human resource databases, and so forth. AD LDS can be used with a metadirectory service, such as Microsoft Identity Integration Server (see <http://technet.microsoft.com/en-us/miis/default.aspx> for more on this service), to consolidate identity information from multiple sources. A directory-integrated application then has a unified view of all these identity sources through AD LDS.
- *Development environment for AD DS applications*—AD LDS and AD DS are based on the same code and programming model, so Active Directory-integrated applications can be developed and tested without the overhead of an AD DS installation. AD LDS is easily installed and uninstalled on Windows Server 2008 computers and doesn't require ancillary services, such as DNS.
- *Migration of legacy X.500 applications*—AD LDS supports some X.500 naming conventions not supported by AD DS. Legacy applications requiring these features can be migrated from older LDAP servers to AD LDS and eventually, if needed, to an AD DS environment.

12

Installing and Configuring AD LDS

AD LDS is installed on a Windows Server 2008 server by adding the Active Directory Lightweight Directory Services server role. It can be installed on all editions of Windows Server 2008 except Windows Web Server 2008 and Itanium. It's a good candidate for deployment on a Server Core installation or as a virtual machine in Hyper-V.



Although you can install AD LDS on a domain controller, it's not recommended. AD DS should, when possible, be installed on a server as a solitary role (along with DNS, as necessary).

NOTE

AD LDS is first installed as a server role, and then one or more instances of AD LDS are created. Before AD LDS can be removed as a server role, all instances must be removed in Control Panel. Each **AD LDS instance** has its own data store and communication ports and a unique service name, so to an application using AD LDS, each instance appears as a unique copy of the service. When you create an AD LDS instance, you're prompted to choose one of these two installation options:

- *A unique instance*—Uses the default configuration and schema partitions and can't replicate with existing instances. Select this option when AD LDS is installed for the first time or when you're creating an instance for a new directory-enabled application.
- *A replica of an existing instance*—Uses the configuration and schema partitions replicated from an existing instance of AD LDS. Use this option when you're installing AD LDS and it's already been installed on another server, perhaps for fault tolerance or load sharing.



NOTE In this activity, when you're instructed to log on as Administrator, make sure you log on as the domain administrator rather than the local administrator account. This instruction applies to all activities that require logging on as Administrator, unless noted otherwise.



Activity 12-1: Installing the AD LDS Server Role

Time Required: 20 minutes

Objective: Install AD LDS on Server1XX.

Description: You're installing a directory-enabled application and plan to use AD LDS. You install the AD LDS server role and create an instance of AD LDS.

1. Log on to **Server1XX** as Administrator.
2. Open Server Manager, and click the **Roles** node. In the right pane, click **Add Roles**. When the Add Roles Wizard starts, click **Next**.
3. In the Select Server Roles window, click the **Active Directory Lightweight Directory Services** check box, and then click **Next**.
4. Read the information in the Introduction to Active Directory Lightweight Directory Services window, and then click **Next**.
5. In the Confirm Installation Selections window, click **Install**. In the Installation Results window, read the messages, and then click **Close**.
6. In Server Manager, under Roles Summary, click **Active Directory Lightweight Directory Services**.
7. In the Summary section, you see the message "No AD LDS instances have been created." Click the **Click here to create an AD LDS instance** link.
8. When the Active Directory Lightweight Directory Services Setup Wizard starts, click **Next**.
9. In the Setup Options window, make sure the default **A unique instance** is selected, and then click **Next**.
10. In the Instance Name window, type **ADLDS1** in the Instance name text box. Note that **ADAM_** is added in front of the name you type automatically. Click **Next**.
11. In the Ports window, accept the defaults of 389 and 636. Note that each instance of AD LDS installed on the same computer requires different port numbers. Click **Next**.
12. In the Application Directory Partition window, click **Yes, create an application directory partition**. (If the directory-enabled application using this instance of AD LDS will create its own partition, you should click **No**.) In the Partition name text box, type **cn=App1,dc=w2k8adXX,dc=com**, and then click **Next**.
13. Accept the default file locations, and then click **Next**.
14. You can use the default Windows service account or select a different account for running the AD LDS service. Accept the default **Network service account**, and then click **Next**.

15. In the AD LDS Administrators window, you can choose which user or groups have administrative permissions for AD LDS. Accept the default **Currently logged on user**, and then click **Next**.
16. You can import one or more LDIF files to configure aspects of the AD LDS application partition schema. If you're running an application that creates its own application directory, there's no need to import any of these files. You can also import LDIF files later. Click **Next**.
17. In the Ready to Install window, review your selections and click **Next** to install the AD LDS instance. When the installation is completed, click **Finish**.

The following list provides more detail on some windows and options in the previous activity:

- **Ports**—Services communicate with clients by using port numbers, which identify a service running on a computer. For example, if you're running a Web server, the default port number for the server is 80. Each instance of a service must use a different port number. The standard LDAP port is 389, and the standard SSL LDAP port is 636. For the first installed AD LDS instance, these ports can be assigned to the instance. However, if AD DS is or will be installed on the same server, you must select different ports for AD LDS because AD DS uses these port numbers. A recommended best practice is using port numbers higher than 50000 for AD LDS instances. After you have installed the first AD LDS instance, subsequent instances use port numbers starting with 50000, by default.
- **Service Account Selection**—The Network service account is selected by default, but you can create accounts for each AD LDS instance, if needed. If the server on which AD LDS is installed is a domain member, a domain account should be used. A strong password should be assigned to this account, and it should be set to never expire. The account must be granted the Log on as a service right.
- **LDIF files**—Preconfigured LDIF files are available to import, which modify the application partition's schema. For example, there are LDIF files that modify the schema to allow synchronizing information with Active Directory or to create user classes, attributes, and so forth. Some applications require custom schema changes. You can build your own LDIF files and place them in the %systemroot%\Adam folder so that they're available for import.

12

AD LDS Management Tools After AD LDS is installed, you can use several tools to manage an AD LDS instance and its data. In most cases, the application using AD LDS is installed and configures the application partition as necessary. However, you can administer many aspects of an AD LDS instance with the following tools:

- **ADSI Edit**—This MMC is opened from Administrative Tools or by clicking the ADSI Edit link in Server Manager when the AD LDS role is selected. When you connect to an AD LDS instance, you can add and edit data in the available partitions.
- **LDP.exe**—Like ADSI Edit, the LDP tool can be used to connect to and manage AD LDS instances, including creating new application partitions. LDP can also be used to administer other LDAP directory services.
- **Server Manager**—Server Manager includes several links to AD LDS tools and recommended configurations, tasks, and resources. To access these links, click Active Directory Lightweight Directory Services in the left pane of Server Manager. You can select tools in the Advanced Tools section and get information in the Resources and Support section (shown in Figure 12-1). When you select an item in the Recommendations list box, you can read detailed instructions about performing configuration tasks, such as creating an AD LDS instance, creating a replica of an AD LDS instance, importing data from LDIF files, creating an application partition, backing up and restoring an AD LDS instance, and synchronizing data between AD DS and AD LDS, among others.

By default, an AD LDS instance's schema doesn't include user object definitions. However, you can extend the schema to allow creating user accounts or adding existing Windows users to groups you create. To extend the schema for user account creation, you import user classes with LDIFDE. You can also extend the schema when creating an instance by importing preconfigured LDIF files.

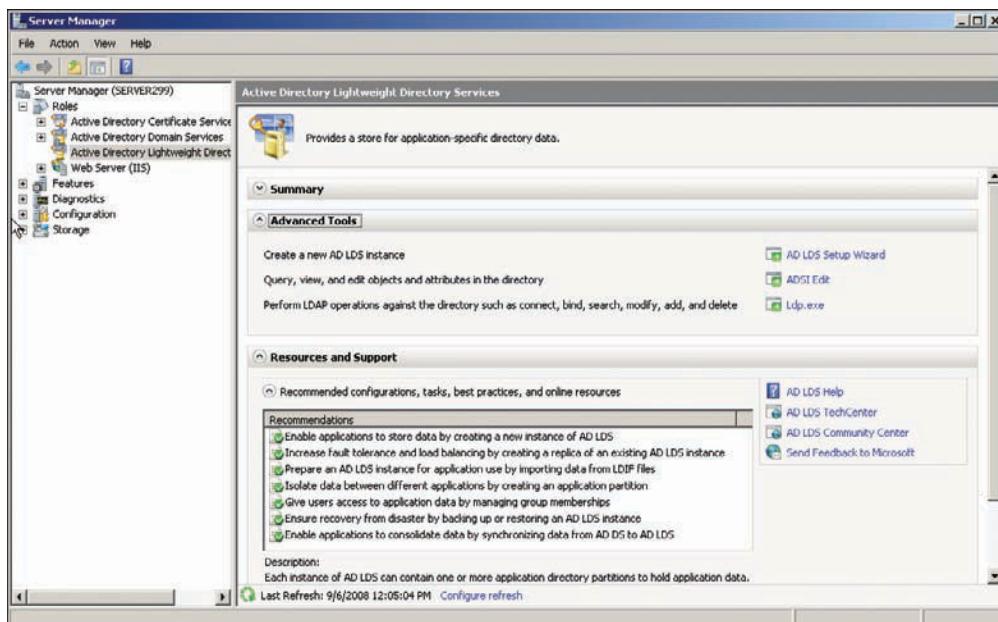


Figure 12-1 The AD LDS role in Server Manager

Activity 12-2: Creating a Group in an AD LDS Instance

Time Required: 20 minutes

Objective: Use ADSI Edit to create a group in an AD LDS instance.

Description: You have created an AD LDS instance with an application directory. The application you're using with this instance has instructions to create a group and a user. You create a group first.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **ADSI Edit**.
3. In ADSI Edit, right-click the **ADSI Edit** node and click **Connect to**.
4. In the Connection Settings dialog box (see Figure 12-2), type **App1** in the Name text box.

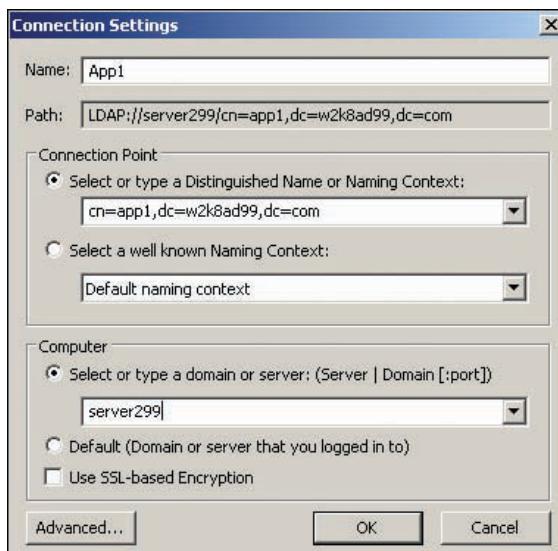
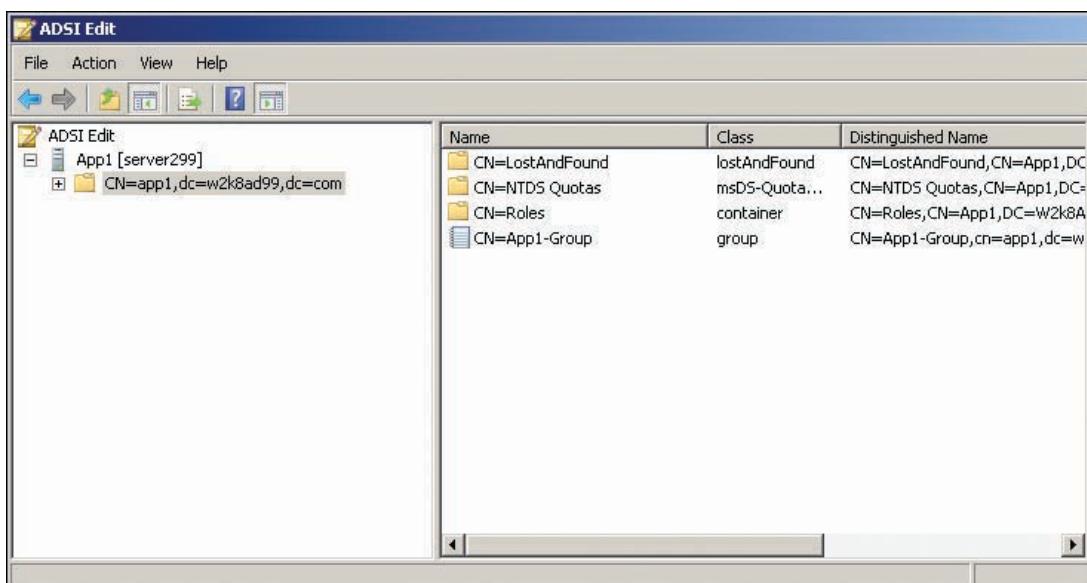


Figure 12-2 The Connection Settings dialog box

5. Click the **Select or type a Distinguished Name or Naming Context** option button, and type **cn=app1,dc=w2k8adXX,dc=com** in the text box below it.
6. Click the **Select or type a domain or server** option button, type **server1XX** in the text box below it, and then click **OK**.
7. In ADSI Edit, click to expand the **App1** node. Right-click the **Cn=app1,dc=w2k8adXX,dc=com** folder, point to **New**, and click **Object**.
8. In the Select a class list box, click **group**, and then click **Next**. In the Value text box, type **App1-Group**, and then click **Next**.
9. Click the **More Attributes** button to open the Attributes dialog box, where you can edit additional attributes of the group object. The adminDescription attribute is selected by default in the Select a property to view list box. In the Edit Attribute text box, type **Group for App1 Users**, and then click **Set**. Click **OK** and then **Finish**.
10. In ADSI Edit, click the **CN=app1,dc=w2k8adXX,dc=com** folder. The new object you created is shown in the middle pane (see Figure 12-3).



12

Figure 12-3 ADSI Edit with a new group object

11. To create a user, you must modify the schema of the AD LDS instance, which you do in the next activity. For now, close ADSI Edit but stay logged on to Server1XX.



Activity 12-3: Extending the AD LDS Schema

Time Required: 20 minutes

Objective: Use LDIFDE to import a user class to the schema of an AD LDS instance.
Description: You want to create users for your AD LDS instance, but first you must extend the schema by importing the ms-user.ldf file in C:\Windows\Adam with LDIFDE.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Open a command prompt window, type **ldifde -i -f c:\windows\adam\ms-user.ldf -s server1XX -k -c "CN=Schema,CN=Configuration,dc=X" "#schemaNamingContext"**, and press **Enter**. (The X after dc= in the command is an actual X and should not be replaced by a value.)
3. Open ADSI Edit. Right-click the **CN=app1,dc=w2k8adXX,dc=com** folder, point to **New**, and click **Object**. In the Select a class list box, click **user**, and then click **Next**. (If you get an error, make sure you close ADSI Edit, restart it, and then try again.)

4. In the Value text box, type **App1-User** and click **Next**. Click **Finish**. You should see the new user object in ADSI Edit.
5. The next step is to add the user to the group. Double-click the group object you created in Activity 12-2 to open it in Attribute Editor. Find and double-click the **member** attribute. The Multi-valued Distinguished Name With Security Principal Editor dialog box opens (see Figure 12-4).

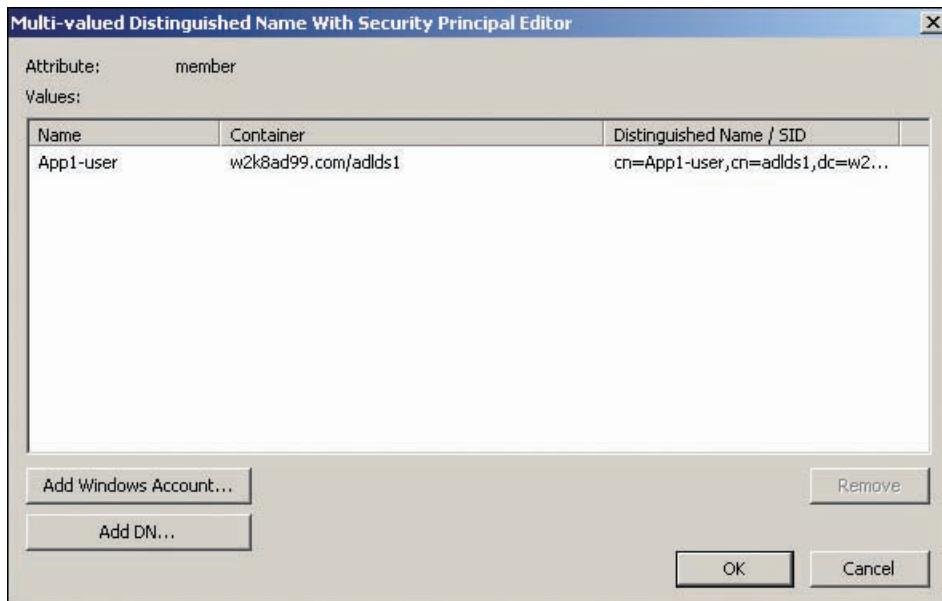


Figure 12-4 Adding a user to a group object

6. Click the **Add DN** button. In the Add Distinguished Name dialog box, type **CN=App1-User,CN=App1,DC=W2k8ADXX,DC=Com**, and then click **OK**. Notice the Add Windows Account button, which you can use to add Active Directory or local users to the group. Click **OK**, and then click **OK** to close the Attribute Editor.
7. Close ADSI Edit, and stay logged on for the next activity.

Configuring AD LDS Replication If your AD LDS application requires fault tolerance or load balancing, you can create replicas of an AD LDS instance and configure replication between the instances. AD LDS instances containing replicas of directory partitions are referred to as **configuration sets**. AD LDS instances that are part of the same configuration set must share common configuration and schema partitions and can share common application partitions.

To create a replica of an existing AD LDS instance, you create a new instance of AD LDS on the server to host the replica. The procedure is similar to creating a unique AD LDS instance:

1. On the server to host the new replica, click the Active Directory Lightweight Directory Services node in Server Manager.
2. In the Advanced Tools section, start the AD LDS Setup Wizard, and then click Next.
3. In the Setup Options window, click A replica of an existing instance, and then click Next.
4. Type a name that describes the instance's purpose in the Instance Name text box, and then click Next.
5. Type LDAP and SSL port numbers (or accept the default values), and then click Next.
6. In the Join a Configuration Set window, type the server name and the LDAP port number for the instance you want to replicate, and then click Next.

7. In the Administrative Credentials for the Configuration Set window, enter administrative credentials. If both servers are in the same domain and you're logged on to the domain as an administrator, the currently logged-on account can be used. Click Next.
8. In the Copying Application Directory Partitions window, select which application directory partitions you want to replicate. (The configuration and schema partitions are always replicated.) Click Next.
9. In the File Locations window, specify where you want the AD LDS files to be stored. By default, the location is C:\Program Files\Microsoft ADAM\instance\data (replacing *instance* with the name you specified in Step 4). Click Next.
10. In the Service Account Selection window, click Network service account (or specify a service account), and then click Next.
11. In the AD LDS Administrators window, you can specify the users or groups with administrative permissions for the AD LDS instance. Accept the default, which is the currently logged-on user, and then click Next.
12. In the Ready to Install window, review your selections, and then click Next. When the installation is completed, click Finish.

Like AD DS, AD LDS uses multimaster replication, and intrasite replication is configured automatically. However, you can configure the frequency of intrasite replication in Active Directory Sites and Services, just as you do for AD DS intersite replication. Before you can manage AD LDS objects in Active Directory Sites and Services, you must install the necessary schema extensions by importing the MS-ADLDS-DisplaySpecifiers.ldf file. If you know you'll be managing AD LDS with Active Directory Sites and Services, you can import this file when installing the AD LDS instance or later with LDIFDE.

Synchronizing AD LDS with AD DS As you have seen, you can create user accounts and groups for AD LDS authentication manually. Manual user creation or importing users with LDIFDE works well when only a few users must authenticate to the AD LDS application or if the users aren't part of a Windows domain. If the AD LDS instance is installed on a member server, however, you can synchronize AD DS user account information with an AD LDS instance.

12

Adamsync, included in AD LDS, synchronizes Active Directory information with an AD LDS instance. Before you can run Adamsync, you must prepare the target AD LDS instance with the necessary schema changes. The LDIF file ms-adamschemaw2k8.ldf in %windir%\Adam must be imported during installation of the instance or with LDIFDE. Next, import the ms-adamsyncmetadata.ldf file. Finally, you edit the ms-adamsyncconf.xml file, which provides Adamsync with information for the synchronization. For detailed instructions on preparing for AD DS synchronization and running Adamsync, click the Active Directory Lightweight Directory Services node in Server Manager, click "Enable application to consolidate data by synchronizing data from AD DS to AD LDS" in the Resources and Support section, and click the "More about this recommendation" link.



Activity 12-4: Uninstalling AD LDS Instances and Removing the AD LDS Role

Time Required: 20 minutes

Objective: Uninstall the AD LDS instance and remove the AD LDS role.

Description: The application you were using that required AD LDS has been superseded by a new application that doesn't use AD LDS. You remove the AD LDS instance with Control Panel's Programs and Features, and then remove the role in Server Manager.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Click **Start**, **Control Panel**. In Control Panel, double-click **Programs and Features**.

3. Right-click the **ADLDS1** instance and click **Uninstall**. Click **Yes** in the warning message and **Yes** again when warned that you're removing the configuration set. Click **OK** in the message stating that AD LDS was removed successfully, and then close Control Panel.
4. Open Server Manager, if necessary. In the left pane, click the **Roles** node, and then click **Remove Roles** to start the Remove Roles Wizard. Click **Next** in the welcome window.
5. In the Remove Server Roles window, click to clear the **Active Directory Lightweight Directory Services** check box, and then click **Next**.
6. In the Confirm Removal Selections window, click **Remove**. If prompted, restart the server, and log on after the server restarts to finish removing AD LDS.
7. Stay logged on to Server1XX and keep Server Manager open for the next activity.

Active Directory Federation Services

Active Directory Federation Services (AD FS) allows single sign-on access to Web-based resources, even when resources are located in a different network belonging to another organization. A typical situation is a user in Company A needs to access resources in partner Company B with a Web browser, so Company B sets up a secondary account for the Company A user. The user is prompted for credentials when attempting resource access. If the number of users involved in this type of transaction is small, the extra work required to maintain users is minimal. The inconvenience of having to enter credentials each time the resource is accessed might not be a major burden. However, if many users must be maintained or users must communicate with many external companies, a single sign-on might be warranted. AD FS is designed for just this situation.

AD FS Overview

AD FS provides functionality similar to a one-way forest trust, except in a forest trust, domain controllers in each forest must be able to communicate directly with one another without interruption of service. As a result, when forests are hosted on separate corporate networks, firewalls on the networks must be configured to allow Active Directory communication, which raises security concerns. AD FS is designed to work over the public Internet with a Web browser interface. The main purpose of AD FS is to allow secure business-to-business transactions over the Internet; users need to log on only to their local networks. AD FS servers and ADFS-enabled Web servers then manage authentication and access to resources on partner networks without additional user logons.

Like most OS technologies, AD FS has its own set of terms for describing its components. The next sections discuss some terms and components used in the role services that make up AD FS.

Federation Trusts A **federation trust**, like other types of trust relationships, involves a trusting party and trusted party. Because AD FS is designed to facilitate business partnerships, the term “partner” is used instead of “party.” A federation trust is inherently a one-way trust, but a two-way trust could be formed simply by creating a trust in both directions.

A typical business partner relationship involves users on one corporate network accessing resources on another corporate network. For example, with a supplier of goods and a wholesale purchaser of those goods, the supplier is likely to be the trusting partner and the purchaser is the trusted partner. Users at the purchasing (trusted) company might access order entry, inventory, and order status applications and databases at the supplier (trusting) company. In AD FS terminology, the trusted company is referred to as the **account partner**, and the trusting company is referred to as the **resource partner**. In the trust relationship in Figure 12-5, the arrow points from the trusting (resource) partner to the trusted (account) partner. Users in the account partner organization are said to have a federated identity, which describes the agreed-on standards for sharing user identity information among two or more parties. This shared identity information is used to grant users privileges and permissions to resources across organizations.

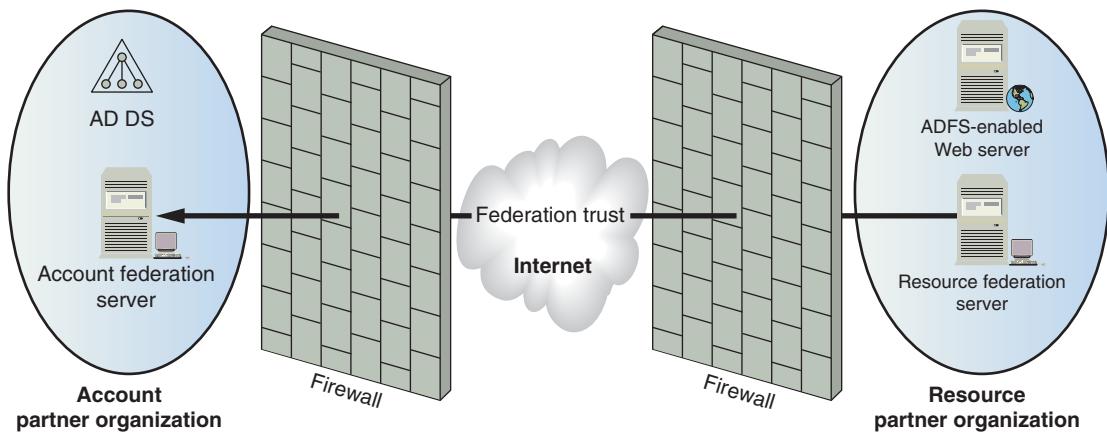


Figure 12-5 A federation trust relationship

Account Partners and Resource Partners User accounts in the account partner can be Active Directory or AD LDS user accounts. The resource partner organization hosts applications and other resources that are accessible to account partner users. When a user in the account partner organization wants to access these resources, a federation server in the account partner's network presents a security token representing the user's credentials to Web resources in the resource partner's network. Based on the security token, the federation server in the resource partner's network grants or denies access. In AD FS parlance, the user credentials packaged in the security token are called claims.

Claims-Aware Applications A **claim** is an agreed-on set of user attributes that both parties in a federation trust use to determine a user's credentials, which specify the user's permissions to resources in the partner's network. Claims typically include a user's logon name and group memberships and can include other attributes, such as department, title, and so forth. A claims-aware application is an ASP.NET application that makes user authorization decisions based on claims packaged in AD FS security tokens.

Windows NT Token Applications Applications that aren't claims aware can still participate in AD FS. These applications rely on Windows NT-style access tokens to determine user authorization. These tokens contain traditional user and group security principal SIDs, and access control lists are used to determine user permissions to a resource. An NT token-based application is an IIS application that relies on standard Windows authentication methods rather than claims. This type of application might be developed by using a legacy scripting language, such as Perl or an older version of ASP that doesn't use the .NET programming interfaces.

AD FS Role Services

The AD FS role consists of four role services that can be installed on one or more servers. The role services that are installed usually depend on whether you're installing AD FS in an account partner's or a resource partner's network:

- **Federation Service**—The function of the Federation Service role service depends on whether the network where it's installed is acting as an account partner or a resource partner. When used in an account partner network, its function is to gather user credentials into claims and package them into a security token. The security token is then passed to the federation service on the resource partner network. The federation service on the resource partner network receives security tokens and claims from the account partner and presents the claims to Web-based applications for authorization. Servers with this role service installed are referred to as **federation servers**.
- **Federation Service Proxy**—Installed on servers in a perimeter network outside the corporate firewall, a **federation service proxy** fields authentication requests from browser clients and passes them to the federation server inside the firewall. A server configured as a federation

service proxy protects the federation server from exposure to the Internet. The Federation Service and Federation Service Proxy role services can't be installed on the same server.

- **AD FS Web agents**—A Web server can host the Claims-aware agent or the Windows token-based agent role service. These servers are called **ADFS-enabled Web servers**. Web agents manage security tokens sent by a federation server to determine whether the user whose credentials are described in the token can access applications hosted by the ADFS-enabled Web server. The two role services that are available are as follows:
 - Claims-aware agent: An AD FS Web agent that handles security tokens using claims.
 - Windows token-based agent: An AD FS Web agent that handles Windows NT-based tokens.

AD FS Design Concepts

AD FS can be deployed in several situations. Depending on the situation, you might use a combination of the AD FS role services to address the organization's federated identity needs. The AD FS designs discussed in the following sections address the federated identity needs most organizations are likely to have.

Web SSO The simplest of the AD FS designs, the **Web SSO** provides single sign-on access to multiple Web applications for users who are external to the corporate network. This design is most often used in consumer-to-business relationships. There's no federation trust between federation servers, as with other AD FS designs, because this design has only one federation server. Usually, it consists of a federation server inside the corporate firewall and a federation proxy server connected to the internal corporate network as well as an Internet-accessible perimeter network. In addition, it contains one or more ADFS-enabled Web servers, also Internet accessible, that are connected to the corporate network. Clients requiring access to Web applications need to log on only once. A username and password must be created for each user in a directory service, such as AD LDS. Credentials are presented to the federation proxy server, which forwards them to the internal federation server, which in turn issues a security token after successful authentication. Figure 12-6 illustrates the following process for authenticating to an ADFS-enabled Web application:



The perimeter network in the figure is sometimes referred to as a DMZ, and there's a firewall (not shown) between the perimeter network and the internal network.

NOTE

1. A user attempts to access an application on the ADFS-enabled Web server.
2. The ADFS-enabled Web server refuses access and redirects the browser to the federation proxy server's logon page.

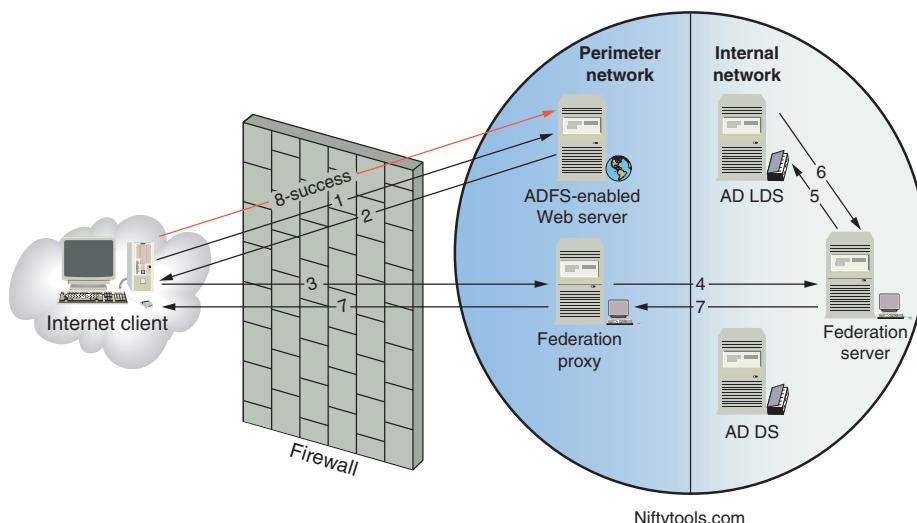


Figure 12-6 Web SSO authentication and authorization

3. The user's browser requests the logon page from the federation proxy server.
4. The user enters logon credentials, and the federation proxy server passes them to the federation server in the internal network.
5. The federation server validates the credentials with a directory server, such as AD LDS.
6. The federation server receives credential information from the directory service and creates the security token.
7. The security token is passed back to the client with the URL of the application on the ADFS-enabled Web server.
8. The client presents the security token to the Web server and accesses the application.

Federated Web SSO The **federated Web SSO** design is similar to Figure 12-5, in which a trust relationship is established between the resource partner and the account partner. A federation server is running on both networks. Although not shown in the figure, federation proxy servers are often used in this design to enhance security. The Web SSO design is inherent in this design, where Internet users who aren't part of the trust can still access Web applications in the resource partner network. In this situation, the account partner users request Web services from the resource partner. The resource partner doesn't authenticate the user locally, but redirects the user back to the federation server in the account partner network. The account federation server validates the credentials and creates a security token for the client to present to the resource federation server. The federation server creates a security token for the client to present to the ADFS-enabled Web server, and the client requests the application. The federated Web SSO design supports business-to-business relationships for collaboration or commerce purposes.

Federated Web SSO with Forest Trust The **federated Web SSO with forest trust** design involves a network with two Active Directory forests. One forest, located in the perimeter network, is considered the resource partner. The second forest, located in the internal network, is the account partner. A forest trust is established between domain controllers in both forests. In this design (see Figure 12-7), internal forest users and external users have access to ADFS-enabled Web applications in the perimeter network. External users have Active Directory accounts in the perimeter forest, and internal users have accounts in the internal forest. This design is used most often when Windows NT token applications are hosted on the Web servers. The AD FS Web agent running in the perimeter network intercepts authentication requests and creates the NT security

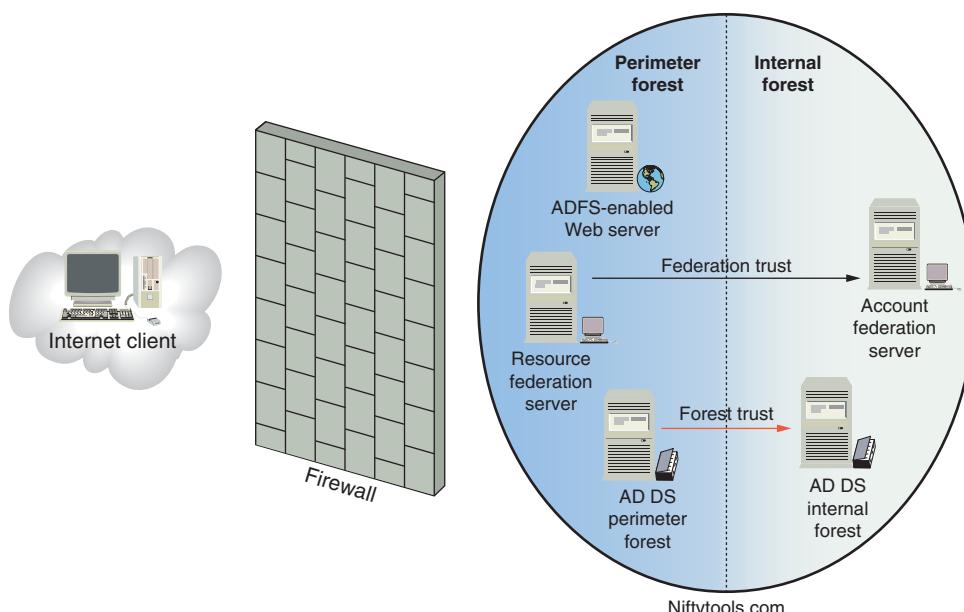


Figure 12-7 The federated Web SSO with forest trust design

tokens the Web applications need to make authorization decisions. The forest trust enables the Web agent to authenticate users from the internal network. External users are authenticated because the Web agent server is a member of the perimeter network forest. The federated Web SSO with forest trust design is most often used in business-to-employee relationships and allows both internal and external employees to access ADFS-enabled Web applications.

Preparing to Deploy AD FS

As discussed, four AD FS role services can be installed with the Add Roles feature in Server Manager. After you have decided on a federation design and know which role services will be installed on which servers, there are a few other requirements to consider:

- AD FS is supported by Windows Server 2003 R2 Enterprise and Datacenter editions and Windows Server 2008 Enterprise and Datacenter editions.
- Federation servers, federation proxy servers, and Web servers hosting AD FS Web agents must be configured with Transport Layer Security/Secure Sockets Layer (TLS/SSL), which is used by the HTTPS protocol. Firewalls must permit HTTPS traffic.
- Web browsers on client computers must have JScript and cookies enabled.
- One or more account stores, such as AD DS or AD LDS, must be running on the network. However, running AD DS on the same server as any AD FS role services isn't recommended.
- Certificates are required by federation servers, federation server proxies, and ADFS-enabled Web servers. Certificates can be requested from a public certification authority (CA) or internally from an AD CS CA. Optionally, you can self-sign certificates, which works well for testing environments.

As you have seen in the figures of AD FS designs, installing and testing AD FS requires a complex network environment and several computers. Setting up and testing AD FS with the simplest design, Web SSO, requires at least four computers. Other designs could require up to eight computers, if proxies are used.

Following is an overview of the steps for implementing a Web SSO design:

1. Install the Federation Service role service on a server in the internal network.
2. Install the Federation Service Proxy role service on a server in the perimeter network (optional).
3. Install the Web Server role service and the AD FS Web Agent role service on your ADFS-enabled Web server.
4. Install AD DS or AD LDS to maintain the account store (the database containing user accounts). With Web SSO designs, AD LDS or a similar LDAP-compatible account store is usually used.
5. Install the claims-aware or Windows NT token-based application on the Web server.

Most of these steps involve several substeps, such as issuing certificates, configuring DNS, and so forth. The Microsoft Technet Web site provides a thorough step-by-step procedure for deploying each AD FS design at <http://technet.microsoft.com/en-us/library/cc771833.aspx>.

Active Directory Rights Management Service

You have learned methods for allowing some users to access information while disallowing other users. Access to digital information stored on computers can be allowed and disallowed by controlling who can authenticate to the servers storing information, assigning permissions to files and folders in the form of DACLs, and using encryption methods, such as EFS. However, what users can do with data after being granted access to it hasn't been discussed.

Active Directory Rights Management Service (AD RMS) helps administrators get a handle on this critical step in securing data. Whether protecting trade secrets, customer account information, or intellectual property, many organizations are struggling with this important facet of network security. With AD RMS, an administrator can create usage policies that define how a document can be used after a user accesses it. Actions such as copying, saving, forwarding, and

even printing documents can be restricted. For example, suppose you send an “eyes only” e-mail to another employee. With AD RMS, you can restrict the recipient from printing the message or forwarding it to someone else.

To be effective, AD RMS requires AD RMS–enabled client or server applications, such as MS Office 2007, Microsoft Exchange 2007, and Microsoft Office SharePoint Server 2007. Developers can also create AD RMS–enabled applications by using the AD RMS Software Development Kit (SDK), available on the Microsoft Web site.

AD RMS Key Features

AD RMS is a new server role in Windows Server 2008, but it requires a client access license for each AD RMS client. A similar product, Rights Management Server (RMS), is available for earlier Windows Server versions, although it must be purchased separately. Some key features of the new AD RMS server role include the following:

- *AD FS integration*—AD RMS can be integrated with AD FS to set up a federated trust between organizations. With AD FS, the benefits of AD RMS can be extended outside the corporate network to ensure document security in business-to-business relationships.
- *AD RMS Server self-enrollment*—An RMS server must connect to the Microsoft Enrollment Service over the Internet to acquire a certificate, which allows the RMS server to issue client licenses and certificates to access protected content. With AD RMS in Windows Server 2008, the server can self-enroll in this certificate, so there’s no need to contact Microsoft servers.
- *Administrator role delegation*—AD RMS enables network administrators to delegate AD RMS responsibilities to different users. There are three AD RMS administrator roles:
 - AD RMS Enterprise Administrator: This role has full administrative authority over an AD RMS installation.
 - AD RMS Auditor: This role can view RMS-related logs and reports.
 - AD RMS Template Administrator: This role can create and manage AD RMS templates.

AD RMS Components

12

An AD RMS environment, like an AD FS environment, consists of several components, usually implemented as separate servers:

- *An AD RMS server*—The AD RMS server role can be installed on one or more servers. Whether it’s installed on one server or multiple servers, the installation is referred to as an **AD RMS root cluster**. Multiple servers can be used for redundancy and load balancing. Only one AD RMS root cluster can be installed in an Active Directory forest. The AD RMS server self-signs a server licenser certificate (SLC), allowing the server to issue AD RMS client licenses and certificates. When the AD RMS role is installed, a number of Web server roles are also installed.
- *An AD RMS database server*—AD RMS uses a database to store AD RMS configuration data and Active Directory group membership information. A SQL database installed on a separate server is recommended for production environments, but you can use the Microsoft internal database for test environments.
- *An Active Directory domain controller*—Servers running the AD RMS server role must be domain members, and users who use or publish AD RMS–enabled content must be in Active Directory with a valid e-mail address.
- *An AD RMS–enabled client computer*—AD RMS client software must be installed on computers using AD RMS content. Windows Vista and Server 2008 computers include the necessary software, and older clients can download it from the Microsoft Web site.

The AD RMS process consists of two distinct actions: publication of AD RMS–protected documents and access of these documents by an AD RMS client. Publication of an AD RMS–protected document requires the user authoring the document to acquire a rights account certificate (RAC)

and a client licenser certificate (CLC). With these certificates, the user can publish AD RMS-protected content, which involves the following steps.

1. Create a document with an AD RMS-enabled application and specify rights for the document. A publishing document with usage policies is created.
2. The document is encrypted by the AD RMS application, and the publishing certificate is bound to the document. The AD RMS server cluster is the only entity that can issue licenses to decrypt the file.
3. The document author can now distribute the application for users to access it.

A user accesses an AD RMS-protected document with the following steps:

1. A user attempts to access the document by using an AD RMS-enabled application.
2. The AD RMS client reads the publishing license.
3. The AD RMS server specified in the publishing license is contacted to request a use license.
4. After verifying that the user is authorized to access the document, the AD RMS server issues a use license to the client.
5. The document is decrypted, and the user can use the document according to the granted rights.

AD RMS Deployment

Before installing the AD RMS role, you must address the following requirements:

- Prepare a domain member server for the AD RMS role; its users should be people who will be using AD RMS-protected content.
- Create a regular domain user account to be used as the AD RMS service account. This account can't be the same account used to install the AD RMS role.
- Make sure the user account for installing AD RMS has the right to create new databases on the SQL server, if you use an external database.
- If an external database is used, install the database server before installing AD RMS.
- Create a DNS CNAME record for the AD RMS cluster URL; this record is used to access the AD RMS service.

When you're ready to install AD RMS, install the role and the required role services in Server Manager with these steps:

1. The Select Role Services window (see Figure 12-8) has the following choices:
 - *Active Directory Rights Management Server*—The main role service required to protect documents from unauthorized use.
 - *Identity Federation Support*—Select this option if you're integrating AD RMS with AD FS to extend document protection outside the corporate network to federated business partners.

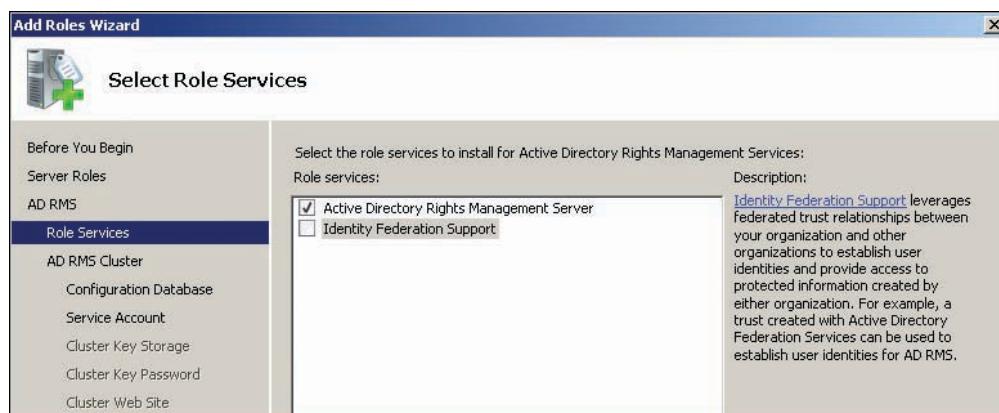


Figure 12-8 The Select Role Services window

- The Create or Join an AD RMS Cluster window (see Figure 12-9) prompts you to create a new AD RMS cluster, which is the only option available if no other AD RMS servers are detected. You can have the current server join an existing AD RMS root cluster, if one is detected in the forest.

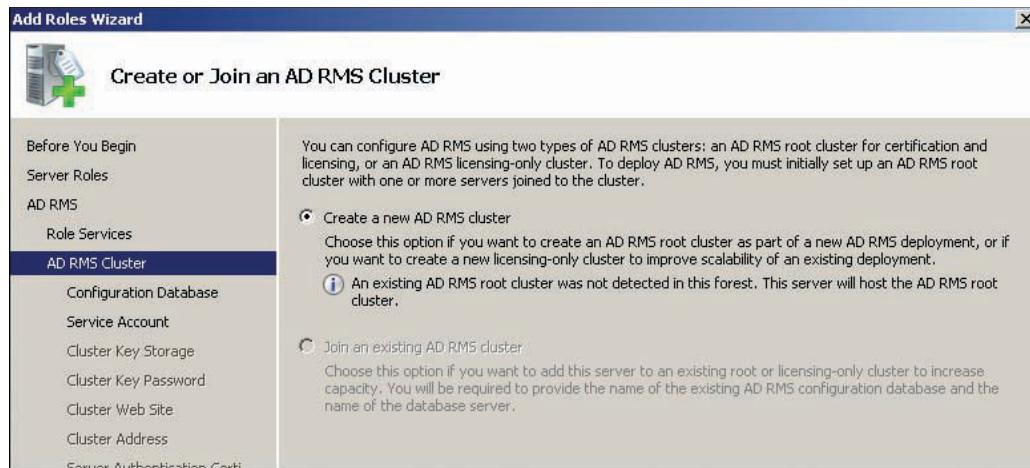


Figure 12-9 The Create or Join an AD RMS Cluster window

- In the Select Configuration Database window, specify where the required database will be hosted:
 - Use Windows Internal Database on this server*—The Windows internal database can be used for test environments or for single-server cluster configurations. If more than one server will participate in the cluster, this option can't be selected.
 - Use a different database server*—If you select this option, you must enter the name of a SQL server and a database instance.
- In the Specify Service Account window, select the account you created to serve as the AD RMS service account.
- In the Configure AD RMS Cluster Key Storage window (see Figure 12-10), you decide how the AD RMS cluster key should be stored:
 - Use AD RMS centrally managed key storage*—This option requires specifying a password to protect an encrypted key, which is shared among all servers in the AD RMS cluster automatically.
 - Use CSP key storage*—This option requires selecting a cryptographic service provider to store the cluster key. If you select this option, the cluster key must be distributed to other servers manually.

12

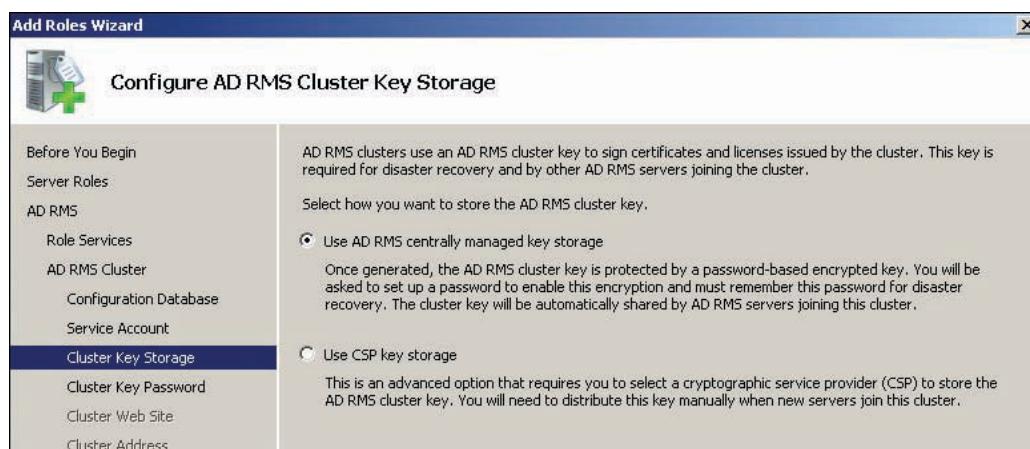


Figure 12-10 The Configure AD RMS Cluster Key Storage window

6. In the next window, enter the cluster key password or select a CSP, depending on your selection on the previous window.
7. The Select AD RMS Cluster Web Site window prompts you to select an IIS virtual directory to host AD RMS. If you set up a virtual directory before starting the AD RMS installation, you select it here; otherwise, the Default Web Site directory is used.
8. The Specify Cluster Address window (see Figure 12-11) prompts you to choose an SSL-encrypted or unencrypted connection type. You can also specify the URL that clients use to access the AD RMS service.

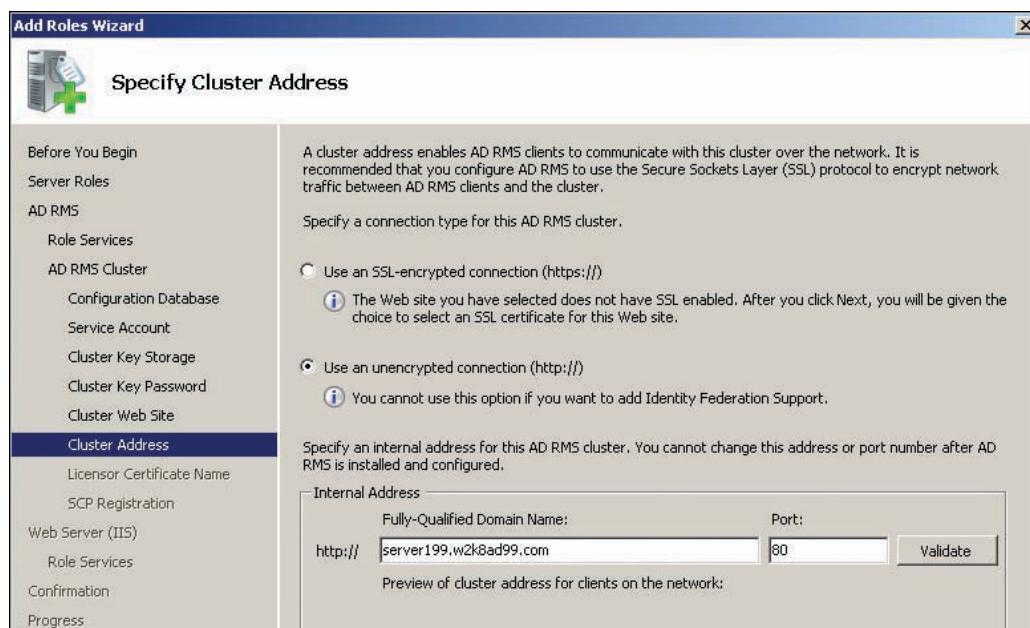


Figure 12-11 The Specify Cluster Address window

9. In the Name the Server Licenser Certificate window, you can specify a friendly name for the certificate used to establish the cluster's identity to clients.
10. In the Register AD RMS Service Connection Point (SCP) window, you can register the SCP now or later. You must be logged on to the domain as a member of Enterprise Admins to register the SCP now. The SCP provides clients with URLs for the AD RMS cluster.
11. The AD RMS portion of the installation is finished. Next, you install the additional IIS role services and confirm the installation.

As you can see, setting up AD RMS takes considerable planning and requires completing several preinstallation tasks. The complexity of this server role, along with AD FS and AD LDS, reflects businesses' growing need to provide users and partners with secure, flexible access to network resources.



The server roles discussed in this chapter are often installed as the only role on a Windows Server 2008 server, so they lend themselves particularly well to virtualization. If you're using AD LDS, AD RMS, or AD FS, consider installing these roles as virtual machines in Hyper-V, discussed in Chapter 2.

Read Only Domain Controllers

Up to now, this chapter has focused on new Active Directory server roles, and this section is no different. However, a read only domain controller (RODC) is not so much a new role as a special implementation of a role you're already familiar with: Active Directory Domain Services.

The RODC was developed to address the need to have a domain controller in a branch office where server expertise and physical security are often lacking. An RODC performs many of the same tasks as a regular domain controller, but changes to Active Directory objects can't be made on an RODC. An RODC maintains a current copy of Active Directory information through replication. However, there are some important differences in the information an RODC keeps that make it more secure than domain controllers. In addition, you should be aware of some factors before installing an RODC in your network. This section discusses the following aspects of using RODCs in a Windows network:

- RODC installation
- RODC replication
- Credential caching
- Administrator role separation
- Read-only DNS

RODC Installation

Before you can install an RODC, you must address these prerequisites:

- A writeable Windows Server 2008 DC that the RODC can replicate with must be operating in the domain.
- The forest functional level must be at least Windows Server 2003.
- If the forest functional level is not set at Windows Server 2008, you must run the adprep /rodcprep command before installing the RODC.

Because an RODC is meant to address the needs of a branch office, administrators can combine the RODC installation with another designed-for-branch-office installation: Server Core, which is Windows Server 2008 without a GUI. On a full Windows Server 2008 installation, you use Server Manager to install a role and Dcpromo.exe to start the Active Directory installation. On a Server Core installation, you start Dcpromo.exe from a command prompt with the /unattend installation option.

Another option for installing an RODC that isn't available with a regular DC is delegated installation. **Delegated installation** doesn't require domain administrator credentials; a regular user at the branch office can perform the installation. To use this feature, you must create a computer account for the server performing the RODC role in the Domain Controllers OU. When you create the account, select the user or group name that can join the computer to the domain (see Figure 12-12).

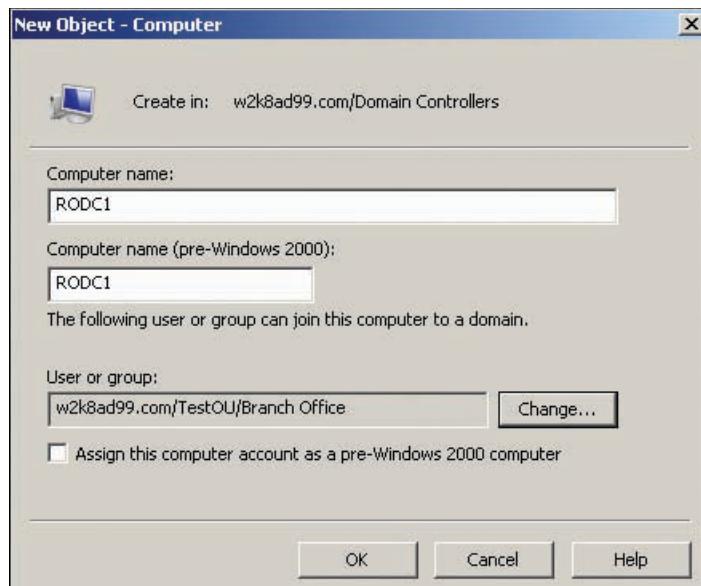


Figure 12-12 Creating an RODC computer account

The server must be a workgroup member, not a domain member, to install the RODC role with delegated installation.



Activity 12-5: Installing an RODC

Time Required: 20 minutes

Objective: Install a domain controller with the RODC option.

Description: You're opening a branch office with about 20 users. No server administrators work in the branch office, and there's no designated equipment room to keep the DC secure. You opt to use an RODC so that branch office users have some benefits of a local DC without the security risks. Before you can install Active Directory Domain Services, you must remove Active Directory Certificate Services because these services can't reside on the same server.

1. Log on to **Server1XX** as Administrator.
2. Open Server Manager and start the Remove Roles Wizard. Click **Next**.
3. In the Remove Server Roles window, click to clear the **Active Directory Certificate Services** check box, and then click **Next**.
4. In the Confirm Removal Selections window, click **Remove**. When the removal is finished, click **Close**.
5. When prompted to restart the server, click **Yes**. When the server restarts, log on as Administrator. The removal of AD CS continues. Click **Close** when the removal is finished.
6. In Server Manager, click the **Roles** node, and then click **Add Roles** to start the Add Roles Wizard. Click **Next**.
7. In the Select Server Roles window, click the **Active Directory Domain Services** check box, and then click **Next**. Read the information in the Active Directory Domain Services window, and then click **Next**.
8. In the Confirm Installation Selections window, read the information messages and click **Install**. When the installation is finished, click **Close**.
9. Open a command prompt window, type **dcpromo**, and press **Enter** to start the Active Directory Domain Services Installation Wizard. Click **Next**. In the Operating System Compatibility window, click **Next**.
10. In the Choose a Deployment Configuration window, click the **Existing forest** option button, and then click **Next**.
11. In the Network Credentials window, the W2k8adXX.com domain and the option to use your current logged-on credentials are selected by default. Click **Next**.
12. In the Select a Domain window, the w2k8adXX.com domain is selected by default. Click **Next**.
13. In the Select a Site window, make sure the **Use the site that corresponds to the IP address of this computer** check box is selected. Click **Next**.
14. In the Additional Domain Controller Options window, click the **Read-only domain controller (RODC)** check box. The DNS server and Global catalog check boxes should be selected by default. Click **Next**.
15. In the Delegation of RODC Installation and Administration window, you can specify a user or group to complete the RODC installation. The user or group members will also have local administrative rights on the server (but not for the domain). If you don't specify a user or group, only members of Domain Admins or Enterprise Admins can continue the installation. You're not delegating administration, so click **Next**.
16. In the Location for Database, Log Files, and SYSVOL window, click **Next**.
17. In the Directory Services Restore Mode Administrator Password window, type **Password01** in the Password and Confirm Password text boxes, and then click **Next**.

18. In the Summary window, click **Next** to start the installation. When the installation is completed, click **Finish**. When you're prompted to restart the computer, click **Restart Now**.
19. Close any open windows, and stay logged on for the next activity.



If theft of the RODC is a likely risk, you can take further precautions to secure its sensitive data by using BitLocker Drive Encryption, which is installed as a server role in Server Manager. With BitLocker, you can secure data on the volume containing the Windows OS and Active Directory as well as on additional volumes.

RODC Replication

Replication on an RODC is unidirectional, meaning the Active Directory database is replicated from a writeable DC to an RODC, but data is never replicated from an RODC to another DC. RODCs can replicate only with Windows Server 2008 writeable DCs. **Unidirectional replication** provides an extra level of security for networks with branch office locations. Even if a server is compromised and someone is able to make malicious changes to Active Directory on the RODC, the changes can't be propagated to DCs in the rest of the network.

To increase security of the Active Directory data stored on an RODC, administrators can configure a **filtered attribute set**, which specifies domain objects that aren't replicated to RODCs. The type of data to filter usually includes credential information that might be used by applications using Active Directory as a data store. Any data that might be considered security sensitive can be filtered, except objects required for system operation. Filtered attribute sets are configured on the schema operations master.

RODC placement in your site topology is important to ensure that replication occurs between an RODC and a Windows Server 2008 DC. A writeable Windows Server 2008 DC is usually placed in the site nearest in the replication topology to the RODC's site. The nearest site is defined as the site with the lowest cost site link. If this placement isn't possible, you must create a site link bridge between the RODC site and a site with a Windows Server 2008 writeable DC.

Credential Caching

By default, neither user nor computer passwords are stored on an RODC. This arrangement makes the RODC more secure, in case an attacker tries to crack locally stored passwords. However, it also negates some advantages of having a domain controller on the local network. If the RODC caches no passwords, each user and computer authentication must be referred to a writeable DC, most likely located across a WAN link. To prevent this problem, **credential caching** can be enabled for a user account on an RODC. The user's password is retrieved from a writeable DC the first time the user logs on, and thereafter, the password is retrieved from the RODC.

Credential caching is controlled by the Password Replication Policy (PRP), accessed in the Properties dialog box of the RODC computer account. A PRP lists users and groups along with a setting of Allow or Deny (see Figure 12-13). Account Operators, Administrators, Backup Operators, and Server Operators are built-in domain local groups added to the PRP with the Deny setting by default. Passwords of these groups' members aren't stored on the RODC. If a user is a member of a group with the Allow setting and a group with the Deny setting, the Deny setting takes precedence.

The PRP also contains groups named Allowed RODC Password Replication Group and Denied RODC Password Replication Group. These two groups are added to the PRP of all RODCs. These groups have no members initially, but administrators can add users or groups to these groups to control password caching on all RODCs centrally. Generally, groups or users with permission to sensitive information should be added to the Denied RODC Password Replication Group. Users who frequently visit the locations where RODCs are deployed might be candidates for membership in the Allowed RODC Password Replication Group.

Besides the default groups added to the PRP for all RODCs, an administrator can customize each RODC's PRP. For example, a group can be created for all users located at a branch office, and this group can be added to the PRP of the RODC at the branch office with an Allow setting.

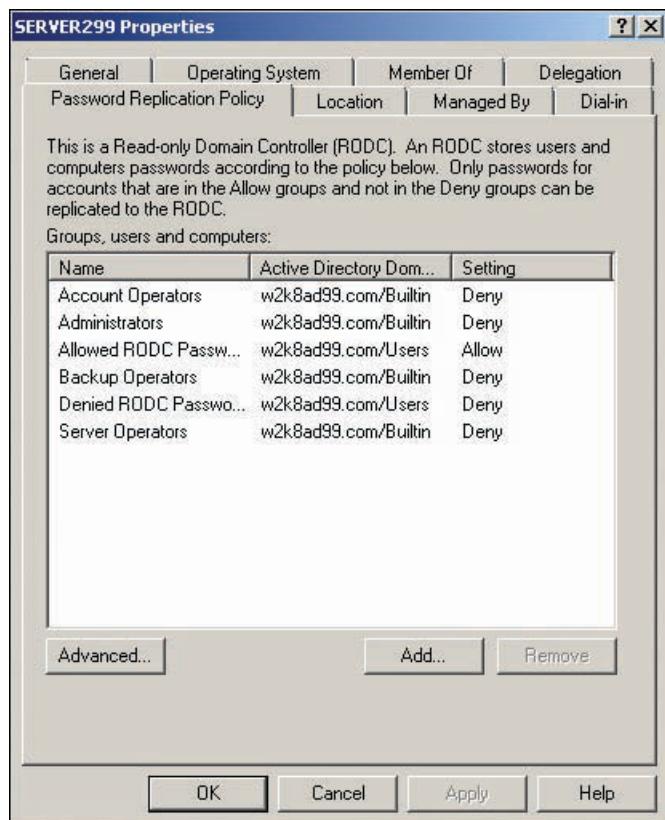


Figure 12-13 The Password Replication Policy tab



Activity 12-6: Configuring Credential Caching

Time Required: 20 minutes

Objective: Create a group and add it to the PRP of the RODC.

Description: You're getting ready to install an RODC at your branch office. Before doing so, you want to make sure office users' credentials are cached by the RODC. Your salespeople will also frequent the branch office and any future branch offices, so you want to make sure their credentials are cached, too.

1. Log on to **Server1XX** as Administrator.
2. Open Active Directory Users and Computers, and click the **Domain Controllers** OU.
3. First, create a new OU and group to represent the branch office users. Click the domain object, and then click the **OU** toolbar icon. In the New Object dialog box, type **Branch1** and click **OK**.
4. Create a new global security group named **Branch1-G** in the Branch1 OU. User and computer accounts located at the branch office should be added to this group.
5. Click the **Users** folder. Double-click the **Denied RODC Password Replication Group** group. Notice that several groups are already members of this group. These group members' passwords aren't replicated to any RODCs in the domain. Click **Cancel**.
6. Double-click the **Allowed RODC Password Replication Group** group. Click the **Members** tab, and then click **Add**. In the Select Users, Contacts, Computers, or Groups dialog box, type **Sales-G**, click **Check Names**, and then click **OK** twice. Now the passwords of all Sales-G members will be replicated to the RODC.
7. In Active Directory Users and Computers, click the **Domain Controllers** OU.

8. In the right pane, right-click **Server1XX** and click **Properties**. Click the **Password Replication Policy** tab, and then click **Add**.
9. Click the **Allow passwords for the account to replicate to this RODC** option button, and then click **OK**.
10. In the Select Users, Computers, or Groups dialog box, type **Branch1-G**, click **Check Names**, and then click **OK**. The credentials of all accounts that are members of the Branch1-G group will be replicated to this RODC. Click **OK**.
11. Close Active Directory Users and Computers and log off to prepare for the next activity.



Activity 12-7: Verifying Credential Caching

Time Required: 20 minutes

Objective: Log on to the RODC and verify whether credentials have been cached.

Description: After configuring credential caching, you want to verify that a user's passwords are being stored on the RODC after the user logs on the first time.

1. Log on to Server1XX as **salesperson1**. Log off and then log on again as **AdvUser1**. Log off and log on again as **Administrator**.
2. Open Active Directory Users and Computers, and click the **Domain Controllers** OU.
3. In the right pane, right-click **Server1XX** and click **Properties**. Click the **Password Replication Policy** tab, and then click the **Advanced** button.
4. Click the **Policy Usage** tab, if necessary. Make sure **Accounts whose passwords are stored on this Read-only Domain Controller** is selected in the drop-down list box (see Figure 12-14). Sales Person1 should be among the objects whose passwords are stored.

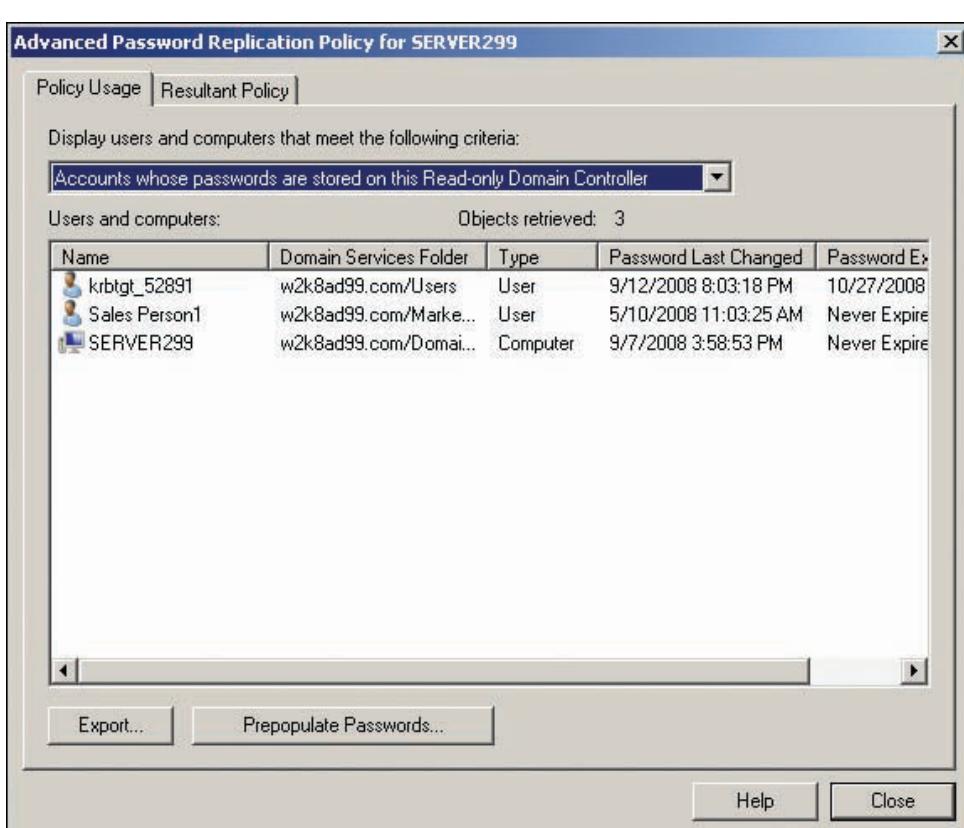


Figure 12-14 The Advanced Password Replication Policy dialog box

5. Click the **Display users and computers that meet the following criteria** list arrow and click **Accounts that have been authenticated to this Read-only Domain Controller**. Notice that each user you have logged on as and the two domain controller accounts are listed.
6. If needed, you can add a user's or computer's password to the RODC (but not a group account) by clicking the Prepopulate Passwords button. By doing so, you transfer the password from a writeable DC to the RODC for the selected user. This transfer prevents the RODC from having to retrieve the password from a DC when the user first logs on to the RODC. Click **Close**, and then click **OK**.
7. Close Active Directory Users and Computers, but stay logged on for the next activity.

Administrator Role Separation

As mentioned, you might want to install an RODC because your branch office has no IT administrator to manage Active Directory. All Active Directory management takes place elsewhere on a writeable DC, and changes are replicated to the RODC. However, you still need someone at the branch office to log on to the RODC to perform maintenance operations, such as system backup and software updates. A writeable DC doesn't have local users and requires a domain account to log on. However, an RODC maintains a local user database, which allows users to log on to perform administrative tasks on the server without needing broader domain-wide permissions. A user logging on with a local user account has administrative capabilities only on the RODC. This feature is called **administrator role separation** and is configured with the Dsmgmt.exe command-line program.



Activity 12-8: Configuring Administrator Role Separation

Time Required: 20 minutes

Objective: Add a domain user as an RODC administrator.

Description: You have set up an RODC at a branch office and have a trusted employee there who you want to handle local administrator tasks on the RODC. However, you don't want to give this user broader administrative permissions in the domain, so you decide to add this user to the Administrators role on the RODC.

1. Log on to **Server1XX** as Administrator, if necessary.
2. Open a command prompt window, and then type **dsmgmt** and press **Enter**.
3. At the dsmgmt prompt, type **local roles** and press **Enter**.
4. At the local roles prompt, type **list roles** and press **Enter**. The roles you can assign to a user, including Administrators, Backup Operators, and so forth, are displayed.
5. Type **add salesperson1 administrators** and press **Enter**.
6. Type **show role administrators** and press **Enter**. The w2k8ADXX\Salesperson1 account should be listed.
7. Type **quit** and press **Enter**, and then type **quit** and press **Enter** again. Salesperson1 is now a local administrator for the RODC.
8. Close the command prompt window.

Read-Only DNS

If you install DNS on an RODC, all Active Directory-integrated DNS zones are read only on the RODC. This is a departure from standard terminology because the zone is still considered a primary zone, even though it's read only. Zone information is replicated from other DNS servers, but zone changes can't be made on the RODC. Client workstations can still perform name resolution queries to the RODC, but workstations in the branch office using Dynamic DNS can't create or update their DNS records on the RODC. Instead, the RODC sends a referral record to the client with the address of a DNS server that can handle the update. To maintain a current DNS database, the RODC requests a single-record replication from the DNS server that updated

the client record. Note that if you attempt to create a new DNS zone on an RODC, you can create only a standard primary, secondary, or stub zone. You can't create a new Active Directory-integrated zone on an RODC.

Chapter Summary

- AD LDS is based on LDAP and provides the functionality of AD DS without some of the structural requirements, such as forests and domains. Multiple instances of AD LDS can be created to support multiple directory-enabled applications.
- AD LDS can be used for directory-enabled applications, directory consolidation, Web application authentication, AD DS application development environments, and migration of legacy X.500 applications.
- AD FS allows single sign-on access to Web-based resources between business partners and in other situations when a single sign-on to diverse Web-based resources is needed. Most business-to-business AD FS environments involve a federation trust between an account partner and a resource partner.
- An AD FS installation involves four role services: Federation Service, Federation Service Proxy, and two AD FS Web agents, Claims-aware and Windows token-based.
- AD RMS extends document security beyond file system permissions. It can restrict not only who can access a document, but also what users can do with a document after accessing it. The AD RMS role requires an AD RMS-enabled application to work.
- AD RMS consists of two distinct actions: publication of AD RMS-protected documents and access of these documents by AD RMS-enabled clients. An AD RMS deployment involves an AD RMS server, an AD RMS database server, an AD DS domain controller, and an AD RMS-enabled client computer.
- RODCs were developed to provide secure Active Directory support in branch office installations where physical server security is lax and there are no on-site server administrators. Before installing an RODC, make sure there's a writeable Windows Server 2008 DC the RODC can replicate with. The forest functional level must be at least Windows Server 2003, and you must run adprep /rodcprep if the functional level isn't Windows Server 2008.
- Replication on an RODC is unidirectional and user passwords aren't stored on the RODC by default. You can configure credential caching if you want the RODC to store passwords of selected users locally. Additionally, you can use administrator role separation to assign administrative roles to local users, but the assigned rights and permissions don't extend beyond the RODC.
- If the DNS Server role is installed on an RODC, Active Directory-integrated zones stored on the RODC are read only, but client computers can use the DNS server for DNS queries.

12

Key Terms

account partner In a federation trust, it's the trusted company whose users will be accessing resources of the trusting company (resource partner). *See also* resource partner.

AD LDS instance A copy of Active Directory Lightweight Directory Services running on a server that has its own data store and communication ports and a unique service name.

AD RMS root cluster One or more servers configured with the AD RMS server role. Multiple servers can be used for redundancy and load balancing.

ADFS-enabled Web servers Web servers that host an AD FS Web agent.

administrator role separation A feature available for RODCs in which a user can be granted local administrative rights on the RODC without needing broader domain administrator capabilities.

claim An agreed-on set of user attributes that both parties in a federation trust use to determine a user's credentials.

configuration sets AD LDS instances containing a replica of an existing AD LDS instance's directory partition. All instances that replicate with one another are referred to as configuration sets.

credential caching The process whereby an RODC can be configured to store passwords of selected accounts on the local server after they are retrieved from a writeable DC. By default, RODCs don't store any password information for user or computer accounts.

delegated installation An RODC installation method that doesn't require domain administrator credentials; a regular user at a branch office can perform the installation.

directory-enabled application An application that uses a directory service to store program, configuration, or user information.

federated Web SSO An AD FS design in which a trust relationship is established between the resource partner and the account partner.

federated Web SSO with forest trust An AD FS design that involves a trust between two Active Directory forests. One forest, located in the perimeter network, is considered the resource partner. The second forest, located in the internal network, is the account partner.

federation servers A server configured to run the Federation Service role service. When used in an account partner network, its function is to gather user credentials into claims and package them into a security token. When used on the resource partner network, it receives security tokens and claims from the account partner and presents the claims to Web-based applications for authorization.

federation service proxy Installed on servers in a perimeter network outside the corporate firewall, this service fields authentication requests from browser clients and passes them to the federation server inside the firewall.

federation trust A trust between two networks using AD FS; one side of the trust is considered the account partner, and the other side is called the resource partner. *See also* account partner and resource partner.

filtered attribute set A collection of attribute data used to specify domain objects that aren't replicated to RODCs, thereby increasing the security of sensitive information.

resource partner In a federation trust, it's the trusting company whose resources are accessed by the trusted company (account partner). *See also* account partner.

unidirectional replication A replication method used with RODCs in which Active Directory data is replicated to the RODC, but the RODC doesn't replicate the data to other domain controllers.

Web SSO An AD FS design that provides single sign-on access to multiple Web applications for users who are external to the corporate network.

Review Questions

1. Your network uses Active Directory running on Windows Server 2008, and your company is about to install an application that integrates with directory services by using LDAP and will require major schema changes. Another application that integrates with a directory service might be installed next year, and it will also require many schema changes that are very different from those the first application requires. Which of the following should you use on your network?
 - a. A new AD DS instance
 - b. One AD LDS instance for each application
 - c. One AD FS instance for each application
 - d. One AD RMS instance for each application
2. Which of the following is true about AD LDS? (Choose all that apply.)
 - a. There's no global catalog.
 - b. Multiple instances on the same server are supported.
 - c. Trust relationships are supported between instances.
 - d. Group policies are supported.

3. AD FS creates an excellent environment for developing AD DS applications. True or False?
4. You have installed AD LDS, and the application using it requires a user account for authentication purposes. The application instructs you to create the user in ADSI Edit. When you connect to the AD LDS instance, you don't find an option to create a user. What should you do?
 - a. Import a user from Active Directory with LDIFDE.
 - b. Uninstall the AD LDS instance in Server Manager and re-create it, being sure to create an application partition.
 - c. Import an LDF file with LDIFDE to modify the schema so that it includes user accounts.
 - d. You can't create users in AD LDS; you must create a group instead.
5. You have been using AD LDS for a few months to support a directory-enabled application. This application has become a critical part of your operations, and there's concern about what might happen if the AD LDS server fails. What should you do?
 - a. Back up the AD LDS server daily, and keep another server on standby.
 - b. Install AD LDS on another server. Create an instance with the option to create a replica of an existing instance.
 - c. Create a second instance of AD LDS on the existing server with the option to create a replica of an existing instance.
 - d. Install AD LDS on another server. Create a new instance of AD LDS on the server, and import the application partition from the existing AD LDS server.
6. In a federation trust, the company whose users are accessing resources is referred to as the _____ partner.
7. What is the term for an agreed-on set of user attributes that both parties in a federation trust use to determine a user's credentials?
8. You're installing AD FS to facilitate transactions with a business partner. You want to keep the federation server secure behind a firewall and don't want direct communication between your partner's computer and the federation server. What should you use?
 - a. Federation service proxy
 - b. AD FS Web agents
 - c. Online responders
 - d. Federated Web SSO with forest trust
9. You have several Web applications that you want trusted Internet clients to be able to access with a single sign-on. The Internet clients aren't from a single company, but can be from anywhere on the Internet. Which AD DS design should you use?
 - a. Web SSO
 - b. Federated Web SSO
 - c. Federated Web SSO with forest trust
 - d. AD FS claims-aware Web agents
10. The federated Web SSO with forest trust design is most often used in business-to-employee applications so that both internal and external employees can access ADFS-enabled applications. True or False?
11. Which of the following isn't a part of a typical AD FS deployment?
 - a. Web browsers with JScript enabled
 - b. Certificates
 - c. An account store
 - d. DHCP

12. Which of the following should be installed to prevent employees from printing security-sensitive e-mails?
 - a. AD LDS
 - b. AD FS
 - c. AD RMS
 - d. AD DS
13. You and another company are engaging in a joint operation to develop a new product. Both companies must access certain Web-based applications in this collaborative effort. Communication between the companies must remain secure, and use of exchanged documents and e-mails must be tightly controlled. What should you use?
 - a. AD CS and AD LDS
 - b. AD RMS and AD DS
 - c. AD FS and AD RMS
 - d. AD LDS and AD RMS
14. Which of the following isn't part of a typical AD RMS installation in a production environment?
 - a. AD RMS database server
 - b. AD DS
 - c. Client certificates
 - d. Microsoft Enrollment Service
15. Which of the following is true about an RODC installation?
 - a. A Windows Server 2008 DC is required.
 - b. The forest functional level must be at least Windows Server 2008.
 - c. Adprep /rodprep must be run in Windows Server 2008 forests.
 - d. Multimaster replication must be used.
16. You need to install an RODC in a new branch office and want to use an existing workgroup server running Windows Server 2008. The office is a plane flight away and is connected via a WAN. You want an employee at the branch office, Michael, to do the RODC installation because he's good at working with computers and following directions. What should you do?
 - a. Add Michael to the Domain Admins group, and give him directions on how to install the RODC.
 - b. Use Dsmgmt.exe to make Michael a local administrator, and give him directions on how to install the RODC.
 - c. Create the computer account for the RODC in the Domain Controllers OU, and specify Michael's account as one that can join the computer to the domain.
 - d. Create a group policy that specifies that Michael's account can join RODCs to the domain. Then use Dsmgmt.exe to specify Michael as an account administrator for the RODC.
17. You have an application integrated with AD DS that maintains Active Directory objects containing credential information, and there are serious security implications if these objects are compromised. An RODC at one branch office isn't physically secure, and theft is a risk. How can you best protect this application's sensitive data?
 - a. Configure the PRP for the RODC and specify a Deny setting for the application object.
 - b. Configure a filtered attribute set and specify the application-related objects.
 - c. Use EFS to encrypt the files storing the sensitive objects.
 - d. Turn off all credential caching on the RODC.

18. You maintain an RODC at a branch office, and you want one employee with solid computer knowledge to perform administrative tasks, such as driver and software updates and backups. How can you do this without giving her broader domain rights?
- Use Dsmgmt.exe to add the user's domain account to the administrator role on the RODC.
 - Create a local user on the RODC and add it to the Administrators group. Have the user log on with that account when necessary.
 - Create a script that adds the user to the Domain Admins group each day at a certain time, and then removes the user from the group one hour later. Tell the user to log on and perform the necessary tasks during the specified time period.
 - Send the user to extensive Windows Server 2008 training, and then add the user to the Domain Admins group.
19. You have installed an RODC at a branch office that also runs the DNS Server role. All DNS zones are Active Directory integrated. What happens when a client computer attempts to register its name with the DNS service on the RODC?
- The DNS service rejects the registration. The client must be configured with a static DNS entry.
 - The DNS service passes the request to another DNS server. After registration is completed, the DNS server that performed the registration sends the record to the DNS service on the RODC.
 - The DNS service creates a temporary record in a dynamically configured primary zone. The record is replicated to other DNS servers, and then is deleted on the RODC.
 - The DNS service sends a referral to the client. The client registers its name with the referred DNS server.
20. You have three users who travel to four branch offices often and need to log on to the RODCs at these offices. The branch offices are connected to the main office with slow WAN links. You don't want domain controllers at the main office to authenticate these four users when they log on at the branch offices. What should you do that requires the least administrative effort yet adheres to best practices?
- Create a new global group named AllBranches. Add the four users to this group, and add the AllBranches group to the Allowed RODC Password Replication group.
 - Add the four users to a local group on each RODC. Add the local groups to the PRP on each RODC with an Allow setting.
 - Add each user to the PRP on each RODC with an Allow setting.
 - Create a group policy and set the "Allow credential caching on RODCs" policy to Enabled. Add the four users to the policy. Link the policy to the Domain Controllers OU.

12

Case Projects



Case Project 12-1: Illustrating a Federated Web SSO Design

This project can be done in groups. Designs should be presented, with discussion of their implementation details.

You have been asked to consult with a publishing company to come up with an AD FS design. The publishing company, WebBooks, wants its largest business partners, several booksellers, to be able to access purchasing and inventory Web applications running on the WebBooks Web servers.

WebBooks has a Windows Server 2008 network with Active Directory. It has a Web server that's publicly accessible through the perimeter network (DMZ) and plans to add a Web server to host the purchasing and inventory Web applications. The applications are

directory enabled, but AD DS shouldn't be used as account, data, or configuration stores for these applications.

Develop an AD FS design, with an accompanying diagram, that WebBooks can use to achieve its goal of giving business partners single sign-on access to its Web-based applications. For clarity, include only one partner bookseller. You should include the following items in your design:

- A diagram, with the account partner and resource partner labeled, showing servers and server roles that will run at both WebBooks and the bookseller location
- An explanation of the role each server will play in the process
- A description of how authentication and authorization to Web applications take place

Case Project 12-2: Devising an AD DS Design with RODC, AD RMS, and AD LDS

This project can be done in groups. Designs should be presented, with discussion of implementation details.

Create a fictitious multilocation company using Windows Server 2008 Active Directory as its primary directory service. Describe the company's line of business and explain why it will benefit from using the following role services and how they will be used:

- AD DS
- AD LDS
- AD RMS
- RODC
- DNS

Keep in mind that the main goal of this project is to create a company in which these role services should be used. Create a diagram showing where servers will be located and which roles will be installed on the servers, and include information about sites. Write documentation explaining why each role service is needed, and include information such as which servers will be global catalog servers and which servers will perform FSMO roles.

Present your project to the class, along with a detailed diagram showing sites, servers, role services, and so forth.

Server Management and Monitoring

After reading this chapter and completing the exercises, you will be able to:

- Perform Active Directory maintenance tasks
- Monitor an Active Directory environment
- Manage a Server Core installation
- Use several command-line tools to manage a Windows Server 2008 environment

You might think that after you have installed, configured, and tested server roles and placed servers into production, you can sit back and relax. For many network administrators, however, the real work has just begun. Computers and operating systems require regular maintenance and monitoring to make sure they're running at peak performance. In addition, regular backups are a must to be able to recover from hardware or software failure.

This chapter discusses Windows and Active Directory backup and restore as well as maintenance tasks for keeping Active Directory in peak operating condition. In addition, you're introduced to tools for monitoring server and Active Directory performance and reliability. Judicious use of these tools can alert you to potential performance problems or operational errors before they affect your network's reliability and performance adversely.

Server Core, a new installation mode in Windows Server 2008, is an ideal candidate for virtualization and as an RODC. This chapter expands on the coverage of Server Core in Chapter 2. Finally, you learn about several command-line tools that can be used to manage a Server Core or full installation of Windows Server 2008.

Active Directory Maintenance

Maintaining an Active Directory environment involves the following tasks:

- Windows server backup and restore
- Active Directory backup and restore
- Active Directory defragmentation



You might also include GPO backup and restore among the list of Active Directory maintenance tasks. This topic was covered in Chapter 7.

NOTE

Windows Server Backup and Restore

Windows Server Backup is new in Windows Server 2008 and supersedes NTBackup.exe from previous server versions. The Administrative Tools folder has a shortcut to Windows Server Backup, but when you try to run it, you're informed that it must be installed with Server Manager, which you do in Activity 13-1. The following list summarizes some noteworthy features and limitations of Windows Server Backup:

- Backups can be run manually or scheduled to run automatically with Task Scheduler.
- You can't choose separate files or folders to back up; you can choose only which volumes you want to back up.
- You can create a system recovery backup that automatically includes all volumes containing critical system data, such as the volume with the Windows folder and the volume with the Active Directory database and log files.
- Manual backups can be stored on network drives, fixed and removable basic disk volumes, and CD or DVD. Tape drives are not supported.
- Scheduled backups require a dedicated fixed or removable disk as the backup destination when you're using Windows Server Backup. (With the Wbadmin command-line program, you can use volumes on a nondedicated disk.) The volume with the OS can't be excluded from the backup. If your server is running as a virtual machine, you can use a virtual disk as the destination.
- Members of the Backup Operators group can perform manual backups only. Only members of the Administrators group can set up scheduled backups. However, you can give other users the Create Scheduled Tasks right by using group policies, if needed.

- You can use a **Volume Shadow Copy Service (VSS)** backup, which means even open files can be backed up.
- By default, Windows Server Backup is configured to back up the local computer, but you can also connect to another computer to back up files remotely.

Although Windows Server Backup is a fine tool for backing up servers, you should be aware of its limitations. It's not a substitute for an enterprise-class backup program, such as Symantec Veritas NetBackup and CommVault Galaxy Backup and Recovery; both offer advanced disaster recovery solutions. These type of programs are called for when you need a comprehensive backup and recovery solution for a large number of servers and servers distributed across multiple sites. Most of these products use a distributed backup strategy, in which backup agents are installed on servers and workstations throughout the enterprise and are controlled by a management console. Network and server administrators who manage large networks should familiarize themselves with these products, but a detailed discussion of them is beyond the scope of this book.



Activity 13-1: Installing Windows Server Backup

Time Required: 20 minutes

Objective: Install Windows Server Backup.

Description: You want to devise a backup program for your server and have decided to use the built-in Windows Server Backup, which must first be installed as a feature in Server Manager.

1. Log on to **ServerXX** as Administrator, and open Server Manager. Click the **Features** node in the left pane.
2. Click **Add Features** in the right pane to start the Add Features Wizard. In the Select Features window, click to expand **Windows Server Backup Features**. Two options are available: Windows Server Backup and Command-line Tools. The Windows Server Backup option installs the MMC snap-in for the backup program as well as the Wbadmin command-line tool. The Command-line Tools option installs tools to create scheduled backups with Windows PowerShell scripts. Click **Windows Server Backup**, and then click **Next**.
3. In the Confirm Installation Selections window, click **Install**.
4. When the installation is finished, click **Close**.
5. Click **Start**, point to **Administrative Tools**, and click **Windows Server Backup** to open the window shown in Figure 13-1. Leave Windows Server Backup open and stay logged on for the next activity.

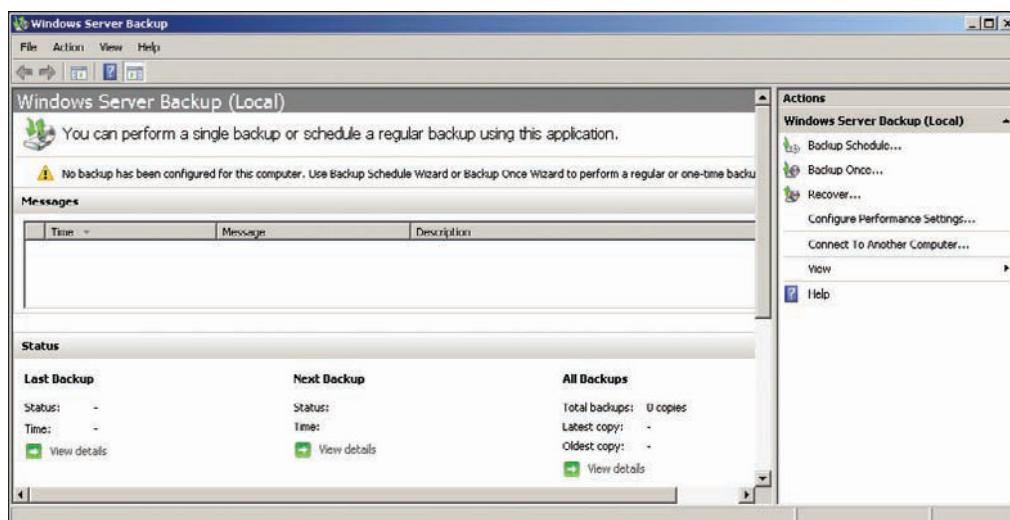


Figure 13-1 The Windows Server Backup window

Windows Server Backup enables administrators to perform one-time backups, schedule regular backups, and perform recovery operations of lost files. You can configure backup performance settings by clicking Configure Performance Settings in the Actions pane (see Figure 13-1) and selecting one of the following options:

- *Always perform full backup*—Saves all files on all volumes to the specified backup media.
- *Always perform incremental backup*—Backs up all files that have changed since the last full or last incremental backup. After a full backup has been made, using incremental backups is much faster and takes less storage space because fewer files must be backed up. However, a restore operation requires the media containing the full backup and all incremental backups made since the last full backup.
- *Custom*—You can select full or incremental backup on a per-volume basis.



Activity 13-2: Performing a One-Time Backup

Time Required: 25 minutes

Objective: Perform a one-time backup with Windows Server Backup.

Description: You want to back up your domain controller. You need to create a volume from free space on one of the server's drives and use that volume to store the backup. (You must have unallocated space on one of your disks that equals or exceeds the size of the space used on the Windows boot volume.)

1. Log on to **ServerXX** as Administrator, and open Server Manager. Click to expand the **Storage** node in the left pane.
2. Click **Disk Management** in the left pane. Right-click unallocated space on Disk 1 (or whichever disk has at least 15 GB of unallocated space) and click **New Simple Volume**. In the New Simple Volume Wizard's welcome window, click **Next**.
3. In the Specify Volume Size window, type **15000** in the Simple volume size in MB text box, and then click **Next**.
4. In the Assign Drive Letter or Path window, click **P** to assign it as the drive letter, and then click **Next**.
5. In the Format Partition window, type **Backup** in the Volume label text box, and then click **Next**. Click **Finish**. The new volume is created, and formatting begins.
6. When formatting of the volume is finished, click **Windows Server Backup** in the left pane of Server Manager.
7. In the Actions pane on the right, click **Backup Once** to start the Backup Once Wizard. In the Backup Options window, you can select the same backup options you used for the previous backup or different options. Because it's your first backup, **Different options** is selected (and is the only available option). Click **Next**.
8. In the Select backup configuration window, the options are Full server, which backs up all volumes on the server, or Custom, which enables you to select backup options. Click **Custom**, and then click **Next**.
9. In the Select backup items window, all volumes needed to perform a system recovery are selected, as is the Enable system recovery check box (see Figure 13-2). You can include other volumes or exclude the volumes needed for system recovery, if needed. For this activity, leave the default settings, and then click **Next**.
10. In the Specify destination type window, verify that the default **Local drives** is selected. (If you're backing up to a network share, you can select Remote shared folder.) Click **Next**.
11. In the Select backup destination window, click the **Backup destination** list arrow, click **Backup (P:)**, if necessary, and then click **Next**.

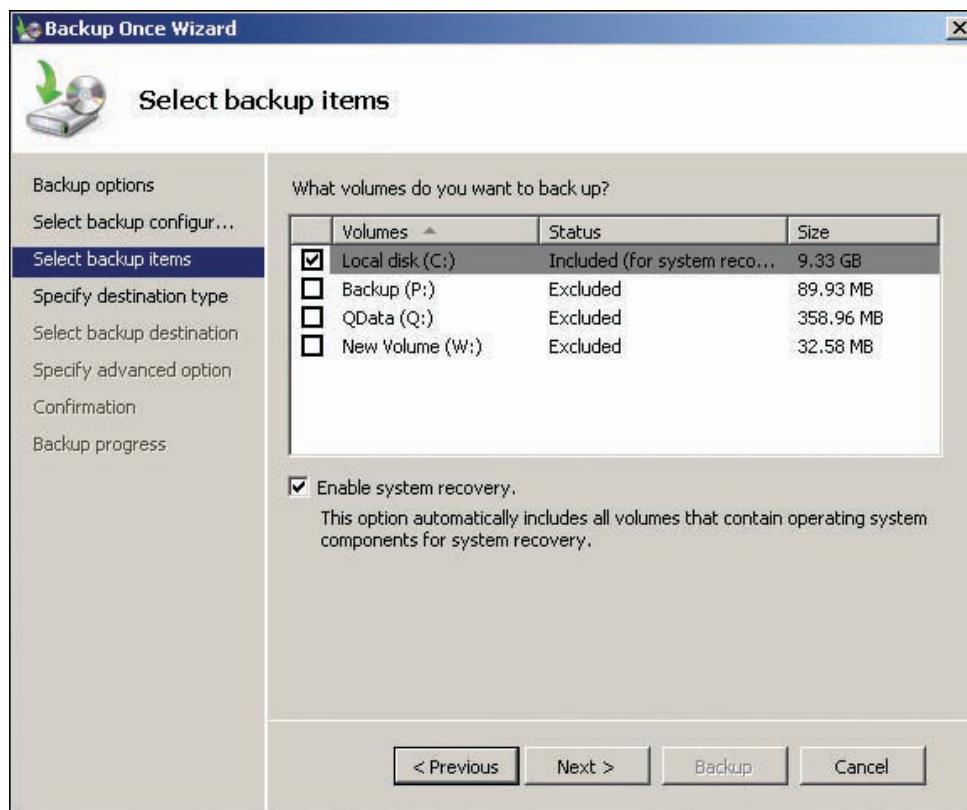


Figure 13-2 The Select backup items window

12. In the Specify advanced option window, you can select a VSS copy backup or a VSS full backup. If you use a third-party backup program, you should choose a VSS copy backup. If you're using Windows Server Backup and will combine full and incremental backups, you should choose a VSS full backup. The full backup option resets the archive bit on each file backed up; the copy backup does not. Click **VSS full backup**, and then click **Next**.
13. In the Confirmation window, review your selections, and then click **Backup**. When the backup is completed, click **Close**. Stay logged on, and leave Windows Server Backup open for the next activity.

13

Creating Scheduled Backups Scheduled backups give you the flexibility to run a backup at a particular time of the day, once per day, or multiple times per day. The Backup Schedule Wizard walks you through creating a scheduled backup. Before using it, make sure you know the answers to the following questions:

- *What do you want to back up?*—You can choose between full server and custom. By default, a full server backup is selected. If you choose a custom backup, you can deselect volumes that aren't needed for a system recovery. Volumes containing data needed for a system recovery can't be deselected.
- *When and how often should the backup occur?*—You can select a time for the backup to occur each day, or you can specify multiple times if you want the backup to occur more than once per day.
- *Where will backups be stored?*—Figure 13-3 shows the Select destination disk window. By default, only external disks are displayed in the Available disks list box. You can click the Show All Available Disks button to see a list of disks that includes internal disks and external disks but doesn't include disks containing system files. Be aware that scheduled

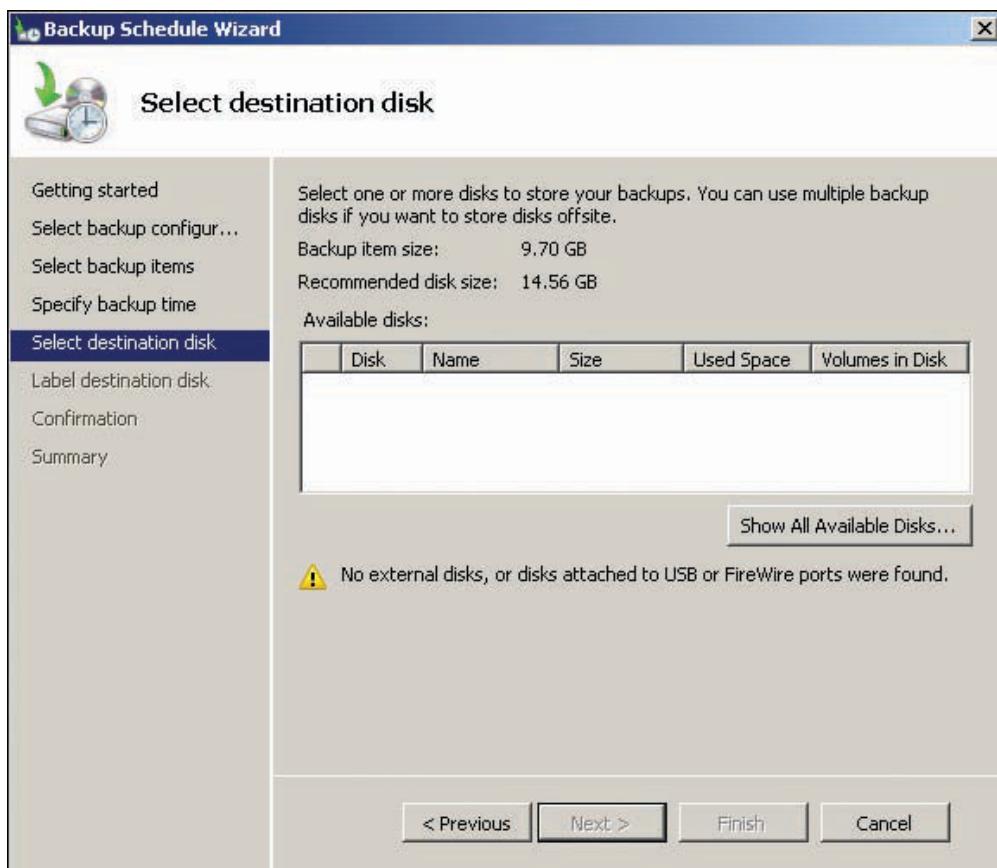


Figure 13-3 The Select destination disk window

backups use the entire disk, not partitions on disks. Disks used for scheduled backup are reformatted, and existing volumes are deleted. Additionally, after a disk has been used in a scheduled backup, it doesn't appear in Windows Explorer.

Data Recovery You can recover files and folders, the system state, Active Directory, or the entire server from a backup, depending on the circumstances. With Windows Server Backup, you can recover only files, folders, and volumes. To recover the system state or perform an Active Directory restore or a complete server recovery, you need to use other recovery methods, discussed later in “Backup and Restore from the Command Line.” To start the recovery process, click Recover in the Actions pane of Windows Server Backup. Some options you have during the recovery process include the following:

- The date and time of the backup from which you want to recover files or volumes, which you select in the Select backup date window of the Recovery Wizard (see Figure 13-4).
- The specific files, folders, or volumes you want to recover. You can also recover specific applications and related data if the application is designed to work with Windows Server Backup and supports VSS.
- If you’re recovering files and folders, you can restore them to their original location or an alternate location. You can also specify what to do if a file already exists in the destination location: Create a copy, overwrite the existing file, or don’t recover the file. Last, you can choose whether to restore a file’s security setting. These options aren’t available when you’re recovering a volume.

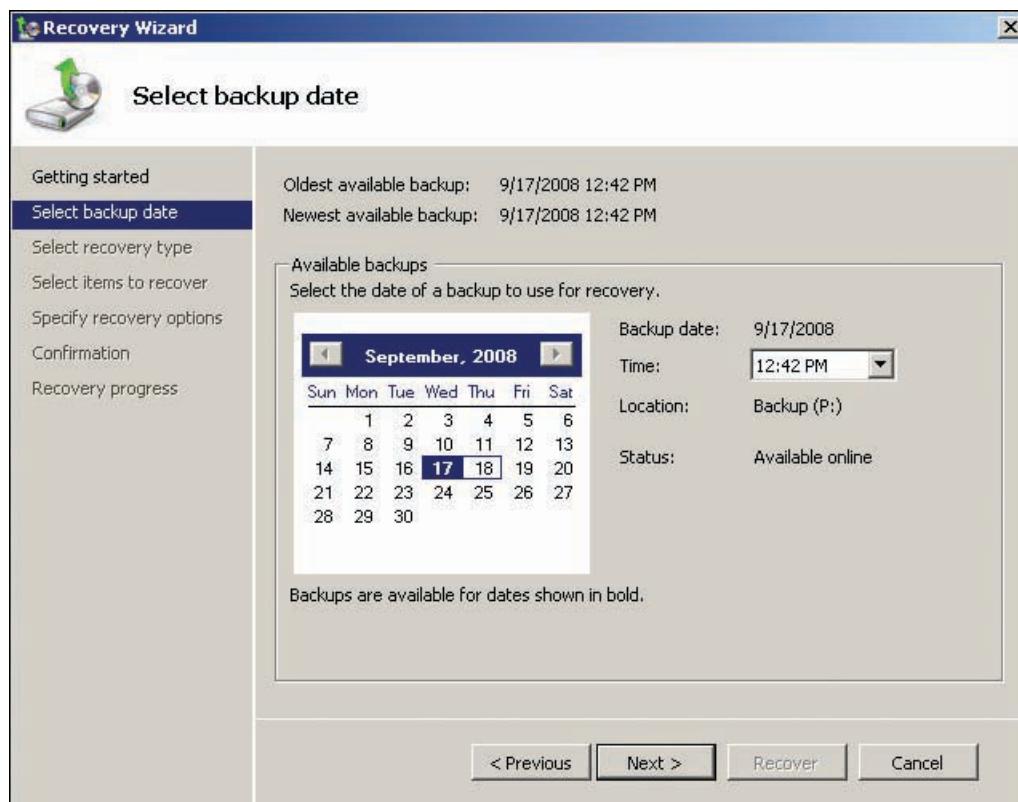


Figure 13-4 The Select backup date window



Activity 13-3: Recovering a File from Backup

13

Time Required: 10 minutes

Objective: Recover a file from backup.

Description: You have backed up your server with the Windows Server Backup program. Because you have just started using this program, you want to run through the process of restoring files. You recover a test user's profile folder after deleting the profile.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Open an Explorer window and navigate to the **C:\Users** folder. Click the **salesperson1** folder and press **Delete**. In the Delete Folder message box, click **Yes**. Close Windows Explorer.
3. If necessary, open Server Manager, click to expand the **Storage** node in the left pane, and then click **Windows Server Backup**.
4. Click **Recover** in the Actions pane to start the Recovery Wizard. In the Getting started window, verify that the **This server (ServerXX)** option button is selected, and then click **Next**.
5. In the Select backup date window, because you have created only one backup, it should already be selected. Click **Next**.
6. In the Select recovery type window, make sure the **Files and folders** option is selected, and then click **Next**.
7. In the Select items to recover window, under Available items, click to expand **ServerXX**, **Local disk (C:)**, and **Users**, and then click the **salesperson1** folder. All files and subfolders are listed in the right pane (see Figure 13-5). Click **Next**.

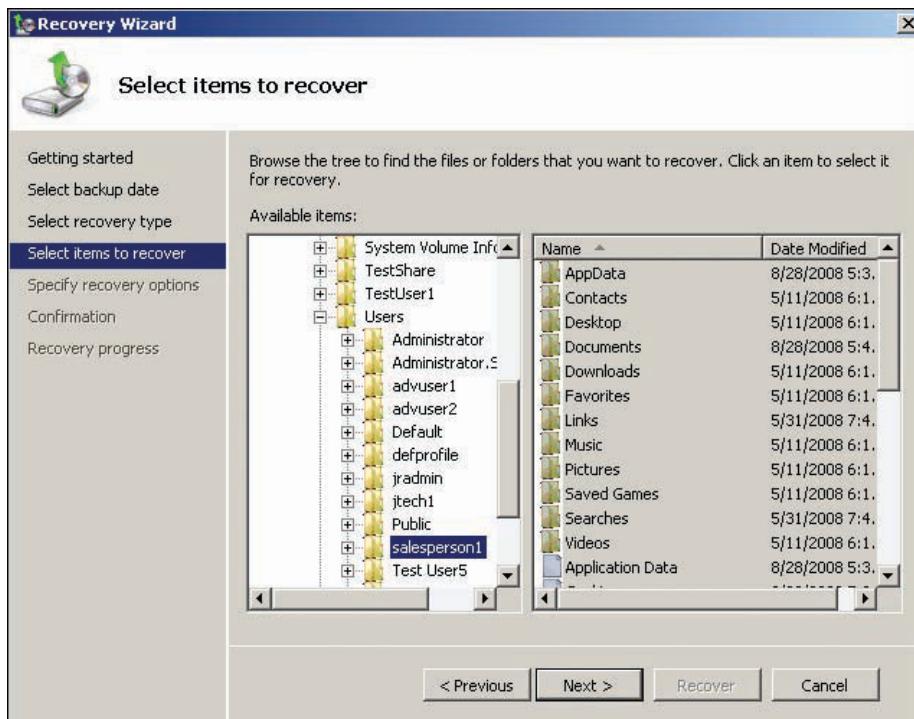


Figure 13-5 The Select items to recover window

8. You get a message stating that one or more system files are selected for recovery and recovery can't be made to the original location. Click **OK**.
9. In the Specify recovery options window (see Figure 13-6), click **Browse**. In the Browse For Folder dialog box, navigate to **C:\Users**, and then click **Make New Folder**. Type **salesperson1** for the folder name, click **OK**, and then click **Next**.

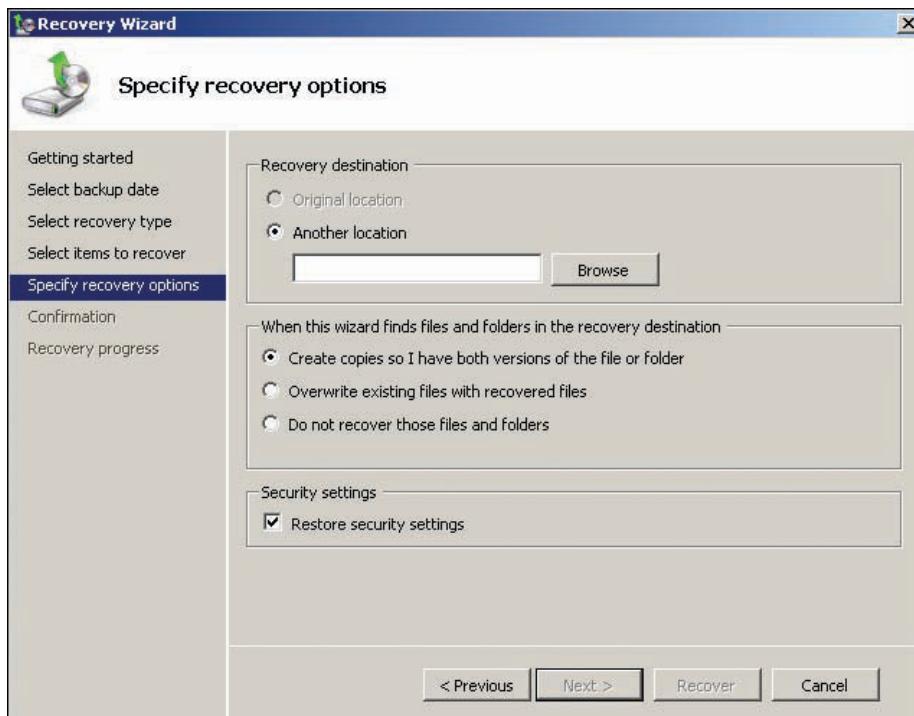


Figure 13-6 The Specify recovery options window

10. In the Confirmation window, click **Recover**.
11. In the Recovery progress window (see Figure 13-7), click **Close** when the recovery is finished.

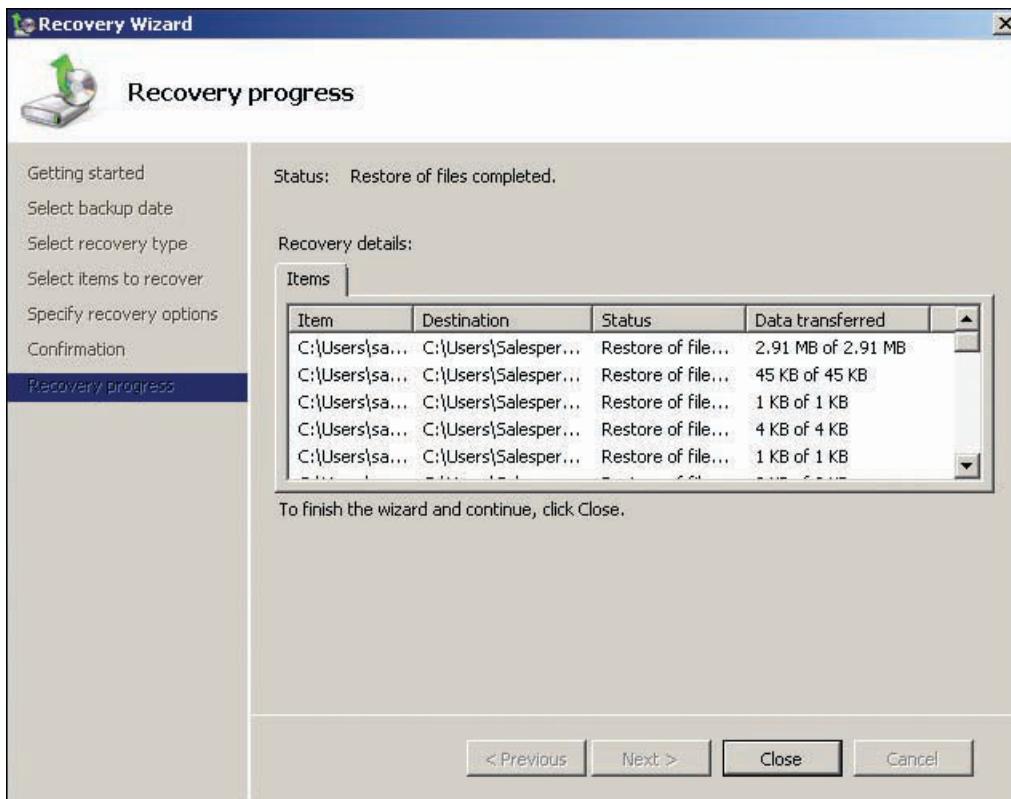


Figure 13-7 The Recovery progress window

12. To verify that the recovery was successful, open Windows Explorer, navigate to **C:\Users\salesperson1**, and confirm that the files have been recovered. Close all open windows, and stay logged on for the next activity.

13

Backup and Restore from the Command Line Windows Server Backup works well for backing up full volumes and servers and restoring files, folders, and volumes. However, as is often the case, the command-line program has the flexibility to perform more specific tasks. With Wbadmin.exe, you can perform all the tasks available with Windows Server Backup and more. You can also use it in a batch file or scripts to perform scheduled backups with Task Scheduler. Some tasks you can perform with Wbadmin but not Windows Server Backup include the following:

- *Perform a system state backup*—Use the command “wbadmin start systemstatebackup” to begin a backup of the system state. A system state backup on a domain controller includes the Registry, boot files, the Active Directory database, the Sysvol folder, some system files, and other files, depending on roles installed on the server.
- *Recover the system state*—To start a system state recovery, including the Active Directory database, use the “wbadmin start systemstaterecovery” command.
- *Delete a system state backup*—The “wbadmin delete systemstatebackup” command deletes one or more system state backups.
- *Restore or delete a backup catalog*—A backup catalog is generated each time a backup is performed. The catalog stores details about each backup and must be available when a recovery procedure is attempted. If the catalog becomes corrupt or deleted, it must be restored before backups can be accessed. To restore a catalog, use the “wbadmin restore catalog” command. To delete a catalog, use the “wbadmin delete catalog” command.

To perform most tasks with the Wbadmin program, you must be a member of the Backup Operators or Administrators group. You must also open a command prompt window with elevated privileges (by right-clicking the command prompt and clicking Run as administrator) if you aren't logged on with the Administrator account.



You can download Ntbackup, available in previous Windows versions, and use it to restore backups created with Ntbackup to a Windows Server 2008 system. However, you can't use it to create backups on a Windows Server 2008 server.

Perform a System Recovery If you must perform a full recovery of your OS because of a disk crash or similar failure, you need the Windows Server 2008 installation disk or access to **Windows Recovery Environment (WinRE)**. You can install WinRE on your server's hard drive and access it by pressing F8 when the boot process starts. You can also access WinRE by booting to the Windows Server 2008 installation DVD and selecting the Repair Your Computer option. Installing WinRE on your hard drive is recommended because the installation DVD might not always be available. You can restore a complete backup from a local or removable disk or a network location.

Active Directory Backup and Restoration

Active Directory is backed up when you perform a full backup of a domain controller or when you back up the volumes containing system recovery information. The Active Directory database is also backed up when you perform a system state backup with Wbadmin.

An Active Directory restoration can be nonauthoritative or authoritative. A **nonauthoritative restore** restores the Active Directory database, or portions of it, and allows it to be updated through replication by other domain controllers. An **authoritative restore** ensures that restored objects aren't overwritten by changes from other domain controllers through replication.

A nonauthoritative restore of Active Directory is usually done when the Active Directory database is corrupt or when you're doing a full server recovery. For a nonauthoritative restore, you must restart the domain controller in Directory Services Restore Mode (DSRM). To do so, press F8 when the server begins to boot to access the Advanced Boot Options menu (see Figure 13-8). After

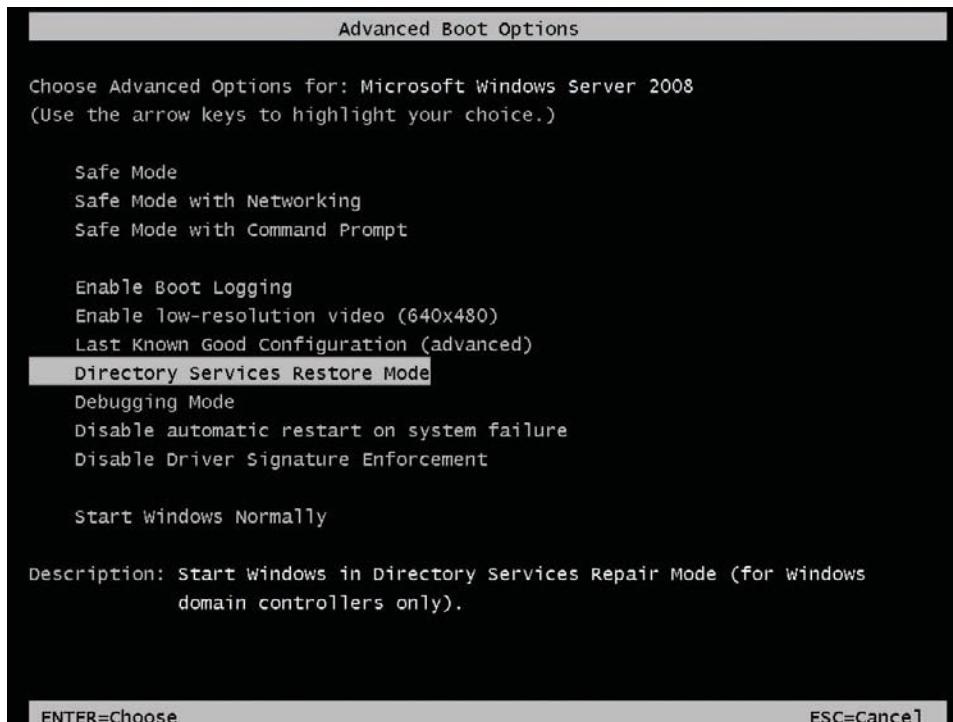


Figure 13-8 The Advanced Boot Options menu

Windows boots into DSRM, log on and run Wbadmin to restore from a system state backup or from a backup that includes all critical volumes. After the restoration, restart the server, and Active Directory replication updates the DC with any objects changed since the backup was created. If you have only one DC, any changes to Active Directory since the last backup are lost.

An authoritative restore is necessary when an Active Directory object has been deleted accidentally. After the restoration, the restored objects are replicated to other domain controllers, instead of other DCs replicating Active Directory information to the restored domain controller, as with a nonauthoritative restore. An authoritative restore is started the same way as a nonauthoritative restore. Before you restart the server after the restore, however, run Ntdsutil to specify which objects are authoritative. You must know these objects' distinguished names.



Activity 13-4: Backing Up the System State with Wbadmin

Time Required: 25 minutes or longer

Objective: Back up the system state with Wbadmin.

Description: System state backups run faster and take less space than complete volume backups. You want to create periodic system state backups separate from your scheduled full backups so that Active Directory can be restored quickly if necessary. You specify the P volume you created earlier as the backup target. You must have enough free space on the P volume, so if necessary, delete the existing backup first.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Open a command prompt window, type **wbadmin start systemstatebackup -backuptarget:P:**, and press **Enter**.
3. You're prompted to start the backup from Local Disk (C:) to P. Type **y** and press **Enter**.
4. The backup must first identify all system state files, and you see progress displays as Wbadmin finds the files. When the files are found, the backup begins. (It might take several minutes.) Wbadmin displays progress lines periodically to show the percentage complete. When the backup is finished, a log of files backed up successfully is created in the C:\Windows\Logs\WindowsServerBackup folder. Close the command prompt window.
5. To view files in the backup, open Windows Explorer and navigate to **P:\WindowsImageBackup\ServerXX**. You'll see a folder named SystemStateBackup where the backup you created is stored. You should also see a folder named Catalog that holds the files composing the catalog of backups.
6. Close Windows Explorer, but stay logged on for the next activity.



Activity 13-5: Restoring Active Directory from a System State Backup

Time Required: 25 minutes

Objective: Restore Active Directory from a backup.

Description: You need to test the effectiveness of a system state backup and the capability to restore Active Directory. On a test DC where you have created a system state backup, you delete an OU from AD, and then perform an authoritative restore on the deleted object.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Open Active Directory Users and Computers. Click **TestOU** and press **Delete**. When prompted to confirm the deletion, click **Yes**.
3. The Confirm Subtree Deletion message box opens. Click the **Use Delete Subtree server control** check box (see Figure 13-9) so that delete-protected objects can be deleted, and then click **Yes**.

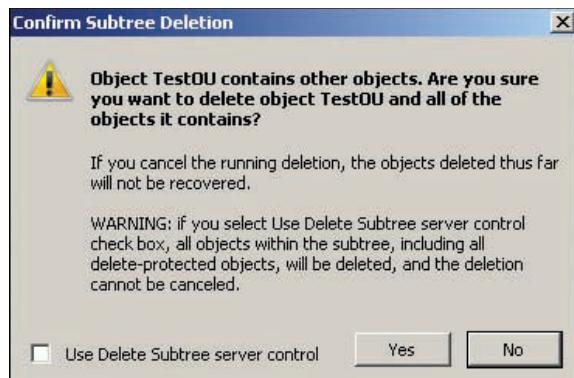


Figure 13-9 The Confirm Subtree Deletion message box

4. When the deletion is finished, restart ServerXX. In the Shutdown Event Tracker dialog box, type **Test AD Restore** in the Comment text box, and then click **OK**.
5. When your server begins to restart, press **F8**. Press **F8** several times until the Advanced Boot Options menu is displayed.
6. In the Advanced Boot Options menu, press the down arrow key to highlight **Directory Services Restore Mode**, and then press **Enter**.
7. You must log on with the *local* Administrator account and the DSRM password, which should be **Password01**. To do so, click **Switch User**, and then type **Administrator** in the User Name text box and **Password01** in the Password text box. “Safe Mode” is displayed in the corner of the desktop.
8. Open a command prompt window. You must get a list of the available backups before you can restore the system state. Type **wbadmin get versions -backuptarget:P:** and press **Enter**. After a minute or so, a list of backups is displayed. Make note of the version identifier of the most recent backup, which is the system state backup you created in Activity 13-4.
9. To begin the recovery, type **wbadmin start systemstaterecovery -version:*DateTime* -backuptarget:P:** (replacing *DateTime* with the version identifier you noted in Step 8) and press **Enter**. When prompted to start the recovery operation, type **y** and press **Enter**.
10. The restoration will probably take several minutes. When it’s finished, you must mark deleted objects as authoritative. Because this server is the only writeable domain controller running, normally this step isn’t necessary, but you should go through the steps so that you’re familiar with the process. With a nonauthoritative restore, you would simply restart the server to complete the restoration. Do *not* restart your server, however.
11. Type **ntdsutil** and press **Enter** to start this utility. Type **activate instance ntds** and press **Enter**. Type **authoritative restore** and press **Enter**. At the authoritative restore prompt, type **restore subtree ou=TestOU,dc=w2k8adXX,dc=com** and press **Enter**. When the Authoritative Restore Confirmation dialog box opens, click **Yes**. Type **quit** and press **Enter** and type **quit** again and press **Enter**. The restore command specifies the object to restore authoritatively. The rest of the Active Directory database is stored nonauthoritatively.



To restore the entire database authoritatively, use the command **restore database** instead of **restore subtree**.

NOTE

12. Close the command prompt window, and restart the server. In the Shut Down Windows dialog box, type **Restore TestOU** in the Comment text box and click **OK**. Your server might restart several times to complete the restoration.
13. Log on as the domain Administrator. The system state recovery performs some final tasks, opens a command prompt window, and displays a “Completed successfully” message. Press **Enter** to continue when prompted.

14. Open Active Directory Users and Computers, and click **TestOU** to verify that the objects have been restored.
15. Close Active Directory Users and Computers, and stay logged on for the next activity.

Active Directory Defragmentation

To maintain performance and efficiency, the Active Directory database requires periodic maintenance in the form of defragmentation and compaction. There are two methods of Active Directory defragmentation: online and offline. **Online defragmentation** occurs automatically when Active Directory performs garbage collection. Garbage collection runs every 12 hours on a DC and removes objects that have been deleted for more than 180 days. Objects that have been deleted but not removed are referred to as “tombstoned.” When an Active Directory object is deleted, it’s not actually removed from the database, much as a deleted file isn’t physically erased from the file system. Instead, the object is marked for deletion and left in the database for a period called the **tombstone lifetime**, which by default is 180 days. During garbage collection, tombstoned objects older than the tombstone lifetime are removed from the database.

The tombstone lifetime has important implications for Active Directory backups. Suppose the tombstone lifetime is set to its default 180 days, and the Active Directory database is backed up on day 1. A user account, Julie, is deleted on day 3. On day 15, the database on a DC becomes corrupted and must be restored from backup. The backup from day 1 is used for the restore, which is before the Julie account was deleted. However, because other DCs still have a record of the Julie account as being deleted, replication deletes the Julie account on the DC being restored. Generally, this result is what you want.

Now suppose the tombstone period is only 10 days. In the same situation, the Julie account is removed from the database during garbage collection on day 13. When the database is restored, the Julie account is restored with it, but the other DCs have no record of the Julie account being deleted, so the account remains, which probably isn’t what you want. Because of this potential database inconsistency, an Active Directory backup is considered invalid if it’s older than the tombstone lifetime. The tombstone lifetime applies to the entire forest and can be changed by using Attribute Editor on the ForestRootDomain object.

Online defragmentation removes deleted objects and frees up space in the database, but it doesn’t compact the database to close up gaps that deleted objects create in the database. **Offline defragmentation** is necessary to keep the database lean and efficient. In previous Windows Server versions, you had to restart the DC in DSRM to perform offline defragmentation, which interrupts other services running on the DC. In Windows Server 2008 Active Directory, offline maintenance is possible because the Active Directory service can be stopped for performing maintenance and then restarted. Microsoft refers to this method as “restartable” Active Directory. Using this method, a server restart isn’t required. However, another DC must be online before you can stop the Active Directory service so that users can continue to log on. While Active Directory is stopped, DNS on that DC stops servicing queries, so client computers should have the address of an alternate DNS server configured, too.

Like a file system, a database becomes fragmented over time because of object deletion and creation. Where deleted objects once were, gaps in the database are created, which makes the database less efficient in performance. Compacting the database removes the gaps, much as defragmenting a hard drive does for the file system.

Active Directory compaction is performed with the Ntdsutil program. The database can’t be compacted in place, so a copy is made to a location you specify. After compaction is finished, the compacted database is copied to the original location.

13



Activity 13-6: Performing Active Directory Maintenance

Time Required: 25 minutes

Objective: Compact the Active Directory database.

Description: Periodic Active Directory database compaction is recommended to keep Active Directory in optimal condition. Your RODC (Server1XX) should be running while you’re performing this operation. Also, you should configure your server with the address of your RODC

as an alternate DNS server. You create folders to hold temporary copies of the database, stop the Active Directory service, and then compact the database with one of the folders you created as the destination. First, you make a copy of the original database in case a problem occurs with compaction, and then you must delete the Active Directory log files and copy the compacted database to replace the original database.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Open the Properties dialog box of the Local Area Connection. In the Internet Protocol settings, change the Alternate DNS Server setting to the address of your RODC, which should be 192.168.100.1XX. This step is done as a precaution. Because DNS doesn't respond to DNS queries while Active Directory is stopped, ServerXX might need to contact a DNS server if you have to log on after Active Directory is stopped. This can happen, for example, if your screen saver comes on and requires a password to access the desktop. Close any open dialog boxes.
3. Create two folders in the root of the C drive: **tempAD** and **backupAD**.
4. Open Server Manager. Click to expand the **Roles** node, if necessary and click **Active Directory Domain Services**. In the System Services section in the right pane, click **Active Directory Domain Services** and click **Stop**.
5. When prompted, click **Stop Dependent Services**.
6. Open a command prompt window, and type the following commands, pressing **Enter** after each one: **ntdsutil activate instance ntds files**, and **compact to c:\tempAD**.
7. The Defragmentation Status display shows the progress of compaction. When you see a message stating that you need to copy the new file over the old file and delete the log files, type **quit** and press **Enter**, and then type **quit** and press **Enter** again.
8. To copy the original database file to the backup folder you created, type **copy c:\windows\ntds\ntds.dit c:\backupAD** and press **Enter**.
9. To delete the log files, type **del c:\windows\ntds*.*.log** and press **Enter**.
10. To copy the compacted database over the original database, type **copy c:\tempAD\ntds.dit c:\windows\ntds\ntds.dit** and press **Enter**. Type **y** and press **Enter** to confirm the copy.
11. Next, to verify the integrity of the new database, type the following commands, pressing **Enter** after each one: **ntdsutil activate instance ntds files**, and **integrity**. Assuming the integrity check was successful, type **quit** and press **Enter**. If it wasn't successful, copy the backup from C:\backupAD to C:\Windows\Ntds, and attempt the compaction process again, starting with Step 6.
12. To check the semantic database integrity (which is recommended), type **semantic database analysis** and press **Enter**, and then type **go fixup** and press **Enter**. Type **quit** and press **Enter**, and then type **quit** and press **Enter** again.
13. To restart Active Directory, in Server Manager, click **Active Directory Domain Services** in the System Services section and click **Start**. You can verify a successful startup by checking the most recent events in the event log. Shortly after the service starts, a new event with ID 1000 should be created, indicating a successful Active Directory start. (If the event doesn't appear, click **Refresh Events**.)
14. Close all open windows, and stay logged on to ServerXX for the next activity.

Active Directory Monitoring

Monitoring Active Directory mainly involves monitoring the performance of the server on which AD DS is running. However, you can also measure several Active Directory-specific performance points. This section discusses general server-monitoring tools, with a focus on Active Directory performance. You also review some tools designed to monitor certain aspects of Active Directory.

If the AD DS server is performing well, AD DS performance is likely to follow suit. Server performance depends on having enough resources to handle tasks required of the system.

Windows Server 2008 provides tools to manage and monitor server operation and resources, including the following:

- Event Viewer
- Task Manager
- Reliability and Performance Monitor
- Windows Server Resource Manager

Event Viewer

Administrators use Event Viewer to examine event log entries generated by system services and applications. A typical event log can contain hundreds or thousands of events, but usually, administrators are interested in events that indicate a problem. Events are categorized by these levels:

- *Information*—Indicated by a blue *i* in a white circle, these events indicate normal operations, such as service stops and starts.
- *Warning*—Indicated by a black *!* inside a yellow triangle, warnings provide information about events that should be brought to the administrator's attention. Warnings aren't necessarily an indication of a problem, but are often an indication of a condition that can lead to a more serious error.
- *Error*—Error events, indicated by a white *!* inside a red circle, are often generated when a process or service is unable to perform a task or stops unexpectedly. Error messages should be addressed immediately, as they indicate a configuration error or an operational problem.

You can examine several log files in Event Viewer (see Figure 13-10), including the Application, Security, and System logs. For Active Directory events, you can view the Directory Service log. AD DS generates many events, but you're usually most interested in warning and error events. By clicking the Level column header, you can sort events and group them by level to spot the most serious events easily. When an event is selected, descriptive information about it is displayed in the bottom pane of the General tab. The Details tab shows additional technical data about the event. For many events, you can also click the Event Log Online Help link in the General tab to get more information.

13

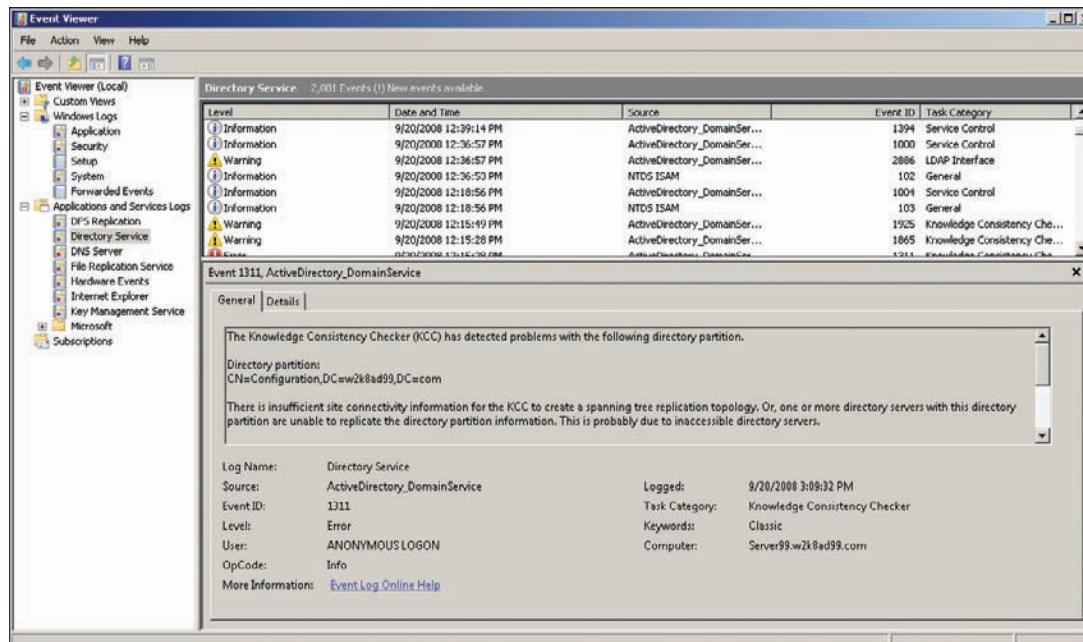


Figure 13-10 Available logs in Event Viewer

Because Active Directory is tightly integrated with DNS, you also need to review the DNS Server logs on DCs configured with this role. The DNS Server log contains events pertaining to availability and replication of zone data as well as the status of the DNS Server service. In addition, the DFS Replication log displays events related to Sysvol replication, which is important for replication of GPOs, scripts, and other files in the Sysvol share.

Task Manager

Task Manager provides a straightforward look at the performance of a Windows computer. It gives you a real-time view of running processes and the resources they're using. In addition, you can fine-tune certain aspects of running processes' performance. To start Task Manager, you can right-click the taskbar and click Task Manager, press Ctrl+Alt+Delete and click Start Task Manager, or type Taskmgr at a command prompt.

Notable additions to Windows Task Manager in Windows Server 2008 are a Services tab and Resource Monitor, opened from the Performance tab. The Services tab displays a snapshot of loaded services and access to the Services MMC with the click of a button. Resource Monitor (see Figure 13-11) shows a real-time graphical display of these key performance indicators:

- CPU utilization
- Disk utilization
- Network utilization
- Memory utilization

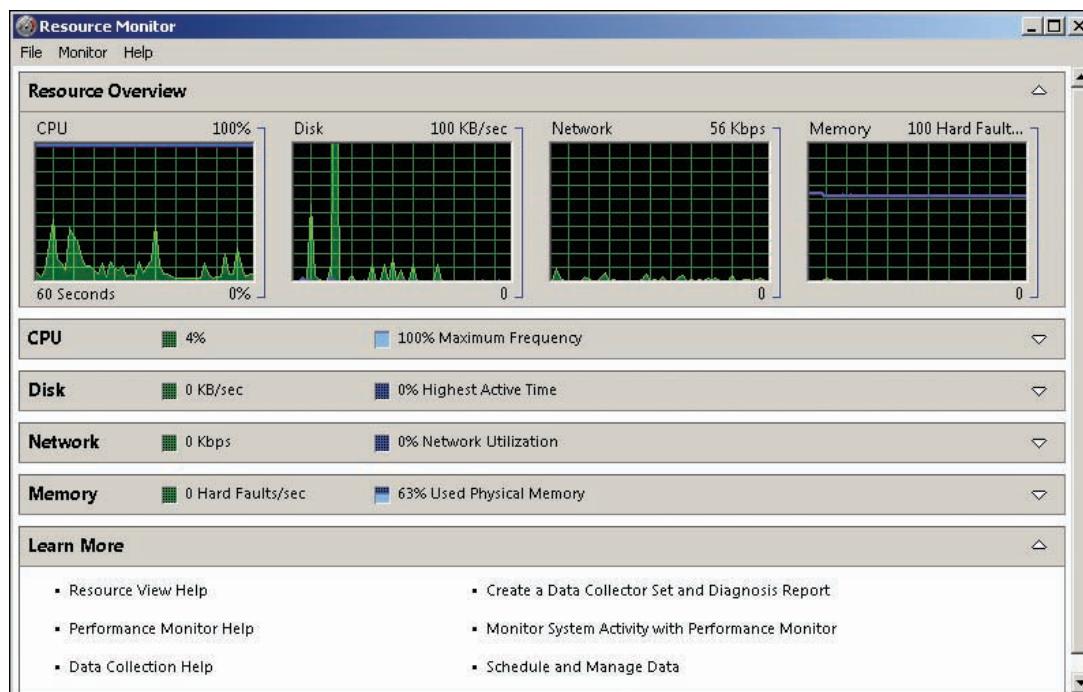


Figure 13-11 Tracking performance indicators in Resource Monitor

Spikes in resource use are common and expected, but if a key indicator approaches 100% utilization and stays at that level for an extended period, server performance is likely suffering. Memory use should stay fairly constant, except when processes or services are being loaded and unloaded. Be aware of resource interaction. If memory use is high, the need for virtual memory increases. Use of virtual memory increases hard disk activity and, to some extent, CPU utilization. Because of these interactions, the need for adequate RAM in a server can't be overstated.



Activity 13-7: Exploring Task Manager

Time Required: 10 minutes

Objective: Start Task Manager and explore its features.

Description: You have recently hired a junior administrator, who will be responsible for monitoring server performance. You ask him to watch as you review several Task Manager features.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Right-click the taskbar and click **Task Manager**. Click the **Processes** tab. You can click column headers in this tab to sort the running processes. If your computer has high CPU utilization, for example, you can sort the processes by CPU utilization. Click the **CPU** column header to sort CPU utilization from lowest to highest. Click the **CPU** column header again to sort from highest to lowest utilization. The System Idle process often tops the list on a server with comparatively low CPU utilization because this process runs when there's no real work for the CPU to do.
3. To add or remove columns from the Processes display, click **View, Select Columns** from the menu. Click the **Page Faults** and **I/O Writes** check boxes, and then click **OK** to add these columns to the display.
4. Start Notepad. In Task Manager, click the **Applications** tab. Right-click the **Notepad** task and click **Go To Process**. You're switched to the Processes tab with the Notepad process selected.
5. Right-click the **Notepad** process and point to **Set Priority**. You can manually increase or decrease a process's priority. For example, if you're running an application that tends to have high CPU use, but you don't want it to affect server performance adversely, you can set the application's priority to Below Normal or Low. The application might respond more sluggishly, but server performance for other tasks is better.



Use the Set Priority feature with care. Setting a higher priority can sometimes have unexpected and undesirable results.

CAUTION

6. Click **End Process**. When prompted to confirm, click **End process**. Notepad is removed from the running process list. Ending a process is useful when a task is exhibiting problems and doesn't terminate on its own.
7. Click the **Performance** tab, which displays graphs of CPU and memory use as well as numerical values of key memory indicators. Click the **Resource Monitor** button to see similar graphs of CPU, disk, network, and memory utilization. Close Resource Monitor.
8. Click the **Users** tab, which lists users who are currently logged on interactively through a console connection, a remote desktop connection, or a Terminal Services connection. You can disconnect and log off, or send a message to connected users. Close Task Manager, and stay logged on for the next activity.

13

Reliability and Performance Monitor

Reliability and Performance Monitor consists of a collection of tools for pinpointing which resources are being taxed and how they are being taxed. You can open it from the Administrative Tools folder or the Diagnostics node in Server Manager. When you first open it, you see the same graphical display as in Resource Monitor. Reliability and Performance Monitor contains the following folders:

- *Monitoring Tools*—Contains the Performance Monitor and Reliability Monitor tools.
- *Data Collector Sets*—Contains user- and system-defined templates with sets of data points called data collectors (discussed later in “Collecting Baseline Performance Data”).
- *Reports*—Contains system- and user-defined performance and diagnostic reports.

Performance Monitor Performance Monitor, under the Monitoring Tools folder, uses counters to track the performance of a variety of objects. Performance can be tracked in real time or scheduled for later review and analysis. A counter is a value representing some aspect of an object's performance. For example, disk drives have counters representing the percent of time the disk is used for read operations and the number of disk requests waiting to be serviced, among many others. There are counters for about almost every hardware and OS component on a server, including, of course, directory services.

Performance Monitor can track counters with a line graph (the default), a histogram (bar graph), or as raw data saved to a report. To use Performance Monitor in real-time mode, you simply add counters to the selected graph or report. You can add as many counters as you like, but as you can see in Figure 13-12, the display can get crowded. If you're tracking several counters and want to emphasize one in the display, click that counter at the bottom and click the Highlight toolbar icon or press Ctrl+H.

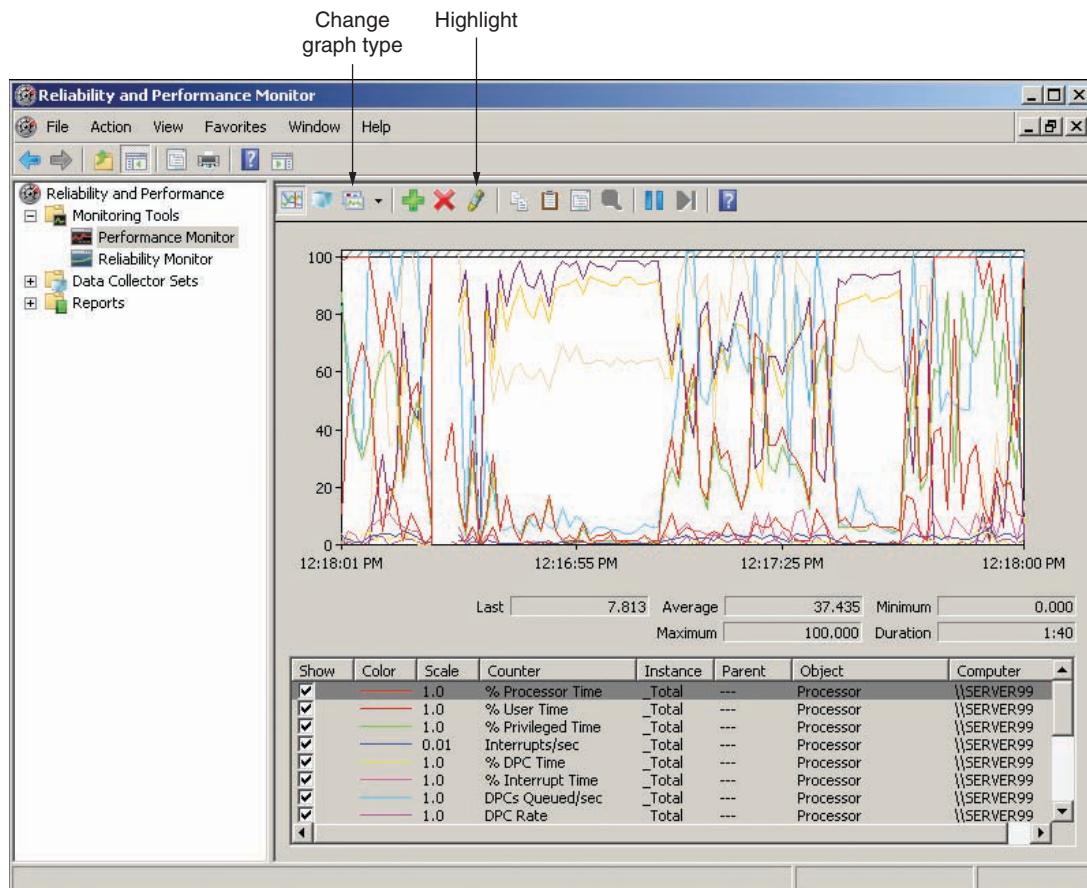


Figure 13-12 Viewing counters in Performance Monitor

Performance Monitor has two modes. You can display counters in real time, or you can open a saved performance log file and view data that has been captured over a period of time. To create a performance log, you create a new data collector set or start a saved data collector set. After the data collector set has finished running, you can view collected performance data in Performance Monitor.

Collecting Baseline Performance Data Viewing performance data in real time is helpful if you want to see the impact certain actions have on selected counters. For example, you might want to see the effect Active Directory replication has on CPU and network

utilization. After adding the necessary counters, you can force replication to occur or make a change to Active Directory to trigger automatic replication. Real-time monitoring of performance counters can also be useful for tracking the cause of a sluggish system. Unless you have a good idea what part of the system to examine, however, finding the cause of the problem could be a hit-and-miss proposition. You might have better results checking the graphs in Resource Monitor.

One reason that tracking the causes of poor performance with real-time monitoring is difficult is that you have no point of reference for comparing data. This point of reference, called a performance baseline (or simply a baseline), is a record of performance data gathered when a system is performing well under normal operating conditions. Generally, baseline data is collected shortly after a system is put into service and then again each time changes are made, such as installing or removing a server role, or when many new users are using the system. The baseline data collected during normal operation conditions can then be compared to data collected during peak resource demands to give you insight into your system's capabilities and limitations.

To create a baseline of performance data, you create a **data collector set** that specifies the performance counters you want to collect, how often to collect them, and the time period. You can create multiple data collector sets that capture different aspects of system performance and measure performance during different time periods. For example, if you know a database application is used heavily between 10:00 a.m. and 3:00 p.m., you can collect CPU, disk, memory, and network performance data during that time period. If Active Directory is used heavily between 7:00 a.m. and 10:00 a.m. because users are starting work, logging on, and changing passwords during these hours, you can collect Active Directory-related data during these hours. You should also collect data for critical resources over an entire day so that you can spot usage trends.

Be aware that performance monitoring uses system resources. It takes memory to run Performance Monitor, CPU cycles to collect and display counter data, and disk resources to update log files. With Performance Monitor, however, you can select a remote computer as the target for monitoring. By monitoring remotely, you lessen the monitoring session's impact on the computer being monitored. You can also adjust the counter sampling interval to collect counter data less frequently than the default values. The more often counter data is collected, the greater the impact that the monitoring session has on system resource use.

13



Activity 13-8: Viewing Real-Time Performance Data

Time Required: 10 minutes

Objective: Add counters to Performance Monitor to view real-time performance data.

Description: You have recently installed a server and want to look at key performance indicators to be sure the server is handling its current load. First, you look at performance data in real time. In the next activity, you save data in a log to view later.

1. Log on to **ServerXX** as Administrator, if necessary.
2. Click **Start**, point to **Administrative Tools**, and click **Reliability and Performance Monitor**. The initial view in the right pane is the Resource Overview window, which is the same as Resource Monitor (shown previously in Figure 13-11).
3. In the left pane, click to expand **Monitoring Tools**, and then click **Performance Monitor**. The % Processor Time counter is already added, and the display is in line mode by default. You can change the graph type to histogram bar, report, and back to line by pressing **Ctrl+G** repeatedly or by clicking the Change graph type toolbar icon. Press **Ctrl+G** to change to a histogram bar, and then press **Ctrl+G** again to change to a report. Press **Ctrl+G** a third time to return to a line graph.
4. Click the **Add** toolbar icon (green plus sign) to open the Add Counters dialog box. You can specify the computer where you want to add counters in the Select counters from computer list box (see Figure 13-13). For now, leave the setting as <Local computer>.

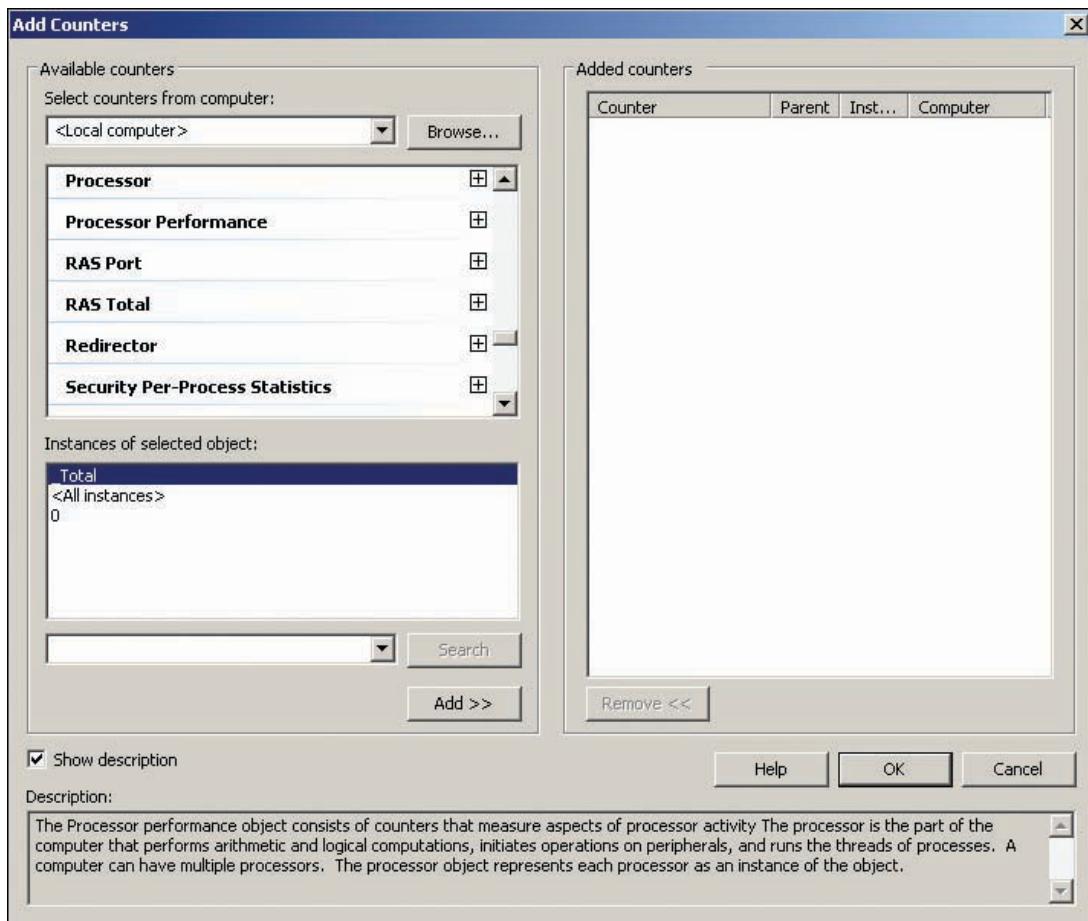
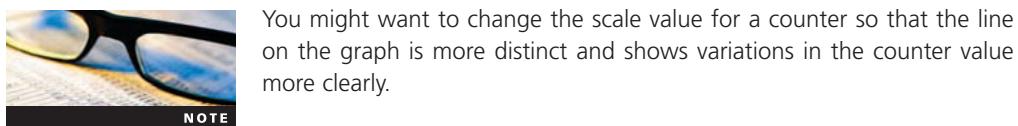


Figure 13-13 The Add Counters dialog box

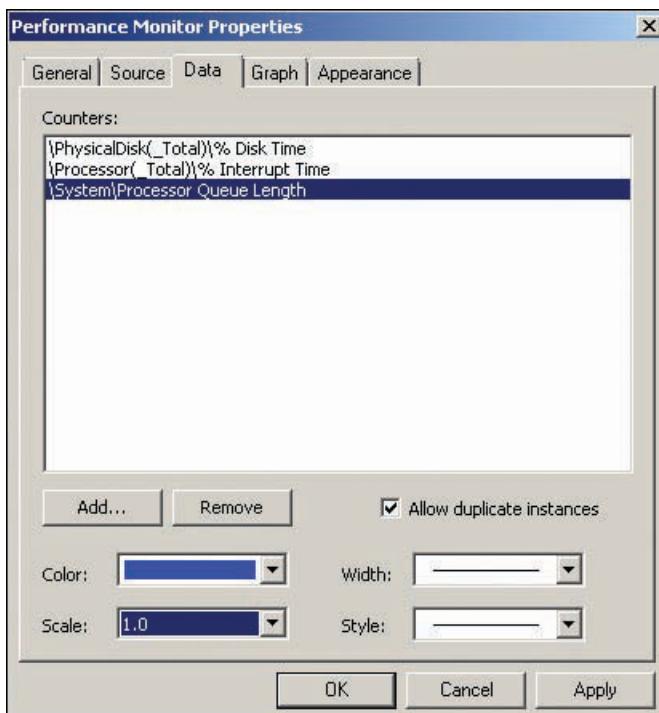
5. Click the **Show description** check box at the bottom so that you can see descriptions of counters you select.
6. Scroll through available counters to see what type of data can be monitored. Click **PhysicalDisk**. The Instances of selected object list box displays the physical disk objects you can select. You can monitor just one disk or multiple disks, or add a counter representing the total counter values for all disks. Click **0 C:** (assuming disk 0 contains the C drive), click the **Add** button, and then click **OK**.
7. Notice that several counters have been added to Performance Monitor. In the bottom pane, click the **Avg. Disk Bytes/Transfer** counter. Emphasize it in the display by clicking the **Highlight** toolbar icon. If the counter isn't showing much activity, create some activity by opening and then closing Internet Explorer.
8. Right-click **Avg. Disk Bytes/Transfer** and click **Remove All Counters**. When prompted to confirm, click **OK**.
9. Click the **Add** toolbar icon. In the Add Counters dialog box, click to expand **PhysicalDisk**. To select a counter for PhysicalDisk, click **% Disk Time**. (If necessary, verify that the **Show description** check box is selected. You might need to check it whenever you open this dialog box.) Read the description of the counter, and then click **Add**.
10. Click to expand **Processor**, and click **% Interrupt Time**. Read the description, and then click **Add**. Click to expand **System**, and click **Processor Queue Length**. Read the description, and then click **Add**. Queue counters indicate how many activities are waiting for work to be done. For most objects with queue counters (such as PhysicalDisk and Network Interface), a sustained queue value of more than a few items in the queue often indicates a bottleneck. Click **OK**.

11. In the bottom pane of Performance Monitor, notice that the value in the Scale column of the Processor Queue Length counter is 10. This value means the graph is showing the counter's actual value multiplied by the scale value. In this case, if the graph shows a value of 30 for Processor Queue Length, the actual value is 3. To adjust the scale, right-click **Processor Queue Length** and click **Properties**. In the Data tab, you can select the color, width, style, and scale of the line graph for the counter (see Figure 13-14). Click the **Scale** list arrow, click **1.0** in the list, and then click **OK**.



You might want to change the scale value for a counter so that the line on the graph is more distinct and shows variations in the counter value more clearly.

NOTE



13

Figure 13-14 The Performance Monitor Properties dialog box

12. Keep Reliability and Performance Monitor open for the next activity.

Data Collector Sets A data collector set can contain a variety of types of information collected and displayed as a graph or report. Information types you might find in a data collector set include the following:

- *Performance counters*—These system performance indicators used to view real-time data are also used in data collector sets.
- *Counter alerts*—Events generated when a counter falls below or exceeds a specified threshold. For example, you can create an alert to log an entry in the Application log if the % Processor Time counter exceeds 90%.
- *Event traces*—Logs information based on system or application events.
- *System configuration*—Monitors and records changes to Registry keys.

Recall that a common use of data collector sets is collecting performance data to establish a baseline. Predefined data collector sets can be run as they are or used as templates to create

user-defined data collector sets. These data collector sets include Active Directory Diagnostics, LAN Diagnostics, System Diagnostics, and System Performance. Data collector sets can be scheduled to run at certain times and certain days for a specified period of time. To specify how long a data collector set runs, you set a stop condition (see Figure 13-15).

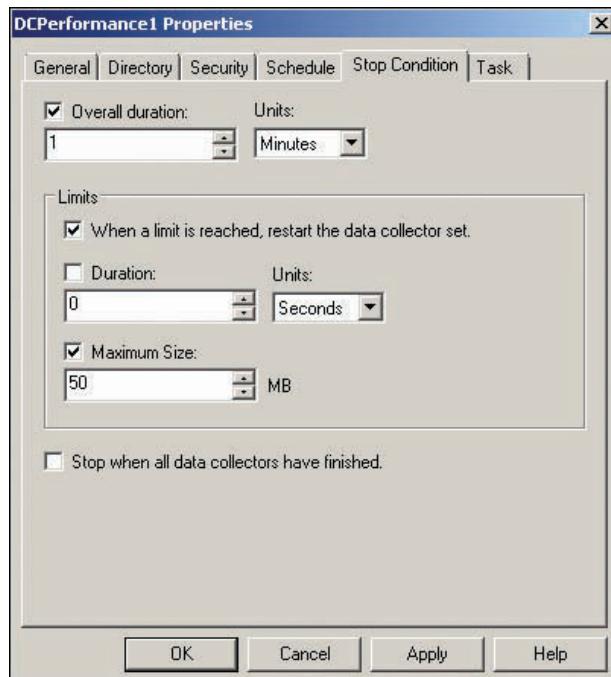


Figure 13-15 Setting stop conditions for data collector sets

Reports The Reports folder contains reports generated from data collector sets. The User Defined subfolder contains reports generated by user-defined data collector sets, and the System sub-folder contains folders for each system data collector set (the four listed in the preceding section). After a data collector set runs, the report is generated automatically and placed in a folder with the name of the data collector set. The report name reflects the date and instance the report was run.



Activity 13-9: Creating a Data Collector Set

Time Required: 15 minutes

Objective: Create a custom data collector set.

Description: You want to create a performance baseline for your DC, so you decide to create a data collector set.

1. Log on to **ServerXX** as Administrator and open Reliability and Performance Monitor, if necessary.
2. In the left pane, click to expand **Data Collector Sets**. Right-click **User Defined**, point to **New**, and click **Data Collector Set**. In the Name text box, type **DCPerformance1**. Verify that the default **Create from a template** is selected, and then click **Next**.
3. In the Which template would you like to use? window, click each template in the Template Data Collector Set list box, and read its description. Click **System Performance** to select this template, and then click **Next**.
4. In the next window, you can change the default path where data is saved. For now, leave the default location, and then click **Next**.
5. In the Create the data collector set window, you can change the user account for running the data collector set. Leave the default setting of **<Default>** in the Run as text box, and then click **Finish**.

6. Notice that the new data collector set has been created and its status is Stopped. Right-click **DCPerformance1** and click **Properties**.
7. Click the **Schedule** tab, where you can create a schedule of when you want the data collector set to run. Click **Add**. You can choose a beginning date and an expiration date. If you choose an expiration date, the data collector set stops collecting data after that date. You can also specify a start time and the days of the week the data collector set should run. You're going to start this data collector set manually, so click **Cancel**.
8. Click the **Stop Condition** tab, where you specify the duration for running the data collector set. If no conditions are selected, the data collector set runs until it's stopped manually. Accept the default value of 1 minute in the Overall duration text box, and then click **OK**.
9. In Reliability and Performance Monitor, right-click **DCPerformance1** and click **Start**. A green arrow on the data collector set icon indicates it's running. Open and close Internet Explorer, Server Manager, and Active Directory Users and Computers several times to create some resource use events.
10. When the status returns to Stopped, right-click **DCPerformance1** and click **Latest Report**. You see a performance report similar to Figure 13-16. In the Diagnostic Results section, counters with suspect values are flagged as warnings. In Figure 13-16, excessive paging was detected. Clicking the **Memory Diagnosis** link opens an Internet Explorer window to a Microsoft Web site that provides suggestions for solving the problem.

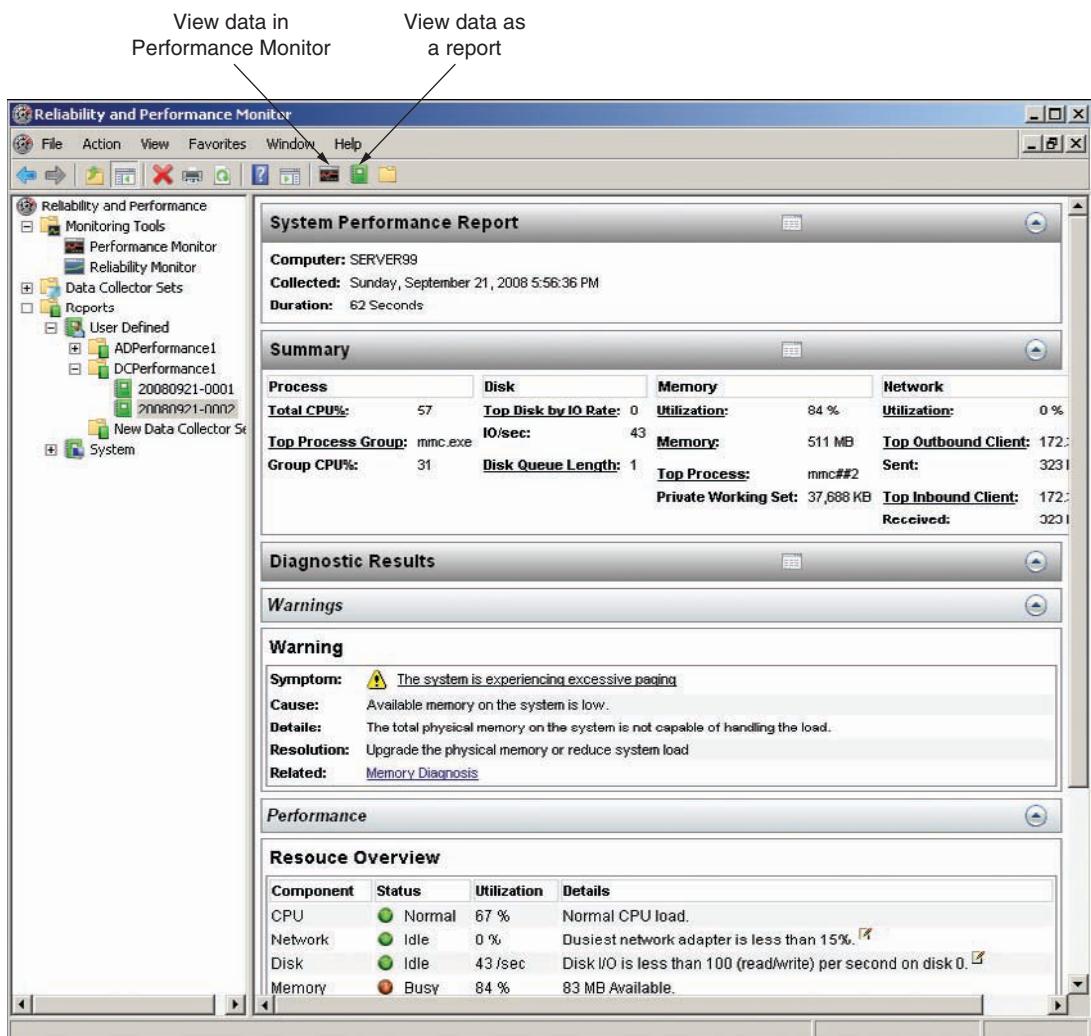


Figure 13-16 Viewing a performance report for a system data collector set

11. Scroll down in the report to view sections for major hardware systems, such as CPU, Network, Disk, and Memory. Click to expand each section to view more detailed information. Quite a bit of information can be garnered from the report.
12. To view the counter data in Performance Monitor, click the **View data in Performance Monitor** toolbar icon (shown in Figure 13-16). To return to Report view, click the **View data as a report** icon.
13. Leave Performance and Reliability Monitor open, and stay logged on for the next activity.



Activity 13-10: Comparing Two Log Files

Time Required: 10 minutes

Objective: Create a new log from your data collector set and compare it with the first log file.

Description: You have created a baseline with a data collector set and want to see how to compare two sets of data. You create another log file from the same data collector set, and then compare the log files by using the overlay feature in the stand-alone version of Performance Monitor.

1. Log on to **ServerXX** as Administrator and open Performance and Reliability Monitor, if necessary.
2. Navigate to the **DCPerformance1** data collector set you created in Activity 13-10. Right-click **DCPerformance1** and click **Start**. Open and close Internet Explorer, Server Manager, and Active Directory Users and Computers several times to create resource use events.
3. When the status returns to Stopped, close Reliability and Performance Monitor.
4. Click **Start**, type **perfmon /sys** in the Start Search text box, and press **Enter** to start Performance Monitor in stand-alone mode (required to compare two log files in overlay mode).
5. Click the **View Log Data** toolbar icon (second one from the left). In the Source tab of the Performance Monitor Properties dialog box, click the **Log files** option button, and then click **Add**.
6. In the Select Log File dialog box, double-click **Admin** and then **DCPerformance1**. Double-click the folder with the earliest modified date and time. Click the **Performance Counter.blg** file, click **Open**, and then click **OK**.
7. You need to specify which counters from the log you want to add to the display for comparison. Click the **Add** icon. In the Add Counters dialog box, click to expand **Memory**, click **Pages/sec**, and then click **Add**. Click to expand **Processor**, click **% Processor Time**, and then click **Add**. Click **OK**.
8. Repeat Steps 4 to 7, but choose the folder with the most recent modified date and time in Step 6. You should have two Performance Monitor windows open.
9. In the second Performance Monitor window you opened, click **Compare** on the menu, point to **Set Transparency**, and click **40%**. Click **Compare** and click **Snap to Compare**. The two Performance Monitor windows align automatically. The fainter line is the first set of counter data. To better see the difference in the line graph, click a counter and click the **Highlight** toolbar icon. The highlighted counter line is displayed in bolded black and is easier to compare to the same counter's colored line in the other data set.
10. Close all open windows, and stay logged on for the next activity.

Reliability Monitor Reliability Monitor tracks system changes and logs a variety of hardware and software failures. Changes are indicated on a timeline graph so that you can select a point on the timeline containing an icon that indicates a failure or software change. For example, Figure 13-17 shows that several updates occurred on the same day as a disruptive shutdown failure. The two events may or may not be related, but the information Reliability Monitor provides can give you context for assessing problems, which aids the troubleshooting process.

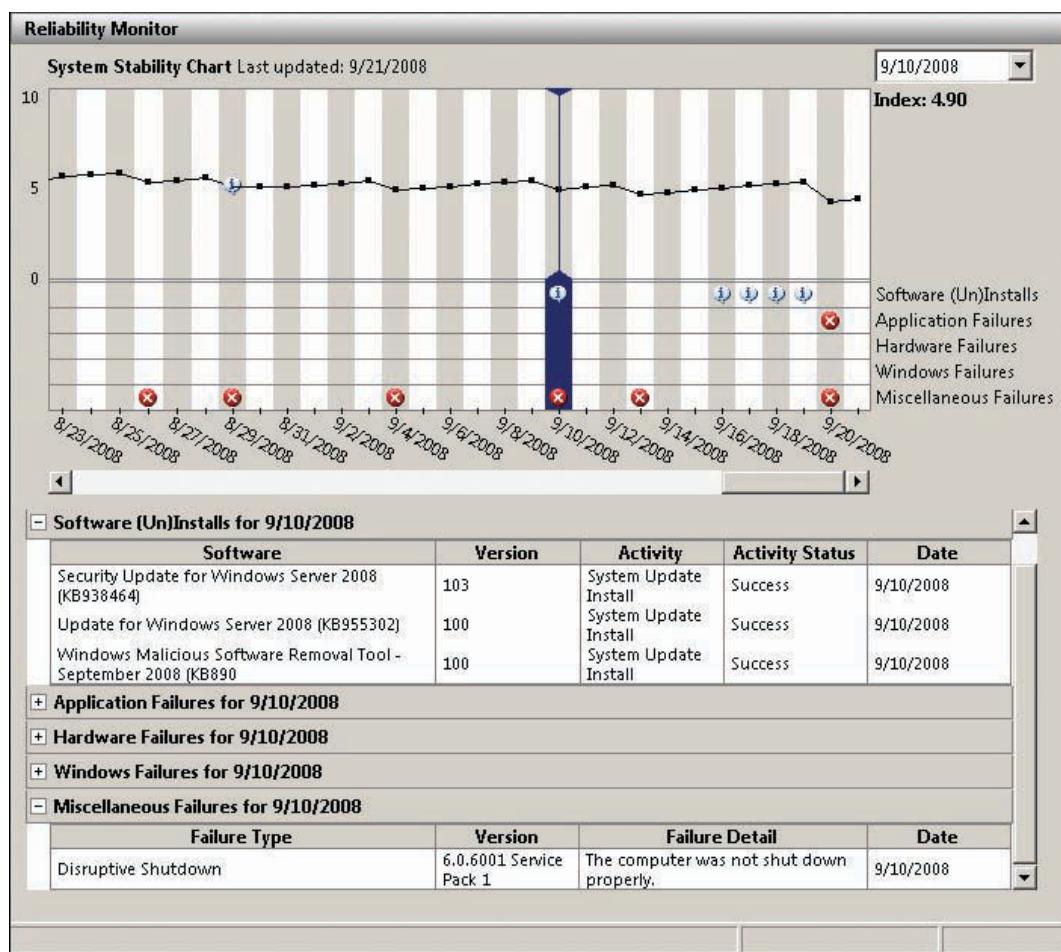


Figure 13-17 Viewing a timeline of changes in Reliability Monitor

13

The Reliability Monitor window has several components to help you determine how stable and reliable your system has been over a period of time. The graph line at the top tracks the system's overall reliability on a scale of 1 to 10. The index at the top right indicates the reliability value for the selected date. In Figure 13-17, on September 10, 2008, the system had a reliability value of 4.9. (A higher value is better.) The test system shown in this figure didn't have a strong history of reliability, mainly because it had been powered off several times without being shut down properly.

The icons that indicate failure (or error), information, or warning are the same as those in Event Viewer. Reliability Monitor tracks five event types: Software (Un)Installs, Application Failures, Hardware Failures, Windows Failures, and Miscellaneous Failures. Each event type has a row in the timeline graph, where you'll find information, warning, or error icons if an event of these types occurred on a given day.

When you click a day in the graph containing an icon, the lower half of the window displays details about the event. For example, you can see that on 9/10/2008, both a Software (Un)Install and a Miscellaneous Failure event occurred. The failure was a disruptive shutdown. The Software (Un)Install event was a series of system updates. Reliability Monitor can often be used with Event Viewer. For example, if a failure occurred on a particular date or a series of failures occurred, Event Viewer might list additional events that occurred in times surrounding the failure in Reliability Monitor.

Windows System Resource Manager

Windows System Resource Manager (WSRM), shown in Figure 13-18, is a Windows Server 2008 feature that's installed in Server Manager. WSRM helps you manage processor and memory resources on heavily used systems. By managing resources, you can give high-priority services and

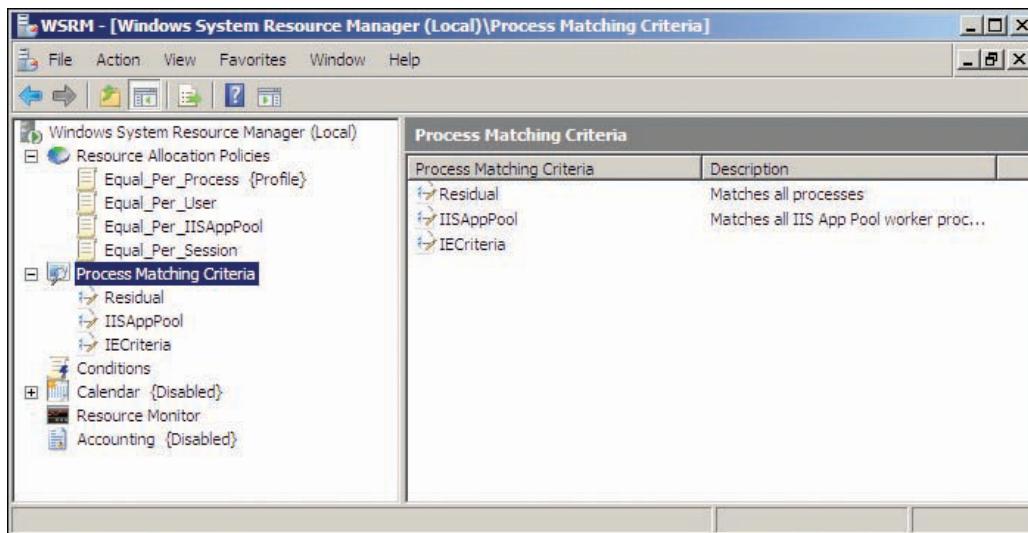


Figure 13-18 Windows System Resource Manager

applications a larger share of CPU time and memory to make sure they can perform critical tasks in a timely manner. You can also fine-tune resource use so that each process has a fairly equal share of resources to ensure that no one service dominates CPU and memory use.

WSRM includes the following features for managing the efficient use of running services:

- Preconfigured and custom policies that allocate resources on a per-process or per-user basis
- Policies based on calendar rules to allow fine-tuning system resource use according to time of day
- Automatic policy application based on server events or changes in memory or CPU resources
- Resource monitoring data stored in a Windows internal database or an SQL database

WSRM Management Policies WSRM is designed to be used on multipurpose servers that have generally high CPU utilization. It has little or no benefit on servers performing a single server role or servers that rarely top 70% CPU utilization for an extended period. WSRM doesn't apply CPU use policies until total utilization reaches 70%. If a server is running multiple resource-heavy services, you can use a preconfigured policy or create a custom policy. Preconfigured policies, called resource allocation policies, available with WSRM include the following:

- *Equal_Per_Process*—All running processes can consume an equal amount of resources.
- *Equal_Per_User*—Applications started by users are given an equal amount of resources, which prevents a few users from using the majority of resources.
- *Equal_Per_IISAppPool*—You can apply this policy to Web servers running Web-based applications to give each application pool equal resources and to ensure that Web-based applications have priority over applications that aren't part of an IIS application pool.
- *Equal_Per_Session*—Useful for servers running Terminal Services, this policy ensures that each terminal session has equal access to resources.

If these preconfigured policies don't work for your environment, you can create a custom policy based on process-matching criteria. Process-matching criteria are processes or commands you specify in the policy and can include users or groups allowed to run them. An application or process that matches the criteria is subject to the policy's parameters. Resource allocation policies enable administrators to define the amount of CPU and memory resources that a process matching the criteria can use.

For example, members of the Administrators group logging on to a server interactively might run foreground applications, such as Internet Explorer. A custom policy can be created to ensure that Internet Explorer doesn't use an inordinate percentage of CPU resources, which

could affect network operations adversely. The policy could limit Internet Explorer to 10% of CPU resources, for instance. You can also use custom policies to exclude users, groups, and processes from WSRM management. In addition, you can use scheduling to enable policies on specific days and times when certain usage patterns have been identified.

Analyzing Active Directory Performance

As mentioned, a large part of keeping Active Directory running in peak performance is ensuring that the AD DS server is running in peak condition. However, you should also monitor some specific Active Directory performance indicators, such as the following, to ensure a healthy directory service:

- **AD DS**—Performance Monitor has an Active Directory Diagnostics data collector set, which includes trace event logs, performance counters, and configuration logs specific to the Active Directory service.
- **DNS**—DNS performance affects Active Directory performance because the services rely on one another for operation. More than 60 counters related to DNS are available in Performance Monitor, including counters that monitor queries, responses, updates, WINS, and zone transfers.
- **Replication**—Active Directory replication and DFS replication must be in good working order. Replication-specific counters for both are available in Performance Monitor. In addition, Repadmin (introduced in Chapter 10), Replmon, and Dcdiag are command-line tools for monitoring DNS and Active Directory replication, discussed in the next section.
- **Active Directory storage**—The volumes on which the Active Directory database is stored must have enough free space at all times. A volume that becomes critically low on free space has a severe adverse affect on general server performance and Active Directory operation and performance.

Monitoring Active Directory Replication

Correct and timely replication of Active Directory objects is critical to the operation of a Windows Server 2008 domain. As discussed, you can monitor replication statistics with Performance Monitor. Three additional tools can be used to monitor aspects of Active Directory replication:

- **Repadmin**—Reports replication status on each domain controller, allowing you to spot potential problems before they affect operations adversely. You can display replication partners for a domain controller with the repadmin /showrepl command. This command informs you if a partner isn't available or communication problems are occurring. You can also display detailed information about connection objects with the repadmin /showconn command and view object replication information with the repadmin /showobjmeta command. For a less detailed summary of replication status, use the repadmin /replsummary command. Repadmin can also be used to manage certain aspects of replication. For example, the repadmin /replicate command is used to force replication of a partition between two partners, and the epadmin /KCC command recalculates the replication topology. For complete syntax help, type repadmin ?.
- **Replmon**—This GUI tool enables you to view the replication topology graphically and monitor replication performance and status. It's included in the Windows Server 2003 support tools, which you can download from the Microsoft Web site. (Windows Server 2008 support tools haven't been released, at the time of this writing.)
- **Dcdiag**—Analyzes the status and overall health of Active Directory and performs replication security checks. Dcdiag also checks for correct DNS configuration and operation. Examples of some tests you can run include the following:
 - Dcdiag /test:DNS: Tests overall DNS operation.
 - Dcdiag /test:Advertising: Ensures that all domain controller roles are advertised so that client computers are aware of available services.
 - Dcdiag /test:Intersite: Tests for failures in intersite replication.
 - Dcdiag /test:Replications: Tests for timely and error-free replication.
 - Dcdiag /test:CheckSecurityError: Verifies replication health, specifically its security.



Replication and general Active Directory health should be verified proactively, when no problems are apparent. Minor problems can be fixed before they turn into larger issues that affect domain functionality.

Managing Server Core

Server Core, the Windows Server 2008 installation option with a minimal user interface, was introduced in Chapter 2. In that chapter, you installed Server Core and performed basic configuration tasks, such as setting the computer name, workgroup name, and IP address. In this chapter, you perform additional configuration tasks, such as joining a domain, installing AD DS, and using MMCs on another computer to perform remote administration tasks.

As discussed previously, the Server Core installation of Windows Server 2008 is an ideal candidate for a branch office server running as an RODC and lends itself well to virtualization. Managing a Server Core installation, however, presents some challenges, as you saw in Chapter 2, particularly for those not well versed in using the command line. This section covers some common tasks performed at the command line and examines some aspects of Server Core that can be managed remotely with a GUI.



This chapter assumes you have a working Server Core installation set up during the Chapter 2 activities. Most important, the server name should be ServerCoreXX, the IP address should be 192.168.100.1XX, the DNS server should be 192.168.100.2XX, and the date and time should be set. Because this server uses the same IP address as Server1XX, Server1XX should not be running during activities in this section.

Common Server Core Configuration Tasks

Chapter 2 covered initial configuration tasks for Server Core. Additional tasks you might need to perform include the following:

- *Activating Windows Server 2008*—To activate a Server Core installation, use the “slmgr.vbs -ato” command.
- *Changing the administrator password*—When you first log on to Server Core, you’re prompted to change the Administrator password, which you do with the “net user administrator *” command.
- *List installed features and roles*—To view a list of available roles and features and see whether they’re installed, use the oclist command.
- *Install new server roles and features*—You use the ocsetup command to install or uninstall server roles and features. However, you must use Dcpromo.exe instead of the ocsetup command to install AD DS.
- *Join a domain*—In Chapter 2, you used Netdom to change the workgroup name of your Server Core computer. To join a domain, use the command “netdom join *computername /domain:domainname*” (replacing *computername* with the name of the Server Core computer and *domainname* with the name of the domain you want to join).



Activity 13-11: Joining Server Core to a Domain

Time Required: 10 minutes

Objective: Join Server Core to a domain.

Description: You have completed the installation of Server Core. You want the server to be a member of the domain, so you use Netdom to join it to w2k8adXX.com. Make sure ServerXX is running during this activity.

1. Log on to **ServerCoreXX** as Administrator, and open a command prompt window.
2. To verify your computer name, type **hostname** and press **Enter**. The hostname should be ServerCoreXX. If not, refer to Activity 2-12 to see how to change the computer name.

3. To join the domain, type **netdom join ServerCoreXX /domain:w2k8adXX.com** and press **Enter**. When the command is completed successfully, restart the server by typing **shutdown /r /t 0** and pressing **Enter**.
4. When the server restarts, log on to the domain as Administrator. If the logon defaults to ServerCoreXX\Administrator, click the **Switch User** button and click **Other User**. When prompted, type **w2k8adXX\administrator** in the User Name text box and **Password01** in the Password text box.
5. Stay logged on to ServerCoreXX for the next activity.

To install AD DS on Server Core, you must run Dcpromo in unattended mode because the installation wizard doesn't run on Server Core. Unattended mode can use a preconfigured file containing all the information needed for the installation, or you can specify the required information on the command line. The Dcpromo commands can be quite long for an unattended installation, so you might want to create them in a batch file for easy editing. Then you can run the batch file to install AD DS. Dcpromo is also used to uninstall AD DS. You can get basic command-line help by typing **dcpromo /?**. For detailed information on using Dcpromo to install AD DS, type **dcpromo /?:Promotion**.



You can have Dcpromo save an unattend file when you install AD DS on a full Windows Server 2008 installation. You can then edit sections of the unattend file for use when installing AD DS on Server Core.

TIP

The next activity walks you through using Dcpromo to install AD DS on Server Core, but first, review the switches used with this program:

- **/replicaOrNewDomain**—Options for this switch are Replica, ReadOnlyReplica, and Domain. Replica means you're installing an additional writeable domain controller in an existing domain. ReadOnlyReplica means you're installing an RODC in an existing domain. Domain means you're installing the first domain controller in a new domain.
- **/replicaDomainDNSName**—You must specify the FQDN of the domain this domain controller will be joining if you're installing an additional DC in an existing domain.
- **/ConfirmGC**—Yes specifies that the DC will also be a global catalog server.
- **/InstallIDNS**—Yes specifies that DNS should also be installed.
- **/UserName**—You can specify a username to be used for completing the operation. If it's not specified, the currently logged-on user's credentials are used.
- **/Password**—If a username is specified, a password must be specified, or you can use an asterisk (*) to indicate that you should be prompted for a password.
- **/RebootOnSuccess**—Yes specifies that the server should restart after successful completion of AD DS installation. If there are errors, the system doesn't restart.
- **/SafeModeAdminPassword**—A password is required to start the server in Safe Mode or DSRM.

13



Activity 13-12: Installing AD DS and DNS in Server Core

Time Required: 15 minutes

ACTIVITY

Objective: Install AD DS in Server Core.

Description: You have decided to deploy your Server Core computer to a branch office that needs a domain controller. You install AD DS in Server Core by using Dcpromo in unattend mode.

1. Log on to the domain from **ServerCoreXX** as Administrator, if necessary.
2. In the command prompt window, type **dcpromo /?:promotion** and press **Enter**. You see a list of options you can specify for installing AD DS. Scroll to read the complete list. Press the **spacebar** to quit.

3. Type `dcpromo /unattend /replicaOrNewDomain:replica /replicaDomainDNSName:w2k8adXX.com /ConfirmGC:Yes /RebootOnSuccess:Yes /SafeModeAdminPassword: Password01` and press **Enter**. Supplying a username and password isn't necessary because you're already logged on to the domain as Administrator. DNS will not be installed.
4. You see a number of information messages as AD DS is installed. When the installation is finished, your server should restart. Log on as Administrator.
5. You have decided that because this server is running at a branch office, it should have DNS installed so that users can make DNS queries to a local server. To verify the currently installed server roles and features, type `oclist | more` and press **Enter**. Notice that Directory Services has been installed, but no other roles or features have been installed. Press the **spacebar** until you're back at the command prompt.
6. To start the DNS installation, type `start /w ocsetup DNS-Server-Core-Role` and press **Enter**. The `/w` in the command prevents the command prompt from returning until the role has been installed successfully.
7. When the installation is finished, type `oclist | more` and press **Enter** to verify that the role has been installed.
8. Test DNS on ServerCoreXX by typing `nslookup` and pressing **Enter**. The default server is ServerXX. Type `server ServerCoreXX` and press **Enter** to change the server Nslookup uses to ServerCoreXX. Type `www.yahoo.com` and press **Enter**. A successful reply indicates that DNS is working on ServerCoreXX.
9. Keep the command prompt window open, and stay logged on to ServerCoreXX for the next activity.

Managing Server Core Remotely

Many tasks can be accomplished on a Server Core installation at the command line. However, some tasks are easier with a GUI, and a GUI provides visual feedback that you can't get with command-line programs. Several MMC snap-ins work with Server Core, as long as they're run from another computer.

Although some snap-ins connect remotely to Server Core without any additional configuration, such as Shared Folders and Services, several snap-ins require firewall configuration before you can connect to the server. In Chapter 2, you had to set a firewall rule to allow Server Core to respond to a Ping request, for example.

To allow remote management of Server Core from any MMC, type the following at a Server Core command prompt:

```
netsh advfirewall firewall set rule group="Remote Administration"
new enable=yes
```

A few snap-ins require additional configuration on Server Core before you can use them:

- *Disk Management*—You must start the Virtual Disk service on Server Core before Disk Management can connect. To do so, type “`net start vds`” at a Server Core command prompt. To start the service when Server Core boots, type “`sc config vds start= auto`.” Alternatively, you can start the Virtual Disk service by using the Services snap-in remotely. You must also enable the Remote Volume Management firewall rule on both the Server Core server and the computer where you're running Disk Management. On both computers, type the following command:

```
netsh advfirewall firewall set rule group="Remote Volume
Management" new enable=yes
```

- *Device Manager*—You must first enable the “Allow remote access to the PnP interface” policy. You can set this policy on the server in Group Policy Object Editor on a Windows Server 2008 or Vista computer and then connect to the Server Core computer.
- *IPSec Management*—At a command prompt, type this command:

```
Cscript \windows\system32\scregedit.wsf /im 1
```

- *Windows Firewall with Advanced Security*—Manage firewall settings on Server Core remotely by entering the following command (setting the Remote Administration rule first isn't necessary):

```
netsh advfirewall set currentprofile settings remotemanagement enable.
```



Activity 13-13: Configuring the Firewall for Remote Management

Time Required: 15 minutes

Objective: Configure the firewall for remote management.

Description: You prefer to perform some Server Core configuration tasks with an MMC snap-in, so you must configure firewall rules on the server to allow remote management.

1. Log on to the domain from **ServerCoreXX** as Administrator and open a command prompt window, if necessary.
2. At the command prompt, type **netsh advfirewall firewall set rule group="Remote Administration" new enable=yes** and press **Enter**.
3. Log on to **ServerXX** as Administrator. Click **Start**, type **mmc** in the Start Search text box, and press **Enter**.
4. In the MMC console, click **File, Add/Remove Snap-in** from the menu. In the Add or Remove Snap-ins dialog box, click **Computer Management**, and then click **Add**.
5. To manage your Server Core computer remotely, click the **Another computer** option button and click **Browse**. In the Select Computer dialog box, type **ServerCoreXX**, click **Check Names**, and then click **OK**. Click **Finish**, and then click **OK**.
6. In the MMC console, click to expand **Computer Management** and **System Tools**, and then click **Event Viewer**. After a few minutes, you can view the event logs on ServerCoreXX.
7. Click to expand **Shared Folders**, and then click **Sessions**. You should see that Administrator is currently connected from ServerXX, reflecting your current connection with ServerCoreXX.
8. Click **Reliability and Performance**. You can monitor resource use on ServerCoreXX.
9. Click to expand **Services and Applications**, and then click **Services**. You can view and change the status of services on ServerCoreXX.
10. To use Device Manager and Disk Management remotely, you must follow the instructions for these snap-ins described previously. Close the MMC. When prompted to save console settings, click **No**.

13

Additional Server and Active Directory Tools

You have seen that command-line tools can be helpful alternatives to GUI tools when repetitive tasks must be performed and when you're working with Server Core. Many tools have been discussed throughout this book, such as Dsadd, Dsmod, and Dsmove to manage Active Directory objects in Chapter 5. This section lists additional tools for managing a Windows Server 2008 environment:

- **Bcdedit**—For those familiar with the Boot.ini file, Windows Server 2008 and Vista have a surprise for you. The boot configuration file is no longer an easy-to-use text file but a file referred to as the boot configuration data store. To display and modify this store, you use the Bcdedit command-line program.
- **Dsacls**—Display or modify Active Directory object permissions (ACLs).
- **Dsdbutil**—Perform database maintenance on AD DS and AD LDS data stores.
- **Dsmgmt**—Manage Active Directory LDS partitions, manage and control FSMOs, and clean up metadata from discarded AD LDS instances.

- *Dfsutil*—Manage the DFS namespace as well as DFS servers and clients.
- *Dnscmd*—Manage the DNS Server role. You can display, modify, create, and delete DNS-related objects, such as zones and resource records, as well as force DNS replication.
- *Icacls*—Display, modify, and back up access control lists on an NTFS file system.
- *Servermanagercmd*—With this command-line version of Server Manager, you can install and remove roles and features as well as query the server for installed and available roles and features. You can use this tool at the command line or in scripts. It can't be used on Server Core, however.
- *Winrs*—Open a secure channel between two servers so that you can run a command remotely. All communication between servers is encrypted. For example, type “winrs -r:ServerCoreXX dir” to run the Dir program on your Server Core computer from another computer. You can also activate a command prompt on the remote server with the command winrs -r:ServerCoreXX cmd. The remote server must be prepared to accept remote commands first with the winrm quickconfig command.

Hundreds of command-line tools are available in Windows Server 2008. To see a complete reference, visit the Microsoft Download Web site (www.microsoft.com/downloads/) and search on “Windows Command Reference.”

Chapter Summary

- Active Directory maintenance involves backup and restore of the server and the Active Directory database as well as offline maintenance tasks. Windows Server Backup is new in Windows Server 2008 and supersedes NTBackup from previous versions.
- Windows Server Backup enables you to back up entire servers, volumes, and the system state. Files and folders, the system state, and the Active Directory database can be restored from a backup. Recovery of the server system state requires the command-line version of Windows Server Backup, Wbadmin. Active Directory restoration requires rebooting the system in Directory Services Restore Mode (DSRM).
- The Active Directory database becomes fragmented over time. Online defragmentation simply deletes deleted objects that have been deleted longer than the tombstone lifetime, a process called garbage collection. You can't restore a backup that's older than the tombstone lifetime. Offline defragmentation compacts the database for more efficient operation. Offline defragmentation can be performed by stopping the AD DS service without having to restart the server.
- Four tools are commonly used to monitor and fine-tune the performance and reliability of Active Directory and the server: Event Viewer, Task Manager, Reliability and Performance Monitor, and Windows Server Resource Manager.
- Task Manager and Resource Monitor provide a real-time look at key performance indicators, such as CPU, disk, network, and memory utilization. Performance Monitor provides a more detailed view of performance counters in real time or over an extended period. You can also use it to create a performance baseline for later comparison with recent indicators.
- Reliability Monitor tracks several different system failures and includes a numeric indicator of your server's reliability. You can use it to correlate certain events with system problems. Many events tracked in Reliability Monitor are also logged in Event Viewer.
- Server Core has a minimal user interface and is ideal for branch office servers and for virtualizing servers performing particular roles. Using the command line, you can add and remove server roles, join a server to a domain, and install or remove AD DS. For remote management of Server Core, you must configure the firewall to allow remote administration. MMC snap-ins can then be used on a Vista computer or a full installation server to manage Server Core remotely.
- Hundreds of command-line tools are available to manage all aspects of a Windows Server 2008 environment. Command-line tools are useful for managing a Server Core installation and performing repetitive tasks.

Key Terms

authoritative restore A method of restoring Active Directory data from a backup to ensure that restored objects aren't overwritten by changes from other domain controllers through replication.

data collector set A Performance Monitor object used to create a baseline of performance data; can contain performance counters, counter alerts, event traces, and system configuration information.

nonauthoritative restore A method of restoring Active Directory data from a backup that restores the database, or portions of it, and allows the data to be updated through replication by other domain controllers.

offline defragmentation Defragmentation of the Active Directory database that also compacts the database to improve performance. The Active Directory service must be stopped before offline defragmentation can occur.

online defragmentation Defragmentation of the Active Directory database that removes deleted objects and frees up space in the database but doesn't compact the database. Online defragmentation occurs automatically when Active Directory performs garbage collection.

tombstone lifetime A period of time in which deleted Active Directory objects are marked for deletion but left in the database. When the tombstone lifetime expires, the object is removed during garbage collection.

Volume Shadow Copy Service (VSS) A backup option that allows a volume to be backed up even while the volume is in use and files are being modified.

Windows Recovery Environment (WinRE) A boot option available on the Windows Server 2008 installation DVD or by pressing F8 when the system boots; allows restoring Windows after a disk crash or similar catastrophic failure.

Review Questions

1. Which of the following is true of Windows Server Backup? (Choose all that apply.)
 - a. Backups can be scheduled with Task Scheduler.
 - b. Files and folders can be backed up.
 - c. Backups can be stored on network drives and tapes.
 - d. You can back up another computer remotely.
2. Which of the following is true about incremental backups? (Choose all that apply.)
 - a. Files that have changed since the last incremental backup are backed up.
 - b. Incremental backups generally take longer than full backups.
 - c. Incremental backups take less storage space than full backups.
 - d. Files that haven't changed since the last backup are backed up.
3. You can choose a full or incremental backup on a per-volume basis. True or False?
4. Your Windows Server 2008 server has been generating sporadic errors that lead you to think elements of the system state are corrupt. The server is not running AD DS. What should you do to restore the system state?
 - a. Start Windows Server Backup. In the Actions pane, click Recover, and click System State Data when prompted to select the items to recover. Restart the server after the recovery is completed.
 - b. Restart the server in Safe Mode. Start Windows Server Backup. In the Actions pane, click System Recovery. Restart the server after the recovery is completed.
 - c. Open a command prompt window and type wbadmin start systemstaterecovery.
 - d. Restart the server in DSRM. Open a command prompt window and type wbadmin start systemstaterecovery.



5. A junior administrator accidentally deleted an OU containing several dozen objects. You have three other domain controllers in the network. You have a backup of Active Directory created about 12 hours before the OU was deleted. What should you do to restore the OU and its objects?
 - a. Restart the DC in DSRM. Start Windows Server Backup. In the Actions pane, click Active Directory Authoritative Restore. Restart the server normally.
 - b. Restart the DC in DSRM. Run Wbadmin and restore the system state backup. Run Ntdsutil to mark the OU as authoritative, and then restart the server normally.
 - c. Restart the DC in DSRM. Run Wbadmin and restore the system state backup. Restart the server normally, and then run Ntdsutil to mark the OU as authoritative.
 - d. Restart the DC in DSRM. Start Windows Server Backup. In the Actions pane, click Active Directory Non-Authoritative Restore. When the restore is completed, use Ntdsutil to specify the OU as authoritative, and then restart the server normally.
6. What's the term for removal of deleted objects in Active Directory?
7. The period of time between when an object is deleted and when it's removed is called what?
8. Your Active Directory database has been operating for several years and has undergone many object creations and deletions. You want to make sure it's running at peak efficiency, so you want to defragment and compact the database. What procedure should you use that will be least disruptive to your network?
 - a. Create a temporary folder to hold a copy of the database. Restart the server in DSRM. Run Ntdsutil and compact the database in the temporary folder. Copy the Ntds.dit file from the temporary folder to its original location. Verify the integrity of the new database, and restart the server normally.
 - b. Create a temporary folder and a backup folder. Stop the AD DS service. Run Ntdsutil and compact the database in the temporary folder. Copy the original database to the backup folder. Delete the Ntds log files. Copy the Ntds.dit file from the temporary folder to its original location. Verify the integrity of the new database, and restart the server.
 - c. Create a temporary folder and a backup folder. Restart the server in DSRM. Run Ntdsutil and compact the database in the temporary folder. Copy the original database to the backup folder. Delete the Ntds log files. Copy the Ntds.dit file from the temporary folder to its original location. Verify the integrity of the new database, and restart the AD DS service.
 - d. Create a temporary folder and a backup folder. Stop the AD DS service. Run Ntdsutil and compact the database in the temporary folder. Copy the original database to the backup folder. Delete the Ntds log files. Copy the Ntds.dit file from the temporary folder to its original location. Verify the integrity of the new database, and restart the AD DS service.
9. Which tool should you use to get a real-time graphical look at key performance indicators?
 - a. Task Viewer
 - b. Resource Monitor
 - c. Event Viewer
 - d. Server Monitor
10. You have been monitoring server performance for the past hour, viewing CPU, memory, disk, and network utilization. You counted 20 different occurrences of one or more of the performance indicators rising to near 100% for a few seconds and then settling down to between 0 and 30% utilization. What does this information indicate?
 - a. Your server is underpowered and should be replaced with a higher performance computer.
 - b. Nothing. Spikes like that are normal.
 - c. You should upgrade the CPU or add another CPU.
 - d. Memory is probably low, which causes other resources to have high utilization.

11. You have installed a server in a branch office with 40 employees. The server is running AD DS, DNS, and File and Printer Sharing services. The number of employees will slowly increase to 60 over the next year. You want to monitor the server's performance so that you know if and when it should be upgraded. What's a good procedure to follow?
- Wait about two weeks after the server has been installed. Query employees for their opinions on server performance. Collect performance data during times the employees say they are most active on their computers. Continue to do so once per month. When performance counters reach 100% on a regular basis, upgrade the server.
 - Monitor Event Viewer for unusual failures or events indicating performance problems. Collect event data each week and chart the information. When the number of events exceeds 1000/week, it's time to upgrade the server.
 - Create a performance baseline of main resources, such as Active Directory, disk drives, CPU, DNS, network, and memory, by using data collector sets. Collect data during peak use times and over a 24-hour period. Perform these baseline measurements each month, and compare the results to the previous month to discern trends.
 - Each day, open Resource Monitor and view the server's real-time performance data remotely. Keep a notebook of your observations to establish trends. When utilization increases an average of 20% for each performance indicator, consider upgrading.
12. Which tool is used to manage processor and memory resources on a per-user and per-process basis?
- Reliability Monitor
 - Task Manager
 - WSRM
 - Replmon
13. Which of the following tools is used to monitor and manage Active Directory replication?
- Replmon
 - Repadmin
 - Dcdiag
 - WSRM
14. Which command is used to activate a Server Core installation?
- Ocsetup
 - Netdom
 - Slmgr.vbs
 - Oclist
15. Which command is best used to install AD DS on Server Core as a new domain controller in a new domain?
- Start ocsetup /unattend /install DirectoryServices /domain: New
 - Netdom /install /unattend ADDS /domain:replica
 - Adprep /unattend /domain:New
 - Dcpromo /unattend /replicaOrNewDomain:domain
16. You're logged on to a Vista computer in your domain. You want to get a list of roles and features installed on a Server Core server named Core1 in another building. What command do you use?
- winrs -r:Core1 oclist
 - telnet Core1 /run:oclist
 - rmcmd Core1 -oclist
 - oclist /server:Core1

17. You want to manage your Server Core server with the Computer Management MMC. Which of the following Computer Management snap-ins can be used without additional configuration after configuring firewall rules? (Choose all that apply.)
 - a. Services
 - b. Device Manager
 - c. Shared Folders
 - d. Event Viewer
18. You run a third-party reporting program periodically on a domain controller to gather Active Directory and file system statistics. The program usually runs for three hours and must be run at various times to collect data during different usage periods. You have determined that running this application adversely affects performance of some critical services, which is causing access problems for your users. What can you do to lessen the impact the program has on services and users?
 - a. Inform your users of the times the program will be running and instruct them to use other servers during those times.
 - b. Create a custom resource allocation policy that matches the name of the third-party reporting program and limit the resources the program can use.
 - c. Use Task Scheduler to schedule the reporting program to run between 8 p.m. and 6 a.m., when use of the system is minimal.
 - d. Install another server to handle the workload of services affected by the reporting program.
19. Your server has had several application failures and system crashes over the past month. You suspect the frequency of problems is increasing and want to find out whether other events, such as software or driver installations, might be one cause. Which tool should you use to determine whether the problems are increasing in frequency and discover what other activities are occurring around the time of the failures?
 - a. Performance Monitor
 - b. Task Manager
 - c. Reliability Monitor
 - d. Event Viewer
20. You want to create a data collector set that monitors changes to the Registry and system and application events. What should you include in the data collector set?
 - a. Performance counters and counter alerts
 - b. Counter alerts and event traces
 - c. Event traces and system configuration
 - d. System configuration and counter alerts

Case Projects

These projects are intended to be done in groups, and the solutions should be discussed and compared among groups. Present the solutions to the class in groups, and discuss each group's solution.



Case Project 13-1: Devising a Backup Routine

You have three servers. Two are domain controllers that run only the AD DS and DNS server roles, and you have split the FSMO roles between them. The third server is a member server running a database application that gets around-the-clock use. Devise a backup routine for each server, including what you will back up, what backup method you use, where data is backed up, and how often backups are performed. Explain your choices.

Case Project 13-2: Using Performance Counters

Create a data collector set that monitors what you believe are the five most critical Active Directory performance counters, the three most critical process counters, the three most critical memory counters, the three most critical disk counters, and the three most critical network counters. List and describe the counters you selected, and explain your reasons for selecting these particular counters.

Case Project 13-3: Configuring Data Collector Sets

For the data collector set you created in Case Project 13-2, define a schedule for running the data collector set you think would be a good baseline for measuring server performance during normal operating conditions. Describe the schedule and why you chose the times for the collector to run. Define the stop conditions for the data collector set, and explain why you chose those parameters. Explain what each field in the Stop Condition tab of a data collector set is used for.

Case Project 13-4: Describing Server Core Environments

Describe five situations in which a Server Core installation, rather than a full installation, is the best choice. Include details about why Server Core should be used, including what roles or features should be installed on the server and details of the environment in which the server is running (type of business, size of business or location, types of users, and so forth). Next, describe three situations in which a Server Core installation clearly isn't a good solution for the computing environment or the requirements, and explain your reasoning.

This page intentionally left blank

MCTS 70-640 Exam Objectives

Table A-1 maps the Windows Server 2008 Active Directory, Configuring (70-640) exam objectives to the corresponding chapter and section title where the objectives are covered in this book. Major sections are listed after the chapter number, and applicable subsections are shown in parentheses. After each objective, the percentage of the exam that includes the objective is shown in parentheses.

Table A-1 Objectives-to-chapter mapping

Domain objective	Chapter and section(s)
Configuring Domain Name System (DNS) for Active Directory (16%)	
Configure zones	Chapter 9: Configuring DNS Zones
Configure DNS server settings	Chapter 9: Using DNS in Windows Server 2008 Chapter 9: Configuring DNS Zones (Zone Delegation) Chapter 9: Advanced DNS Server Settings
Configure zone transfers and replication	Chapter 9: Using DNS in Windows Server 2008 (Creating DNS Zones) Chapter 9: Configuring DNS Zones (Zone Transfers)

(Continued)

Domain objective	Chapter and section(s)
Configuring the Active Directory Infrastructure (25%)	
Configure a forest or a domain	Chapter 4: Working with Forests, Trees, and Domains Chapter 10: Examining Active Directory Functional Levels Chapter 10: Adding and Removing Domains
Configure trusts	Chapter 4: Working with Forests, Trees, and Domains (Understanding Trusts) Chapter 10: Configuring Active Directory Trusts
Configure sites	Chapter 4: Understanding Sites Chapter 10: Understanding and Configuring Sites
Configure Active Directory replication	Chapter 4: Working with Forests, Trees, and Domains (Active Directory Replication) Chapter 10: Configuring Intrasite Replication
Configure the global catalog	Chapter 4: Working with Forests, Trees, and Domains (The Importance of the Global Catalog Server) Chapter 10: Configuring Intrasite Replication (Global Catalog Replication) Chapter 10: Understanding and Configuring Sites (The Global Catalog and Universal Group Membership Caching)
Configure operations masters	Chapter 4: Working with Forests, Trees, and Domains (Operations Master Roles) Chapter 10: Working with Operations Master Roles
Configuring Additional Active Directory Server Roles (9%)	
Configure Active Directory Lightweight Directory Services (AD LDS)	Chapter 12: Active Directory Lightweight Directory Services
Configure Active Directory Rights Management Services (AD RMS)	Chapter 12: Active Directory Rights Management Services
Configure the read-only domain controller (RODC)	Chapter 12: Read Only Domain Controllers
Configure Active Directory Federation Services (AD FS)	Chapter 12: Active Directory Federation Services
Creating and Maintaining Active Directory Objects (24%)	
Automate creation of Active Directory accounts	Chapter 3: What's Inside Active Directory? (Active Directory Leaf Objects) Chapter 5: Automating Account Management
Maintain Active Directory accounts	Chapter 4: Working with Organizational Units Chapter 5: All
Create and apply Group Policy objects (GPOs)	Chapter 3: Introducing Group Policies Chapter 7: All
Configure GPO templates	Chapter 7: Group Policy Architecture (Group Policy Objects) Chapter 7: Group Policy Settings Chapter 7: Using Security Templates
Configure software deployment GPOs	Chapter 7: Group Policy Settings (Computer Configuration: Software Settings, User Configuration: Software Settings)

(Continued)

Domain objective	Chapter and section(s)
Configure account policies	Chapter 3: Introducing Group Policies (The Computer Configuration Node) Chapter 7: Group Policy Settings (Computer Configuration: Windows Settings)
Configure audit policy by using GPOs	Chapter 7: Group Policy Settings (Computer Configuration: Windows Settings)
Maintaining the Active Directory Environment (13%)	
Configure backup and recovery	Chapter 13: Active Directory Maintenance (Windows Server Backup and Restore, Active Directory Backup and Restoration)
Perform offline maintenance	Chapter 13: Active Directory Maintenance (Active Directory Defragmentation)
Monitor Active Directory	Chapter 13: Active Directory Monitoring
Configuring Active Directory Certificate Services (13%)	
Install Active Directory Certificate Services	Chapter 11: Deploying the Active Directory Certificate Services Role
Configure CA server settings	Chapter 11: Configuring a Certification Authority
Manage certificate templates	Chapter 11: Configuring a Certification Authority (Configuring Certificate Templates)
Manage enrollments	Chapter 11: Configuring a Certification Authority (Configuring Certificate Enrollment Options)
Manage certificate revocations	Chapter 11: Configuring a Certification Authority (Configuring the Online Responder, Creating a Revocation Configuration)



This page intentionally left blank

Windows Server 2008 Active Directory Configuration Resources

Books are one of the best resources for providing a comprehensive look at a topic. After reading this book, you should be well prepared to work with Active Directory and ancillary server roles in a Windows Server 2008 environment. However, your education shouldn't stop here. At times you need to delve into a topic in more detail than this book includes, or you might need detailed instructions to perform a task not covered in this book. This appendix serves as a reference for Web sites and other books you can use to research topics related to Windows Server 2008 and Active Directory configuration.

General Windows Server 2008

- File Systems: http://en.wikipedia.org/wiki/Comparison_of_file_systems
- Technical Library: <http://technet.microsoft.com/en-us/library/cc706994.aspx>
- Windows Catalog: www.windowsservercatalog.com
- Windows Editions: www.microsoft.com/windowsserver2008/en/us/editions.aspx
- Windows Server 2008 Step-by-Step Guides: www.microsoft.com/downloads/details.aspx?FamilyID=518d870c-fa3e-4f6a-97f5-acaf31de6dce&DisplayLang=en
- Windows Server 2008 Tips/Tricks: www.petri.co.il/windows-server-2008.htm
- Windows Server 2008 Wiki: http://en.wikipedia.org/wiki/Windows_Server_2008

Active Directory Configuration

- AD Object Permissions: <http://redmondmag.com/columns/article.asp?EditorialsID=328>
- Adprep Reference: <http://technet.microsoft.com/en-us/library/cc731728.aspx>
- Default Groups: <http://technet.microsoft.com/en-us/library/cc756898.aspx>
- DFS Replication: [http://msdn.microsoft.com/en-us/library/bb540031\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb540031(VS.85).aspx)

- FSMO Placement: <http://support.microsoft.com/kb/223346>
- Functional Levels: www.serverwatch.com/tutorials/article.php/3734071
- Global Catalog: <http://technet.microsoft.com/en-us/library/cc728188.aspx>
- Group Scope Reference: <http://technet.microsoft.com/en-us/library/cc755692.aspx>
- Reimer, Stan. *Windows Server 2008 Active Directory Resource Kit*. Microsoft Press, 2008 (ISBN 0-7356-2515-8).
- Repadmin: <http://technet.microsoft.com/en-us/library/cc736571.aspx>
- Replication Topology: <http://technet.microsoft.com/en-us/library/cc755994.aspx>
- RODC Features: <http://technet.microsoft.com/en-us/library/cc753223.aspx>
- RODCs: www.serverwatch.com/tutorials/article.php/3740341
- Seize FSMO Roles: <http://support.microsoft.com/kb/255504>

Active Directory Services

- AD FS Design: <http://technet.microsoft.com/en-us/library/cc771833.aspx>
- AD FS Overview: <http://technet.microsoft.com/en-us/library/cc772593.aspx>
- AD LDS: <http://technet.microsoft.com/en-us/library/cc731868.aspx>
- AD RMS Overview: <http://technet.microsoft.com/en-us/library/cc772403.aspx>
- Federation Trusts: <http://technet.microsoft.com/en-us/library/cc772593.aspx>
- MS Identity Integration Server (AD LDS): <http://technet.microsoft.com/en-us/miis/default.aspx>

Certificate Services

- CAPolicy.inf: <http://technet.microsoft.com/en-us/library/cc728279.aspx>
- CA Role-Based Administration: <http://technet.microsoft.com/en-us/library/cc739182.aspx>
- Certificate Autoenrollment: <http://technet.microsoft.com/en-us/library/cc773385.aspx>
- Cryptography and PKI: www.microsoft.com/technet/security/guidance/cryptographyetc/cryptpki.mspx
- How SSL Works: www.ourshop.com/resources/ssl.html
- NDES: <http://technet.microsoft.com/en-us/library/cc753784.aspx>
- User Key Recovery: <http://technet.microsoft.com/en-us/library/cc776056.aspx>

DNS

- DNS Aging: http://searchwindowsserver.techtarget.com/tip/0,289483,sid68_gci1040355,00.html
- DNSCmd: <http://support.microsoft.com/kb/884116>
- DNSLint: <http://support.microsoft.com/kb/321045>
- DNS RFC 2182: www.faqs.org/rfcs/rfc2182.html
- DNS Tech Reference: <http://technet.microsoft.com/en-us/library/cc779926.aspx>
- Stub Zones: <http://technet.microsoft.com/en-us/library/cc770842.aspx>

Group Policy

- Auditpol.exe: <http://support.microsoft.com/kb/921469/>
- Fine-Grained Password Policy: <http://technet.microsoft.com/en-us/library/cc770842.aspx>

- Group Policy Changes: www.windowsecurity.com/articles/Group-Policy-related-changes-Windows-Server-2008-Part1.html
- Melber, Derek. *Windows Group Policy—Windows Server 2008 and Windows Vista Resource Kit*. Microsoft Press, 2008 (ISBN 0-7356-2514-X).

Networking

- Hagen, Silvia. *IPV6 Essentials*. O'Reilly, 2006 (ISBN 0-596-10058-2).
- IPv6: <http://technet.microsoft.com/en-us/library/bb878121.aspx>
- Learn to Subnet: www.learntosubnet.com/
- Multihomed Computers: <http://support.microsoft.com/kb/157025>
- Network and Sharing Center: <http://technet.microsoft.com/en-us/library/cc770751.aspx>
- Network Location Awareness: <http://technet.microsoft.com/en-us/library/cc753545.aspx>
- New Networking Features: <http://technet.microsoft.com/en-us/library/bb726965.aspx>
- Peer-to-Peer Networking: www.microsoft.com/technet/network/p2p/p2pintro.mspx
- Shadow Copies: <http://technet.microsoft.com/en-us/windowsserver/bb405951.aspx>
- Shared Folders Best Practices: <http://technet.microsoft.com/en-us/library/bb726965.aspx>
- Supernetting: http://articles.techrepublic.com.com/5100-10878_11-5034906.html
- Tomsho, Greg. *Guide to Networking Essentials*. Course Technology, 2007 (ISBN 1-4188-3718-0).

Server Core

- Net User Command: <http://support.microsoft.com/kb/251394>
- Server Core Blog: http://blogs.technet.com/server_core/
- Server Core Installation: <http://technet.microsoft.com/en-us/library/cc753802.aspx>
- Server Core Network Configuration: www.petri.co.il/configuring-windows-server-2008-networking-settings.htm

Windows Server 2008 Certifications

- 70-640 Exam Objectives: www.microsoft.com/learning/en/us/exams/70-640.aspx
- MCTS Certifications: www.techexams.net/forums/viewtopic.php?p=155678
- Windows Server 2008 Learning Portal:
www.microsoft.com/learning/windowsserver2008/default.mspx



This page intentionally left blank

Virtual Machine Instructions for Selected Activities

All the activities in this book can be completed on physical computers, but several activities require two or more machines. Virtual machines are an excellent substitute for multiple physical computers. In fact, virtual machines can be used in all activities except those including the Hyper-V server role (Activities 2-14 through 2-17). Appendix D includes general information about using virtualization software, and this appendix provides instructions for using virtual machines with specific activities: 2-1, 2-7, and 2-11. There are few differences between using virtual and physical machines, but the differences that do exist are specified here. Reading Appendix D before performing these activities is highly recommended if you aren't already familiar with virtualization.



NOTE

If you use a different version of the virtualization software used to write these activities, keep in mind that your screens and steps might differ slightly.



ACTIVITY

Activity 2-1: Installing Windows Server 2008 in VMware Workstation 6.5

Time Required: 30 minutes to more than an hour

Objective: Install Windows Server 2008.

Description: You're ready to install Windows Server 2008 on your client's new network. You have verified the hardware configuration and have the installation DVD in hand. The server has a single hard drive and all space is unallocated, so there's no need to change the BIOS boot order.

1. First, you must create the virtual machine. Start VMware Workstation. Click **File** from the menu, point to **New**, and click **Virtual Machine** to start the New Virtual Machine Wizard. Click **Next** in the welcome window.
2. In the Select the Appropriate Configuration window (see Figure C-1), verify that the **Typical** option button is selected, and then click **Next**.

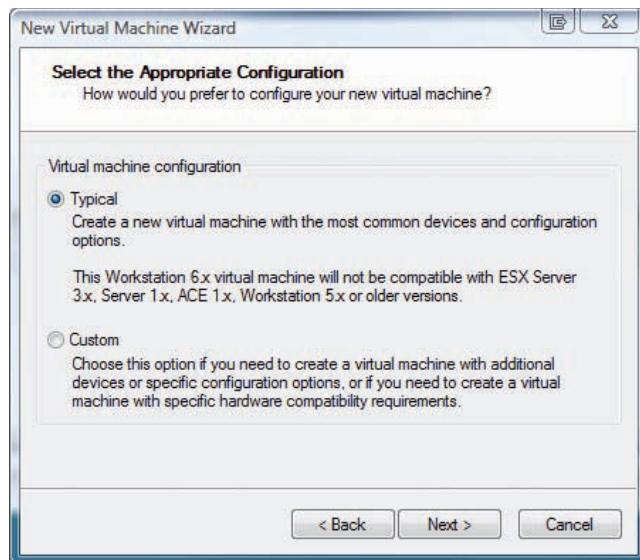


Figure C-1 The Select the Appropriate Configuration window

3. In the Select a Guest Operating System window (see Figure C-2), verify that the **Microsoft Windows** option button is selected. Click the **Version** list arrow, and click **Windows Server 2008**. Click **Next**.

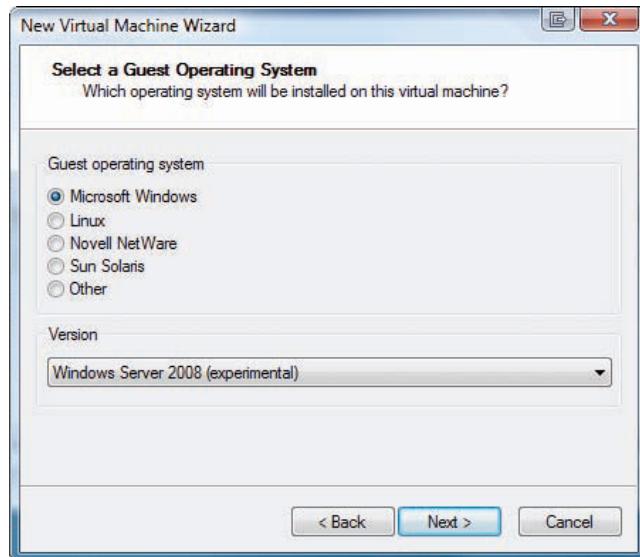


Figure C-2 The Select a Guest Operating System window

4. In the Name the Virtual Machine window, type **ServerXX** (replacing XX with your student number) in the Virtual machine name text box, and then click **Next**.
5. In the Network Type window (see Figure C-3), verify that the **Use bridged networking** option button is selected, or ask your instructor whether to choose a different network connection type. Click **Next**.

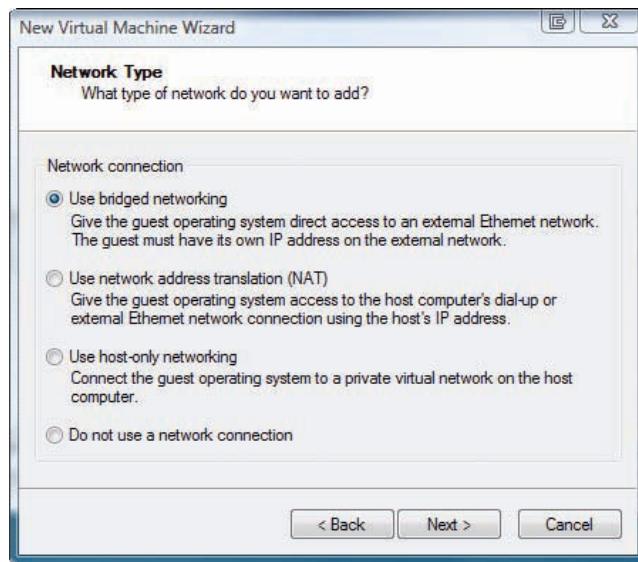


Figure C-3 The Network Type window

6. In the Specify Disk Capacity window (see Figure C-4), verify that the amount in the Disk size (GB) is 16.0 (recommended minimum), and then click **Finish**.

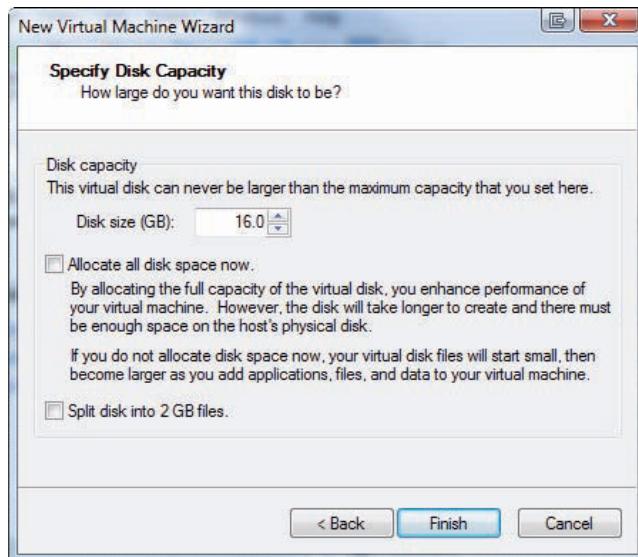


Figure C-4 The Specify Disk Capacity window

7. In the Virtual machine created successfully window, click **Close**. Review the configuration of your virtual machine (see Figure C-5). Ask your instructor whether any changes should be made.

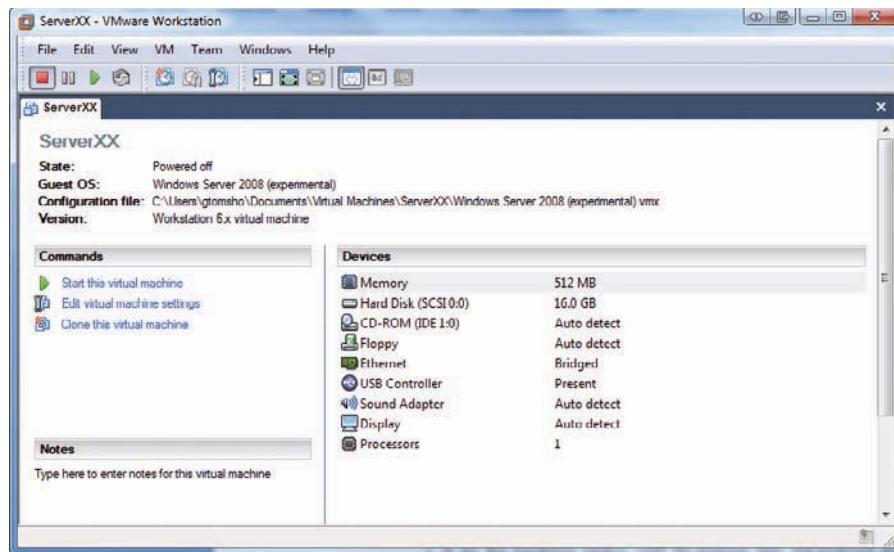


Figure C-5 Virtual machine configuration summary

8. Insert the Windows Server 2008 installation DVD in your computer's DVD-ROM drive. In VMware Workstation, click the **Start this virtual machine** link. From this point, the instructions are for installing Windows Server 2008 are the same as on a physical computer. Note that you must click inside the VMware window to transfer keyboard and mouse control to the virtual machine. To transfer control back to your physical computer, press **Ctrl+Alt**.
9. In the first installation window, verify the language, time, and keyboard choices for your environment. Make changes if necessary, and then click **Next**.
10. In the next window, click the **What to know before installing Windows** link. Browse through the help document, and then close it. Click **Install now**.
11. In the next window, if necessary, enter your product key, and then click **Next**. Click **Windows Server 2008 Enterprise (Full Installation)** in the list box, and then click **Next**.
12. If necessary, click the option to accept the license agreement, and then click **Next**. In the Which type of installation do you want? window, click **Custom (advanced)**.
13. In the Where do you want to install Windows? window, click **Drive options (advanced)**. In the window that opens, you can select options for drive partitions and load drivers for a disk controller. If you simply click Next with an unallocated disk selected, Windows uses the entire disk and formats it as NTFS. Click to select **Disk 0 Unallocated Space**, and then click **Next**. Now you can just sit back and let Windows do the rest. Your computer restarts at least twice, and then you see a prompt to change the password. Click **OK**.



In the Where do you want to install Windows? window, you can press Shift+F10 to open a command prompt window in the MINWINPC environment. From this command prompt, you can use a host of utilities, including Diskpart for performing advanced disk configuration tasks.

14. In the next window, enter **Password01** twice, and then click the arrow to log on. In the message box stating that your password has been changed, click **OK**.
15. After you're logged on, the Initial Configuration Tasks applet is displayed. If you're continuing to another activity in Server 2008 right away, you can leave this window open, or you can log off.



Activity 2-1: Installing Windows Server 2008 in Microsoft Virtual PC 2007

ACTIVITY

Time Required: 30 minutes to more than an hour

Objective: Install Windows Server 2008.

Description: You're ready to install Windows Server 2008 on your client's new network. You have verified the hardware configuration and have the installation DVD in hand. The server has a single hard drive and all space is unallocated, so there's no need to change the BIOS boot order.

1. First, you must create the virtual machine. Start Microsoft Virtual PC 2007, and click the **New** button to start the New Virtual Machine Wizard. Click **Next** in the welcome window.
2. In the Options window (see Figure C-6), verify that the **Create a virtual machine** option button is selected, and then click **Next**.

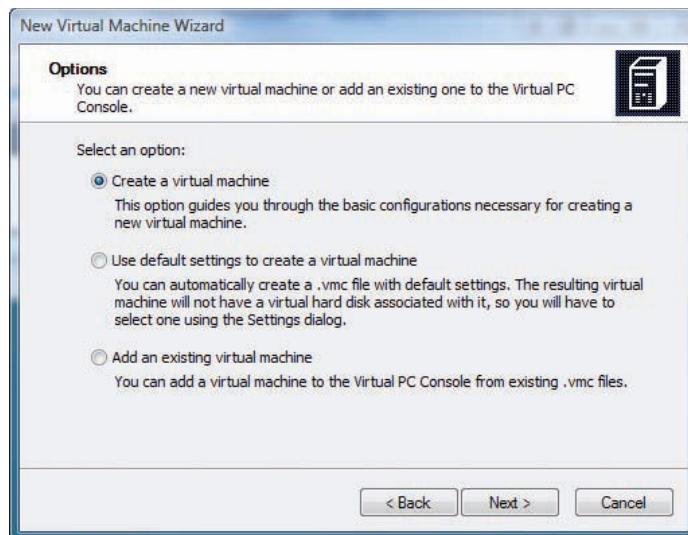


Figure C-6 The Options window

3. In the Virtual Machine Name and Location window (see Figure C-7), type **ServerXX** in the Name and location text box, and then click **Next**.

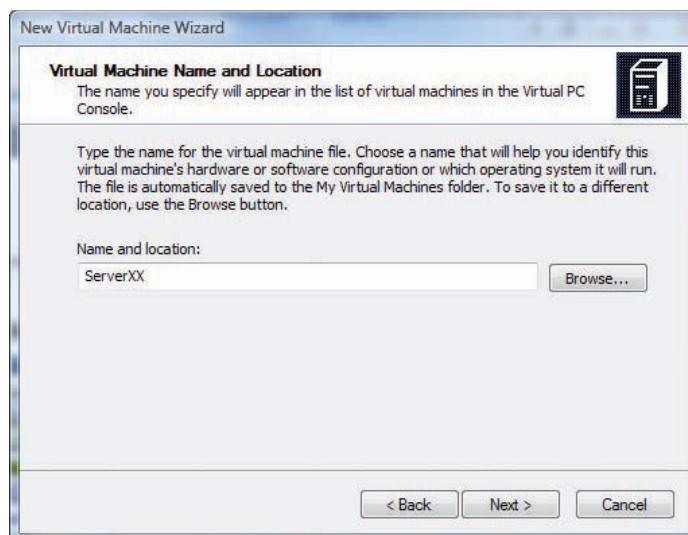


Figure C-7 The Virtual Machine Name and Location window

4. In the Operating System window, click the **Operating system** list arrow and click **Windows Server 2003** in the list. (At the time of this writing, Windows Server 2008 is not an option in Virtual PC 2007.) Click **Next**.
5. In the Memory window, click the **Adjusting the RAM** option button (see Figure C-8), type **512** in the MB text box, and then click **Next**.

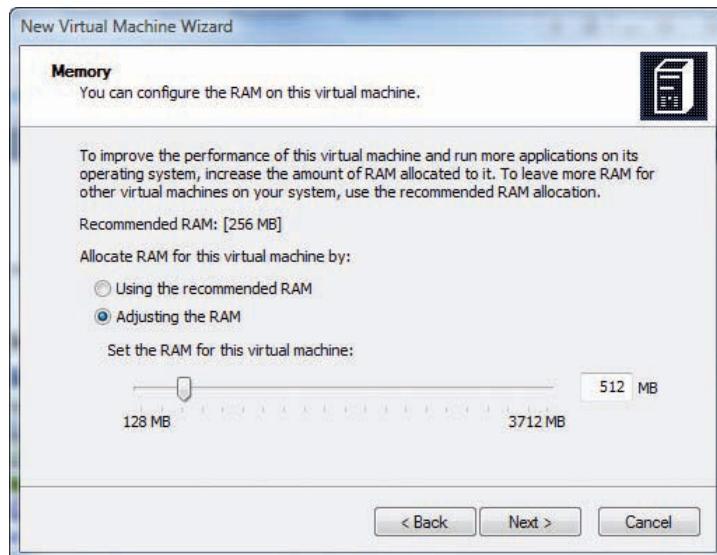


Figure C-8 Adjusting the RAM

6. In the Virtual Hard Disk Options window, click the **A new virtual hard disk** option button, and then click **Next**.
7. In the Virtual Hard Disk Location window, accept the default location and size for the virtual hard disk file, click **Next**, and then click **Finish**.
8. Insert the Windows Server 2008 installation DVD in your computer's DVD-ROM drive. In the Virtual PC Console (see Figure C-9), click the **Start** button. From this point, the instructions for installing Windows Server 2008 are the same as on a physical computer.

If the virtual machine doesn't boot to the DVD-ROM drive automatically, click CD, Use Physical Drive from the menu. Then click Action, Reset from the menu.

NOTE

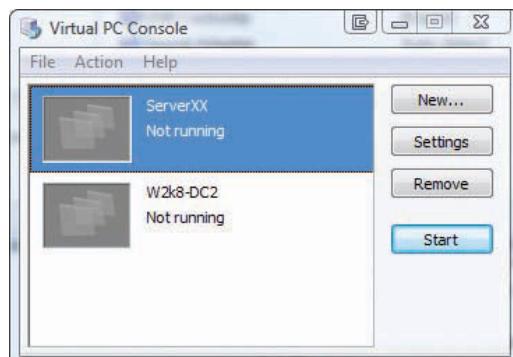


Figure C-9 The Virtual PC Console

9. In the first installation window, verify the language, time, and keyboard choices for your environment. Make changes if necessary, and then click **Next**.
10. In the next window, click the **What to know before installing Windows** link. Browse through the help document, and then close it. Click **Install now**.
11. In the next window, if necessary, enter your product key, and then click **Next**. Click **Windows Server 2008 Enterprise (Full Installation)** in the list box, and then click **Next**.
12. If necessary, click the option to accept the license agreement, and then click **Next**. In the Which type of installation do you want? window, click **Custom (advanced)**.
13. In the Where do you want to install Windows? window, click **Drive options (advanced)**. In the window that opens, you can select options for drive partitions and load drivers for a disk controller. If you simply click **Next** with an unallocated disk selected, Windows uses the entire disk and formats it as NTFS. Click to select **Disk 0 Unallocated Space**, and then click **Next**. Now you can just sit back and let Windows do the rest. Your computer restarts at least twice, and then you see a prompt to change the password. Click **OK**.



In the Where do you want to install Windows? window, you can press Shift+F10 to open a command prompt window in the MINWINPC environment. From this command prompt, you can use a host of utilities, including Diskpart for performing advanced disk configuration tasks.

14. In the next window, enter **Password01** twice, and then click the arrow to log on. In the message box stating that your password has been changed, click **OK**.
15. After you're logged on, the Initial Configuration Tasks applet is displayed. If you're continuing to another activity right away, you can leave this window open, or you can log off.



Activity 2-7: Installing Server Core in VMware Workstation 6.5

Time Required: 30 minutes or longer, depending on the server's speed

Objective: Install Server Core.

Description: You're unfamiliar with the new Server Core installation option in Windows Server 2008. You have read about some benefits of using Server Core in your network, but you want to become familiar with it before deploying it in a production environment.

1. First, you must create the virtual machine. Start VMware Workstation. Click **File** from the menu, point to **New**, and click **Virtual Machine** to start the New Virtual Machine Wizard. Click **Next** in the welcome window.
2. In the Select the Appropriate Configuration window, verify that the **Typical** option button is selected, and then click **Next**.
3. In the Select a Guest Operating System window, verify that the **Microsoft Windows** option button is selected. Click the **Version** list arrow, and click **Windows Server 2008 (experimental)**. Click **Next**.
4. In the Name the Virtual Machine window, type **ServerCore** in the Virtual machine name text box, and then click **Next**.
5. In the Network Type window, verify that the **Use bridged networking** option button is selected, or ask your instructor whether to choose a different network connection type. Click **Next**.
6. In the Specify Disk Capacity window, verify that the amount in the Disk size (GB) is 16.0 (recommended minimum), and then click **Finish**.
7. In the Virtual machine created successfully window, click **Close**. Review the configuration of your virtual machine. Ask your instructor whether any changes should be made.
8. Insert the Windows Server 2008 installation DVD in your computer's DVD-ROM drive. In VMware Workstation, click the **Start this virtual machine** link. From this point, the instructions are for installing Windows Server 2008 are the same as on a physical computer. Note

- that you must click inside the VMware window to transfer keyboard and mouse control to the virtual machine. To transfer control back to your physical computer, press **Ctrl+Alt**.
9. In the first installation window, verify the language, time, and keyboard choices for your environment. Make changes if necessary, and then click **Next**.
 10. In the next window, click **Install now**. In the next window, if necessary, enter your product key, and then click **Next**.
 11. Click **Windows Server 2008 Enterprise (Server Core Installation)** in the list box, and then click **Next**.
 12. If necessary, click the option to accept the license agreement, and then click **Next**. In the Which type of installation do you want? window, click **Custom (advanced)**.
 13. In the Where do you want to install Windows? window, click **Disk 0 Unallocated Space**, and then click **Next**.
 14. When the installation is finished, click **Action, Send Ctrl-Alt-Del** from the menu to log on.
 15. Click the **Other User** icon. In the User Name text box, type **Administrator**, and then click the arrow next to **Password prompt**. (Don't enter a password at this time; the initial password for Administrator is blank.)
 16. In the next window, you're prompted to change the user's password. Click **OK**.
 17. Type **Password01** in the New password text box and the Confirm password text box.
 18. Click the arrow next to the Confirm password text box. When you see a message that the password has been changed, click **OK**. You're now logged on.



Activity 2-7: Installing Server Core in Microsoft Virtual PC 2007

Time Required: 30 minutes or longer, depending on the server's speed

Objective: Install Server Core.

Description: You're unfamiliar with the new Server Core installation option in Windows Server 2008. You have read about some benefits of using Server Core in your network, but you want to become familiar with it before deploying it in a production environment.

1. First, you must create the virtual machine. Start Microsoft Virtual PC 2007, and click the **New** button to start the New Virtual Machine Wizard. Click **Next** in the welcome window.
2. In the Options window, verify that the **Create a virtual machine** option button is selected, and then click **Next**.
3. In the Virtual Machine Name and Location window, type **ServerCore** in the Name and location text box, and then click **Next**.
4. In the Operating System window, click the **Operating system** list arrow and click **Windows Server 2003** in the list. (At the time of this writing, Windows Server 2008 is not an option in Virtual PC 2007.) Click **Next**.
5. In the Memory window, click the **Adjusting the RAM** option button, type **512** in the MB text box, and then click **Next**.
6. In the Virtual Hard Disk Options window, click the **A new virtual hard disk** option button, and then click **Next**.
7. In the Virtual Hard Disk Location window, accept the default location and size for the virtual hard disk file, click **Next**, and then click **Finish**.
8. Insert the Windows Server 2008 installation DVD in your computer's DVD-ROM drive. In the Virtual PC Console, click the **Start** button. From this point, the instructions for installing Windows Server 2008 are the same as on a physical computer.
9. In the first installation window, verify the language, time, and keyboard choices for your environment. Make changes if necessary, and then click **Next**.

10. In the next window, click **Install now**. In the next window, if necessary, enter your product key, and then click **Next**.
11. Click **Windows Server 2008 Enterprise (Server Core Installation)** in the list box, and then click **Next**.
12. If necessary, click the option to accept the license agreement, and then click **Next**. In the Which type of installation do you want? window, click **Custom (advanced)**.
13. In the Where do you want to install Windows? window, click **Disk 0 Unallocated Space**, and then click **Next**.
14. When the installation is finished, click **Action, Send Ctrl-Alt-Del** from the menu to log on.
15. Click the **Other User** icon. In the User name text box, type **Administrator**, and then click the arrow next to the Password text box. (Don't enter a password at this time; the initial password for Administrator is blank.)
16. In the next window, you're prompted to change the user's password. Click **OK**.
17. Type **Password01** in the New password text box and the Confirm password text box.
18. Click the arrow next to the Confirm password text box. When you see a message that the password has been changed, click **OK**. You're now logged on.



Activity 2-11: Configuring the Server Core Firewall for Ping

Time Required: 10 minutes

Objective: Configure the Windows Server 2008 firewall to allow Echo Request packets.

Description: You have configured networking for your Windows Server 2008 Server Core network, and now you want to test the configuration by pinging known IP addresses and then ping-
ing your server from another computer. In this activity, you work with two virtual machines
rather than a partner computer.

1. Log on to Server Core as Administrator and open a command prompt window, if necessary.
Log on to ServerXX as Administrator and open a command prompt window.
2. On ServerXX, to view your basic IP address settings, type **ipconfig** and press **Enter**.
3. Ping your default gateway by typing **ping 192.168.100.1** (or the address Ipconfig displayed as your default gateway) and pressing **Enter**. If it's successful, you should receive output that starts with "Reply from *ip_address*" (substituting the address you typed after the Ping command for *ip_address*.)
4. If Step 3 was successful, type **ping 192.168.100.1XX** (or the IP address Ipconfig displayed for your Server Core computer) and press **Enter**. If the ping isn't successful, you should see the message "Request timed out".
5. To change the firewall settings so that Echo Request packets are permitted through the firewall, on your *Server Core* computer, type **netsh firewall set icmpsetting 8** and press **Enter**.
6. From ServerXX, try to ping your Server Core computer again by typing **ping 192.168.100.1XX** (or the IP address Ipconfig displayed for your Server Core computer) and pressing **Enter**. You should receive successful replies. If not, verify that your IP address settings are correct and the command in Step 5 was entered correctly.



If you want to disable ping requests again, simply type **netsh firewall set icmpsetting 8 disable** and press Enter.

7. If you're continuing to the next activity in Chapter 2, leave the command prompt windows open.

This page intentionally left blank

A Step-by-Step Guide to Using Server Virtualization Software

Virtualization enables a school or student to get the most out of computer resources. Schools can use virtualization to turn a single server-grade computer into a virtual server that can host two, three, or more operating systems. For example, one computer can house three virtual servers running Windows Server 2008. This capability saves the school money on servers and enables more students to be able to work on their own operating systems.

Another capability of virtualization is the ability for a school or student to turn a single PC into a virtual system on which to run another operating system—without having to alter the current operating system running on the PC. A single computer lab PC or a student’s home PC can be turned into a host for Windows Server 2008. This is ideal, for example, when your textbook comes with an evaluation copy of Windows Server 2008. You can install virtualization software and then install Windows Server 2008 for completing hands-on projects and activities. You can use your originally installed operating system, such as Windows XP or Vista, and also use Windows Server 2008 in a virtual “window” or “session,” for example. When you are finished learning Windows Server 2008, you simply remove the virtualization software and you’re back where you started with your original operating system.

This appendix is a step-by-step guide for turning a single computer into a virtual system hosting one or more virtual machines. The main focus is on three popular virtualization systems that are available free:

- *Microsoft Virtual PC*—Intended for a workstation-grade PC to host another operating system, such as a Windows Server 2008 virtual machine
- *Microsoft Virtual Server*—Intended for a server-grade computer to host multiple virtual machines, including Windows Server 2008 and other operating systems
- *VMware Server*—Intended for server-grade computers to host multiple virtual machines, such as Windows Server 2008

For each of these virtualization systems, you learn how to:

- Obtain a free download version.
- Install it.
- Create a virtual machine.
- Install a guest operating system, such as Windows Server 2008, in the virtual machine, and then how to access that virtual machine's operating system.
- Install ISO images.
- Configure virtual networking.
- Configure hardware components.

At the end of the appendix, a brief look at VMware Workstation 6 and Microsoft Hyper-V is also provided.

Microsoft Virtual PC

Microsoft Virtual PC can be installed in Microsoft Windows XP, Vista, and Windows Server 2003 operating systems. At this writing, it is not adapted to be installed in Windows Server 2008. Although Microsoft Virtual PC is intended to host workstation operating systems as virtual machines, you can also use it to create a Windows Server 2008 Standard Edition virtual machine.

Microsoft Virtual PC is available from Microsoft as a free download. From a student's perspective, this is ideal for running the Windows Server 2008 Standard Edition evaluation DVD (available from Microsoft at www.microsoft.com) on a Windows XP or Windows Vista computer. It works equally well on Windows XP or Windows Vista computers in a student computer lab.

Requirements for Microsoft Virtual PC

At this writing, Microsoft Virtual PC 2007 with Service Pack 1 (SP1) is the most recently available version. It can be loaded on the following operating system hosts:

- Windows XP Professional with SP2 or SP3
- Windows Server 2003 Edition SP2 (x86 or x64)
- Windows Vista Business Edition (x86 or x64 versions with or without SP1)
- Windows Vista Enterprise Edition (x86 or x64 versions with or without SP1)
- Windows Vista Ultimate Edition (x86 or x64 versions with or without SP1)

The hardware requirements for Microsoft Virtual PC 2007 SP1 are as follows:

- *CPU*—Intel Celeron, Pentium II, Pentium III, Pentium 4, Core Duo, or Core 2 Duo CPU or AMD Athlon or Duron CPU (400 MHz or faster; x86 or x64).
- *RAM*—Enough RAM for at least the minimum requirements of the total number of operating systems you will be running. For example, if you are running Windows XP Professional (128 MB minimum) and want to load Windows Server 2008 (512 MB minimum) as a virtual machine, you need a minimum of 640 MB to 1 GB RAM. If Windows Vista is the host and you want to run a Windows Server 2008 Standard Edition virtual machine, you need a minimum of 1 GB RAM.
- *Disk space*—Enough disk storage for the operating systems you plan to run. For example, Windows XP requires at least 1.5 GB, Windows Vista requires at least 15 GB, and Windows Server 2008 requires at least 10 GB (but 15 GB to 20 GB is better for using different roles and services).

Virtual Machine Operating Systems Supported

After Virtual PC 2007 SP1 is loaded, you can run any of the following operating systems as virtual machines (guests) in Virtual PC 2007 SP1:

- Windows 98 and 98 SE
- Windows Me
- Windows 2000 Professional
- Windows XP Home or Professional with SP1, SP2, SP3 (or no service pack)
- Windows Vista Business Edition (x86 or x64 versions with or without SP1)
- Windows Vista Enterprise Edition (x86 or x64 versions with or without SP1)
- Windows Vista Ultimate Edition (x86 or x64 versions with or without SP1)
- Windows Server 2008 Standard Edition
- OS/2 Warp

How to Download Microsoft Virtual PC

Microsoft Virtual PC can be downloaded from Microsoft's Web site for no cost. The steps to download Microsoft Virtual PC 2007 SP1 are as follows:

1. Log on to your computer.
2. Create a folder in which to download the setup.exe file for Microsoft Virtual PC (such as a temporary folder or a folder under your Program Files folder).
3. Open a Web browser, such as Microsoft Internet Explorer.
4. Go to the URL www.microsoft.com/downloads/Search.aspx?displaylang=en (for English).



Web links and specific instructions change periodically. You might need to search www.microsoft.com for the most current link if these links do not work.

NOTE

5. Look for Microsoft Virtual PC in the Popular Downloads or Recommended Downloads sections. (Also check the New Downloads section in case a new version is available.) If you find it in one of these sections, click the link for **Microsoft Virtual PC**. If you do not see a link, click **Windows** under the Product Families heading. Click the **down arrow** in the Show downloads for list box, and click **Microsoft Virtual PC**. Click **Go**.
6. Click the link for **VPC 2007 SP1**.



To use Microsoft Virtual PC 2007 with Windows Server 2008 or Windows Vista as the virtual machine (guest) operating system, you must use the download containing SP1.



NOTE

7. Click the **Download** button for the setup.exe file that matches your computer, which is 32 BIT\setup.exe for an x86 computer or 64 BIT\setup.exe for an x64 computer.
8. Click the **Save** or **Save File** button.
9. Select the folder you created in which to save the setup.exe file.
10. Click **Save**.
11. Click **Close** in the Download complete dialog box.
12. Close your Web browser.

How to Install Microsoft Virtual PC

Microsoft Virtual PC 2007 SP1 is easy to install. The installation steps are as follows:

1. Browse to the folder in which you saved the setup.exe file for Microsoft Virtual PC.
2. Double-click **setup.exe**.
3. Click **Next** after the Microsoft Virtual PC 2007 SP1 Wizard starts (see Figure D-1).



Figure D-1 Microsoft Virtual PC 2007 SP1 Wizard

4. Click the option button for **I accept the terms in the license agreement**. Click **Next**.
5. Enter your username and name of your organization (if an organization name is appropriate). Notice that the product key should already be provided. Also, if you see this option, leave **Anyone who uses this computer (All Users)** selected. Click **Next**.
6. Click **Install**. The installation process takes a few minutes.
7. Click **Finish**.

Creating a Virtual Machine and Installing a Guest OS

After Microsoft Virtual PC 2007 SP1 is installed, the next step is to create a virtual machine in which to install a guest operating system.



Microsoft Virtual PC 2007 SP1 might not be compatible with hardware virtualization on some CPUs. If you experience a crash dump when configuring the virtual machine or loading the guest OS, first make sure you have enabled hardware virtualization in Step 12. If this does not work, try disabling hardware virtualization in the BIOS and restart these steps from the beginning.

The following are sample steps for setting up the virtual machine with Windows Server 2008 Standard Edition as the guest operating system:

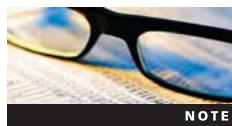
1. From the host operating system, such as Windows XP or Windows Vista, click **Start**.
2. Point to **All Programs** and click **Microsoft Virtual PC**.
3. The New Virtual Machine Wizard opens (see Figure D-2). Click **Next**.
4. Ensure that **Create a virtual machine** is selected and click **Next**.
5. Provide a name for the virtual machine, such as **Windows Server 2008**. Click **Next**.
6. Ensure that **Windows Server 2008** is selected as the operating system to install and click **Next**.



Figure D-2 New Virtual Machine Wizard

7. Ensure that at least 512 MB to 1 GB RAM is allocated for the virtual machine. If necessary, click **Adjusting the RAM** and use the slider bar to allocate enough memory. Click **Next**.
8. Ensure that **A new virtual hard disk** is selected and click **Next**.
9. Make sure the virtual hard disk is sized to meet your needs, or leave the default size. (You need 15 GB for Windows Server 2008 and might use at least 20–40 GB, for example.) Click **Next**.
10. Click **Finish**.
11. You should see the Virtual PC Console open on the desktop. If it is not open, click Start, point to **All Programs**, and click **Microsoft Virtual PC**.
12. You can configure options at this point by clicking **File, Options** from the menu. Click each option to see what it does and configure any options as necessary. When you are finished, click **OK**. The options are as follows:
 - **Restore at Start**—Pauses a running virtual machine when you exit the console and restores the virtual machine when you reopen the console.
 - **Performance**—Specifies how CPU time is allocated to virtual machines and specifies what happens when Virtual PC is a process running in the background.
 - **Hardware virtualization**—Enable hardware virtualization, if your CPU has this capability.
 - **Full-Screen Mode**—Enables the screen resolution to be adjusted so it is the same for the host and guest OSs. (Note the previous caution if this setting is enabled.)
 - **Sound**—Configures virtual machine sound. Sound is muted by default. If you enable it, the sounds from the host and guest OS can be difficult to differentiate.
 - **Messages**—Turn off error and informational messages from Virtual PC.
 - **Keyboard**—Specifies the host key for the guest operating system. The default host key is the right Alt key. When you press this key, you can switch the mouse between the guest and host windows and you can execute guest key combinations, such as pressing Alt+Delete to send the Ctrl+Alt+Delete key combination to the guest OS for logging on.
 - **Mouse**—Specifies how the pointer is captured for use in the virtual machine window.
 - **Security**—Determines how to control access to Virtual PC functions.
 - **Language**—Specifies the language to use for Virtual PC.

13. Insert the Windows Server 2008 Standard Edition installation DVD.



At this point, you could install any of the supported guest operating systems. If you are installing a different operating system, you would insert the CD/DVD now, complete Step 14, and then Steps 15 through 30 (or whatever steps are required) would be unique to the operating system you are installing.

14. Click the **Start** button in the Virtual PC Console. This opens a second larger window, which is the Microsoft Virtual PC 2007 console. Wait a few minutes for the DVD to start loading. Click in the console to enable the mouse to operate in this window. (If necessary, you can switch the mouse movement back so that it can go all over the screen by pressing the right Alt key, which is the “host” key.)



Occasionally, the mouse might seem stuck, move slowly, or stop functioning in the active portion of the console. If this happens, close all windows and go to Step 11 to start again. Also, some installation processes take longer to install in a virtual machine. Don’t close the window or stop the installation prematurely, even if you seem to be stuck on a black screen for several minutes.

15. Click the language to install, such as **English**, in the Language to install drop-down list. In the Time and currency format list box, make your selection, such as **English (United States)**. In the Keyboard or input method list box, make your selection, such as **US**. Click **Next**.
16. Click **Install now**.
17. Click **Windows Server 2008 Standard (Full Installation)** and click **Next**.
18. Read the license terms, click the **I accept the license terms** check box, and click **Next**.
19. Click **Custom (advanced)**.
20. You’ll see the amount of unallocated disk space highlighted, which is the disk space you specified when you configured the virtual machine. Ensure that it is highlighted and click **Next**.
21. The installation program begins installing Windows Server 2008. You’ll see progress information about copying files, expanding files, installing features, installing updates, and completing the installation. This part of the installation can take 30 minutes or longer.
22. The installation program restarts the operating system.
23. You see the message *Please wait while Windows sets up your computer*.
24. Next, you see the Install Windows window in the Completing installation phase.
25. The system restarts again.
26. You’ll see the message (a red circle with a white x in it) *The user’s password must be changed before logging on the first time*. Click **OK**. (You might have to click inside the active portion of the console first to have the mouse function in it.)
27. Enter a new password for the Administrator account and then enter the same password again to confirm it. Click the **blue circle** with the white right-pointing arrow inside.



If you enter a password that is not a strong password, you’ll see the message (with a white x in a red circle) *Unable to update the password*. This means the value provided for the new password does not meet the length, complexity, or history requirements of the domain. Click **OK** and enter a different password that is more than seven characters and uses letters, numbers, and special symbols, such as &.

28. When you see the message *Your password has been changed*, click **OK**.
29. At this point, the Windows desktop is displayed and the Initial Configuration Tasks window opens.

30. You can configure Windows Server 2008 as you would in a nonvirtual environment.
31. When you close the Microsoft Virtual PC 2007 console, you can turn off the virtual machine or save its current state. Unless you want to save its state, a good practice is to shut down the server before closing the window. (Saving the state means to keep the server in its current state, without shutting it down.) When you shut down the server in this way, the Microsoft Virtual PC 2007 console closes but leaves the Virtual PC Console open. Also, to restart the virtual machine, open the Virtual PC Console, click Start, and wait for the system to boot in the Microsoft Virtual PC 2007 console.

**NOTE**

When you log on to Windows Server 2008 from the console, the normal Ctrl+Alt+Delete key sequence does not work. Instead, click the Action menu and press Ctrl+Alt+Delete. Another alternative is to press right Alt+Delete.

Installing an OS from an ISO Image

An ISO file is an optical disc (CD/DVD) image file with the .iso file extension. An ISO file can be accessed in several ways, such as from a CD/DVD, from a hard drive, or as a shared network file. Typically, when you download an operating system, such as an evaluation copy of a Windows operating system, you download an ISO file. One advantage of using an ISO file for installing a guest operating system on a virtual machine is that the installation process can go faster. Virtual PC enables you to install from an ISO file by using the following general steps:

1. Follow Steps 1 through 12 in the previous section, “Creating a Virtual Machine and Installing a Guest OS.”
2. Click the **Start** button in the Virtual PC Console.
3. After the Microsoft Virtual PC 2007 console opens, press the **right Alt** key if necessary to access the menu at the top of the window.
4. Click **CD, Capture ISO Image** from the menu.
5. Navigate to the ISO file, click the file, and click the **Open** button.
6. You return to the Microsoft Virtual PC 2007 console, and then you should restart the virtual machine.

Configuring Networking and Hardware Options

You can configure a range of networking and hardware options in Microsoft Virtual PC. For example, if the host computer has two or more NICs, you can specify which NIC to use for a virtual machine. In another example, you might need to create one or more additional virtual hard disks for a virtual machine.

Use these steps to configure networking and hardware options:

- 
1. Open the Virtual PC Console, if it is not open. Also, ensure that the virtual machine is turned off before you start.
 2. Click the **Settings** button, or click the **Action** menu and click **Settings** to open the dialog box shown in Figure D-3.
 3. Click **Networking** in the left pane. If your computer has multiple adapters, you can select the specific adapter (or multiple adapters) to associate with a virtual machine.
 4. In the right pane, click the list arrow for the adapter that is selected by default. The following options are available:
 - *Not connected*—Used if you do not intend to enable the virtual machine to access a network (including the Internet) and so that it cannot be accessed from a network.
 - *Local*—If two or more virtual machines are set up, they can access each other; however, virtual machines cannot access the network.

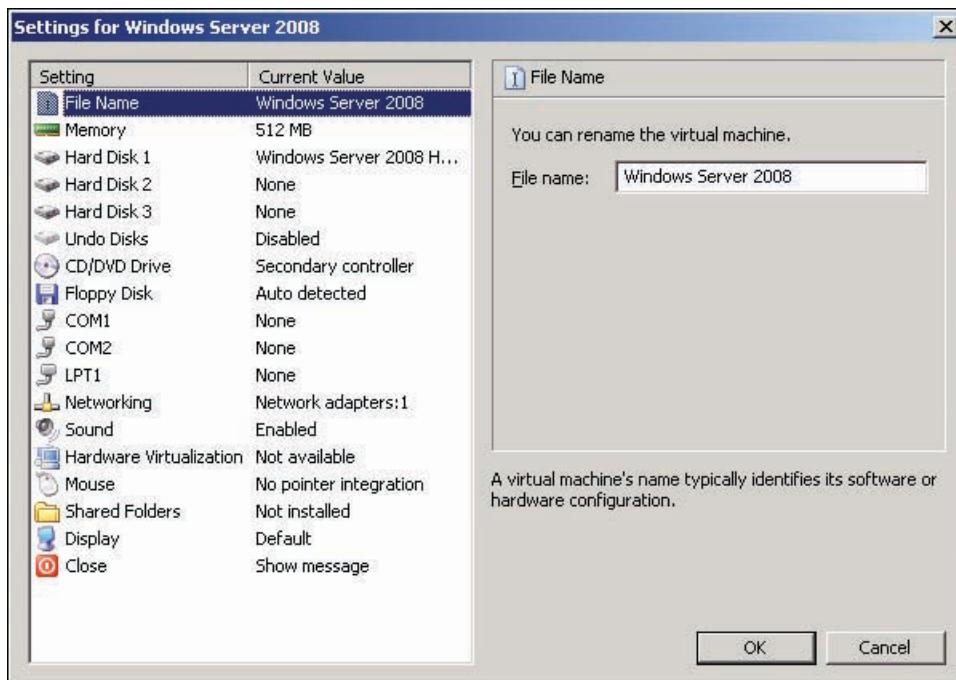


Figure D-3 Settings for a virtual machine

- *NetworkInterfaceName*—The actual name of a NIC model, such as an Intel or Broadcom NIC, that the virtual machine is directly connected to for regular network and Internet access. With this selection, network configuration tasks that apply to other network computers also apply to the virtual machine. If a DHCP server is on the network or if the network uses a router with Network Address Translation (NAT), the virtual machine’s network connection can be configured to use these services. The same applies if a DNS server is set up.
- *Shared Networking (NAT)*—Used to create a private Virtual PC network that has a virtual DHCP server and a virtual NAT-enabled router or firewall. Typically, the first virtual computer created acts as the DHCP server and provides NAT services. In this arrangement, Microsoft Virtual PC performs as a virtual DHCP server, leasing IP addresses for virtual machines in the range of 192.168.131.1 to 192.168.131.253. Further, the virtual machines appear as computers in a private NAT-protected network. A connection to the Internet is shared among the virtual machines and is protected in a way similar to a NAT-enabled router or firewall.
- *Loopback Adapter*—You see this option if the operating system is configured to have a Microsoft loopback adapter (configured as a network adapter, such as through the Add Hardware option in Control Panel). This option is used in two contexts. One context is when no physical network connection is present, but you want to simulate network connectivity between the host and all virtual machines. A second context is when you are creating a network with many routers and firewalls as well as many virtual machines.

5. Make the networking selections that are appropriate for your situation.
6. Click **Memory** in the left pane. Notice that you can increase the memory allocation for the virtual machine by using the slider bar in the right pane.
7. In the left pane, click **Hard Disk 1** and notice that the right pane shows the path to the virtual hard disk file. Also, notice you can configure the Hard Disk 2 and Hard Disk 3 options for additional virtual hard disks. To do this, click Hard Disk 2 in the left pane, for example,

and click the Virtual Disk Wizard button in the right pane. (A virtual machine can have up to three hard disks.)

8. Click **CD/DVD Drive** in the left pane and notice you can attach a CD or DVD drive via the right pane.
9. Click **Hardware Virtualization** in the left pane, and notice in the right pane that you can enable hardware virtualization, if your computer supports it.
10. Notice you can configure additional hardware, such as communication (COM) ports, a floppy disk, printer (LPT) ports, sound, the mouse, the display, and other devices.
11. When you are finished with the configurations, click **OK**.

Host Key Options

Because a virtual machine represents an operating system running inside an operating system, it is necessary to have a way to use the keyboard so that the keys you press communicate directly with the guest operating system. For example, you'll notice that pressing Ctrl+Alt+Delete opens the Windows Security dialog box or a menu of options, depending on which version of Windows is the host operating system. It does not take you to a logon screen in the guest operating system.

Microsoft Virtual PC enables you to communicate with the guest operating system by using the host key, which is the right Alt key by default. Table D-1 lists important host key combinations you can use while you are accessing a virtual machine.

Table D-1 Host key options for Microsoft Virtual PC

Keyboard combination	Result
HostKey	Enables you to move the mouse outside the window area used by the guest OS. (Move the mouse back into the guest OS display and click when you want to work in the guest OS.)
HostKey + Delete	The virtual machine OS responds to this as Ctrl+Alt+Delete.
HostKey + P	Toggles the virtual machine between pause and resume.
HostKey + R	Causes the virtual machine to reset.
HostKey + A	Selects all items in the active window in the guest OS.
HostKey + C	Copies selected text and items in the active window in the guest OS.
HostKey + V	Pastes text and items in the active window in the guest OS.
HostKey + Enter	Switches between full screen and window modes.
HostKey + down arrow	Causes the virtual machine to minimize.
HostKey + I	Enables you to install virtual machine additions.

Microsoft Virtual Server

Microsoft Virtual Server 2005 is intended to host server operating systems as virtual machines. At this writing, Microsoft Virtual Server 2005 R2 SP1 is the most recent version. This version supports hardware (integrated in the CPU) virtualization, such as AMD CPUs equipped with AMD-V and Intel CPUs with Intel VT. Other new features include the following:

- Can be installed in x64 operating systems
- Provides support for Internet Small Computer System Interface (iSCSI), which is a technology used in Storage Area Networks (SANs)
- Has the ability to cluster virtual servers on a single computer
- Provides enhanced Active Directory support by publishing Virtual Server binding data through service connection points



Other features of Microsoft Virtual Server include the following:

- Virtual disks can expand dynamically
- Supports most popular x86 operating systems
- Can mount a virtual disk on a different operating system
- Enables use of Volume Shadow Copy Service (VSS) for backups (used in newer versions of Windows operating systems, such as Windows Server 2008 and Vista)
- Offers virtual server management through the Virtual Server Web console
- Can use scripting to control virtual machine setups
- Memory access can be resized

Microsoft Virtual Server Guest Operating Systems Supported

Microsoft Virtual Server can house virtual machines for popular Windows and Linux server and workstation operating systems. The following operating systems can be guests:

- Windows Server 2008 Standard, Enterprise, Datacenter, and Web Server (x86 and x64)
- Windows Server 2003 Standard, Enterprise, Datacenter, and Web Server SP1 or SP2 (x86 or x64)
- Windows Server 2003 Standard, Enterprise, Datacenter, and Web Server R2 (x86 or x64)
- Windows Small Business Server 2003 (Standard and Premium Editions)
- Windows 2000 Server
- Windows XP Professional SP2
- Windows Vista Business, Ultimate, and Enterprise
- Red Hat Enterprise Linux versions 2.1 to 4.0
- SUSE Linux Enterprise Server 9.0
- SUSE Linux versions 9.2 to 10.0



Other operating systems can also run experimentally in Microsoft Virtual Server.

NOTE

Microsoft Virtual Server Host Operating Systems Supported

Microsoft Virtual Server can be installed on the following Windows host operating systems:

- Windows Server 2008 Standard and Enterprise (x86 or x64)
- Windows Server 2003 Standard, Enterprise, and Web Server with SP1 or SP2 (x86 or x64)
- Windows Server 2003 Standard, Enterprise, and Web Server R2 (x86 or x64)
- Windows Small Business Server 2003 (Standard and Premium Editions, also R2 versions)
- Windows 2000 Server with SP3 or SP4
- Windows XP Professional (x86 and x64)
- Windows Vista Business, Ultimate, and Enterprise Editions

Requirements for Microsoft Virtual Server

The hardware requirements for Microsoft Virtual Server 2005 R2 with SP1 are as follows:

- **CPU**—Intel Celeron, Pentium III, Pentium 4, Xeon, or AMD Opteron, Athlon, Athlon 64, Althon X2, Duron, or Sempron (550 MHz or faster; x86 or x64).
- **RAM**—Enough RAM to match at least the minimum requirements of the total number of operating systems you will be running. For example, if you are running Windows XP

Professional (256 MB minimum required for Virtual Server) and want to load Windows Server 2008 (512 MB minimum) as a virtual machine, you need a minimum of 768 MB to 1 GB RAM. If Windows Server 2003 R2 Standard Edition is the host and you want to run a Windows Server 2008 Enterprise Edition virtual machine, then you need a minimum of 768 MB to 1 GB RAM.

- **Disk space**—Enough disk storage for the operating systems you plan to run. For example, Windows Server 2003 R2 Standard Edition requires at least 3 GB, and Windows Server 2008 requires at least 10 GB (but 15 to 20 GB enables you to load more roles and services).

How to Download Microsoft Virtual Server

You can download Microsoft Virtual Server from Microsoft's Web site free by following these steps:

1. Log on to your computer.
2. Establish a folder in which to store the download (such as a temporary folder or a folder under your Program Files folder).
3. Start your Web browser, such as Internet Explorer.
4. Go to the URL www.microsoft.com/downloads or www.microsoft.com/downloads/Search.aspx?displaylang=en (for English).



Web links and specific instructions change periodically. You might need to search www.microsoft.com for the most current link if these links do not work.

NOTE

5. Look for Microsoft Virtual Server in the Popular Downloads or Recommended Downloads sections. (Also check the New Downloads section in case there is a new version.) If you find it in one of these sections, click the link for **Microsoft Virtual Server**. If you do not see a link, ensure that you set the search box near the top of the Web page to **Windows**, if Windows is not already selected. Enter **Virtual Server** in the blank text box next to the Go button, and click **Go**.
6. Click the link for **Virtual Server 2005 R2 SP1**.
7. Click the **Continue** button to register for the free download.
8. The information you provide next depends on whether you have already signed up for Windows Live ID or whether you already have an MSN Hotmail, MSN Messenger, or Passport account. If you already have an account, provide your e-mail address and password for the Windows Live ID information, click **Sign in** to verify your information (and answer any required questions), and click **Continue**. If you do not have an account or do not have a Windows Live ID, follow the steps to sign up for a Windows Live ID.
9. Click the **Download** button for the setup.exe file that matches your computer, which is 32 BIT\setup.exe for an x86 computer or 64 BIT\setup.exe for an x64 computer.
10. Click the **Save** or **Save File** button.
11. Select the folder you created in which to save the setup.exe file.
12. Click **Save**.
13. Click **Close** in the Download complete dialog box.
14. Close your Web browser.



How to Install Microsoft Virtual Server

The general steps for installing Microsoft Virtual Server on the host operating system are as follows:

1. Browse to the folder in which you saved the setup.exe file for Microsoft Virtual Server.
2. Double-click **setup.exe**.

3. Click **Install Microsoft Virtual Server 2005 R2 SP1** (see Figure D-4).

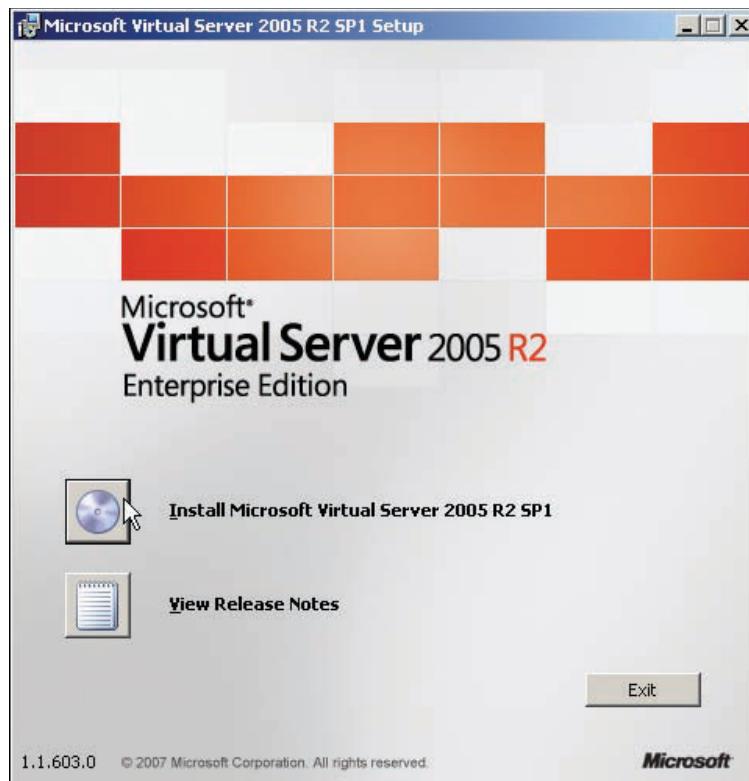


Figure D-4 Installing Microsoft Virtual Server 2005 R2 SP1

4. Click **I accept the terms in the license agreement**. Click **Next**.
5. Enter your username and the name of your organization (if you represent an organization). Notice that the product key information is provided by default. Click **Next**.
6. Ensure that **Complete** is selected in the Setup Type window, as shown in Figure D-5, and click **Next**.



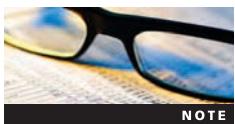
Figure D-5 Selecting the setup type

7. Notice that the Virtual Server Administration Website will be added to Internet Information Services (IIS), and the default Website port is 1024. Further, if you see the option **Configure the Administration Website to always run as the authenticated user (Recommended for most users)**, ensure that it is selected. Click **Next**.

**NOTE**

After you click **Next**, you might see the informational message *The installed version of Internet Information Services (IIS) does not allow multiple websites.* The Virtual Server Administration Website will be added as a virtual directory under the default site.

8. If the Windows Firewall is enabled on your computer, you can have the setup process create firewall exceptions for Virtual Server. Make sure **Enable Virtual Server exceptions in Windows Firewall** is selected, and click **Next**.
9. Click **Install**.
10. If the required IIS components needed for the Virtual Server Administration Website are not already installed, click **Yes** to install them. Click **Install** again, if necessary. You'll see a dialog box showing that the components are being installed.

**NOTE**

In Step 10, if you see a message that the installation program needs to have the IIS World Wide Web service installed and there is no option to install it, this typically means the Virtual Server installation program cannot install IIS. Click **OK** when you see the message, click **Cancel** to stop the installation, and follow the steps for your host OS to install IIS. (You might need the host OS installation CD/DVD.) Start the Virtual Server installation again from Step 1.

11. You'll see a window showing that Microsoft Virtual Server 2005 R2 SP1 is being installed.
12. Click **Finish** and close any open windows.

Creating a Virtual Machine and Installing a Guest OS

After Microsoft Virtual Server is installed, you can use the Virtual Server Administration Website tool to configure Microsoft Virtual Server, configure a virtual machine, and install a guest operating system.

Here are the steps for creating a virtual machine and installing a guest operating system (using Windows Server 2008 as the guest operating system):

1. Click **Start**, point to **All Programs**, and click **Microsoft Virtual Server**.
2. Click **Virtual Server Administration Website**.
3. In the Connect to dialog box, provide a username and password (for an account that has administrator privileges), and click **OK**.
4. If you are using a recent version of the Windows Firewall, you might see the Internet Explorer dialog box to enable you to add this Web site to the list of trusted sites. (You are likely to see this dialog box the first time you access the Virtual Server Administration Website tool.) Click the **Add** button. In the Trusted sites dialog box, click the **Add** button for the site you are adding and click **Close**. Also, if you see the Microsoft Phishing Filter dialog box, select whether you want to turn on the Phishing Filter (turning the filter on is recommended) and click **OK**.
5. The Virtual Server Administration Website tool is displayed through Internet Explorer, as shown in Figure D-6. Notice that the left pane contains options to navigate, create and add virtual machines, manage virtual disks, manage virtual networks, and manage the virtual server.
6. In the left pane under Virtual Machines, click **Create**.
7. Enter the name for the virtual machine and set the virtual machine memory. For Windows Server 2008, you should set it for at least 512 MB to 1024 MB. Also, click **Create a new virtual hard disk** and set at least 15 GB (more is better) for Windows Server 2008. Finally, specify the virtual network adapter, such as an external network interface. Click **Create**.



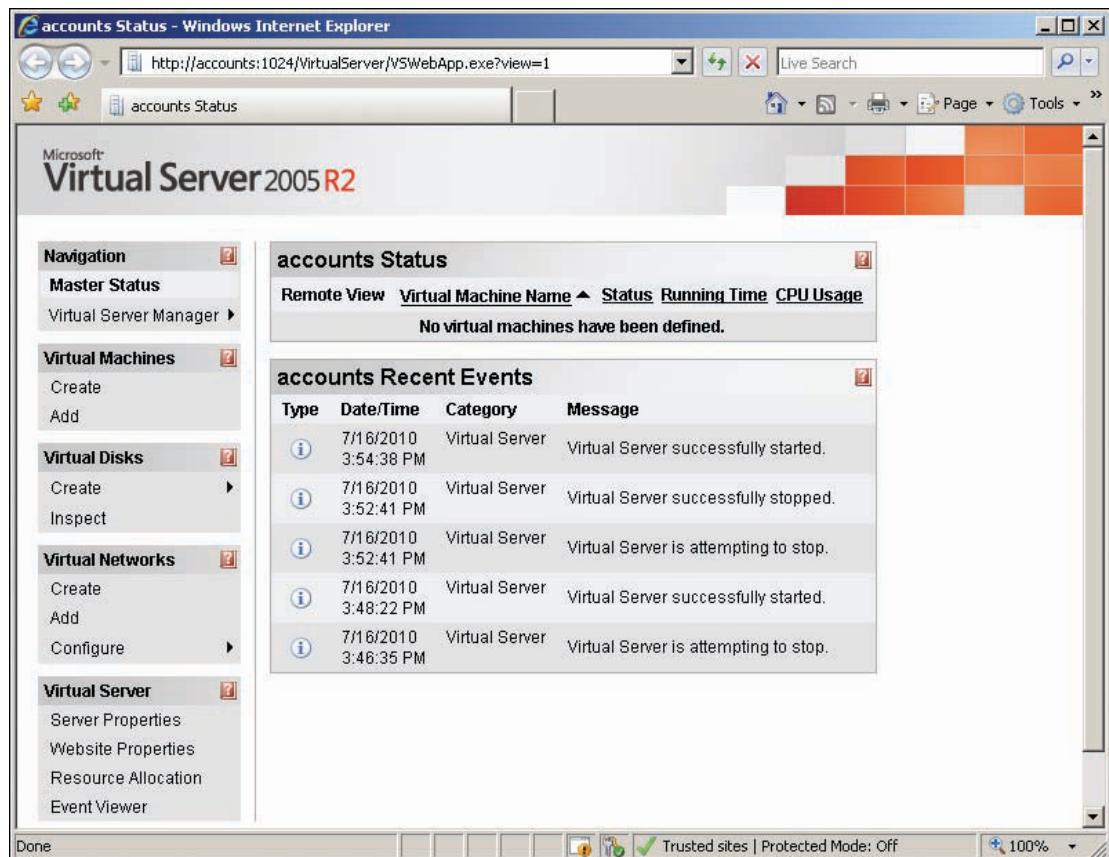


Figure D-6 Virtual Server Administration Website



The virtual network adapter options are Not connected, External Network, and Internal Network. Not connected (the default) does not provide any type of connection, so you can access the virtual machine only from the server. External Network means users can connect to the virtual machine through the computer's network interface card. Internal Network means there can be a connection between virtual machines on the same computer.

8. If you see the option to enable AutoComplete (to remember your entries in Web forms), select whether to use this feature by clicking **Yes** or **No**.
9. In the right pane, review the configuration information for your test server. Notice that you can use this pane to make changes to the configuration. (See “Configuring Networking and Hardware Options,” later in this appendix, for more information about configuring these options.)
10. So that you can access a window in which to use the virtual server, click **Server Properties** under Virtual Server in the left pane.
11. In the right pane, click **Virtual Machine Remote Control (VMRC) Server**.
12. Ensure that the **VMRC server** check box is selected for the **Enable** option and that the TCP/IP address of the host server is entered. (If you have trouble connecting after entering the TCP/IP address of the host server, try leaving the TCP/IP address setting at “All unassigned.”) Also, ensure that Authentication is set to **Automatic**. Click to clear the **Enable** check box for **Disconnect idle connections** (so that you are not disconnected during the OS installation). Click the **Enable** check box for **Multiple VMRC connections** and for **SSL 3.0/TLS 1.0 encryption**.

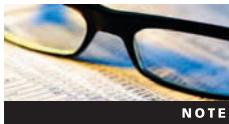
If necessary, set the SSL 3.0/TLS 1.0 certificate to **Keep** or **Request** (if Keep is disabled). Make sure the hostname is the same as the name of the computer you are using. Click **OK** in the lower-right corner of the window. (If you have any problems using VMRC Server, remember that you can come back to this window to adjust any parameters.)

13. In the left pane, point to **Configure** under Virtual Machines and click the name of the virtual machine you created.
14. Next, you need to turn on the virtual machine. In the right pane, click the thumbnail image for the virtual machine to turn on the virtual machine.

**NOTE**

You might see a message that you need to configure Internet Explorer security to proceed. Make the necessary security configurations. Also, if you see a message from Internet Explorer to install an add-on, click the message and click Install ActiveX Control, and then follow the directions to continue.

15. Insert the Windows Server 2008 installation DVD.
16. If necessary, click the thumbnail again for the virtual machine. If you see a security message, click **Yes** to proceed.
17. Enter your username and password (using an account with administrator privileges). Click **OK**.
18. If you see another security message, such as for NTLM Authentication, click **Yes** to proceed.
19. If necessary, scroll down to view the information for working in the Remote Control window. Notice the options Pause, Save State, Turn Off, and Reset for the virtual machine.
20. Scroll back to the top of the Remote Control window.
21. You should see a beginning installation screen for Windows Server 2008. Move the mouse pointer into that screen. (The mouse pointer becomes a small black dot.) Click in the screen until you see the normal arrow for the mouse pointer. Notice that you can work only in the console for the virtual machine. Press the **right Alt** key (the default host key) to be able to use the mouse throughout the Remote Control window. Remember that you can always use the right Alt key to leave the console as needed. (Also, to work inside the console again, click the mouse inside the console.) In the upper-right corner of the Remote Control window, click the down arrow for **Remote Control**. Review the options on the menu, such as Special Keys and Connect To Server.

**NOTE**

When you point to Special Keys, note that pressing the host key (the right Alt key) with the Delete key can be used to send the Ctrl+Alt+Delete key sequence to the virtual machine. (This is important to know later for logging on after you have installed Windows Server 2008.)

22. Move the mouse pointer back into the console and click it so that you can work in this area again. You can now proceed with the installation of Windows Server 2008.
23. In the Install Windows window, specify the language to install, such as **English**, in the Language to install drop-down list. In the Time and currency format list box, make your selection, such as **English (United States)**. In the Keyboard or input method list box, make your selection, such as **US**. Click **Next**.
24. Click **Install now**.

**NOTE**

If your connection stops before the installation is finished, use the left arrow at the top of the window to go back to the main Status window. Click the virtual machine thumbnail to open a new connection via the Remote Control window. Respond to any security messages, log back on, and respond to any additional security messages. The installation should still be running.



25. Click **Windows Server 2008 Enterprise (Full Installation)** (or select a different full installation edition, such as Standard Edition if it is available) and click **Next**.
26. Read the license terms, click the **I accept the license terms** check box, and click **Next**.
27. Click **Custom (advanced)**.
28. You'll see the amount of unallocated disk space highlighted, which is the disk space you specified when you configured the virtual machine. Ensure that it is highlighted and click **Next**.
29. The installation program begins installing Windows Server 2008. You'll see progress information about copying files, expanding files, installing features, installing updates, and completing the installation. This process takes 30 minutes or more.
30. The installation program restarts the operating system.
31. You see the message *Please wait while Windows sets up your computer*.
32. Next, you see the Install Windows window in the Completing installation phase.
33. The system restarts again.
34. You see the message (a red circle with a white x in it) *The user's password must be changed before logging on the first time*. Click **OK**. (You might have to click inside the active portion of the console first to have the mouse function in it.)
35. Enter a new password for the Administrator account and then enter the same password again to confirm it. Click the **blue circle** with the white right-pointing arrow inside.



NOTE

If you enter a password that is not a strong password, you see the message (with a white x in a red circle) *Unable to update the password*. This means the value provided for the new password does not meet the length, complexity, or history requirements of the domain. Click **OK** and enter a different password that is more than seven characters and uses letters, numbers, and special symbols, such as &.

36. When you see the message *Your password has been changed*, click **OK**.
37. At this point, the Windows desktop is displayed and the Initial Configuration Tasks window opens. From here, you can start configuring Windows Server 2008.
38. You can close the Remote Control window (the Virtual Machine Remote Control Server) or the Status window (the Virtual Server Administration Website) at any time. The virtual machine continues running in the background. Also, when in the Remote Control window, you can go back to the Administrator window by clicking the left-pointing arrow at the top of the Remote Control window.



NOTE

You can shut down a server by first logging on through the Remote Control window. Also, you can use this window and the Status window to turn off a virtual machine (but make sure you shut down the server first).



TIP

To access the documentation for Microsoft Virtual Server, click Start, point to All Programs, click Microsoft Virtual Server, and click Virtual Server Administrator's Guide.

Installing an OS from an ISO Image

If you have an ISO image file for the guest operating system, you have the option to install it instead of performing a traditional installation through the installation DVD. Here are the general steps for installing an ISO image file on a virtual machine in Microsoft Virtual Server:

1. Follow Steps 1 through 13 in the previous section, “Creating a Virtual Machine and Installing a Guest OS.”
2. The bottom portion of the right pane should now show the configuration options for the virtual machine.

3. Click the link for **CD/DVD**.
4. Under Virtual CD/DVD Drive 1, click the **Known image files** option button. Next, click the **Known image files** list arrow and select the image file. If the ISO image file is not listed, enter the path to the ISO image file in the Fully qualified path to file text box.
5. Click **OK** to return to the Master Status listing.

Configuring Networking and Hardware Options

The Microsoft Virtual Server Administration Website offers the ability to configure virtual networks. For example, as you learned earlier, a connected network has two default virtual network options: external network and internal network. You can customize settings for both types of networks, such as settings for a virtual DHCP server. You can also create a new virtual network with properties you define.



A virtual network is one used by virtual machines in a network and is independent of other virtual networks. In Microsoft Virtual Server, the number of virtual machines connected to a virtual network is unlimited.

The Microsoft Virtual Server Administration Website also provides options to configure hardware settings, such as adding more memory for use by a virtual server. In the next sections, you learn how to configure virtual networking and configure hardware for a virtual machine.

Configuring Virtual Networking In the following steps, you examine how to configure virtual networking:

1. Open the Microsoft Virtual Server Administration Website, if it is not open. (Click **Start**, point to **All Programs**, click **Microsoft Virtual Server**, and click **Virtual Server Administration Website**.)
2. In the left pane under Navigation, click **Master Status**, if necessary. Access each virtual server that is running (if any) and shut it down. To do this, point to the server name (that has a right-pointing arrow) under Virtual Machine Name in the right pane, click **Turn Off**, and click **OK**. (You can configure virtual networking while virtual machines are running, but turning them off first is recommended.)
3. In the left pane under Virtual Networks, point to **Configure** and click **View All**.
4. In the right pane, point to **External Network (NICname)** and click **Edit Configuration**.
5. Review the information in the right pane.
6. In the right pane, click the link for **Network Settings**.
7. Review the properties information, including information about the NIC. Click **OK**.
8. In the right pane, click the link for **DHCP server**.
9. You can use the right pane to configure a virtual DHCP server that leases IP addresses through Microsoft Virtual Server (see Figure D-7). To enable the virtual DHCP server, click the **Enabled** check box in the right pane. When you enable the virtual DHCP server, you can configure the following:
 - *Network address*—Enter the network address for the virtual network.
 - *Network mask*—Enter the network mask.
 - *Starting IP address*—Enter the beginning address for the range (scope) of IP addresses that can be leased.
 - *Ending IP address*—Enter the ending address for the range of IP addresses that can be leased.
 - *Virtual DHCP server address*—Enter the IP address of the virtual DHCP server.

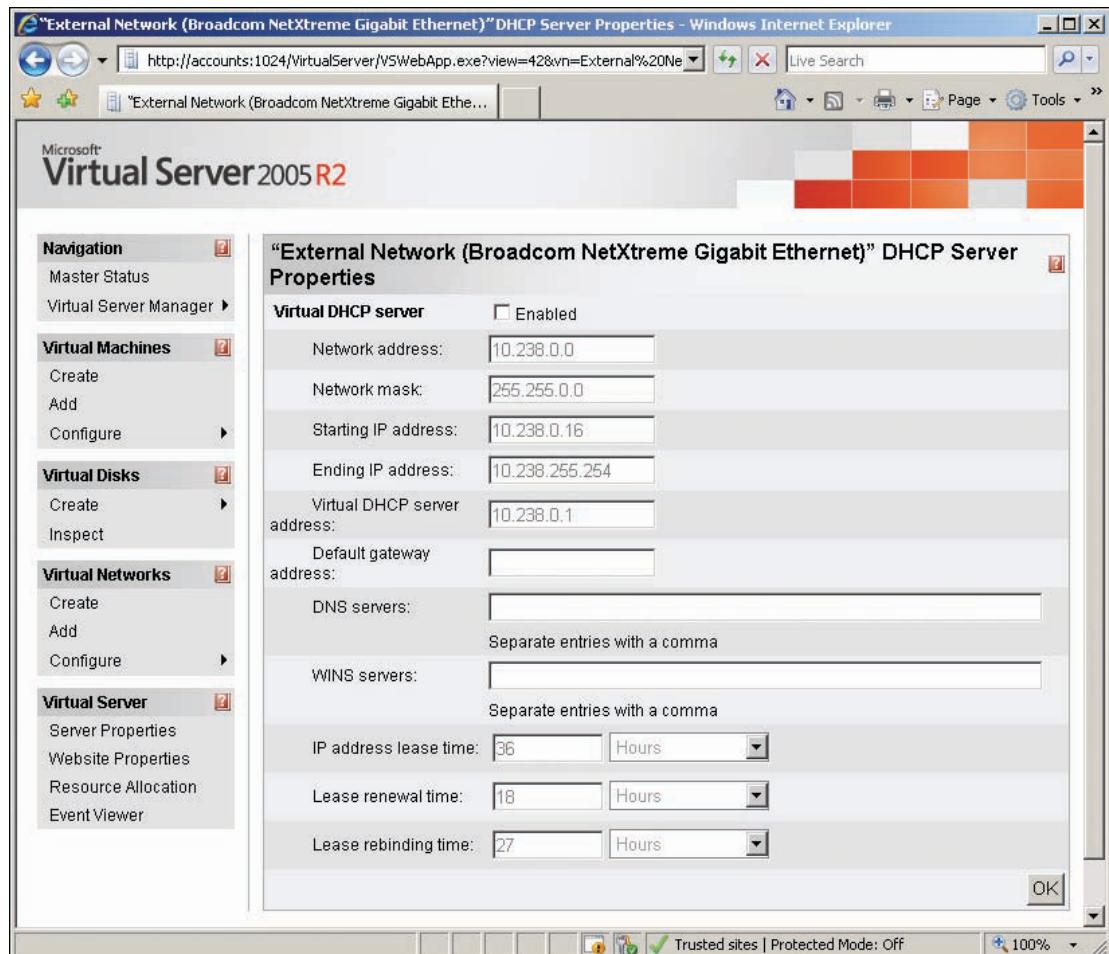


Figure D-7 Virtual DHCP server configuration options

- **Default gateway address**—Enter the IP address of a router that transports packets beyond the virtual network.
 - **DNS servers**—Enter the IP address of one or more DNS servers already on the network.
 - **WINS servers**—Enter the IP addresses of any Windows Internet Naming Service (WINS) servers (for converting NetBIOS computer names to IP addresses).
 - **IP address lease time**—Enter the amount of time that an IP address can be leased, which can be set in days, hours, minutes, or seconds. (Typically, you set it for one or more days.)
 - **Lease renewal time**—Enter the amount of time in which the client can contact the virtual DHCP server to renew a lease (in days, hours, minutes, or seconds, but with a minimum of 30 seconds).
 - **Lease rebinding time**—Enter the amount of time it takes to enable the client to contact another server to renew its lease, when the main leasing server cannot be reached (in days, hours, minutes, or seconds, but with a minimum of 45 seconds).
10. In the left pane under Virtual Networks, point to **Configure** and click **Internal Network**.
 11. Review the information in the right pane for the virtual network properties.
 12. Click **Network Settings** in the right pane and review the information.
 13. Click the **back arrow** at the top of the window.

14. Click **DHCP Server** in the right pane and notice that you can enable a virtual DHCP server and configure it.
15. Leave the window open for the next set of steps.

Configuring Hardware for a Virtual Machine In addition to configuring a virtual network, you can configure hardware and other options for a virtual machine. In the following steps, you examine the options that can be configured:



The virtual machine you select in the steps that follow should be turned off before you start.

NOTE

1. Make sure the Microsoft Virtual Server Administration Website is open.
2. In the left pane under Virtual Machines, point to **Configure** and click the name of the virtual server you have configured.
3. Scroll to the configuration section in the right pane. Review the options that can be configured, which include the following:
 - General properties
 - Virtual Machine Additions
 - Memory
 - Hard disks
 - CD/DVD
 - SCSI adapters
 - Network adapters
 - Scripts
 - Floppy drive
 - COM ports
 - LPT ports
4. In the right pane, click **General properties**. If your computer supports hardware-assisted virtualization, notice that you can enable it here. You can also specify a user account under which to run the virtual machine, and you can specify what action to take when the virtual server stops. If you make changes, click **OK** at the lower left.
5. Click the **back arrow** at the top of the window to return to the previous configuration display in the right pane.
6. In the right pane, click **Memory**. Now you can change the amount of memory allocated to the virtual machine. If you make changes, click **OK**.
7. Click the **back arrow** at the top of the window.
8. In the right pane, click the link for **Hard disks**. In the right pane, you see the configuration of the virtual disk used by the virtual machine. Notice the option “Enable undo disks.” When you select this option, configuration and other changes on the virtual machine are saved so that you can undo those changes, if necessary. Also, notice that you can add a new virtual disk by clicking the Add disk button. If you make changes, remember to click **OK** so that they take effect.
9. Click the **back arrow**.
10. Click **CD/DVD** in the right pane. In the right pane, you can click the Remove check box to remove a CD/DVD drive, and you can click the Add CD/DVD Drive button to add a new drive. If you make changes, click **OK**.
11. Click the **back arrow**.



12. Click each of the remaining configuration options in the right pane to view what they cover. In particular, notice that you can add NICs by using the Network adapters option.
13. Close the Microsoft Virtual Server Administration Website when you are finished (or restart your virtual server so that it is in use).

Host Key Options

Microsoft Virtual Server designates the right Alt key as the default host key and offers host key options that are similar to those in Microsoft Virtual PC. Table D-2 lists important host key combinations you can use while you are accessing a virtual machine.

Table D-2 Host key options for Microsoft Virtual Server

Keyboard combination	Result
HostKey	Enables you to move the mouse outside the window used by the guest OS. (Move the mouse back into the guest OS display and click when you want to work on the guest OS.)
HostKey + Delete	The virtual machine OS responds to this as Ctrl+Alt+Delete.
HostKey + C	Displays the Connect to server dialog box for connecting to a specific virtual machine. (or if you have selected text first, it can be used to copy the text.)
HostKey + A	Toggles to the Administrator display window.
HostKey + I	Shows the VMRC Connection Properties dialog box with information about the connected virtual machine.
HostKey + B	Provides information about the VMRC client software.
HostKey + V	Pastes text and items saved in the Clipboard into the active window in the guest OS.
HostKey + H	Enables you to configure a different key as the host key.

VMware Server

VMware Server enables you to set up virtual machines to run Windows or Linux operating systems. VMware Server version 2 is a major update compared with previous 1.x versions. The new features of VMware Server 2 include the following:

- Ability to manage virtual machines from the Web Access management interface or the VMware Remote Console
- Ability to configure different levels of permissions
- Ability to configure which operating systems are started when VMware is started
- Editors for hardware devices
- New support for Windows Vista, Windows Server 2008, Red Hat Enterprise 5.0, and Ubuntu Linux up through version 8.x
- Ability to handle increased memory (to 8 GB) and more NICs (up to 10) in the host machine
- Supports 64-bit guest operating systems on 64-bit (x64) host computers
- Hot-add capability for new SCSI and tape devices (without shutting down a virtual machine)
- Supports VSS for backups on Microsoft guest systems
- Enables use of Firefox 3 or Internet Explorer for the Web Access management interface
- Supports hardware virtualization, such as through AMD CPUs with AMD-V capability and Intel CPUs with Intel VT
- Supports multiple monitors (to see different virtual machines on different displays)

VMware Server Guest Operating Systems Supported

VMware Server supports the following guest operating systems:

- Windows Server 2008 Standard, Enterprise, Datacenter, and Web Server (x86 or x64)
- Windows Server 2003 Standard, Enterprise, Datacenter, and Web Server with SP1 or SP2 (x86 or x64)
- Windows Server 2003 Standard, Enterprise, Datacenter, and Web Server R2 (x86 or x64)
- Windows Small Business Server 2003 (Standard and Premium Editions)
- Windows 2000 Server and Professional
- Windows XP Professional
- Windows Vista Business and Ultimate (x86 and x64)
- Red Hat Enterprise Linux Server and Desktop versions up through version 5 (x86 and x64)
- Ubuntu Linux 6.x to 8.x
- SUSE Linux Enterprise Server up to 10.x (x86 and x64)
- SUSE Linux versions up to 10.x (x86 and x64)
- Novell NetWare
- Solaris

VMware Server Host Operating Systems Supported

VMware Server 2.x runs on more different kinds of host operating systems than Microsoft Virtual PC or Server because it can run on several different Linux distributions. It also runs on x86 and x64 computers. The list of VMware host operating systems includes the following:

- Windows Server 2008 Standard, Enterprise, Datacenter, and Web Server (x86 or x64)
- Windows Server 2003 Standard, Enterprise, Datacenter, and Web Server with SP1 or SP2 (x86 or x64)
- Windows Server 2003 Standard, Enterprise, Datacenter, and Web Server R2 (x86 or x64)
- Windows Small Business Server 2003 (Standard and Premium Editions)
- Windows 2000 Server and Professional with SP3 or SP4
- Windows XP Professional and Home through the current service pack
- Windows Vista Business and Ultimate (x86 and x64)
- Red Hat Enterprise Linux Server and Desktop versions up through version 5 (x86 and x64)
- Ubuntu Linux 6.x to 8.x
- SUSE Linux Enterprise Server up to 10.x (x86 and x64)
- SUSE Linux versions up to 10.x (x86 and x64)
- Mandrake Linux up to 10.x

VMware Server also can run on other Windows and Linux distributions, such as other Windows Vista editions or Fedora Linux, but they should be considered “experimental” because they might not be fully tested.



NOTE For Windows host operating systems, you must download the VMware Server version for Windows, which is in .exe format. For Linux host operating systems, you must download the VMware Server version for Linux, which is in .tar format.



Windows Server Core is not a supported host at this writing.



Requirements for VMware Server

VMware Server has the following hardware requirements:

- **CPU**—Any standard x86 or x64 computer, including the following processors: dual- or quad-core Intel Zeon, Intel Core 2, AMD Opteron, or Athlon (733 MHz or faster)
- **RAM**—A minimum of 512 MB, but must include enough RAM for at least the minimum requirements of the total number of operating systems you'll be running (host and guest)
- **Disk space**—Enough disk storage for the operating systems you plan to run (host and guest)
- **Console Web Access**—Internet Explorer 6.0 or later (for Windows hosts) or Mozilla Firefox 2.0 or later (for Linux hosts)



VMware Server 2.x virtual machines can connect to hard, optical, and floppy drives. VMware 2.x also supports USB 2.x connections.

NOTE

How to Download VMware Server

VMware Server can be downloaded from VMware's Web site at no cost by following these steps.

1. Log on to your computer.
2. Establish a folder in which to store the download (such as a temporary folder or a folder under your Program Files folder).
3. Start your Web browser, such as Internet Explorer.
4. Go to the URL www.VMware.com/products/server.



Web links and specific instructions change periodically. You might need to search for the most current link at www.vmware.com if this link does not work.

NOTE

5. Click **Download Now**.
6. Find the latest version of VMware Server (if multiple versions are listed) and click **Download** or **Download Now**.
7. If asked to provide registration information, complete the registration form.
8. Read the licensing information and click **Yes** or **Accept**.
9. Record the serial number for the Windows version (used later when you install VMware Server).
10. Click the link to download the Binary (.exe) file for VMware Server for Windows Operating Systems.
11. Click the **Save** button.
12. Select the folder you created in which to save the file.
13. Click **Save**.

14. Click **Close** in the Download Complete dialog box.
15. Close your Web browser.

How to Install VMware Server

The general steps for installing VMware Server on the host operating system are as follows:

1. If possible, connect to the Internet so that updates can be installed automatically during the installation process.
2. Browse to the folder in which you saved the install file for VMware Server.
3. Double-click **VMware-server-2.x.x-xxxxxx** (2.x.x-xxxxxx is the version of VMware Server).
4. You'll see a message box noting it is preparing for the installation, followed by the Windows Installer dialog box.
5. When the Installation Wizard for VMware Server starts (see Figure D-8), click **Next**.



Figure D-8 The Installation Wizard for VMware Server

6. Read the license agreement, click **Yes, I accept the terms in the license agreement**, and click **Next**.
7. Verify that the VMware server files will be written to the correct destination folder (or click the **Change** button to select a different destination). Click **Next**.
8. Verify the fully qualified domain name for the host computer, and verify that the server HTTP (port 8222) and server HTTPS (port 8333) ports are selected by default. Make any changes as needed, such as to the host and domain names (but leave the defaults for the ports). Click **Next**.
9. Make sure the shortcuts you want are selected, as shown in Figure D-9. Click **Next**.

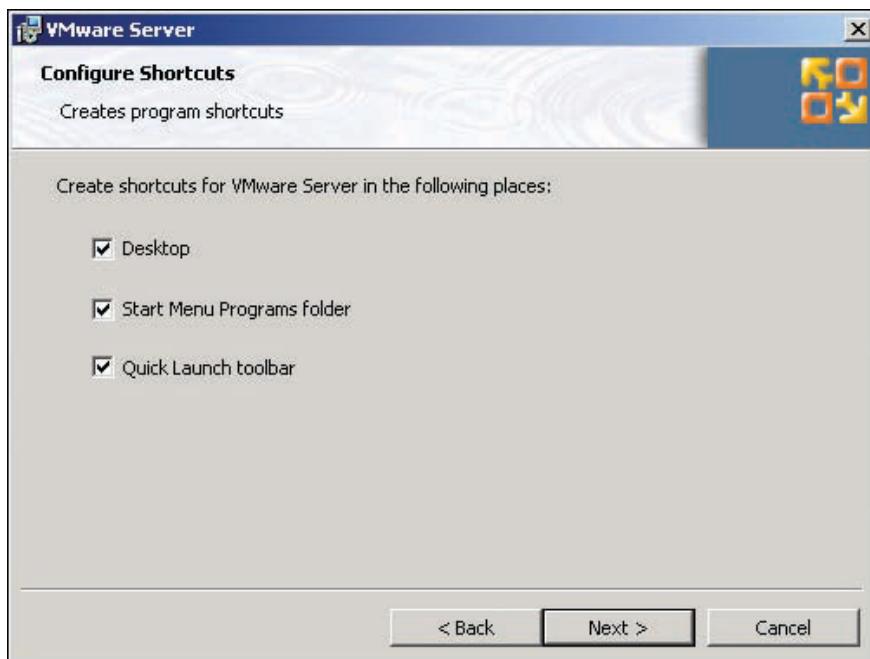


Figure D-9 Shortcut options

10. Click **Install**.
11. You'll see a message that the installation might take several minutes.
12. If you see any message boxes to install device software, click **Install**.
13. For the registration information, enter your name and the name of your company (or school), if appropriate. Next, enter the serial number you obtained when you downloaded the software. Click **Enter**.
14. Click **Finish**.
15. Make sure all programs are closed and click **Yes** to restart the system.

Creating a Virtual Machine and Installing a Guest OS

Now that VMware Server is installed, the next step is to create a virtual machine and install the guest operating system. Here are the general steps using Windows Server 2008 as the guest:



The VMware Remote Console that you use later in these steps requires that the VMware virtual server (host computer) be resolvable through Domain Name System (DNS). Before you start, make sure your server can be resolved through DNS on your network (or that DNS is installed on the host). For example, there should be a host address (A) resource record in the DNS server for the host computer.

1. Double-click the **VMware Server Home Page** icon on the desktop or the taskbar. (Alternatively, you can click **Start**, point to **All Programs**, click **VMware Server**, and click **VMware Server Home Page**.)



You might need to resolve security requirements for Internet Explorer, such as providing a digital certificate, answering whether to set up a phishing filter, and adding this site as a trusted site. These issues are related to Internet Explorer.

2. Log on with your host computer account name (or the administrator account) and enter the password. (Use the same account that you used to install VMware Server.)
3. You see the VMware Infrastructure Web Access window, as shown in Figure D-10.

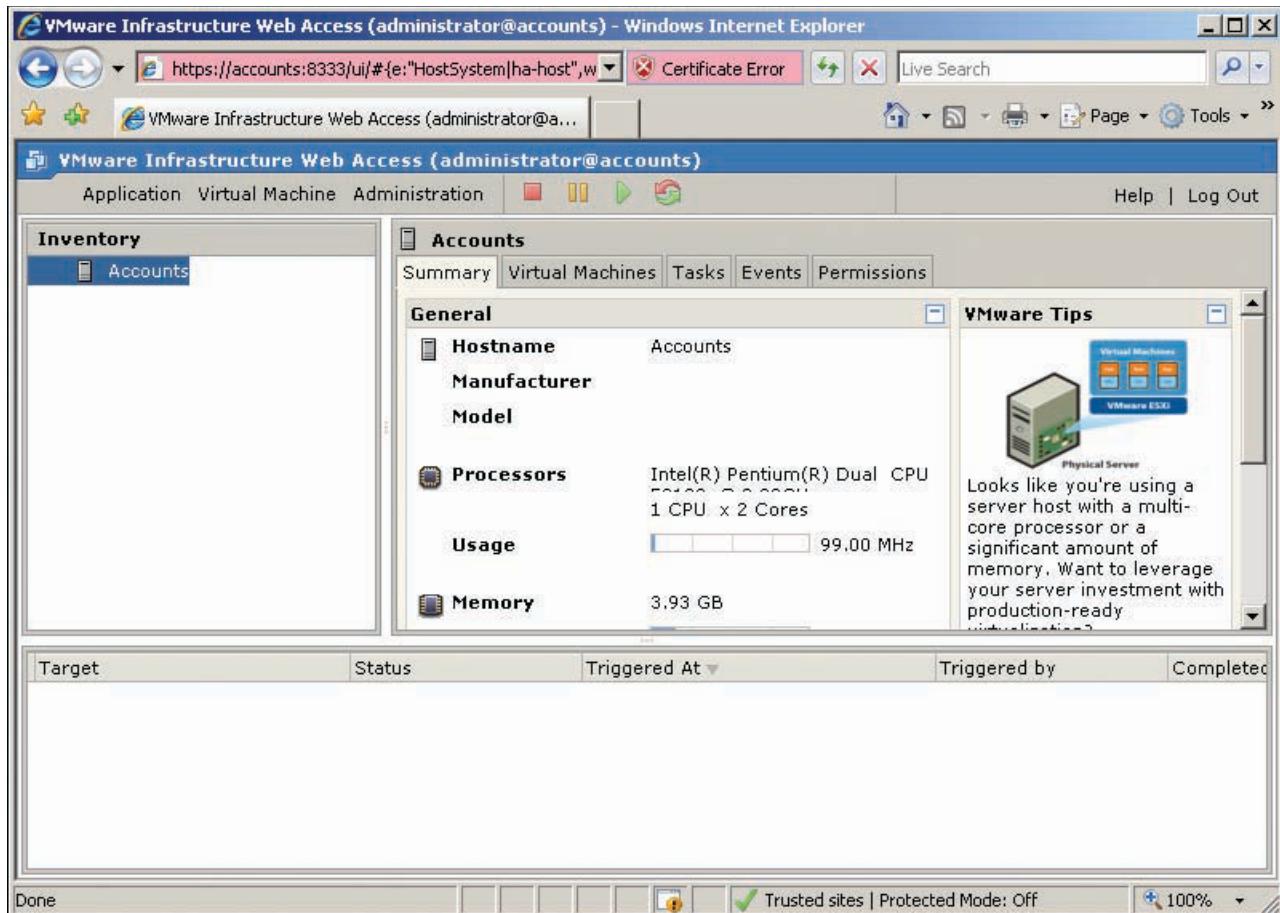


Figure D-10 VMware Infrastructure Web Access window



Notice that a certificate error is reported in Figure D-10 because this new site does not yet have a trusted certificate. If you have this problem, you might be able to import a certificate by clicking the Certificate Error box at the top of the window, clicking the link for View certificates, and clicking Install Certificate. Another option is to talk to your network administrator about importing a certificate.

4. Make sure your host computer is highlighted in the left pane.
5. Click the **Virtual Machines** tab.
6. In the right pane under the Commands heading, click **Create Virtual Machine**.
7. Enter the name for the virtual machine and click **Next**.
8. Ensure that **Windows operating system** is selected for the type of guest operating system, click the operating system (in the Version list box), and click **Next**.
9. Set the memory size to **512 MB** or higher. (1024 MB is the default when installing Windows Server 2008.) Also, if your system has a dual- or quad-core CPU or is an SMP system, you can select the number of processors to use. Notice, however, that you should not reconfigure the setting for number of processors after the virtual machine is set up. Click **Next**.

10. Select the virtual disk to use, such as by clicking **Create a New Virtual Disk** (a disk on the current computer). (The other option is Use an Existing Virtual Disk, which is a disk on a shared drive or hard disk on a different computer.) Enter the capacity for the virtual disk, such as **20 GB** (see Figure D-11). Adjust any parameters as needed, which include the following:
- *Location for the virtual disk file*—A file location other than the default
 - *File Options*—Ability to allocate disk space now and ability to split the disk into two files
 - *Disk Mode*—Ability to create independent disks not affected by snapshots
 - *Virtual Device Node*—Ability to select the SCSI or IDE adapter and device
 - *Policies*—Ability to optimize for safety (the default) or for performance

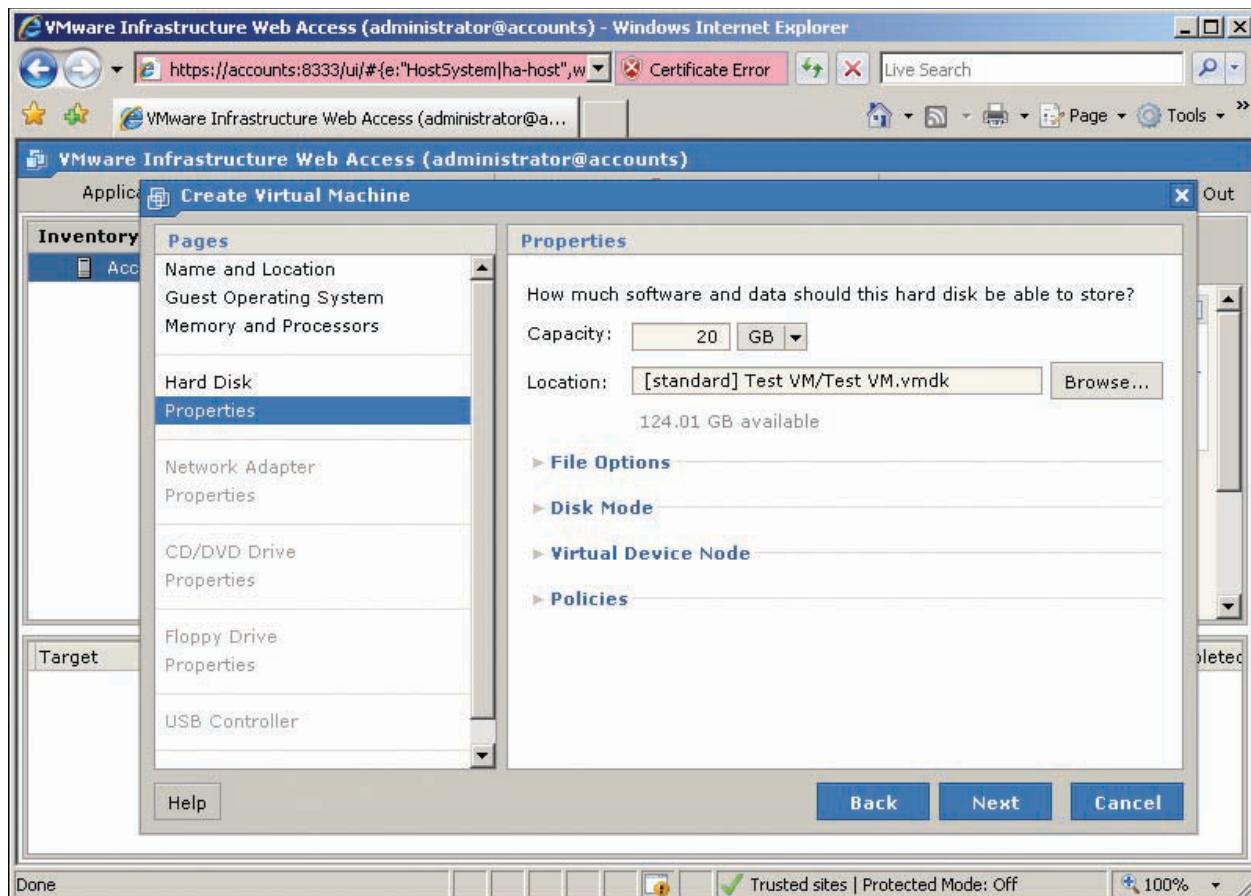


Figure D-11 Configuring virtual disk properties

11. Click **Next**.
12. In the next window, you can add a network adapter for access over a network. Click **Add a Network Adapter**. If you do not want to use the default settings for Network Connection (Bridged) and for Connect at Power On (Yes), configure those settings. The network settings you can configure for the Network Connection parameter are as follows:
 - *Bridged*—This setting gives the virtual machine its own network identity (so that it is seen as a different computer from the host), which enables other computers on the network to communicate with it. The bridged setting also means the virtual machine can access the Internet through the local network.
 - *HostOnly*—With this setting, only the host computer and other virtual machines on the same host can access the virtual machine, which means the virtual machine is not accessible through the local network.

- **NAT**—The virtual machine and host use the same IP and MAC addresses, which means the virtual machine does not have its own identity on the local network. This selection might be made if IP addresses are in short supply for the specific network or because an organization's network policy is to allow only one IP address for a specific computer.

13. Click **Next**.
14. You can configure whether to enable access to a CD/DVD drive or use an ISO image for the installation of the operating system. For this activity, click **Use a Physical Drive**. Ensure that the correct CD/DVD drive is selected, such as drive E, and ensure that Connect at Power On is set to **Yes**. Click **Next**.
15. If your computer has a floppy drive, you can configure it to provide an image for the operating system. Select the appropriate configuration options. (To install Windows Server 2008, click **Don't Add a Floppy Drive**.) Click **Next**, if necessary. (Depending on your selection, you might need to configure additional properties.)
16. In the next window, you can specify whether to add a USB controller, such as to access a flash drive. Make your selection and click **Next**, if necessary.
17. Review your configuration selections and click **Finish**.
18. In the bottom pane, you should see Success under the Status column to show that you successfully created the virtual machine.



NOTE In some cases, if you have selected different configuration options and then clicked the Back button to go back to the preceding steps, VMware Server might give you an error message or you might not end up with an installed virtual machine. If this happens, start from scratch and avoid undoing selections you have made.

19. Insert the Windows Server 2008 installation DVD.
20. In the left pane, click the new virtual machine name under the host server name. (You might have to expand entries under the host server name first.)
21. Ensure that the **Summary** tab is selected.
22. In the right pane, scroll to the Hardware section. Click the **down arrow** next to CD/DVD Drive 1 (*drivetype*) and click **Edit**.
23. Review the parameters set for the host media (CD/DVD drive), make any needed changes, and click **OK**.
24. Click the **Console** tab.
25. Click **Install plug-in** to install the Remote Console plug-in.



NOTE If you see a message box about noticing the Information Bar, click Close. Also, if the plug-in is not successfully installed in Internet Explorer, you might see a message at the top of the window that you must click to continue. Click the message and click to install the elements required by Internet Explorer, such as Install the ActiveX Control. Next, click Install plug-in again, and, if necessary, click Install.



26. In the right pane, click **Powered off** (which is like a switch to turn the virtual machine on or off.)
27. Click anywhere in the reduced console area in the right pane.
28. In the Install Windows window, specify the language to install, such as **English**, in the Language to install drop-down list. In the Time and currency format list box, make your selection, such as **English (United States)**. In the Keyboard or input method list box, make your selection, such as **US**. Click **Next**.
29. Click **Install now**.
30. Click **Windows Server 2008 Enterprise (Full Installation)** (or select a different full installation edition, such as Standard Edition if it is available), and click **Next**.

31. Read the license terms, click the **I accept the license terms** check box, and click **Next**.
32. Click **Custom (advanced)**.
33. You'll see the amount of unallocated disk space highlighted, which is the disk space you specified when you configured the virtual machine. Ensure that it is highlighted, and click **Next**.
34. The installation program begins installing Windows Server 2008. You'll see progress information about copying files, expanding files, installing features, installing updates, and completing the installation. This process takes 30 minutes or longer.
35. The installation program restarts the operating system.
36. You see the message *Please wait while Windows sets up your computer*.
37. Next, you see the Install Windows window in the Completing installation phase.
38. The system restarts again.
39. You see the message (a red circle with a white x in it) *The user's password must be changed before logging on the first time*. Click **OK**. (You might have to click inside the active portion of the console first to have the mouse function in it.)
40. Enter a new password for the Administrator account and then enter the same password again to confirm it. Click the **blue circle** with the white right-pointing arrow inside.

**NOTE**

If you enter a password that is not a strong password, you see the message (with a white x in a red circle) *Unable to update the password*. This means the value provided for the new password does not meet the length, complexity, or history requirements of the domain. Click **OK** and enter a different password that is more than seven characters and uses letters, numbers, and special symbols, such as &.

41. When you see the message *Your password has been changed*, click **OK**.
42. At this point, the Windows desktop is displayed and the Initial Configuration Tasks window opens. From here, you can start configuring Windows Server 2008 or log off and use the Remote Control window later to access Windows Server 2008.
43. You can close the VMware Remote Console window at any time (but note that the virtual machine keeps running).
44. Close the VMware Infrastructure Web Access window when you are finished using it. (The virtual machine continues running, unless you shut it down in the VMware Remote Console window and power it off in the VMware Infrastructure Web Access window.)

**NOTE**

You can access online help documentation while you are in the VMware Infrastructure Web Access window. Click the Help option near the upper-right corner of the window.

Installing an OS from an ISO Image

VMware Server supports installing an operating system via an ISO image file. The general steps for this type of installation are as follows:

1. Follow the steps to create a virtual machine.
2. In the Inventory pane of the VMware Infrastructure Web Access window, click the virtual server you have created.
3. Click the **Summary** tab.
4. Scroll down to view the Hardware section.
5. Click the **down arrow** next to **CD/DVD Drive 1** and click **Edit**.
6. Under the Connection section, click the **ISO Image** option button.
7. Enter the optical disk image path or use the **Browse** option to find and select it.
8. If necessary, select the device node in the Virtual Device Node section.

9. Click **OK**.
10. Click the **Console** tab.
11. Power on the virtual machine, if necessary.
12. Click inside the console and follow the instructions from the operating system.

Configuring Networking Options

As you learned earlier, the three network connection options are Bridged, HostOnly, and NAT. Each of these network types has a default name, as follows:

- Bridged is called VMnet0.
- HostOnly is called VMnet1.
- NAT is called VMnet8.

You can configure virtual networking, including VMnet0, VMnet1, and VMnet8, with the Virtual Network Editor. For example, you can configure VMware internal DHCP server capability for HostOnly and NAT networks. Bridged networks use an external DHCP server, such as a Windows Server 2008 server configured for this service.

To explore the Virtual Network Editor, follow these steps:

1. Click **Start**, point to **All Programs**, click **VMware**, click **VMware Server**, and click **Manage Virtual Networks**.
2. The Virtual Network Editor has the following tabs (see Figure D-12):
 - *Summary*—Provides a summary of the virtual networks, including VMnet0, VMnet1, and VMnet8
 - *Automatic Bridging*—Controls bridging between the VMnet0 network and the network adapter
 - *Host Virtual Network Mapping*—Enables you to link virtual networks to physical network adapters and virtual network adapters as well as configure subnet and DHCP properties
 - *Host Virtual Adapters*—Shows virtual adapter connections, virtual networks, and the status of connections

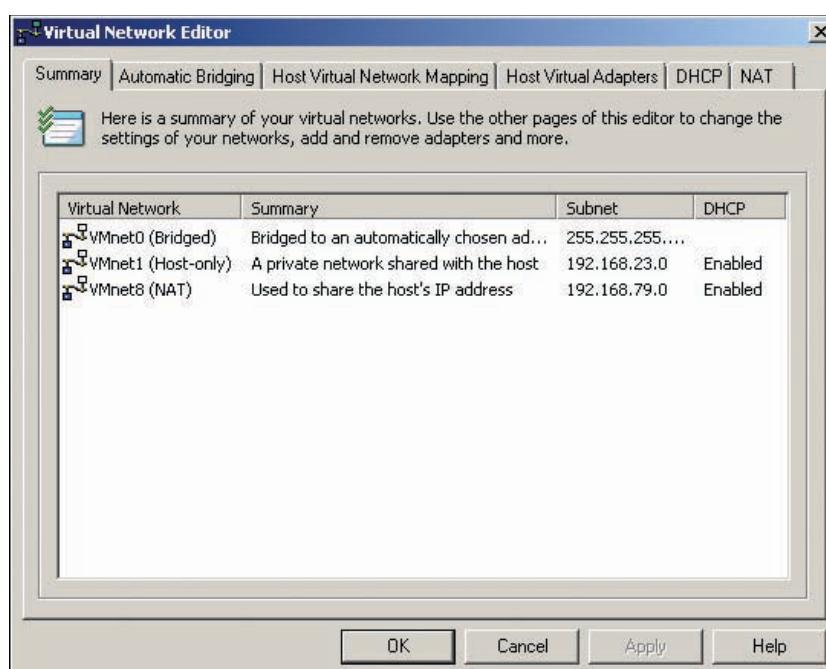


Figure D-12 Virtual Network Editor

- **DHCP**—Enables you to configure DHCP for VMnet1 and VMnet8
 - **NAT**—Enables you to control the NAT service and configure NAT settings
3. Click each tab to view what it does.
 4. Click the **DHCP** tab again.
 5. Click **VMnet1** and click **Properties**.
 6. In the DHCP Settings dialog box, notice that you can configure the range of IP addresses to use. You can also configure the lease duration parameters for clients. Click **Cancel**.
 7. Notice that you can start, stop, and restart the DHCP service in the DHCP tab.
 8. Click the **NAT** tab. You can use this tab to associate the NAT service with a virtual network and to start, stop, and restart the NAT service.
 9. Close the Virtual Network Editor when you are finished.

Configuring Hardware Options

After you set up a virtual machine, you might want to go back and configure hardware options. For example, you might change the configuration of the network and decide to go from a Bridged network to a HostOnly network.

The following steps enable you to configure hardware:

1. Open the VMware Infrastructure Web Access window.
2. In the Inventory pane, expand to view the virtual machines under the host server, if necessary.
3. Click the virtual machine you want to configure.
4. To configure hardware, you first need to ensure that the virtual machine is turned off. Use the Console tab to shut down the OS. Also, click **Virtual Machine** on the toolbar and click **Power Off**.
5. Click the **Summary** tab.
6. Scroll down to view the Hardware section.
7. Click the down arrow next to **Processors** and click **Edit**. You'll see a note that advises against changing the number of virtual processors, if you have more than one processor. Click **Cancel**.
8. Click the down arrow next to **Memory** and click **Edit**. Notice the recommended size information for memory allocation. Also, you can use the Size (in multiples of 4) text box to change the memory allocation. Click **Cancel**.
9. Click the down arrow next to **Hard Disk 1** and click **Edit**. You can increase the virtual disk capacity, configure the virtual device node, configure the disk mode, and configure policies. Click **Cancel**.
10. Click **Network Adapter 1** and click **Edit**. You can change the type of network connection, such as from Bridged to HostOnly. Information about the connection status, MAC address, and virtual device is also displayed. Click **Cancel**.
11. Click the down arrow next to **CD/DVD Drive 1** and click **Edit**. Review the properties you can set and the connection status information. Click **Cancel**.
12. Review information about any other hardware devices.
13. Restart the virtual machine when you are finished.

Installing VMware Tools

VMware Tools is an add-on that provides additional ways to manage a virtual machine and improve its performance. The elements of VMware Tools include the following:

- *VMware Tools control panel* to conveniently change virtual machine settings and connect devices
- *VMware user processes* for Linux and Solaris guest operating systems

- *Device drivers* for enhanced video, audio, mouse, network, and SCSI disk performance
- *Tools service* that provides a variety of tools for messaging, mouse performance, screen resolution, and others

When you install VMware Tools, the virtual machine must be started and you should be logged on to the guest operating system account from which you manage the Virtual Server software. This is because VMware Tools, including drivers, is installed on the guest operating system and you can access it from Control Panel in Windows Server 2008 (and other Windows operating systems).

To install VMware Tools, follow these steps:

1. Open the VMware Infrastructure Web Access window.
2. In the Inventory pane, click a virtual machine.
3. Ensure that the guest operating system is running, and if it is not, start it. Log on to the Administrator account or an account that has Administrator privileges.
4. In the VMware Infrastructure Web Access window, click **Install VMware Tools** in the Status column of the right pane for the virtual machine.
5. Click **Install**.
6. Open the virtual machine console by clicking the **Console** tab and clicking inside the console.
7. It might take several minutes for the AutoPlay message box to appear in the guest operating system desktop. Click the option **Run setup.exe**.
8. You see the Windows Installer dialog box with the message *Preparing to install*. This process might take several minutes.
9. Click **Next** in the Welcome to the installation wizard for VMware Tools window (see Figure D-13).

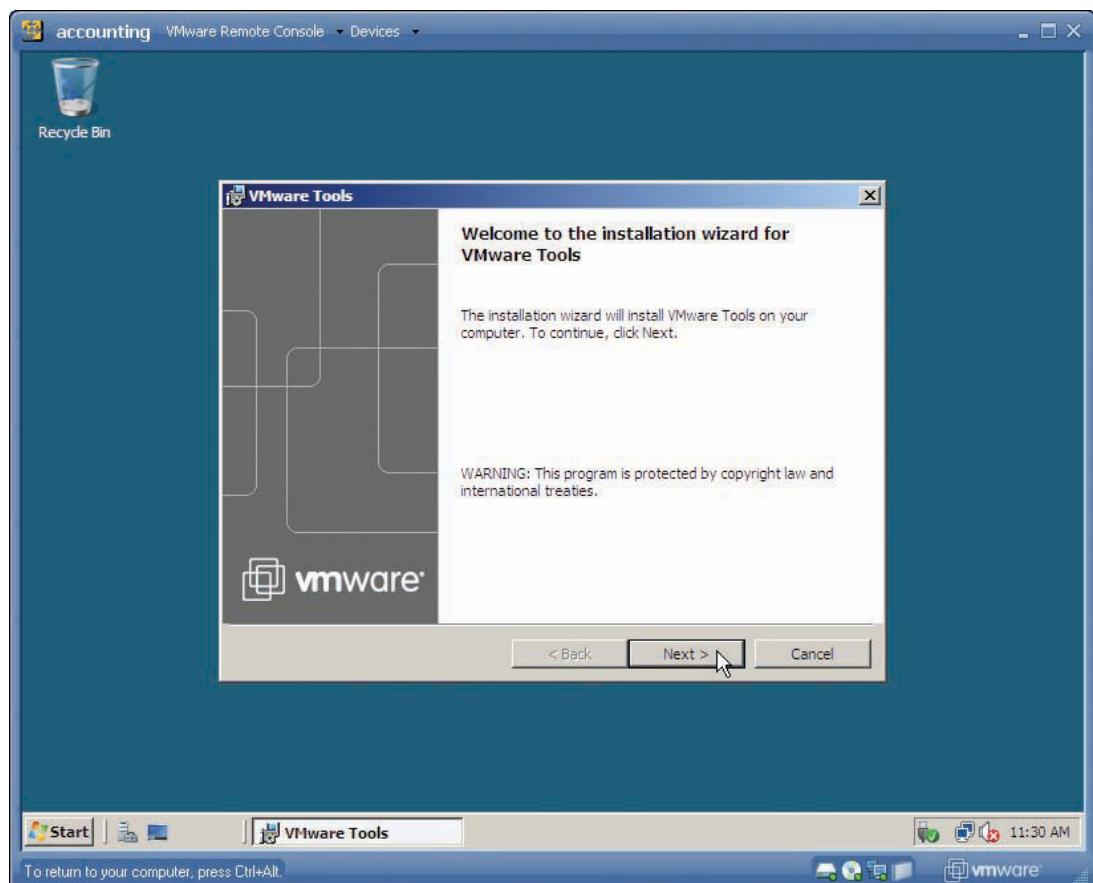


Figure D-13 Installation wizard for VMware Tools

10. Select the setup type option from the following options:
 - *Typical*—If you plan to use only VMware Server
 - *Complete*—If you plan to use VMware Server and other VMware products
 - *Custom*—If you want to choose the specific features to install
11. Click **Next**.
12. Click **Install**.
13. If you see the message *Windows can't verify the publisher of the driver software*, click the option **Install this driver software anyway**. (You might see this message several times.)
14. If you see a Windows Security dialog box asking whether you want to install this device software, click the **Always trust software from "VMware, Inc."** check box. Click **Install**.
15. Click **Finish**.
16. Save any work you have open on the virtual machine and click **Yes** to restart.
17. Log back on to the guest operating system in the console window.
18. In the guest operating system (Windows Server 2008), click **Start, Control Panel**.
19. Click **Classic View** and click the new applet **VMware Tools**.
20. The VMware Tools Properties dialog box opens, as shown in Figure D-14.

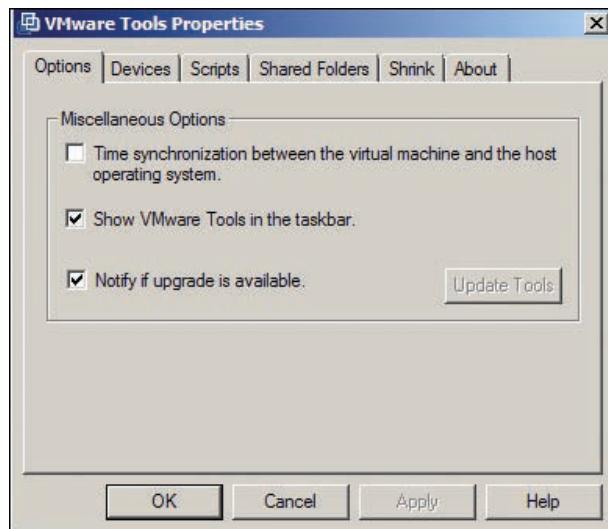


Figure D-14 VMware Tools Properties dialog box

21. Click each tab to see what it does.
22. Click the **Help** button to learn more about VMware Tools capabilities.
23. Close the VMware Tools Help window when you are finished with the Help feature.
24. Click **Cancel** to close the VMware Tools Properties dialog box.
25. Notice that a new icon is displayed on the guest operating system's taskbar, which can be used to open the VMware Tools Properties dialog box.
26. Close Control Panel in the guest operating system.

Other Virtual Systems

This appendix has focused on virtualization systems that are free. Other systems are available at a cost. On the desktop side, VMware Workstation has grown in use along with desktop virtualization. Another system is Microsoft Hyper-V, which is new to Windows Server 2008. The following

sections give you a brief overview of these systems but are not intended to provide instructions about how to use them.



NOTE

VMware Workstation is free for academic institutions approved in the VMware Academic Program. Entry in this program is free for two- and four-year degree-granting higher education institutions and accredited technical schools. For more information, visit <http://vmware.com/partners/academic>.

VMware Workstation

VMware Workstation is popular among software developers and testers because it provides a safe environment in which to write and test development software before it is released to live production. It is also used by people who need to run multiple operating systems on one workstation-class computer, including legacy operating systems. This can be useful for running old software without having to convert it for a new operating system. It's also useful for learning a new operating system.

VMware Workstation 6.04 (and later) supports Windows, Linux, and other operating systems as host and guest OSs. Newer operating systems supported as both hosts and guests include the following:

- Windows Server 2008 Standard, Enterprise, and Datacenter editions (x86 and x64)
- Windows Vista Home Basic, Home Premium, Enterprise, Business, and Ultimate (x86 and x64)
- Red Hat Enterprise Linux up to 4.6 (x86 and x64)
- Ubuntu Linux up to 7.10 (x86 and x64)
- SUSE Linux Enterprise Server 10 (x86 and x64)
- openSUSE Linux up to 10.3

VMware Workstation has several of the same new features as VMware Server, which include the following:

- Handles increased memory (to 8 GB)
- Supports 64-bit guest operating systems on 64-bit host computers
- Supports hardware virtualization, such as through AMD CPUs that have AMD-V capability and Intel CPUs with Intel VT
- Supports USB 2.0 (including on Linux operating systems)
- Supports multiple monitors (to see different virtual machines on different displays)

As with VMware Server, you can configure hardware for the virtual machine, including multiple processors, memory, hard disks, USB access, floppy access, and other hardware elements. You can also configure Bridged, HostOnly, and NAT virtual networks. A virtual DHCP server can be configured when you use HostOnly and NAT virtual networking. Setting up a virtual machine is also done with a step-by-step wizard.

Also, as in VMware Server, you can install VMware Tools, which includes specialized drivers, such as drivers for enhanced video and audio functions for the guest operating system. VMware Workstation has a console for accessing the guest operating system that resembles the VMware Server console.

VMware Workstation is specifically designed for workstation host machines and offers a wider range of host and guest operating system compatibility than Microsoft Virtual PC (at this writing). You can download a 30-day free evaluation version at www.vmware.com/products/ws.

Microsoft Hyper-V

Microsoft Hyper-V was released just a few months after Windows Server 2008. Unlike the other virtualization systems discussed in this appendix, Microsoft Hyper-V is intended to run only on Windows Server 2008. It is loaded through Server Manager like any other role in Windows Server 2008. In this regard, Windows Server 2008 offers perhaps the smoothest installation

process of any of the virtual systems discussed in this appendix. Also, unlike the other systems in this appendix, Hyper-V runs only on x64 computers, which means the host systems include only the following:

- Windows Server 2008 Standard Edition x64
- Windows Server 2008 Enterprise Edition x64
- Windows Server 2008 Datacenter Edition x64



For a general introduction to the features and requirements of Hyper-V, see Chapter 2.

NOTE

You can purchase any of Windows Server 2008 Standard, Enterprise, or Datacenter Editions with Hyper-V (for an extra \$28 at this writing) or you can purchase Hyper-V separately (also for \$28). The low cost and seamless installation and integration with Windows Server 2008 are designed to make this virtualization system particularly appealing to Windows Server 2008 users.

The guest operating systems that can be installed in Hyper-V include the following:

- Windows Server 2008 Standard, Enterprise, Datacenter, and Web Server (x86 or x64)
- Windows Server 2003 Standard, Enterprise, and Datacenter (x86 or x64)
- Windows Server 2003 Web Edition
- Windows 2000 Server and Advanced Server with SP4
- Windows Vista Business, Enterprise, and Ultimate (x86 and x64)
- Windows XP Professional with SP2 or SP3 (x86)
- Windows XP Professional with SP2 (x64)
- SUSE Linux Enterprise Server 10 with SP1 or SP2 (x86 or x64)

After Hyper-V is installed as a server role, you can open Hyper-V Manager as a Microsoft Management Console (MMC) snap-in or from the Administrative Tools menu—steps familiar to Windows Server 2008 administrators. Hyper-V Manager is easy to use because it is designed in the same format as most Windows Server 2008 administrative tools. For example, to create a new virtual machine, click the New option in the right pane and follow the steps in the New Virtual Machine Wizard.

To configure hardware and management settings for a virtual machine, click Settings under the name of the virtual machine in the right pane of Hyper-V Manager. The Settings dialog box (see Figure D-15) enables you to add hardware, configure hardware, and configure management capabilities.

You can access the Virtual Network Manager dialog box from Hyper-V Manager to configure a virtual network. There are three types of virtual networks:

- *Private*—Communication only between virtual machines on the same virtual server
- *Internal*—Communication between virtual machines and the host virtual server
- *External*—Communication between virtual machines and the physical network (using a network adapter)

For an external virtual network, you can specify a virtual LAN identification number. This is a unique number used for communication through the network adapter that distinguishes the virtual network from other networks.

The guest operating system appears in a console that has an Action menu from which you can send a Ctrl+Alt+Delete keystroke for logging on and start, turn off, shut down, or pause a virtual machine (as well as other options). You also can expand the console to completely fill the

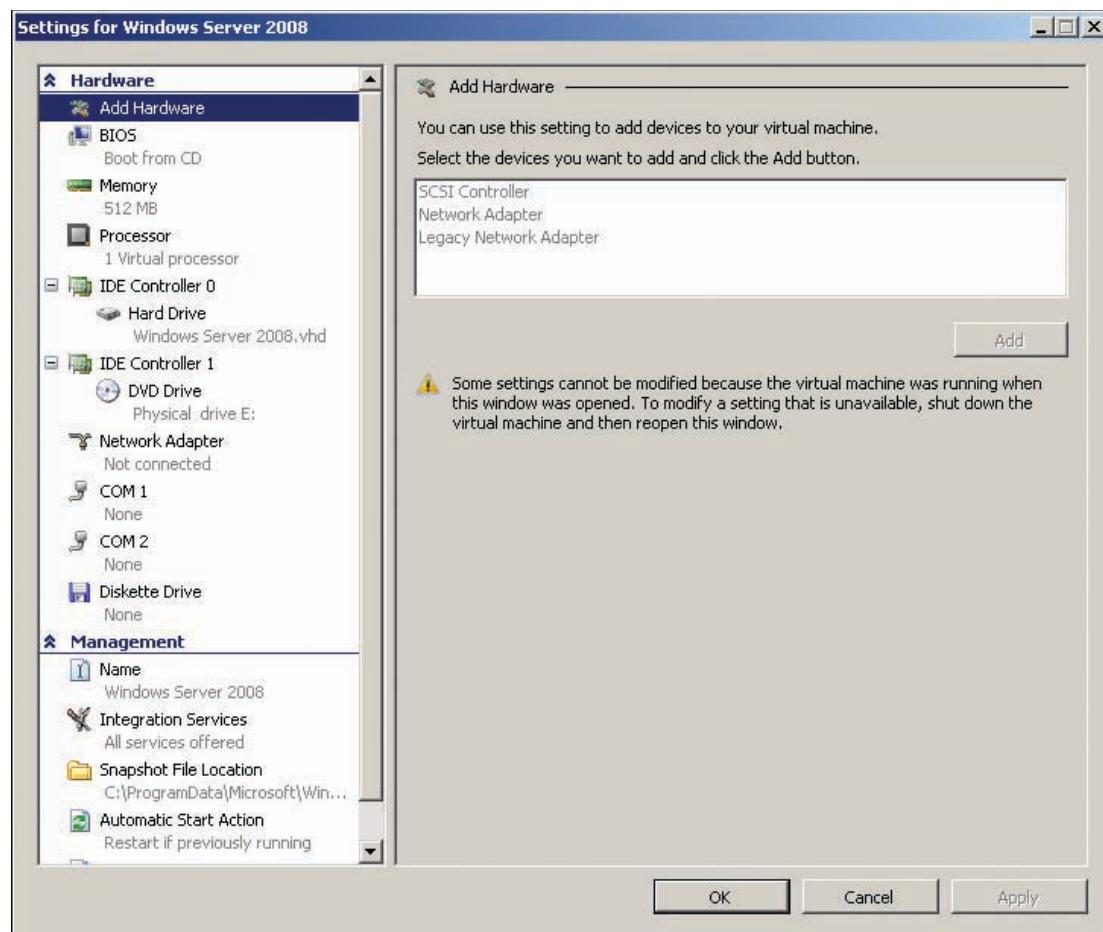


Figure D-15 Configuring settings for a virtual machine

desktop display. The console can be started by clicking its thumbnail. When the console opens, it displays a message about how to start the guest operating system.

At this writing, Hyper-V does not include as extensive a range of guest and host operating systems as other virtualization systems. However, it is a good fit with Windows Server 2008 environments, and more guest operating systems likely will be added in the future. Windows Server 2008 administrators will find that installation and administration are consistent with how other server roles are installed and administered.



This page intentionally left blank

Glossary

account partner In a federation trust, it's the trusted company whose users will be accessing resources of the trusting company (resource partner). *See also* resource partner.

Active Directory The Windows directory service that enables administrators to create and manage users and groups, set network-wide user and computer policies, manage security, and organize network resources.

Active Directory-integrated zone A primary or stub zone with the DNS database stored in an Active Directory partition rather than a text file. Because Active Directory zones are replicated to other domain controllers automatically, only primary and stub zones can be Active Directory integrated.

Active Directory replication The transfer of information among domain controllers to make sure all domain controllers have consistent and up-to-date information.

AD LDS instance A copy of Active Directory Lightweight Directory Services (AD LDS) running on a server that has its own data store and communication ports and a unique service name.

AD RMS root cluster One or more servers configured with the Active Directory Rights Management Services (AD RMS) server role. Multiple servers can be used for redundancy and load balancing.

ADFS-enabled Web servers Web servers that host an Active Directory Federation Services (AD FS) Web agent.

administrative shares Hidden shares created by Windows that are available only to members of the Administrators group; they include the root of each volume, the %systemroot% folder, and IPC\$. Hidden shares' names end with a dollar sign.

administrative template files XML format text files that define policies in the Administrative Templates folder in a GPO. You can create custom ADMX files to create your own policies.

administrator role separation A feature available for RODCs in which a user can be granted local administrative rights on the RODC without needing broader domain administrator capabilities. *See also* read only domain controller (RODC).

ADMX central store A centralized location for maintaining ADMX files so that when an ADMX file is modified from one domain controller, all DCs receive the updated file.

alternate UPN name suffixes This method enables users to log on with another name in place of the “domain” in the typical UPN suffix format *username@domain*. These suffixes are used for security reasons or to simplify logons with lengthy suffixes.

application directory partition A directory partition that applications and services use to store information that benefits from automatic Active Directory replication and security.

attribute value Information stored in each attribute. *See also* schema attributes.

authentication A process that confirms a user's identity; the account is then assigned permissions and rights that authorize the user to access resources and perform certain tasks on the computer or domain.

authoritative restore A method of restoring Active Directory data from a backup to ensure that restored objects aren't overwritten by changes from other domain controllers through replication.

authoritative server A DNS server that holds a complete copy of a zone's resource records (typically a primary or secondary zone).

built-in user accounts User accounts created by Windows automatically during installation.

caching-only DNS server A DNS server with no zones. Its sole job is to field DNS queries, do recursive lookups to root servers, or send requests to forwarders, and then cache the results.

CA Web proxy A server configured with the Web Enrollment role service. *See also* registration authority.

certificate practice statement (CPS) A document describing how a CA issues certificates containing the CA identity, security practices used to maintain CA integrity, types of certificates issued, renewal policy, and so forth.

certificate templates A shell or model of a certificate used to create new certificates; it defines characteristics of the certificate, such as the intended use and expiration date.

claim An agreed-on set of user attributes that both parties in a federation trust use to determine a user's credentials.

conditional forwarder A DNS server to which other DNS servers send requests targeted for a specific domain.

configuration partition A directory partition that stores configuration information that can affect the entire forest, such as details on how domain controllers should replicate with one another.

configuration sets AD LDS instances containing a replica of an existing AD LDS instance's directory partition. All instances that replicate with one another are referred to as configuration sets.

connection object An Active Directory object created in Active Directory Sites and Services that defines the connection parameters between two replication partners.

contact An Active Directory object that usually represents a person for informational purposes only, much like an address book entry.

credential caching The process whereby an RODC can be configured to store passwords of selected accounts on the local server after they are retrieved from a writeable DC. By default, RODCs don't store any password information for user or computer accounts.

data collector set A Performance Monitor object used to create a baseline of performance data; can contain performance counters, counter alerts, event traces, and system configuration information.

Datacenter Edition A Windows Server 2008 edition with support for up to 64 processors, primarily intended for organizations managing huge amounts of data, using virtualization on a large scale, consolidating servers, or running high-volume, transaction-heavy applications.

dedicated forest root domain The first domain in a forest; contains only the forest-wide administrative accounts and domain controllers needed to run the forestwide operations master roles.

delegated installation An RODC installation method that doesn't require domain administrator credentials; a regular user at a branch office can perform the installation.

delegation of control The process of a user with higher security privileges assigning authority to perform certain tasks to a user with lesser security privileges; usually used to give a user administrative permission for an OU.

directory-enabled application An application that uses a directory service to store program, configuration, or user information.

directory partition A section of an Active Directory database stored on a domain controller's hard drive. These sections are managed by different processes and replicated to other domain controllers in an Active Directory network.

directory service A database that stores information about a computer network and includes features for retrieving and managing that information.

Directory Services Restore Mode A boot mode used to perform restore operations on Active Directory if it becomes corrupted or parts of it are deleted accidentally.

disk quotas An option on NTFS volumes that enables administrators to limit how much disk space a user can occupy with his or her files.

Distributed File System (DFS) A feature that makes shared files more accessible by grouping shared folders from multiple servers into a single folder hierarchy.

distribution group A group type used when you want to group users together, mainly for sending e-mails to several people at once with an Active Directory-integrated e-mail application, such as Microsoft Exchange.

distribution list An Active Directory object consisting of a list of users in a distribution group, used for sending an e-mail to multiple people simultaneously.

DNS namespace Defines the structure of the names used to identify resources in Internet domains. It consists of a root name (defined as a period), top-level domains, second-level domains, optionally one or more subdomains, and hostnames separated by periods.

domain The core structural unit of Active Directory; contains OUs and represents administrative, security, and policy boundaries.

domain controller A Windows server that has Active Directory installed and is responsible for allowing client computers access to domain resources.

domain directory partition A directory partition that contains all objects in a domain, including users, groups, computers, OUs, and so forth.

domain GPOs Group Policy Objects stored in Active Directory on domain controllers. They can be linked to a site, a domain, or an OU and affect users and computers whose accounts are stored in these containers.

domain local group A group scope that's the main security principal recommended for assigning rights and permissions to domain resources.

domain user account A user account created in Active Directory that provides a single logon for users to access all resources in the domain for which they have been authorized.

dual-IP layer architecture The current implementation of IPv6 in Windows Vista and Server 2008. Both IPv4 and IPv6 share the other components of the stack; the dual-stack layer used by Windows XP and Server 2003 duplicates the other TCP/IP layers.

Dynamic DNS (DDNS) A DNS name-registering process whereby computers in the domain can register or update their own DNS records.

Echo Reply An ICMP message that's the response when a computer receives an Echo Request, generated by the Ping program.

Echo Request An ICMP message generated by the Ping program used to test network connectivity and IP configuration. If a computer receives an Echo Request, it responds with an Echo Reply.

effective permissions A combination of a user's assigned permissions through group membership, explicit user permission assignments, and inherited permissions.

Enterprise Edition A Windows Server 2008 edition suitable for medium to large businesses that need high-availability network services. Supports up to eight processors and up to 2 TB RAM. Its most notable feature that isn't available in Standard Edition is clustering.

external trust A one-way or two-way nontransitive trust between two domains that aren't in the same forest.

failover clustering A Windows Server 2008 feature in Enterprise and Datacenter editions in which a group of servers is connected by both cabling and software; if one server fails, another takes over to provide services.

federated Web SSO An AD FS design in which a trust relationship is established between the resource partner and the account partner.

federated Web SSO with forest trust An AD FS design that involves a trust between two Active Directory forests. One forest, located in the perimeter network, is considered the resource partner. The second forest, located in the internal network, is the account partner.

federation servers A server configured to run the Federation Service role service. When used in an account partner network, its function is to gather user credentials into claims and package them into a security token. When used on the resource partner network, it receives security tokens and claims from the account partner and presents the claims to Web-based applications for authorization.

federation service proxy Installed on servers in a perimeter network outside the corporate firewall, this service fields authentication requests from browser clients and passes them to the federation server inside the firewall.

federation trust A trust between two networks using AD FS; one side of the trust is considered the account partner, and the other side is called the resource partner. *See also* account partner and resource partner.

file system Defines the method and format an OS uses to store, locate, and retrieve files from electronic storage media.

filtered attribute set A collection of attribute data used to specify domain objects that aren't replicated to RODCs, thereby increasing the security of sensitive information.

fine-grained password policies A new feature in Server 2008, used to set different password and account lockout policies for targeted users and groups. These policies are created by defining a Password Settings Object (PSO) in the Password Settings Container (PSC).

Flexible Single Master Operation (FSMO) roles Specialized domain controller tasks that handle operations that can affect the entire domain or forest. Only one domain controller can be assigned a particular FSMO.

folder redirection A feature that enables administrators to set policies that redirect folders in a user's profile directory, usually to a location on a server.

forest A collection of one or more Active Directory trees. A forest can consist of a single tree with a single domain, or it can contain several trees, each with a hierarchy of parent and child domains.

forest root domain The first domain created in a new forest.

forest trust A trust that provides a one-way or two-way transitive trust between forests, which enables security principals in one forest to access resources in any domain in another forest.

forest-wide authentication A property of a forest trust in which all users in a trusted forest can be authenticated to the trusting forest.

forward lookup zone (FLZ) A DNS zone containing records that translate names to IP addresses, such as A, AAAA, and MX records. It's named after the domain whose resource records it contains.

forwarder A DNS server to which other DNS servers send requests they can't resolve themselves.

fully qualified domain name (FQDN) A domain name that includes all parts of the name, including the top-level domain.

global catalog partition A directory partition that stores the global catalog, which is a partial replica of all objects in the forest. It contains the most commonly accessed object attributes to facilitate object searches and user logons across domains.

global group A group scope used mainly to group users from the same domain who have similar access and rights requirements. A global group's members can be user accounts and other global groups from the same domain.

GlobalNames zone (GNZ) A new feature in Windows Server 2008 that provides a method for IT administrators to add single-label names (computer names that don't use a domain suffix) to DNS, thereby allowing client computers to resolve these names without including a DNS suffix in the query.

glue A record An A record used to resolve the name in an NS record to its IP address.

GPO filtering A method to alter the normal scope of a GPO and exclude certain objects from being affected by its settings. GPO filtering methods include security filtering, which uses GPO permissions, and WMI filtering, which uses Windows Management Instrumentation queries to select objects.

Group Policy Container (GPC) A GPO component that's an Active Directory object stored in the System\Policies folder. The GPC stores GPO properties and status information but no actual policy settings.

Group Policy Object (GPO) A list of settings that administrators use to configure user and computer operating environments remotely through Active Directory.

Group Policy Template (GPT) A GPO component that's stored as a set of files in the Sysvol share. It contains all the policy settings that make up a GPO as well as related files, such as scripts.

group scope A property of a group that determines the reach of a group's application in a domain or a forest—which security principals in a forest can be group members and to which forest resources a group can be assigned rights or permissions.

guest operating systems OSs running in virtual machines on host computers.

hash algorithm A mathematical function that takes a string of data as input and produces a fixed-size hash value as output. Hash values are used to verify that the original data hasn't been changed and to sign CA certificates and certificates issued by the CA.

host computer The physical computer on which Windows Server 2008 is installed.

host operating system An OS running virtualization software for the purpose of running virtual machines or guest operating systems.

hot-add A high-end feature that allows adding hardware (usually memory, processors, or disk drives) to a system while it's running.

hot-replace A high-end feature that allows replacing faulty hardware (usually memory, processors, or disk drives) in a system while it's running.

hypervisor A layer of software between hardware and OSs that allows multiple OSs or multiple instances of the same OS to share physical hardware resources.

interforest migration Moving objects between domains in different forests. Migrated objects are actually copied and exist in both domains simultaneously so that users can continue working while the migration is in progress.

intermediate CAs A CA in a multilevel CA hierarchy that issues certificates to issuing CAs, which respond to user and device certificate requests. Sometimes called a policy CA.

intersite replication Active Directory replication that occurs between two or more sites.

intraforest migration Moving objects between domains in the same forest. The domain from which objects are moved is the source domain, and the domain to which they're being moved is the target domain.

intrasite replication Active Directory replication between domain controllers in the same site.

issuing CAs A CA that interacts with clients to field certificate requests and maintain the CRL.

item-level targeting A feature of group policy preferences that enables administrators to target users or computers for each preference based on a set of criteria.

iterative query A type of DNS query to which a DNS server responds with the best information it has to satisfy the query. The DNS server doesn't query additional DNS servers in an attempt to resolve the query.

Kerberos An open-standard security protocol used to secure authentication and identification between parties in a network.

key archival A method of backing up private keys and restoring them if users' private keys are lost.

Knowledge Consistency Checker (KCC) A process that runs on every domain controller to determine the replication topology.

Lightweight Directory Access Protocol (LDAP) A protocol that runs over TCP/IP and is designed to facilitate access to directory services and directory objects. LDAP is based on a suite of protocols called X.500, developed by the International Telecommunications Union.

link-local address Similar in function to the IPv4 APIPA addresses, link-local IPv6 addresses begin with fe80, are self-configuring, and can't be routed.

local GPOs A Group Policy Object that's stored on local computers and can be edited by the Group Policy Object Editor snap-in.

local group A group created in the local SAM database on a member server or workstation or a stand-alone computer.

local profile A user profile stored on the same system where the user logs on.

local user account A user account defined on a local computer that's authorized to access resources only on that computer. Local user accounts are mainly used on stand-alone computers or in a workgroup network with computers that aren't part of an Active Directory domain.

mandatory profile A user profile that can be changed during a user's logon session, but the next time the user logs on, the changes aren't saved, and the profile reverts to its original state.

member server A Windows server that's in the management scope of a Windows domain but doesn't have Active Directory installed.

metric A value assigned to the gateway based on the speed of the interface used to access the gateway.

multimaster replication The process for replicating Active Directory objects in which changes to the database can occur on any domain controller and are propagated, or replicated, to all other domain controllers.

network client The part of the OS that sends requests to a server to access network resources.

network connection An icon in the Network Connections window that shows the components needed for the computer to connect to a network.

Network Device Enrollment Service (NDES) A service that allows network devices, such as routers and switches, to obtain certificates by using Simple Certificate Enrollment Protocol (SCEP), a Cisco proprietary protocol.

network discovery The process whereby a computer finds other computers on a network and allows other computers to find it.

network map A graphical view of the network from your computer's perspective. It includes your computer, the networks to which your computer is connected, other devices on the network, and the Internet.

network protocol Software that specifies the rules and format of communication between devices on a network.

network provider A software component that allows Windows applications to connect to resources on other computers.

network server software The part of the OS that receives requests for shared network resources and makes those resources available to a network client.

New Technology File System (NTFS) A file system used on Windows OSs that supports compression, encryption, and fine-tuned permissions.

nonauthoritative restore A method of restoring Active Directory data from a backup that restores the database, or portions of it, and allows the data to be updated through replication by other domain controllers.

NTFS permissions Permissions set on folders or files on an NTFS-formatted volume. NTFS permissions protect both network and interactive file access.

object A grouping of information that describes a network resource, such as a shared printer, or an organizing structure, such as a domain or an OU.

octet An 8-bit value; a number from 0 to 255 that's one of the four numbers found in a dotted decimal IP address.

offline defragmentation Defragmentation of the Active Directory database that also compacts the database to improve performance. The Active Directory service must be stopped before offline defragmentation can occur.

one-way trust A trust relationship in which one domain trusts another, but the reverse is not true.

online defragmentation Defragmentation of the Active Directory database that removes deleted objects and frees up space in the database but doesn't compact the database. Online defragmentation occurs automatically when Active Directory performs garbage collection.

online responder (OR) A role service that enables clients to check a certificate's revocation status without having to download the certificate revocation list (CRL).

operations master A domain controller with sole responsibility for certain domain or forestwide functions.

organizational unit (OU) An Active Directory container used to organize a network's users and resources into logical administrative units.

Patches Software updates normally intended to fix security vulnerabilities and software bugs.

permission inheritance The process of transmitting permissions from a parent object to a child object.

permissions Settings that define which resources users can access and what level of access they have to resources.

Ping A utility used to test network connectivity and IP address configuration.

piping Sending the output of one command as input to another command.

primary zone A DNS zone containing a read/write master copy of all resource records for the zone; this zone is authoritative for the zone.

public key infrastructure (PKI) A security system that binds a user's or device's identity to a cryptographic key that secures data transfer with encryption and ensures data authenticity with digital certificates.

read only domain controller (RODC) A new feature of Active Directory Domain Services in Windows Server 2008, an RODC provides the same authentication and authorization services as a standard domain controller, but administrators can't make changes on an RODC directly.

realm trust A trust used to integrate users of other OSs into a Windows Server 2008 domain or forest; requires the OS to be running Kerberos V5 authentication.

recursive query A query in which the DNS server processes the query until it responds with an address that satisfies the query or with an "I don't know" message. The process might require the DNS server to query several additional DNS servers.

referral A response to an iterative query in which the address of another name server is returned to the requester.

registration authority A server configured with the Web Enrollment role service. *See also* CA Web proxy.

relative identifier (RID) The part of the SID that's unique for each Active Directory object. *See also* security identifier (SID).

resolver A DNS client that sends a recursive query to a DNS server.

resource partner In a federation trust, it's the trusting company whose resources are accessed by the trusted company (account partner). *See also* account partner.

resource record Data in a DNS database that contains information about network resources, such as hostnames, other DNS servers, and services, and is identified by a letter code.

restricted enrollment agent An enrollment agent that's limited to enrolling only specific users or security groups. Restricted enrollment agents are available only with an enterprise CA.

Resultant Set of Policy (RSOP) A report showing which policy settings apply to a user, computer, or both and where these policy settings originated. RSOP reports can be created using the RSOP snap-in, the Group Policy Results Wizard in GPMC, and the Gpresult.exe command-line program.

reverse lookup zone (RLZ) A DNS zone containing PTR records that map IP addresses to names; it's named with the IP network address (IPv4 or IPv6) of the computer whose records it contains.

right A setting that specifies what types of actions a user can perform on a computer or network.

roaming profile A user profile that follows the user no matter which computer he or she logs on to. It's stored on a network share so that when a user logs on to any computer in the network, the profile is copied from the network share to the profile folder on the local computer.

role services Services that can be installed in Server Manager to add functions to the main server role. *See also* server role.

root CA The first CA installed in a network. Clients are configured to trust the root CA's certificate, and then implicitly trust the certificate of any CA that's subordinate to the root.

root hints A list of name servers preconfigured on Windows DNS servers that point to Internet root servers, which are DNS servers located on the Internet and managed by IANA.

root servers DNS servers that keep a database of addresses of other DNS servers managing top-level domain names.

round robin A method of responding to DNS queries when more than one IP address exists for the queried host. Each IP address is placed first in the list of returned addresses an equal number of times so that hosts are accessed alternately.

scavenging A process whereby the DNS server checks the zone file for stale records periodically and deletes those meeting the criteria for a stale record.

schema Information that defines the type, organization, and structure of data stored in the Active Directory database.

schema attributes A category of schema information that defines what type of information is stored in each object.

schema classes A category of schema information that defines the types of objects that can be stored in Active Directory, such as user or computer accounts.

schema directory partition A directory partition containing the information needed to define Active Directory objects and object attributes for all domains in the forest.

secondary zone A DNS zone containing a read-only copy of all resource records for the zone. Changes can't be made directly on a secondary DNS server, but because it contains an exact copy of the primary zone, it's considered authoritative for the zone.

security groups A group type that's the main Active Directory object administrators use to manage network resource access and grant rights to users.

security identifier (SID) A numeric value assigned to each object in a domain that uniquely identifies the object; composed of a domain identifier, which is the same for all objects in a domain, and the RID. *See also* relative identifier (RID).

security principals An Active Directory object that can be assigned permissions or rights to Active Directory objects and network resources.

security templates Text files with an .inf extension that contain information to define policy settings in the Computer Configuration\Policies\Windows Settings\Security Settings node of a local or domain GPO.

selective authentication A property of a forest trust that enables administrators to specify users who can authenticate to selected resources in the trusting forest.

Server Core A new Windows Server 2008 installation option that uses a limited version of the GUI to take up fewer resources.

server features Components you can install that provide functions to enhance or support an installed role or add a stand-alone feature.

server operating systems OSs designed to emphasize network access performance and run background processes as opposed to desktop applications.

server role A major function or service that a server provides.

service pack A collection of bug fixes and security updates or patches that can be installed on an OS to bring it up to date.

shadow copies A feature on the Windows file system that allows users to access previous versions of files in shared folders and restore files that have been deleted or corrupted.

share permissions Permissions applied to shared folders that protect files accessed across the network. Share permissions are the only method for protecting files on FAT volumes.

shortcut trust A manually configured trust between domains in the same forest for the purpose of bypassing the normal referral process.

SID filtering When enabled, this option causes the trusting domain to ignore any SIDs that aren't from the trusted domain.

single sign-on (SSO) An authentication feature that makes it possible for users to access resources in their own organization as well as partner organizations with just a single logon.

site A physical location in which domain controllers communicate and replicate information regularly.

site link A logical connection between two sites that determines the replication schedule and frequency between the sites.

site link bridging A default property of a site link that makes it transitive. To control the transitive nature of site links, you can create site link bridges manually.

snapshot A set of files containing a virtual machine's state at a particular time.

stand-alone server A Windows server that isn't a domain controller or a member of a domain.

Standard Edition A Windows Server 2008 edition suitable for most small to medium businesses that need a robust solution for file and printer sharing, centralized control over user accounts and network resources, and common services found in most networks.

standard zone A primary, secondary, or stub zone that isn't Active Directory integrated.

Starter GPO A GPO template that can be used as a baseline for creating new GPOs, much like user account templates.

stub zone A DNS zone containing a read-only copy of only the zone's SOA and NS records and the necessary A records to resolve NS records. A stub zone forwards queries to a primary DNS server for that zone and is not authoritative for the zone.

subnet mask A 32-bit dotted decimal number consisting of an unbroken series of binary 1s followed by an unbroken series of binary 0s; used with an IP address to determine the network ID.

super mandatory profile A user profile type that prevents a user from logging on to the domain when the mandatory profile is unavailable.

Sysvol folder A shared folder that stores information from Active Directory that's replicated to other domain controllers.

tombstone lifetime A period of time in which deleted Active Directory objects are marked for deletion but left in the database. When the tombstone lifetime expires, the object is removed during garbage collection.

top-level domain (TLD) servers DNS servers that maintain addresses of other DNS servers that are authoritative for second-level domains that use the top-level domain. For example, a TLD server for the com top-level domain contains NS records for authoritative DNS servers for all domains ending in .com.

transitive trust A trust relationship based on the transitive rule of mathematics; therefore, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C.

tree A grouping of domains that share a common naming structure.

trust relationship An arrangement that defines whether and how security principals from one domain can access network resources in another domain.

two-way trust A trust in which both domains in the relationship trust each other, so users from both domains can access resources in the other domain.

unidirectional replication A replication method used with RODCs in which Active Directory data is replicated to the RODC, but the RODC doesn't replicate the data to other domain controllers.

universal group A group scope that can contain users from any domain in the forest and be assigned permission to resources in any domain in the forest.

universal group membership caching When enabled for a site, this Windows Server 2008 feature stores universal group membership information retrieved from a global catalog server, so the global catalog server doesn't have to be contacted for each user logon.

user principal name (UPN) A user logon name that follows the format *username@domain*. Users can use their UPNs to log on to their own domain from a computer that's a member of a different domain.

user profile A collection of a user's personal files and settings that define his or her working environment.

user template A user account that's copied to create users with common attributes.

virtual machine A software environment that simulates the computer hardware an OS requires for installation. A virtual machine creates in software all the hardware you find on a computer, including BIOS, disk controllers, hard drives, CD/DVD drives, serial ports, USB ports, RAM, network interfaces, video cards, and even processors.

volume mount points A feature that enables users to access a volume as a folder in another volume instead of by using a drive letter.

Volume Shadow Copy Service (VSS) A backup option that allows a volume to be backed up even while the volume is in use and files are being modified.

Web SSO An AD FS design that provides single sign-on access to multiple Web applications for users who are external to the corporate network.

Windows domain A group of Windows computers that share common management and are subject to rules and policies that an administrator defines.

Windows Recovery Environment (WinRE) A boot option available on the Windows Server 2008 installation DVD or by pressing F8 when the system boots; allows restoring Windows after a disk crash or similar catastrophic failure.

Windows Web Server 2008 A Windows Server 2008 edition designed to operate as a single-purpose Web server running IIS 7.0.

Windows workgroup Also called a peer-to-peer network, it's a small collection of Windows computers whose users typically have something in common, such as the need to share files or printers with each other. No computer has authority or control over another. Logons, security, and resource sharing are decentralized.

zone A grouping of DNS information that represents one or more domains and possibly subdomains.

zone delegation The transfer of authority for a subdomain to a new zone, which can be on the same server as the parent zone or on another server.

zone transfer An operation that copies all or part of a zone from one DNS server to another and occurs as a result of a secondary server requesting the transfer from another server.

Note: Page numbers referencing figures are italicized and followed by an “*f*”. Page numbers referencing tables are italicized and followed by a “*t*”. Entries formatted in bold mark the page on which a term is defined.

Special Characters

\$ (dollar sign), 228
:: (double colon), 345
| (pipe), 190–191

A

-a option, 335, 336
access control entries (ACEs), 118
access control lists (ACLs), 117, 202
Account expires option, 162
Account is disabled check box, 156
Account lockout duration policy, 282
Account Lockout Policy option, 286–287
Account Lockout Policy subnode, 282
Account lockout threshold policy, 282
account management, 151–195
 automating, 188–194
 computer accounts, 186–187
 group accounts, 175–186
 user accounts, 152–167
 user profiles, 167–175
Account Operators default group, 183*t*
account partners, **494–495, 509**
Account Policies subnode, 281–283
Account tab, 89, 161–162
ACEs. *See* access control entries (ACEs)
ACLs. *See* access control lists (ACLs)
Active Directory, 75–105, 111–145, 397–442, 485–510
 backup and restoration, 524–527
 components of, 82–96
 defined, **8, 31**
 domains, 138–139, 405–409
 forests, 130–134
 functional levels, 398–406

Group Policy Objects, 96–104
importing and exporting bulk data, 192–194
installing, 80–82
maintaining, 516–528
monitoring, 528–542
new roles, 29
object management, 188–191
operations master roles, 436–440
organizational units, 112–126
replication, **76, 105, 129–130, 388, 421–428, 541–542**
search function, 82, 91, 93, 154, 161, 186, 231
server roles, 486–508
sites, 139–143, 428–436
structure of, 77–80
terminology, 126–130
tools, 545–546
trees, 138–139
trusts, 134–138, 410–421
Active Directory Application Mode (ADAM), 486
Active Directory Certificate Services (AD CS), 19, 449–481
 Certification Authority, 461–475
 deploying, 454–461
 public key infrastructure, 450–453, 476–480
 terminology, 453
Active Directory Domain Services (AD DS), 19
 installing, 41, 80–82, 543–544
 synchronizing AD LDS with, 493–494
Active Directory Domain Services Installation Wizard, 429*f*

Active Directory Federation Services (AD FS), 29, 494–498
 design concepts, 496–498
 integrating AD RMS with, 499
 preparing to deploy, 498
 role services, 495–496
Active Directory Lightweight Directory Services (AD LDS), 29, 486–494
 creating groups in instances of, 490–491
 extending schema, 491–492
 installing, 487–489
 instances, **488, 509**
 management tools, 489–492
 replication, 492–493
 synchronizing with AD DS, 493–494
 uninstalling, 493–494
 when to use, 487
Active Directory Migration Tool (ADMT), 409
Active Directory Rights Management Service (AD RMS), 29, 498–502
 components of, 499–500
 deploying, 500–502
 key features of, 499
 root clusters, **499, 509**
Active Directory Schema snap-in, 158
Active Directory Sites and Services, *131f, 425, 428*
Active Directory Users and Computers window, *83f–84f, 261f*
Active Directory–integrated zone, **362, 391**
AD CS. *See* Active Directory Certificate Services (AD CS)
AD DS. *See* Active Directory Domain Services (AD DS)
AD FS. *See* Active Directory Federation Services (AD FS)

- AD LDS. *See* Active Directory Lightweight Directory Services (AD LDS)
- AD RMS. *See* Active Directory Rights Management Service (AD RMS)
- ADAM. *See* Active Directory Application Mode (ADAM)
- Adapters and Bindings tab, 341, 342*f*
- Add Counters dialog box, 533, 534*f*
- Add to a group option, 159
- Additional Clocks tab, 46
- Additional Drivers button, 241
- Additional Rules folder, 294
- Address Resolution Protocol (ARP), 328
- ADFS-enabled Web servers, 496, 509
- Admin\$ share, 228
- administrative shares, 228, 246
- administrative template (ADMX) files, 291–292, 298, 307–308, 312
- Administrative Templates folder, 98, 278, 291–292, 298
- Administrative Tools folder, 9
- Administrator account, 153
- Administrator password window, 43*f*
- administrator role delegation, 499
- administrator role separation, 508–509
- Administrators group, 88*f*, 183*t*, 516
- ADMT. *See* Active Directory Migration Tool (ADMT)
- ADMX central store, 307–308, 312
- ADMX files. *See* administrative template (ADMX) files
- Adprep tool, 406–407
- ADSI Edit tool, 289–290, 489, 491*f*
- Advanced Boot Options menu, 524*f*
- Advanced Encryption Standard (AES) support, 400
- Advanced Features option, 118–119
- Advanced Password Replication Policy dialog box, 507*f*
- Advanced redirection option, 296
- Advanced Security Settings dialog box, 120*f*, 219*f*, 276
- Advanced Settings dialog box, 341, 342*f*
- Advanced Sharing dialog box, 224
- Advanced tab, 241, 242*f*, 384*f*
- Advanced TCP/IP Settings dialog box, 332*f*
- Advances Attributes dialog box, 212*f*
- AES support. *See* Advanced Encryption Standard (AES) support
- Aging button, 368
- aging resource records, 368–370
- AIA. *See* Authority Information Access (AIA)
- All descendant objects permission setting, 122
- /all option, 335, 388
- All Settings subnode, 292
- Allow both nonsecure and secure dynamic updates option, 365
- Allow only secure dynamic updates option, 365
- Allow permission, 118
- Allowed RODC Password Replication group, 183*t*
- alternate UPN name suffixes, 420, 441
- Always available option, 241, 242*f*
- Always perform full backup option, 518
- Always perform incremental backup option, 518
- Anonymous Logon group, 184*t*
- AppData folder, 168
- application directory partitions, 127, 144, 486
- Application Server, 20
- Apply to option, 219
- ARP. *See* Address Resolution Protocol (ARP)
- Arp command, 335–338
- assigned applications, 292
- asymmetric cryptography, 451
- Attribute Editor tab, 119, 192
- attribute values, 83, 105
- Audit Policy option, 288
- Audit Policy subnode, 283
- auditing object access, 284–289
- Auditor role, 476
- Auditpol.exe tool, 284
- Authenticated Use group, 184*t*
- authentication, 86, 105, 450
- Authentication tab, 420–421
- authoritative restores, 524, 547
- authoritative server role, 357, 391
- Authority Information Access (AIA), 453
- Auto-Enrollment policy options, 465*f*
- automatic account management, 188–194
- CSVDE tool, 192–193
- DSADD tool, 189–190
- DSMOD tool with pipe, 190–191
- DSQUERY tool with pipe, 190–191
- LDIFDE tool, 193–194
- automatic updates, 49–51, 59
- Available from option, 241, 242*f*
- AXFR Request Received counter, 389
- B**
- backup and restoration, 516–527
- Active Directory, 524–527
 - Certification Authority, 476–477
 - GPOs, 303–304, 516
 - Windows Server Backup, 516–524
- backup catalogs, 523
- Backup Operator role, 476
- Backup Operators group, 183*t*, 516
- Backup Schedule Wizard, 519
- baselines. *See* performance baselines
- Basic redirection option, 296
- Basic User setting, 294
- batch files, 188
- Bcdedit tool, 545
- BitLocker Drive Encryption, 505

- Block Inheritance option, 271–272, 274t
blocking GPO inheritance, 271, 273
bridgehead servers, 433–434
Browse for a Group Policy Object dialog box, 256f
browsing networks, 231, 232f
Builtin folder, 85, 182–183
built-in user accounts, **86, 105**
bulk data importing and exporting, 191–194
- C**
- CA. *See* certification authority (CA)
CA Administrator role, 476
CA certificate manage approval option, 465
CA Web proxy, **469, 481**
Caching button, 224f, 225
caching-only DNS server role, **357, 391**
Canonical Name (CNAME) records, 355t
Categories tab, 280
CDP. *See* certificate distribution point (CDP)
certificate archival and recovery, 477–480
certificate autoenrollment, 464–468
certificate distribution point (CDP), 453
certificate enrollment, 453, 464–472
Certificate Enrollment Wizard, 468f
Certificate Export Wizard, 477
Certificate Manager role, 476
certificate practice statement (CPS), **456, 481**
certificate revocation lists (CRLs), 453
certificate templates, **453, 461–464, 481**
certificates, application, 294
Certificates Templates snap-in, 462f
Certification Authority (CA), 452–453, 461–475
Change permission level, 216
Change Schedule button, 432f, 433
Change Schedule field, 424
Change Schema Master dialog box, 438f
Change settings dialog box, 50f
Change Type button, 175
CIDR. *See* Classless Interdomain Routing (CIDR)
ciphertext data, 451
claims, **495, 509**
Claims-aware agents, 496
claims-aware applications, 495
Classless Interdomain Routing (CIDR), 330
CLCs. *See* client licensor certificates (CLCs)
/ClearCache option, 387
Client for Microsoft Networks service, 338, 341
client licensor certificates (CLCs), 500
Client Side Extensions (CSE) for Vista, 308–309
clients, defined, 321
Clipboard menu, 68
clustering, 3
CNAME records. *See* Canonical Name (CNAME) records
command prompt window, 45, 55–56
Command-line Tools option, 517
Comments field, 224f, 225
Common tab, 310f
Compress this drive to save disk space option, 212
computer accounts, 87, 186–187
Computer Configuration node, 97–98, 277–279, 291–292, 308
computer names, 49, 58–59, 354
computer workgroups, 49, 58–59
Computers folder, 85
conditional DNS forwarders, 381–382
conditional forwarders, **357, 375, 381, 391, 414–416**
confidentiality, 450
/Config option, 387
Configuration Model options, 464
Configuration node, 24
configuration partitions, **127, 144**
configuration sets, **492, 510**
configuration tasks, 36
Configure AD RMS Cluster Key Storage window, 501f
Configure Cryptography page, 460f
Configure Performance Settings in the Actions pane, 517f, 518
Confirm password field, 155
Confirm Subtree Deletion message box, 525, 526f
Connect to a network window, 324, 325f
connection objects, **423–426, 441**
Connection Settings dialog box, 490f
Contact leaf object, 87
contacts, **165–167, 195**
container objects, 84–86
Control Panel Settings subnode, 308
Control Panel subnode, 291
Copy To button, 175
Cost field, 143
counter alerts, 535
CPS. *See* certificate practice statement (CPS)
CPU architecture, 39
Create all child objects permission, 117
Create files/write data permission level, 218t
Create folders/append data permission level, 218t
Create GPOs permission, 302
Create Now button, 209f, 210
Create or Join an AD RMS Cluster window, 501
Create Scheduled Tasks right, 516
/.CreateDirectoryPartition option, 387
Creator Owner group, 184t
credential caching, **505–508, 510**
CRLs. *See* certificate revocation lists (CRLs)

- CRM. *See* customer relationship management (CRM)
- Cross-Domain Copying Wizard, 306
- cryptographic service provider (CSP) list box, 460
- CSE for Vista. *See* Client Side Extensions (CSE) for Vista
- CSP list box. *See* cryptographic service provider (CSP) list box
- CSVDE command-line tool, 192–193
- Ctrl+Alt+Delete menu, 55*f*
- Custom option, 518
- customer relationship management (CRM), 29
- Cut option, 159
- d option, 336
- D**
- DACLs. *See* discretionary access control lists (DACLs)
- DAP. *See* Directory Access Protocol (DAP)
- data collector sets, 533, 535–538, 547
- Data Collector Sets folder, 531
- data storage, 202
- Datacenter Edition, Windows Server 2008, 3–4, 31
- date, setting
- in Server Core, 56
 - in Windows Server 2008, 46
- Dcdiag tool, 541
- Dcpromo tool, 407–408, 543
- DDNS. *See* Dynamic DNS (DDNS)
- debug logging, 385–386
- Debug Logging tab, 386*f*
- dedicated forest root domain, 133, 144
- Default Domain Controllers Policy, 96
- Default Domain Policy, 96, 101–102, 269*t*, 270, 271*t*–272*t*, 274*t*
- default groups, 182–186
- default shares, 228
- Default-First-Site-Name Properties dialog box, 141*f*
- Default-First-Site-Name site, 139
- DEFAULTSITELINK link, 428, 432, 434
- defragmentation, 527–528
- delegated installation, 503, 510
- delegation of control, 115–117, 144
- Delegation tab, 275, 302*f*
- Delete all child objects permission, 117
- Delete permission level, 218*t*
- Delete subfolders and files permission level, 218*t*
- Delta CRLs, 453
- Denied RODC Password Replication group, 183*t*
- Deny disk space to users exceeding quota limit check box, 204*f*, 205
- Deny permissions, 118, 215, 227–228
- Deny setting, 118
- department folders, 250
- Deployed Printers subnode, 281, 293
- Deployment tab, 280, 281*f*
- Descendant [object type] objects permission setting, 122
- descendant objects, 120
- Designated File Types policy, 294
- Desktop Experience feature, 19
- Desktop folder, 168
- desktop operating systems, 2–3
- Desktop subnode, 298
- Details button, 17, 209*f*, 210
- Details tab, 262*f*, 461*f*
- Device Manager snap-in, 544
- DFS. *See* Distributed File System (DFS)
- DFS Management MMC, 236, 237*f*
- DFSR. *See* Distributed File System Replication (DFSR)
- Dfsutil tool, 546
- DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
- Diagnose and repair link, 325*f*
- Diagnostics node, 23
- Dial-up group, 184*f*
- digital certificates, 452
- digital signatures, 452
- Direction of trust field, 418
- Direction of Trust window, 411*f*
- Directory Access Protocol (DAP), 112
- directory partitions, 126–127, 144
- directory replication, 486
- directory services, 76, 105
- Directory Services Restore Mode (DSRM), 81, 105, 524–525, 527
- directory-enabled applications, 486, 510
- Disable Account option, 159
- Disable recursion (also disables forwarders) option, 384
- disabling
- default auditing, 287
 - services, 340–341
- Disallow setting, 294
- discretionary access control lists (DACLs), 117
- disk compression, 212–214
- Disk Management snap-in, 9*f*, 10–12, 236, 544
- Disk Management window, 206*f*
- disk quotas, 204–207, 246
- Display name field, 161
- /displaydns option, 335, 388
- displayName attribute, 259
- Distributed File System (DFS), 12, 52, 140, 233, 236–238, 247
- Distributed File System Replication (DFSR), 262, 400
- distribution groups, 176, 195
- distribution lists, 165–167, 166, 195
- DNS. *See* Domain Name System (DNS)
- DNS Manager, 359–361, 387
- DNS Manager window, 359*f*, 373*f*
- DNS Server check box, 81
- DNS Server log, 388, 530
- DnsAdmins/domain local default group, 183*t*

- Dnscmd tool, 367–368, 387, 546
Dnslint tool, 387, 388
Do not allow dynamic updates option, 365
Do not automatically reenroll if a duplicate certificate exists in Active Directory check box, 464
Do not limit disk usage option, 204f, 205
Do not replicate this record check box, 379
Documents and Settings folder, 167
Documents folder, 168
dollar sign (\$), 228
Domain Admins global group, 180, 183t
Domain Computers/global default group, 183t
domain controllers, 14, 31, 358, 404–408
Domain Controllers/global default group, 183t
domain directory partitions, 126–127, 144
domain functional levels, 399–406
 raising, 402, 405–406
 trying to use unsupported features, 405
 Windows 2000, 399–400
 Windows Server 2003, 400
 Windows Server 2008, 400–401
domain GPOs, 257–258, 312
domain local groups, 177–178, 195
domain model, defined, 14
Domain Name System (DNS), 327, 353–392
 DNS Manager, 359–361
 domain controllers, 358
 forwarders, 380–382
 installing, 358, 361–362, 543–544
 logging, 385–386
 monitoring performance of, 389–390
 namespaces, 354, 391
recursive queries, 384–385
root hints, 382–383
round robin process, 383–384
server roles, 20, 357
structure of, 354–357
troubleshooting, 387–389
zones, 357–358, 362–380
domain naming master role, 127, 437, 438t
domain networks, 322
domain objects, 85–86, 409
domain user account, 105, 153f
Domain Users global group, 180, 183t
domain-linked GPOs, 270
domains
 defined, 78, 105
 designing structure of, 138–139
 joining, 542–543
 removing, 408
domain-wide FSMO roles, 436
double colon (::), 345
Downloads folder, 168
Drive\$ share, 228
Driver field, 242
drives, mapping, 231–233
Dsacls tool, 545
DSADD tool, 91, 188–190
Dsdbutil tool, 545
DSGET tool, 188
Dsmgmt tool, 545
DSMOD tool, 188, 190–191
DSMOVE tool, 188
DSQUERY tool, 188, 190–191
DSRM. *See* Directory Services Restore Mode (DSRM)
DSRM tool, 188
dual-IP layer architecture, 344, 348
Dynamic DNS (DDNS), 355, 391
Dynamic Host Configuration Protocol (DHCP), 20, 327
dynamic updates, 355, 365–367
Dynamic updates option, 368
- ## E
- Echo Reply, 48, 70
Echo Request, 48, 70
Edit settings, delete, modify security permission, 303
Edit Settings permission, 303
effective permissions, 118, 144
Effective Permissions tab, 124f
EFS. *See* Encrypting File System (EFS)
EFS certificate template, 462–464
E-mail field, 161
Enable advanced printing features check box, 242f, 243
Enable quota management check box, 204f, 205
Enable system recovery check box, 518, 519f
Enable Universal Group Membership Caching check box, 436
Encrypt contents to secure data check box, 212f
Encrypting File System (EFS), 204, 212–215, 462–464
end user license agreement (EULA), 63
Enforce password history policy, 282
Enforced option, 271–272
Enforcement policy, 294
enforcing GPO inheritance, 271–274
Enroll subject without requiring any user input option, 465
enrollment agents, 453
Enterprise Admins/universal default group, 183t
enterprise CAs, 453–454
Enterprise Edition, Windows Server 2008, 3–4, 31
enterprise-class backup programs, 517
Environment tab, 164
Equal_Per_IISAppPool policy, 540
Equal_Per_Process policy, 540

- Equal_Per_Session policy, 540
 Equal_Per_User policy, 540
 Error event level, 529
 EULA. *See* end user license agreement (EULA)
 Event Log Online Help link, 529
 Event Log subnode, 291
 event logging, 385–386
 Event Logging tab, 385
 event traces, 535
 Event Viewer, 387, 529–530, 539
 Everyone group, 184*t*
 Expires after field, 371
 exporting bulk data, 191–194
 /ExportSettings option, 387
 extending AD LDS schema, 491–492
 Extensions tab, 473*f*
 external queries, 380
 external trusts, 137, 144, 418
- F**
- failover clustering, 19, 52, 70
 FAT file system. *See* File Allocation Table (FAT) file system
 Favorites folder, 168
 Fax Server, 20
 federated Web SSO design, 497, 510
 federated Web SSO with forest trust design, 497–498, 510
 federation servers, 495, 510
 federation service proxy, 495–496, 510
 federation trusts, 494–495, 510
 File Allocation Table (FAT) file system, 203, 216–217
 File and Printer Sharing for Microsoft Networks service, 339
 file attributes, 202
 file compression, 204
 file encryption, 212–215
 File menu, 68
 file ownership, 218–219
 File Replication Service (FRS), 234, 262
 File Screening Management tool, 238, 239*f*
 File Server Resource Manager (FSRM), 27, 233, 238–240
 File Services, 20–21, 203–240
 file sharing, 223–233
 file systems, 203–215
 permissions, 215–223
 storage management, 233–240
 file sharing, 12–13, 223–233
 accessing from client computers, 231–233
 administrative shares, 228
 advanced, 226
 creating shared folders, 250–251
 default shares, 228
 easing access to shares, 251
 File Sharing Wizard, 225–226
 mapping drives, 231–233
 monitoring access, 230–231
 publishing access, 230–231
 restricting access, 226–228
 Shared Folders snap-in, 228–231
 File sharing option, 324
 File Sharing Wizard, 94*f*, 223–226
 File System subnode, 291
 file systems, 203–217
 defined, 202, 247
 FAT, 203, 216–217
 NTFS, 203–215
 filenames conventions, 202
 filtered attribute sets, 505, 510
 filtering GPOs, 274–277
 Find Users, Contacts, and Groups dialog box, 92*f*
 finding objects, 91–96
 fine-grained password policies, 289–290, 312, 400
 firewalls, 57–58, 435, 545
 flags attribute, 260
 Flexible Single Master Operation (FSMO) roles, 127, 144, 436–438
 /flushdns option, 335, 388
 FLZs. *See* forward lookup zones (FLZs)
 folder objects, 85
 folder ownership, 218–219
 folder redirection, 312
 Folder Redirection subnode, 293, 295–297
 For automatic renewal of smart card certificates, use the existing key if a new key cannot be created check box, 464
 ForeignSecurityPrincipals folder object, 85
 forest functional levels, 398–406
 raising, 402–406
 Windows 2000, 398
 Windows Server 2003, 398–399
 Windows Server 2008, 399
 forest root domains, 131*f*, 132–133, 144
 forest trusts, 136–137, 144, 380, 399, 414–418
 forests, 79, 105, 130–134, 135*f*
 forest-wide authentication, 415, 441
 forest-wide FSMO roles, 436
 forward lookup zones (FLZs), 364–366, 391
 forwarders, 357, 380–382, 391
 Forwarders tab, 381
 FQDNs. *See* fully qualified domain names (FQDNs)
 FRS. *See* File Replication Service (FRS)
 FSMO roles. *See* Flexible Single Master Operation (FSMO) roles
 FSRM. *See* File Server Resource Manager (FSRM)
 Full control permission level, 117, 216, 217*f*, 218
 Full name field, 155
 full zone transfers, 376
 fully qualified domain names (FQDNs), 80, 105, 354

- functional levels, 398–406
domain, 399–402, 405–406
forest, 398–399, 402–406
- G**
- g option, 336
 - Gateway column, 333
 - General tab, 161, 368, 418–419, 459f
 - generic top-level domain (GTLD) servers, 360
 - global catalog caching, 436
 - Global catalog check box, 81
 - global catalog partitions, **127, 144**
 - global catalog replication, 426–427
 - global catalog servers, 131–132, 426
 - global groups, *177t, 178–179, 195*
 - globally unique identifiers (GUIDs), 257
 - GlobalNames zone (GNZ), **379–380, 391**
 - glue A records, **372, 391**
 - GNZ. *See* GlobalNames zone (GNZ)
 - gPCFileSysPath attribute, 259
 - GPCs. *See* group policy containers (GPCs)
 - GPMC. *See* Group Policy Management Console (GPMC)
 - GPME. *See* Group Policy Management Editor (GPME)
 - GPO status: All Settings Disabled state, 303
 - GPO status: Computer Configuration Settings Disabled state, 303
 - GPO status: Enabled state, 303
 - GPO status: User Configuration Settings Disabled state, 303
 - GPOs. *See* Group Policy Objects (GPOs)
 - Gpotool tool, 263
 - GPP CSE package. *See* Group Policy Preference Client Side Extensions (GPP CSE) package
 - Gpresult tool, 307
 - GPT.ini file, 258
 - GPTs. *See* group policy templates (GPTs)
 - GptTmpl.inf file, 259
 - Gpupdate tool, 267
 - group accounts, 175–186
 - creating, 199
 - default groups, 182–186
 - group scope, 176–182
 - nesting groups, 180–181
 - types of, 176
 - group conversion, 399
 - group nesting, 180–181, 399
 - group policy, 254–292, 298–311
 - ADMX central store, 307–308
 - architecture of, 254–278
 - backing up and restoring, 303–304
 - GPMC, 302–303
 - inheritance, 269–278
 - migration, 303, 305–306
 - preferences, 308–311
 - results and modeling, 306–307
 - security templates, 298–302
 - settings, 278–292
 - group policy containers (GPCs), **257, 259–262, 312**
 - Group Policy Creator Owners/global default group, *184t*
 - Group Policy Editor snap-in, 254
 - Group Policy Management Console (GPMC), *97f, 263–264, 275f–276f, 302–303, 305–307, 322*
 - Group Policy Management Editor (GPME), *101f, 263*
 - Group Policy Modeling tool, 307
 - Group Policy Object Editor snap-in, *254, 255f*
 - Group Policy Objects (GPOs), *96–104, 254–269*
 - applying, 101–104
 - backup and restoration, 303–304, 516
 - Computer Configuration node, *97–98*
 - configuring, 266–267
 - creating, 109, 265–266, 317
 - default, 99–101
 - defined, **96, 105**
 - domain, 257–258
 - editing existing, 263–265
 - filtering, **275, 312**
 - GPCs, 259–262
 - GPTs, 258–259
 - linking, 265–266
 - local, 254–257
 - migration, 303, 305–306
 - Starter, 267–269
 - testing, 266–267
 - unlinking, 265–266
 - User Configuration node, *98–101*
- Group Policy Preference Client Side Extensions (GPP CSE) package, *97, 308*
- Group Policy Results report, *306f*
- group policy templates (GPTs), *257–259, 258, 262, 312*
- group scope, 176–182
 - converting, 181–182
 - creating groups with different, 181–182
 - defined, **176, 195**
 - domain local groups, *177–178*
 - global groups, *178–179*
 - local groups, *180*
 - universal groups, *179–180*
- groups, *86–87*
- GTLD servers. *See* generic top-level domain (GTLD) servers
- Guest account, *153–154*
- guest operating systems, **60, 70**
- Guests default group, *183t*
- GUIDs. *See* globally unique identifiers (GUIDs)

H

Hardware Abstraction Layer (HAL), 39
 hash algorithm, 294, 460, 481
 HCAP. *See* Host Credential Authorization Protocol (HCAP)
 Health Registration Authority (HRA), 21
 hierarchical file organization, 202
 Highlight toolbar icon, 532
 Hold mismatched documents check box, 242
 Home folder, 163
 Host (A) records, 355*t*
 host computer, 60, 70
 Host Credential Authorization Protocol (HCAP), 21
 host IDs, 330–331, 345–346
 host operating systems, 60, 70
 Hosts file, 357, 388
 hot-add, 40, 70
 hot-replace, 40, 70
 HRA. *See* Health Registration Authority (HRA)
 hub-and-spoke topology, 435*f*
 hubs, 320
 Hyper-V, 4, 21, 25–27, 60–69
 Hyper-V Manager console, 26*f*, 63*f*, 64*f*, 67*f*
 hypervisor, 70

I

-i TTL option, 335
 IANA. *See* Internet Assigned Numbers Authority (IANA)
 Icacls tool, 546
 ICMP. *See* Internet Control Message Protocol (ICMP)
 ICMP Echo Request packets, 334–337
 Identity Federation Support, 500
 Idle Time column, 230
 IETF. *See* Internet Engineering Task Force (IETF)

IIS. *See* Internet Information Services (IIS)
 IIS_IUSRS default group, 183*t*
 importing bulk data, 191–194
 Include inheritable permissions from this object's parent check box, 219
 incremental zone transfers, 376–378
 Indexing Service, 234
 inetOrgPerson object class, 116
 /Info option, 387
 Information event level, 529
 infrastructure master role, 127, 438–440
 inheritance, group policy, 254, 269–278
 blocking, 271, 273
 domain-linked GPOs, 270
 enforcing, 271–274
 filtering, 274–277
 loopback policy processing, 277–278
 OU-linked GPOs, 270–271
 site-linked GPOs, 270
 Initial Configuration Tasks applet, 44*f*, 49
 initial installation window, 41*f*
 Install Updates button, 51
 installing
 Active Directory, 80–82
 AD CS, 456–461
 AD DS, 41, 80–82, 543–544
 AD LDS, 487–489
 CSE for Vista, 308–309
 DNS, 358, 361–362, 543–544
 domain controllers in subdomain, 358
 Hyper-V, 61–62
 new server roles and features, 542
 printers, 243–244
 RODCs, 503–505
 Server Core, 54–55
 updates, 49–51
 Windows Server 2008, 38–52, 56, 58–59, 65–66, 74
 Windows Server Backup, 517–518
 integrity, PKI, 450
 Interactive group, 184*t*
 Interface column, 333
 interforest migration, 409, 441
 intermediate CAs, 456, 481
 International Telecommunications Union (ITU), 112
 Internet Assigned Numbers Authority (IANA), 382
 Internet Control Message Protocol (ICMP), 328
 Internet Engineering Task Force (IETF), 112, 344
 Internet Explorer Maintenance subnode, 293, 297–298
 Internet Information Services (IIS), 17–19, 22
 Internet Information Services (IIS) Manager window, 18*f*
 Internet Printing role, 21, 245
 Internet Protocol (IP) command-line tools, 334–338
 Internet Protocol version 4 (IPv4) addresses, 328–334
 assigning classes, 329–330
 assignment rules, 330
 configuring default gateway, 332
 configuring multiple, 331–332
 subnetting, 330–331
 using multihomed servers, 332–333
 using Route command, 333–334
 Internet Protocol version 4 (TCP/IPv4) Properties dialog box, 329*f*
 Internet Protocol version 6 (IPv6), 339, 341, 343–347
 Internet Time tab, 46
 internetworks, 321
 intersite replication, 129, 145
 Intersite Topology Generator (ISTG), 143, 433–434

intersite transport protocols, 434–435
Inter-Site Transports folder, 432
intraforest migration, **409, 441**
intrasite replication, **129, 145**
IP address field, 379
IP command-line tools. *See* Internet Protocol (IP) command-line tools
IP next generation (IPng), 344
IP Security Policies on Active Directory subnode, 291
IP subfolder, 432
IPC\$ share, 228
Ipconfig tool, 335, 387–388
IPng (IP next generation). *See* IP next generation (IPng)
IPSec Management snap-in, 544
IPv4 addresses. *See* Internet Protocol version 4 (IPv4) addresses
IPv6. *See* Internet Protocol version 6 (IPv6)
IPv6 Host (AAAA) records, 355*t*
Issuance Requirements tab, 465
issuers, 461
issuing CAs, **456, 481**
ISTG. *See* Intersite Topology Generator (ISTG)
Itanium Edition, Windows Server 2008, 4
item-level targeting, **312**
iterative queries, **356, 391**
ITU. *See* International Telecommunications Union (ITU)

J

joining domains, 542–543

K

KCC. *See* Knowledge Consistency Checker (KCC)
Keep printed documents check box, 242
Kerberos, **137, 145**
Kerberos Policy subnode, 283
key archival, **477–480, 481**

key character length text box, 460
key recovery agents (KRAs), 478–479
key usage, 461
keys, 451–453
Knowledge Consistency Checker (KCC), **129, 145, 399, 422–423, 425, 435**
KRAs. *See* key recovery agents (KRAs)

L

-l size option, 335
LANs, 139, 333
Last interactive logon information, 401*f*
LDAP. *See* Lightweight Directory Access Protocol (LDAP)
LDIF files, 489
LDIFDE tool, 193–194
LDP tool, 489
leaf objects, 86–91
Lightweight Directory Access Protocol (LDAP), **112, 145**
Limit disk space to option, 204*f*, 205
Limit the number of simultaneous users to option, 224*f*, 225
Line Printer Daemon (LPD) role, 21, 245
Link GPOs permission, 303
Link Layer Topology Discovery (LLTD) protocol, 323, 339
Link status: disabled state, 303
Link status: enabled state, 303
Link status: unlinked state, 303
linked-value replication, 399
linking GPOs, 265–266, 270–271, 303
link-local addresses, **345, 348**
List folder contents permission level, 217
List folder/read data permission level, 218*t*
List in the directory check box, 241
listing installed features and roles, 542
LLTD protocol. *See* Link Layer Topology Discovery (LLTD) protocol
load balancing, 3
Local Administrators GPO, 255
Local Area Connection Properties dialog box, 47, 339*f*
Local Computer Policy object, 255
local GPOs, **254–257, 312**
local groups, **180, 195**
Local Non-Administrators GPO, 255
Local Policies subnode, 283–284
local print devices, 240
local profiles, **168, 195**
Local Security Policy MMC, 254, 266*f*
local user accounts, **86, 105, 153*f***
Local Users and Groups snap-in, 152
locally cached data, 388
Located on this volume menu, 209*f*, 210
Lock the Taskbar policy, 269*t*, 270, 271*t*–272*t*, 274*t*
Log event when a user exceeds their quota limit check box, 204*f*, 205
Log event when a user exceeds their warning level check box, 204*f*, 205
Log On To button, 162
logging, 385–386
Logon Hours button, 162
Logon script, 163
loopback policy processing, 277–278
LostAndFound folder, 118
LPD role. *See* Line Printer Daemon (LPD) role
ls -d domain option, 388

M

Machine folder, 257–258
Mail Exchanger (MX) records, 355*t*
MAK license. *See* Multiple Activation Key (MAK) license
Manage documents permission level, 244
Manage network connections link, 325*f*
Manage printers permission level, 244

- managed policy settings, 278
 mandatory profiles, 169–171, **170**, 174, **195**
 manual archival, 477
 Map Network Drive dialog box, 232
 mapping drives, 231–233
 Maximum password age policy, 282
 Maximum size options, 209*f*, 210
 Media menu, 68
 Member Of tab, 88, 163–165
 member servers, **14**, **31**
 Members tab, 88–89
 Memory Diagnosis link, 537
 metadata, 202
 metric, **332**, **348**
 Metric column, 333
 Microsoft Management Console (MMC), 8–10
 migrating
 domain objects, 409
 GPOs, 303, 305–306
 Minimum (default) TTL field, **371***f, 372
 Minimum password age policy, 282
 Minimum password length policy, 282
 mirrored services, 383–384
 Miscellaneous Failure events, 539
 MMC. *See* Microsoft Management Console (MMC)
 modeling group policy, 306–307
 Modifications tab, 280
 Modify permission level, 217*f*, 218
 monitoring
 Active Directory, 516–542
 DNS, 389–390
 Monitoring Tools folder, 531–532
 Move option, 159
 MSI files, 279–280
 multihomed servers, 332–333
 multilevel CA hierarchies, 456
 multilevel OU structure, 113*f*
 multimaster replication, **129**, **145**
 Multiple Activation Key (MAK) license, 45
 Music folder, 168
 MX records. *See* Mail Exchanger (MX) records
 My Documents folder, 168
 My Music folder, 168
 My Pictures folder, 168
N
 -n *count* option, 335
 Name Server (NS) records, 372–373
 Name Servers tab, 372*f*
 Name Suffix Routing tab, 419–420
 NAP. *See* Network Access Protection (NAP)
 NDES. *See* Network Device Enrollment Service (NDES)
 nesting groups, 180–181, 399
 Netdom tool, 187, 400
 NETLOGON share, 228
 Netmask column, 333
 netsh interface command, 56–57
 Network Access Protection (NAP), 21, 28, 291
 Network and Sharing Center, 12*f*, 320–327
 network maps, 322–324
 Sharing and Discovery section, 324
 Tasks section, 324–327
 network bindings, 341–343
 network clients, **15**, **31**
 Network Configuration Operators default group, 183*t*
 network connection icon, **321**, **348**
 Network Connections window, 14*f*
 Network Destination column, 333
 Network Device Enrollment Service (NDES), **471**, **481**
 network discovery, **321**, 324, 327, **348**
 Network Error message, 340*f*
 Network File System (NFS), 233–234
 Network group, 184*t*
 network interface cards (NICs), 14, 320, 332
 network interfaces, 14–15
 Network List Manager Policies subnode, 291
 network maps, 16*f*, **322**–**324**, **348**
 network media, 320
 Network Policy Server (NPS), 21
 network print devices, 240
 network protocol, **15**, **31**, 320
 network providers, **342**–**343**, **348**
 network server software, **15**, **31**
 Network subnode, 292
 Network window, 93*f*, 322
 network zones, 294
 networking concepts
 Internet Information Services, 17–19
 Windows, 13–17
 networking enhancements, 28
 networks, defined, 321
 New Conditional Forwarder dialog box, 382*f*
 New Object - User dialog box, 154*f*
 New Technology File System (NTFS), 203–215
 defined, **6**–**8**, **31**
 disk compression, 212–214
 disk quotas, 204–207
 file encryption, 212–215
 permissions, 215, **217**–**223**, **247**
 shadow copies, 208–212
 volume mount points, 208
 New Template dialog box, 463*f*
 New Trust Wizard window, 414*f*
 New Zone Wizard, 362*f*–**364***f*
 NFS. *See* Network File System (NFS)
 NIC drivers, 320
 NICs. *See* network interface cards (NICs)
 nonauthoritative restores, **524**, **547***

- nonrepudiation, 450
- No-refresh interval pane, 369–370
- Notify button, 376
- NPS. *See* Network Policy Server (NPS)
- NS records. *See* Name Server (NS) records
- Nslookup tool, 336–338, 387–389
- NT Directory Service (NTDS) Quotas folder, 118
- Ntbackup tool, 516, 523
- NTDS Site Settings Properties dialog box, 431*f*
- Ntdsutil tool, 408, 527
- NTFS. *See* New Technology File System (NTFS)
- Ntuser.dat system file, 168
- O**
- object distinguished name (ObjectDN), 188
- Object owner, 117
- object permissions, 117–126
- Advanced Features option, 118–119
 - effective, 120–126, 149–150
 - permission inheritance, 118, 123–124
 - using Deny in ACEs, 118
 - viewing, 119–120
- Object tab, 118
- ObjectDN. *See* object distinguished name (ObjectDN)
- objects, 83, 105
- OCSP. *See* Online Certificate Status Protocol (OCSP)
- OCSP Response Signing Certificate, 472–474
- octets, 328–329, 348
- offline CA, 455
- offline defragmentation, 527, 547
- one-way trusts, 135, 145
- online CA, 455
- Online Certificate Status Protocol (OCSP), 472
- online defragmentation, 527, 547
- online responders (ORs), 453, 472–474, 481
- Only to servers listed on the Name Servers tab option, 375, 376*f*
- Only to the following servers option, 375, 376*f*
- Open Files node, 229, 230*f*
- Open Systems Interconnection (OSI) protocol, 112
- Operating System tab, 88
- operating systems (OSs), 2–3, 60, 70
- operations master roles, 127–129, 436–440
 - best practices, 437–438
 - defined, 127, 145
 - seizing, 440
 - transferring, 438–440
 - viewing, 128–129
- organizational units (OUs), 112–126
 - Active Directory, 84
 - creating structure, 115, 148–149
 - defined, 78, 105
 - delegation of control, 115–117
 - expanding structure, 149
 - object permissions, 117–126, 149–150
- ORs. *See* online responders (ORs)
- OSI protocol. *See* Open Systems Interconnection (OSI) protocol
- OSs. *See* operating systems (OSs)
- OU-linked GPOs, 270–271
- OUs. *See* organizational units (OUs)
- Outgoing Trust Authentication Level window, 420
- Owner Rights group, 184*t*
- P**
- packet capturing, 385, 386*f*, 450
- Partially Replicated Naming Context(s) field, 424, 426
- Password Export Server (PES), 409
- Password field, 155
- Password must meet complexity requirements policy, 282
- Password never expires check box, 156
- password policies, 285–286, 289–290
- Password Policy option, 285–286
- Password Policy subnode, 282
- Password Replication Policy (PRP), 505–506
- Password Settings Container (PSC), 289
- Password Settings Objects (PSOs), 289–290
- passwords
- changing administrator, 542
 - user account, 59, 427
- patches, 49, 70
- paths, 294
- PDC emulator, 128, 427–428, 437, 438*t*
- peer-to-peer networks, 14
- Perform Group Policy Modeling analyses permission, 303
- performance analysis, 541
- performance baselines, 532–535
- performance indicators, 530, 533, 535
- Performance Monitor, 387, 389, 390*f*, 532
- Performance Monitor Properties dialog box, 535*f*
- perimeter networks, 496
- Permission Entry dialog box, 219*f*
- permission inheritance, 118, 122–124, 145, 219–223
- permissions
- assigning to objects, 112
 - defined, 86, 105
 - printer, 244–245
 - securing access to files with, 215–223
- Permissions button, 224*f*, 225
- PES. *See* Password Export Server (PES)
- Pictures folder, 168
- Ping tool, 48, 57–58, 70, 334–335, 389
- pipe (|), 190–191

- piping, 190, 195
- PKI. *See* public key infrastructure (PKI)
- Plaintext data, 451
- Pointer records (PTRs), 355*t*, 389
- Policies folder, 258*f*, 278
- Policy Events tab, 306
- Policy-based QoS subnode, 281, 293
- ports, 489
- Preferences folder, 278, 308
- Primary server field, 371
- primary zone, 357, 392
- print devices, 240
- Print Operators default group, 183*t*
- Print permission level, 244
- Print Processor button, 242*f*, 243
- print queues, 240, 244*f*
- print servers, 240–245
- connecting to shared printers, 244–245
 - installing printers, 243–244
 - printer permissions, 244–245
 - sharing printers, 243–244
- Print Services role, 21, 240–245
- Print spooled documents first check box, 242
- Printer icon, 240
- Printer leaf object, 87
- printers
- connecting to shared, 244–245
 - installing, 243–244
 - pooling, 240
 - sharing, 12–13, 243–245, 324
- Printers subnode, 292
- Printing Defaults button, 242*f*, 243
- Priority option, 242
- private keys, 451
- private networks, 322
- processors, 39
- Profile path, 163, 169*f*
- Profile tab, 163
- Program Data folder, 118
- Programs and Features applet, 51
- Prompt the user during enrollment and require user input when the private key is used option, 465
- Prompt the user during enrollment option, 465
- Properties button, 17
- Properties for Multiple Items dialog box, 160*f*
- Properties option, 159
- Protocol analyzer tool, 387
- Provider Order tab, 342*f*
- PRP. *See* Password Replication Policy (PRP)
- PSC. *See* Password Settings Container (PSC)
- PSOs. *See* Password Settings Objects (PSOs)
- PTRs. *See* Pointer records (PTRs)
- public folders, 250–251, 324
- public key infrastructure (PKI)
- defined, 450, 481
 - maintaining, 476–480
 - terminology, 451–453
- Public Key Policies subnode, 291
- public keys, 451, 461
- public networks, 322
- Publish certificate in Active Directory check box, 464
- Publish tab, 95*f*
- published applications, 292
- Q**
- QoS Packet Scheduler service, 338–339
- Query tab, 307
- Quota Entries button, 204*f*, 205
- Quota Entries window, 205*f*
- Quota Management tool, 238
- Quota tab, 12, 204*f*
- R**
- RACs. *See* rights account certificates (RACs)
- RAID volumes. *See* redundant array of independent drives (RAID) volumes
- Raise domain functional level dialog box, 402*f*
- Raise forest functional level dialog box, 403*f*
- RDC. *See* remote differential compression (RDC)
- Read & execute permission level, 217
- Read attributes permission level, 218*t*
- Read extended attributes permission level, 218*t*
- Read Group Policy Results data permission, 303
- read only domain controllers (RODCs), 502–509
- administrator role separation, 508
 - credential caching, 505–508
 - defined, 19, 32
 - deploying, 399
 - installing, 503–505
 - preparing for, 407
 - read-only DNS, 508–509
 - replication, 428, 505
- Read permission, 117, 216–217, 303
- Read permissions permission level, 218*t*
- read-only DNS, 508–509
- Read-only domain controller (RODC) check box, 81
- Read-only Domain Controllers/global default group, 184*t*
- realm trusts, 137–138, 145, 418
- /RecordAdd option, 387
- /RecordDelete option, 387
- recovery agents, 212–213
- Recovery progress window, 523*f*
- recursive queries, 356, 375, 384–385, 392
- Redircmp tool, 186
- redundant array of independent drives (RAID) volumes, 3, 236
- referrals, 356, 392
- Refresh interval pane, 369–371
- /registerdns option, 335
- registration authority, 469, 481

- Registry Editor, 59
Registry subnode, 291
relative identifier (RID) role, 127, 145, 437–438
/release option, 335
Reliability and Performance Monitor, 531–539
Reliability Monitor, 538–539
Remote control tab, 164*f*
Remote Desktop Users default group, 183*t*
remote differential compression (RDC), 262
Remote Installation Services (RIS), 22, 293
Remote Procedure Call (RPC) over IP, 434–435
RemoteApp programs, 30
Render print jobs on client computers check box, 241
Renew expired certificates, update pending certificates, and remove revoked certificates check box, 464
/renew option, 335
Renewal period option, 464
Repadmin tool, 425–426, 541
Replace all existing inheritable permissions on all descendants with inheritable permissions from this object check box, 219
Replicate from Server field, 424
Replicate from Site field, 424
Replicated Naming Context field, 424
replication, 129–130, 421–428
 - Active Directory–based GPO, 254
 - AD LDS, 492–493
 - defined, 76, 105
 - group policy, 262–263
 - monitoring, 541–542
 - RODC, 428, 505
 - verifying, 388
 - zone, 363
Replication option, 368
Replmon tool, 541
- Reports folder, 531
Request Certificates window, 468*f*
Request Handling tab, 465
request-handling options, 466
Reset account lockout counter after policy, 282
resolvers, 356, 392
resource allocation policies, 540
Resource Monitor, 530*f*
resource partners, 494–495, 510
resource records, 355, 355*t*, 370, 392
Responsible person field, 371
restoring. *See also* backup and restoration
 - Certification Authority, 476–477
 - GPOs, 303–304
restricted enrollment agents, 453, 481
Restricted Groups subnode, 291
Resultant Set of Policy (RSOP) snap-in, 306, 312
Retry interval field, 371
reverse lookup zones (RLZs), 364–367, 392
revocation configuration, 474–475
RID role. *See* relative identifier (RID) role
rights, 86, 105
rights account certificates (RACs), 499–500
RIS. *See* Remote Installation Services (RIS)
RLZs. *See* reverse lookup zones (RLZs)
roaming profiles, 168–173, 175, 195
RODCs. *See* read only domain controllers (RODCs)
role services, 19, 32
roles, *see also* specific roles
 - choosing, 36
 - overview, 19–21
 - on second server, 74
Roles node, 23
- root CAs, 455, 481
root hints, 382–383, 392
root servers, 355, 392
round robin process, 383–384, 392
Route command, 333–334
Route Print command, 333
routers, defined, 320
Routing and Remote Access Services (RRAS), 21
RPC over IP. *See* Remote Procedure Call (RPC) over IP
RRAS. *See* Routing and Remote Access Services (RRAS)
RSOP snap-in. *See* Resultant Set of Policy (RSOP) snap-in
- S**
- s* option, 336
SACLs. *See* system access control lists (SACLs)
SalesDocs folder, 178
SAM database. *See* Security Accounts Manager (SAM) database
SANs. *See* storage area networks (SANs)
SAS system. *See* serial attached SCSI (SAS) system
SATA drives. *See* serial ATA (SATA) drives
Save As button, 418
Scavenge stale resource records check box, 369
scavenging resource records, 368–370, 369, 392
SCEP. *See* Simple Certificate Enrollment Protocol (SCEP)
Schedule panel, 209*f*, 210
schema, 83–84, 105, 491–492
Schema Admins/universal default group, 184*t*
schema attributes, 83, 105
schema classes, 83, 105
schema directory partitions, 127, 145
schema master role, 127, 437–439

- scope
 group policy, 254, 269–271
 zone replication, 363–364
- Scope tab, 99f, 264f, 275f
- Scripts subnode, 281, 293
- Secedit tool, 301–302
- second installation window, 42f
- secondary zones, 357, 392, 414
- secret keys, 451
- Secure Socket Tunneling Protocol (SSTP), 28
- security
 Active Directory, 77
 permissions, 215–223
- Security Accounts Manager (SAM) database, 152
- Security Configuration and Analysis snap-in, 299–301
- security filtering, 275, 277
- Security Filtering dialog box, 275
- security groups, 176, 195
- security identifiers (SIDs), 127, 145, 399, 409, 418, 421, 442
- Security log, 284
- Security Options subnode, 284f
- security principals, 117, 145
- Security Settings subnode, 281–284, 291, 293–295
- Security tab, 7f, 119, 465–466
- security templates, 298–302, 312, 317
- Security Templates snap-in, 298–299
- seizing operations master roles, 440
- Select backup date window, 520, 521f
- Select backup items window, 518, 519f
- Select destination disk window, 519, 520f
- Select Groups dialog box, 90f
- Select items to recover window, 521, 522f
- Select Role Services window, 500f
- Select Signing Certificate window, 475f
- selective authentication, 415, 442
- Self group, 184t
- Send Mail option, 159
- Separator Page button, 242f, 243
- serial ATA (SATA) drives, 39
- serial attached SCSI (SAS) system, 39
- Serial number field, 371
- Server Core, 24–25, 53–60
 computer names, 58–59
 computer workgroups, 58–59
 configuration tasks, 542–545
 defined, 4, 32
 enabling automatic updates, 59
 firewall, configuring for ping, 57–58
 installing, 54–55
 interface, 24f
 restoring command prompt window, 55–56
 setting time and date, 56
 static IP address, setting, 56–57
 when not to use, 60
- server features, 19, 32
- server management and monitoring, 515–551
 backup and restoration, 524–527
 defragmentation, 527–528
 Event Viewer, 529–530
 performance analysis, 541
 Reliability and Performance Monitor, 531–539
 replication monitoring, 541–542
 Server Core, 542–545
 Task Manager, 530–531
 tools, 545–546
 Windows Server Backup and Restore, 516–524
 WSRM, 539–541
- Server Manager, 23–24, 489, 490f
- Server Manager window, 23f
- Server Message Block (SMB), 27, 234, 338
- server names, 40
- server operating systems, 2–3, 32
- Server Operators default group, 183t
- server roles, 19, 32, 357
- Servermanagercmd tool, 546
- Service (SRV) records, 355t
- Service Account Selection, 489
- Service group, 184t
- service packs, 49, 70
- services, defined, 321
- Services tab, 530
- session keys, 452
- Sessions node, 229–230
- Sessions tab, 165
- Set Aging/Scavenging for All Zones option, 370
- Set Priority feature, 531
- Set up a connection or network Wizard, 325, 325f
- Settings dialog box, 209f
- Settings tab, 100f, 306
- shadow copies, 11, 204, 208–212, 247
- Shadow Copies column, 234
- Shadow Copies tab, 208, 209f
- Share and Storage Management snap-in, 28f, 225, 234–236
- Share name field, 224f, 225, 241
- share permissions, 215–217, 216, 247
- Share this folder check box, 224
- Share this printer check box, 241
- Shared folder leaf object, 87
- Shared Folders snap-in, 225, 228–231
- Shared Folders subnode, 298
- shares. *See* file sharing
- Shares node, 229–230
- sharing
 files. *See* file sharing
 folders, 12–13
 printers, 12–13, 243–245, 324
- Sharing and Discovery section, 324
- Sharing tab, 241
- shortcut trusts, 136, 145, 410–413

- Show All Available Disks button, 519, 520*f*
- Show Domains dialog box, 305*f*
- Show me all the files and folders I am sharing link, 324
- Show me all the shared network folders on this computer link, 324
- SID filtering, 418, 421, 442
- Sides of Trust window, 412
- SIDs. *See* security identifiers (SIDs)
- signature algorithm, 461
- Simple Certificate Enrollment Protocol (SCEP), 471
- Simple Mail Transport Protocol (SMTP), 432, 434–435
- single sign-on (SSO), 29, 32
- single-level hierarchy, 455
- single-level OU structure, 113*f*, 115*f*
- site link bridging, 435–436, 442
- site links, 142–143, 145, 432–436
- site replication topology, 143*f*
- site-linked GPOs, 270
- sites, Active Directory, 139–143
- components of, 141–143
 - creating, 428–430
 - defined, 77, 105
 - global catalog caching, 436
 - site links, 432–436
 - universal group membership caching, 436
- smart card enrollment, 471–472
- SMB. *See* Server Message Block (SMB)
- SMTP. *See* Simple Mail Transport Protocol (SMTP)
- SMTP subfolder, 432
- snapshots, 60, 70
- SOA records. *See* Start of Authority (SOA) records
- Software (Un)Install events, 539
- Software Installation extension, 279, 292
- software restriction policies, 293–295
- Software Restriction Policies subnode, 291, 293–294
- Software Settings folder, 97–98, 279–281, 292
- Source Starter GPO list box, 267, 268*f*
- special identity groups, 184–186
- Specify Cluster Address window, 502*f*
- Specify recovery options window, 522*f*
- spooling options, 242
- SRV records. *See* Service (SRV) records
- SSO. *See* single sign-on (SSO)
- SSTP. *See* Secure Socket Tunneling Protocol (SSTP)
- standalone CAs, 453, 454
- stand-alone servers, 14, 32
- Standard Edition, Windows Server 2008, 3–4, 32
- standard zones, 362, 377–378, 392
- Start Menu and Taskbar subnode, 298
- Start menu, customized, 173*f*
- Start of Authority (SOA) records, 355*f*, 371–372
- Start Search text box, 46
- Starter GPOs, 267–269, 312
- static IP address, 46–48, 56–57
- static updates, 355
- /Statistics option, 387
- Status option, 368
- stop conditions, 536
- storage area networks (SANs), 27, 234
- storage management, 233–240
 - configuring requirements, 251
 - DFS, 236–238
 - enhancements to, 27–28
 - FSRM, 238–240
 - running out of disk space, 251
 - Share and Storage Management snap-in, 234–236
- Storage node, 24
- Storage Reports Management tool, 238*f*, 239
- Storage Reports Task Properties dialog box, 239*f*
- Store passwords using reversible encryption policy, 282
- stub zones, 357, 374–375, 392, 414–416
- subfolders, restricting access to, 226–227
- subnet masks, 328, 330, 348
- subnetting, 141–142, 330–331, 346–347, 428–432
- Summary tab, 306
- super mandatory profiles, 174, 195
- supernetting, 334
- switches, defined, 320
- symmetric cryptography, 451
- system access control lists (SACLs), 117
- System folder, 118
- System group, 184*t*
- System Properties dialog box, 5–6, 400
- System Services subnode, 291
- system state backup and recovery, 523
- System subnode, 292
- Sysvol folder, 81, 105
- Sysvol share, 228, 262
- T**
- t option, 335
- Take ownership permission level, 218*t*
- tape drives, 516
- Targeting Editor, 310*f*
- Task Manager, 530–531
- Tasks section, 324–327
- TCP/IP. *See* Transmission Control Protocol/Internet Protocol (TCP/IP)
- Template display name/Template name option, 463
- Terminal Services Gateway (TS Gateway), 30
- Terminal Services Profile tab, 164
- Terminal Services (TS), 22, 29–30, 164–165
- Terminal Services Web Access (TS Web Access), 30*f*

- testing
 GPOs, 266–267
 network connectivity, 48
- three-level hierarchy, 455–456
- time, setting, 46, 56
- time to live (TTL) text box
 setting, 379
- time zones, 40, 46, 56
- TLD servers. *See* top-level domain (TLD) servers
- TLS/SSL. *See* Transport Layer Security/Secure Sockets Layer (TLS/SSL)
- tombstone lifetime, 527, 547
- top-level domain (TLD) servers, 355–356, 392
- Total Query Received/sec counter, 389
- Tracert tool, 336, 338
- traditional DNS forwarders, 381
- transitive trusts, 135–136, 145
- Transitivity of trust field, 418
- Transmission Control Protocol/Internet Protocol (TCP/IP), 327–343
 command-line tools, 334–338
 IPv4 addresses, 328–334
 managing protocols, 338–343
- Transport Layer Security/Secure Sockets Layer (TLS/SSL), 498
- Traverse folder/execute file permission level, 218*t*
- trees, 78, 105, 138–139
- trust relationships, 130, 134*f*, 145
- Trust Selections Complete window, 412
- Trust Type window, 411*f*
- Trusted Publishers policy, 294
- trusts, 134–138, 410–421
 configuring, 137–138
 external, 137, 418
 forest, 136–137, 414–418
 one-way, 135
- properties, 418–421
 realm, 137–138, 418
 shortcut, 136, 410–413
 transitive, 135–136
 two-way, 135
- Trusts tab, 137*f*
- TS. *See* Terminal Services (TS)
- TS Gateway. *See* Terminal Services Gateway (TS Gateway)
- TS Web Access. *See* Terminal Services Web Access (TS Web Access)
- Turn off Local Group Policy objects processing option, 256
- Turn on sharing option button, 13
- two-level hierarchy, 455–456
- two-way trusts, 135, 136*f*, 145
- Type option, 368
- U**
- UDDI Services. *See* Universal Description, Discovery, and Integration (UDDI) Services
- UDP. *See* User Datagram Protocol (UDP)
- UNC path, 231, 237
- unidirectional replication, 505, 510
- Universal Description, Discovery, and Integration (UDDI) Services, 22
- universal group membership caching, 436, 442
- universal groups, 177*t*, 179–180, 195, 399
- unlinking GPOs, 265–266
- Unlock account check box, 162
- unmanaged policy settings, 278
- Unrestricted setting, 294
- Update certificates that use certificate templates check box, 465
- updates
 automatic, 49–51, 59
 dynamic, 365–367
- Upgrades tab, 280
- UPN. *See* user principal name (UPN)
- Use AD RMS centrally managed key storage option, 501
- Use CSP key storage option, 501
- Use Delete Subtree server control check box, 525, 526*f*
- Use root hints if no forwarders are available check box, 384
- Use WINS forward lookup check box, 378, 379*f*
- User Access to dialog box, 212*f*
- user accounts, 86, 152–167
 contacts lists, 165–167
 creating, 156–157, 199
 distribution lists, 165–167
 editing, 159–160
 passwords, 59, 427
 properties of, 160–165
 user templates, 157–158, 199
- User Accounts applet, 152
- User cannot change password check box, 156
- User Configuration node, 97–101, 277–279, 292–298, 308
- User Datagram Protocol (UDP), 327
- User folder, 257–258
- User logon name field, 155, 161
- User must change password at next logon check box, 155
- User Name and Password window, 412
- user principal name (UPN), 131, 145
- user profiles, 167–175
 adding Vista computer to domain, 171
 defined, 167, 195
 managing, 175
 mandatory, 169–171, 174
 roaming, 168–169, 171–173, 175
- User Profiles dialog box, 170*f*
- User Rights Assignment policies, 103*f*

User Rights Assignment subnode, 283, 284*f*

user templates, 157–158, 195

Users default group, 183*t*

Users folder, 85, 183–184

user-specific GPOs, 255

V

Validate button, 418

Validity period option, 464

Version 1 templates, 461–462

Version 2 templates, 462

Version 3 templates, 462

versionNumber attribute, 260

View available updates link, 51

View computers and devices link, 324

View full map link, 16, 322

View status link, 17, 322

Virtual Machine Connection console, 67*f*

virtual machines (VMs), 21, 26*f*, 32, 60, 63–69

virtual private networks (VPNs), 21

virtualization, 27, 36

VMs. *See* virtual machines (VMs)

volume mount points, 204, 208, 247

Volume Shadow Copy Service (VSS), 517, 547

VPNs. *See* virtual private networks (VPNs)

W

WANs. *See* wide area networks (WANs)

Warning event level, 529

Wbadmin tool, 516, 523–524, 525

WDS. *See* Windows Deployment Services (WDS)

Web enrollment, 469–471

Web Server (IIS), 22

Web SSO design, 496–497, 510

Web transactions, secure, 452*f*

wide area networks (WANs), 52, 139

Windows 2000

domain functional levels, 399–400

forest functional levels, 398

Windows Active Directory. *See* Active Directory

Windows Components subnode, 292

Windows Deployment Services (WDS), 22, 29, 38

Windows domains, 14, 32

Windows File Services. *See* File Services

Windows Firewall with Advanced Security, 291, 545

Windows Hyper-V. *See* Hyper-V

Windows Installer service, 279

Windows Internet Name Service (WINS), 378–380

Windows Management Instrumentation (WMI) filtering, 275–277

Windows Network Diagnostics message, 340*f*

Windows networking

components, 14–17

concepts, 13–14

IPv6, 343–347

Network and Sharing Center, 321–327

TCP/IP, 327–343

terminology, 320–321

Windows NT token applications, 495

Windows Print Services, 21, 240–245

Windows Recovery Environment (WinRE), 524, 547

Windows Search Service, 233

Windows Server 2003

domain functional levels, 400

File Services, 234*f*

forest functional levels, 398–399

Windows Server 2008

activating, 542

configuration tasks, 36

core technologies, 6–13

domain functional levels, 400–401

editions of, 3–6, 36

forest functional levels, 399

installing, 38–52

networking concepts, 13–19

new features in, 22–30

roles, *see also specific roles*, 19–22, 36

server operating systems, 2–3

system properties, 5–6

upgrading to, 53

virtualization, 36

Windows Server Backup, 27, 516–524

from command line, 523–524

data recovery, 520–523

installing, 517–518

one-time backups, 518–519

scheduled backups, 519–520

system recovery, 524

Windows Server Backup window, 517*f*

Windows Settings folder, 98, 278, 281–298, 308

Windows System Resource Manager (WSRM), 539–541

Windows token-based agents, 496

Windows Vista

adding computers to domain, 171

Client Side Extensions for, 308–309

new local GPOs in, 255–257

Windows Web Server 2008, 5, 32

Windows workgroup, 14, 32

WinRE. *See* Windows Recovery Environment (WinRE)

Winrs tool, 546

WINS. *See* Windows Internet Name Service (WINS)

- Wired Network (IEEE 802.3) Policies
 subnode, 291
- Wireless Network (IEEE 802.11)
 Policies subnode, 291
- WMI filtering. *See* Windows Management Instrumentation (WMI) filtering
- workgroup model, 14
- Write attributes permission level, 218t
- Write extended attributes permission level, 218t
- Write permission, 117
- Write permission level, 217f, 218
- WSRM. *See* Windows System Resource Manager (WSRM)
- Z**
- Zone Aging/Scavenging Properties dialog box, 369
- zone delegation, 373–375, 388, 392
- Zone Transfer Success counter, 389
- zone transfers, 375–378, 388, 392
- Zone Transfers tab, 375
- /ZoneAdd option, 387
- /ZoneDelete option, 387
- /ZoneInfo option, 387
- zone-name text file, 363
- zones, 355, 357–358, 362–380, 392